

Cisco Spaces Configuration Guide

First Published: 2018-12-18

Last Modified: 2026-10-22

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)

© 2026 Cisco Systems, Inc. All rights reserved.



Preface

This preface describes the audience, organization, acronyms, and conventions used in the document.

This document contains the following sections:

- Audience, on page iii
- Document Conventions, on page iii
- List of Acronyms and Abbreviations, on page iv
- Communications, services, and additional information, on page iv

Audience

This guide is meant for account administrators who manage the Cisco Spaces user accounts and perform the configurations required for Cisco Spaces. This guide is also meant for business and store administrators who use Cisco Spaces to create the proximity rules to send notifications to customers and business users.

Other target audience includes portal designers and access code managers.

Document Conventions

This document uses the following conventions:

Table 1: Document Conventions

Convention	Description
Boldface	Commands, command options, and keywords are in boldface.
Italics	Arguments for which you supply values are in italics
Option > Option	Used to describe a series of menu options.

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

Tip Means *reader take tip*. Tips contain helpful suggestions to resolve issues.

List of Acronyms and Abbreviations

Table 2: List of Acronyms and Abbreviations

Acronym	Expansion
ACL	Access Control List
BLE	Bluetooth Low Energy
CUWN	Cisco Unified Wireless Network
CNA	Captive Network Assistant
RSSI	Received Signal Strength Indicator
SSID	Service Set Identifier
UUID	Universally Unique Identifier

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

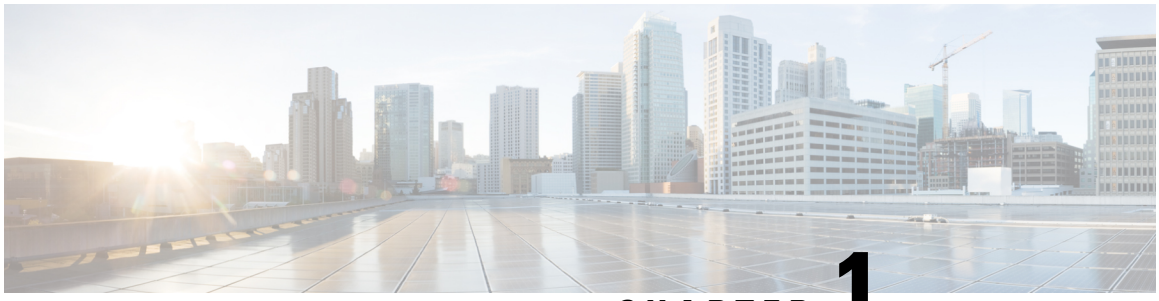
To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



PART I

Prerequisites

- Cisco Spaces Prerequisites, on page 1



CHAPTER 1

Cisco Spaces Prerequisites

This chapter describes the system requirements for Cisco Spaces, the bandwidth requirements to deploy Cisco Spaces, and ports and IP addresses for Cisco Spaces.

This chapter contains the following sections:

- System Requirements, on page 1
- Bandwidth Requirements to Deploy Cisco Spaces, on page 2
- Accessible Ports and IP Addresses, on page 2
- Cisco Spaces IP Addresses, on page 3
- Cisco Smart Licensing, on page 4
- Cisco Spaces Compatibility Matrix, on page 5

System Requirements

The system requirements for Cisco Spaces is described in the following table:

Table 3: System Requirements

Item	System Requirements
Operating System	• Microsoft Windows XP or a later version • macOS X 10.6 or a later version
Browser	Windows OS • Firefox Version 30 or a later version • Chrome Version 34 or a later version • Safari Version 5.1.7 or a later version macOS • Firefox Version 30 or a later version • Chrome Version 34 or a later version • Safari Version 5.1.7 or a later version

Item	System Requirements
Cisco AireOS Wireless Controller	8.3 or a later version **Note** 8.3 is End-of-Life (EOL). We recommend that you migrate to one of the recommended releases as per the *Guidelines for Cisco Wireless Software Release Product Bulletin* at: https://www.cisco.com/c/en/us/products/collateral/wireless/wireless-controllers/bulletin-c25-738147.html
Cisco Connected Mobile Experiences (CMX) - this is required only for Cisco AireOS/Catalyst Controllers used with Cisco CMX.	10.6 or a later version
Cisco Spaces: Connector (Only applicable for Cisco AireOS/Catalyst Controllers)	• vCPU: 2/4/8 • RAM: 4/8/16 GB • Hard Disk: 60 GB

Bandwidth Requirements to Deploy Cisco Spaces

The following table shows the internet bandwidth requirements for Cisco Spaces: Connector and Cisco Wireless Controller Direct Connect to send location updates.

Table 4: Bandwidth Requirements

Test Data	Type	Required Bandwidth
5000 APs 60000 clients	Cisco Wireless Controller Direct Connect	250 Kbps
5000 APs 60000 clients	Cisco Spaces: Connector	4 Mbps

Accessible Ports and IP Addresses

Cisco Spaces is a cloud-based solution, and there is no physical installation involved. So, there is no need to open any port to deploy Cisco Spaces for cloud-based wireless networks such as Cisco Meraki.

For some networks such as Cisco AireOS or Cisco Catalyst that are not cloud-based, you must open the required ports to establish a connection between your wireless network and. You can establish this connection through a public IP or VPN. In addition, some Cisco Spaces IP addresses must be allowed in the customer infrastructure. For more information on the IP addresses to be allowed, refer to the Cisco Spaces IP Addresses, on page 3.

Note For a default Cisco Unified Wireless Network installation, port 443 must be open to be publicly accessible.

Cisco CMX must be publicly accessible in the following scenarios where Cisco Spaces has to establish a connection with Cisco CMX:

- Connect to Cisco CMX
- Import location and access points
- View Cisco CMX maps
- View Cisco Spaces reports

Cisco Spaces IP Addresses

To establish a connection between Cisco Spaces and a Cisco AireOS or a Cisco Catalyst 9800 Series Wireless Controller, you must allow some Cisco Spaces IP addresses in your network infrastructure.

To view the IP addresses that should be allowed, in the Cisco Spaces dashboard, choose **Captive Portal** > **SSIDs** > **Configure Manually** link.

To establish a VPN connection, contact Cisco Spaces support team.

Note A publicly resolvable domain name is not required to connect to Cisco Spaces.

Certain domain names must also be allowed in a customer's infrastructure for the Cisco CMX instances that are deployed in a customer's network to be able to communicate with the Cisco Spaces analytical and notification servers. To know the domain names that should be allowed in the Cisco Spaces dashboard, in the **SSIDs** window, click **Configure Manually** link.

Approved IP addresses

As we transition or migrate the Cisco Spaces domain, ensure that the newly provided IP addresses are added to your approved IP address list. This will allow uninterrupted access to Cisco Spaces services for all systems, users, and services associated with these IPs.

Cisco Spaces Connector Type	Additional			Existing		
	Domain	IPv4	IPv6	Domain	IPv4	IPv6
Connect via CMX Tethering	cmx.ciscospaces.io	75.2.50.127	[illegible]	cmx.dnaspaces.io	52.20.144.155	-
	cmx.ciscospaces.io	99.83.199.229	[illegible]	cmx.dnaspaces.io	34.231.154.95	-
Connect via Spaces Connector	connector.ciscospaces.io	75.2.50.127	[illegible]	connector.dnaspaces.io	34.231.154.95	[illegible]
	connector.ciscospaces.io	99.83.199.229	[illegible]	connector.dnaspaces.io	52.20.144.155	[illegible]

Cisco Spaces Connector Type	Additional			Existing		
	Domain	IPv4	IPv6	Domain	IPv4	IPv6
Connect AireOS Controller/Catalyst 9800 Wireless Controller Directly	data.ciscospaces.io	52.1.37.236	-	data.dnaspaces.io	34.231.154.95	-
	-	-	-	-	52.20.144.155	-
Partner Firehose	partners.ciscospaces.io	75.2.96.93	[illegible]	partners.dnaspaces.io	44.199.137.87	-
	partners.ciscospaces.io	99.83.155.204	[illegible]	partners.dnaspaces.io	3.90.124.39	-
Captive portal	splash.ciscospaces.io	15.197.234.109	[illegible]	splash.dnaspaces.io	52.55.235.39	-
	splash.ciscospaces.io	3.33.232.255	[illegible]	splash.dnaspaces.io	34.235.248.212	-
Smart Workspaces Webex Integration - Webex Setup for analytics via Webex login	workspaces.ciscospaces.io	dsm16f[illegible]	-	workspaces.dnaspaces.io	34.206.36.139	-
	kiosk.ciscospaces.io	dsm16f[illegible]	-	signage.dnaspaces.io	34.206.36.139	-
	webex.ciscospaces.io	-	-	webex.dnaspaces.io	52.45.218.46	-
	webex.ciscospaces.io	-	-	webex.dnaspaces.io	54.165.127.208	-
Connect Via Meraki Integration	location.ciscospaces.io	75.2.25.96	[illegible]	location.dnaspaces.io	52.20.144.155	-
	location.ciscospaces.io	99.83.245.239	[illegible]	location.dnaspaces.io	34.231.154.95	-
Meraki Camera with Cisco Spaces	mqtt.ciscospaces.io	13.248.186.114	[illegible]	mqtt.dnaspaces.io	52.87.123.75	-
	mqtt.ciscospaces.io	76.223.47.253	[illegible]	mqtt.dnaspaces.io	-	-

Cisco Smart Licensing

Cisco Smart Licensing is a flexible software licensing deployment and management model that simplifies the way you activate and manage licenses across your organization. Cisco Smart Licensing simplifies the way you purchase, deploy, organize, and optimize Cisco software licenses.

The benefits of Cisco Smart Licensing include:

- **Easy Activation**: Smart Licensing establishes a pool of software licenses that can be used across your company; no more entering Product Activation Keys.
- **Unified Management**: Cisco provides a complete view into all of your Cisco products and services licensing under this program in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility**: Your software is not node-locked to your hardware, so you can easily use and move licenses as needed.

For detailed information about Cisco Smart Licensing, refer to Cisco Software Licensing Guide.

For more information about enabling Cisco Smart License in Cisco Spaces, refer to Activate Smart License.

Cisco Spaces Compatibility Matrix

Table 5: Compatibility Matrix

Application	Cisco AireOS Controller	Cisco Catalyst 9800 Series Wireless Controller	Cisco Embedded Wireless Controller	Cisco Prime Infrastructure/Cisco Catalyst Center
Cisco Spaces (with Detect and Locate, Captive Portal, Engagements, Location Personas, Behavior Metrics)	• Cisco Wireless Controller Native Cloud Connector - 8.3 or a later version (except 8.3.102 for Presence) **Note** 8.3 is End-of-Life (EOL). We recommend that you migrate to one of the recommended releases as per the *Guidelines for Cisco Wireless Software Release Product Bulletin* at: https://www.cisco.com/c/en/us/products/collateral/wireless/wireless-controllers/bulletin-c25-738147.html • Cisco Spaces: Connector - 8.0.119 or a later version.	16.10 or a later version	16.11.1s or a later version	3.0 or a later version for maps **Note** Cisco Prime support is not there for maps on Cisco Embedded Wireless Controller.

Note 3375 Appliance is not supported.

Compatibility Matrix for Location Service

For detailed information about Location Service compatibility matrix, refer to Compatibility Matrix for Location Service.

Compatibility Matrix for Cisco Spaces: IoT Service (Wireless)

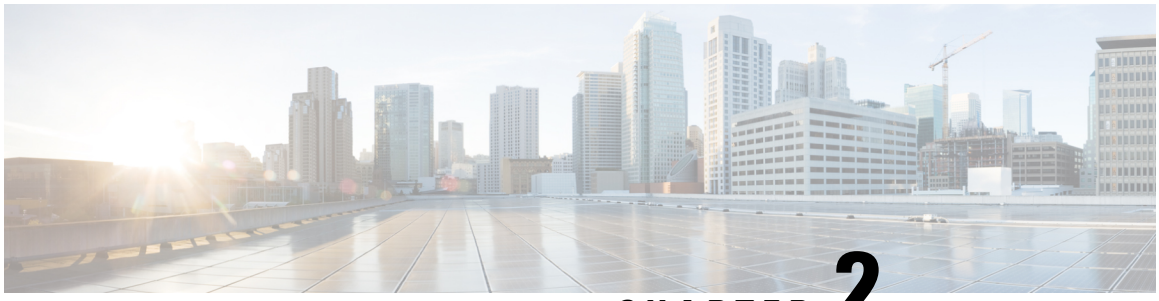
For detailed information about Cisco Spaces: IoT Service (Wireless) compatibility matrix, refer to, Compatibility Matrix for IoT Service (Wireless).



PART II

Getting Started

- Get Started with Cisco Spaces, on page 9



CHAPTER 2

Get Started with Cisco Spaces

This chapter provides an overview of Cisco Spaces, its features, the process flow, license packages, and system requirements for Cisco Spaces.

This chapter contains the following sections:

- Overview of Cisco Spaces, on page 9
- Process Flow for Cisco Spaces, on page 11
- Cisco Spaces License Packages, on page 11
- Cisco Spaces License Types and Features Compatibility, on page 14
- Log In, on page 17
- Cisco Federation Process, on page 19
- Start Working with Cisco Spaces, on page 27
- Cisco Spaces Dashboard GUI Enhancements, on page 30
- Verticals overview, on page 31
- Cisco Meraki Integration Workflow, on page 31
- Manage Networks in Cisco Meraki Dashboard, on page 32
- Cisco Magnetic Design, on page 32
- Cisco Spaces: Connector 3.0, on page 33
- Idle Timeout for Cisco Spaces, on page 33
- Migrate Data from Cisco Prime Infrastructure to Catalyst Center, on page 33
- Contact Cisco Spaces Support, on page 34
- Cisco Spaces Documentation, on page 36

Overview of Cisco Spaces

Cisco Spaces is a multichannel engagement platform that enables you to connect, know, and engage with visitors at their physical business locations.

Cisco Spaces is the industry's most scalable end-to-end indoor location services cloud platform that empowers customers to achieve business outcomes at scale. With its comprehensive suite of services, it offers a robust solution for all your location-based needs.

Cisco Spaces provides solutions for monitoring and managing the assets in your premises.

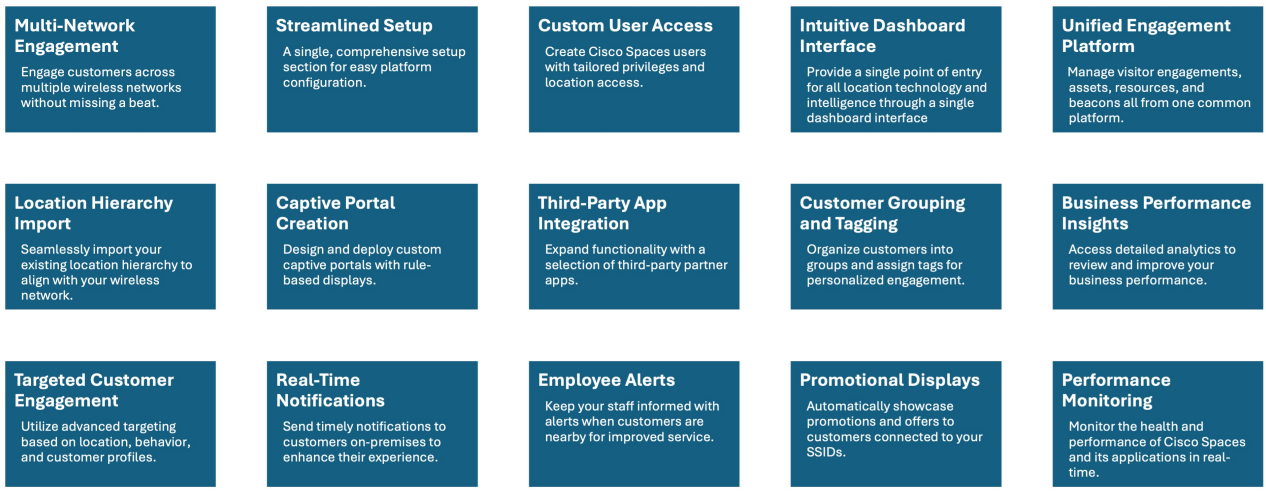
It covers various verticals of business such as

- retail

- manufacturing
- hospitality
- healthcare
- education
- financial services
- enterprise workspaces, and so on.

With Cisco Spaces, users gain centralized access to all location technology and intelligence via a unified dashboard interface. Designed for compatibility with existing Cisco Aironet, Cisco Catalyst, and Cisco Meraki infrastructure, Cisco Spaces stands out as a versatile solution for location-based service needs.

Figure 1: Feature Highlights



Use Case Scenario

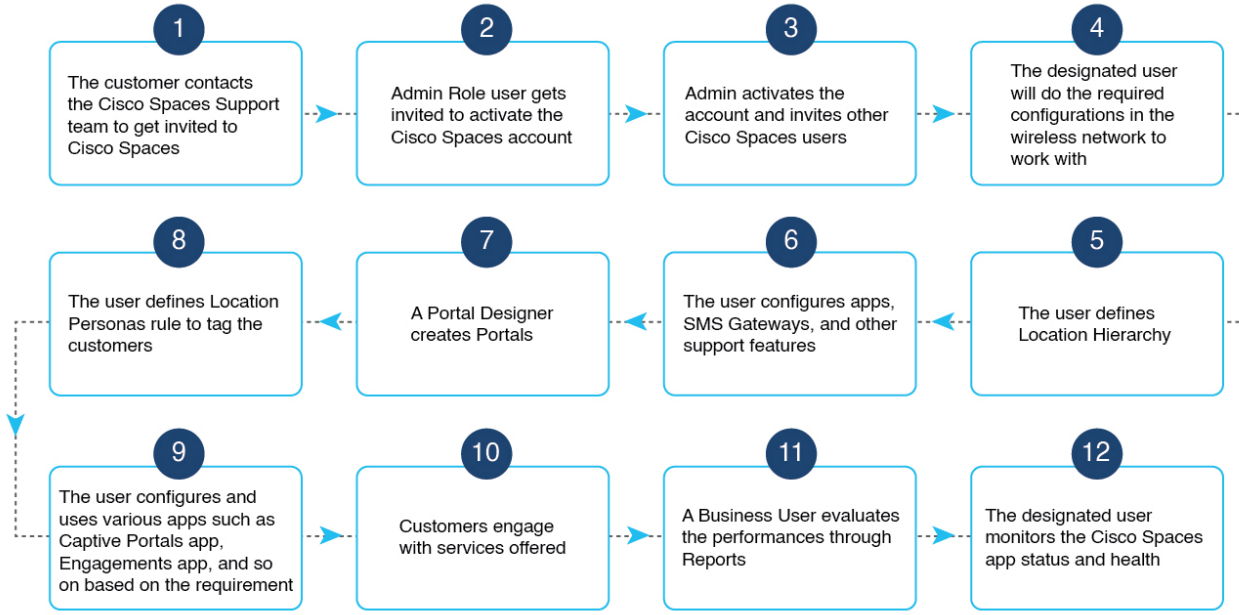
In the ABC shopping mall, to get free Wi-Fi, the customers must connect to an SSID once they enter the mall. ABC wanted to provide a personalized experience to each customer who connects to the Wi-Fi based on their purchase history and visit frequency. After installing Cisco Spaces, ABC could collect the Wi-Fi user's details through the captive portals, and utilize these details to send notifications to the customers regarding the offers and services available to them. The customers once connected to the Wi-Fi are taken to a captive portal, where they are provided with an option to register themselves by filling in details such as name, e-mail address, telephone number, and so on. This information captured is stored in Cisco Spaces. When customers re-visit the mall, promotional offers are sent to the customers through SMS, or e-mail.

Cisco Spaces can also be configured to notify business users such as employees regarding customer activities. For example, you can identify and tag repeat customers as platinum members on Cisco Spaces dashboard. When a platinum customer enters a restaurant and their device is detected by a wireless access point, the restaurant representatives would receive alerts on their devices and can provide personalized services to the customer.

Process Flow for Cisco Spaces

The process flow for Cisco Spaces is as shown in the following figure:

Figure 2: Process Flow for Cisco Spaces



Cisco Spaces License Packages

Overview of Cisco Spaces License Packages

Cisco Spaces supports multiple license packages to meet different user and deployment needs, enabling the right set of features based on your selected subscription.

Cisco Spaces license packages feature helps administrators validate subscription entitlements, activate licenses, choose the appropriate package, and ensure the correct features are enabled in Cisco Spaces.

The Cisco Spaces License package supports these licenses:

- **ESSENTIAL**
- **ADVANTAGE**
- **EXTEND**
- **SMART_VENUES**
- **SMART_OPERATIONS**
- **UNLIMITED**
- **PREMIER (W)**

- **PREMIER (CW)**

License Information

With Cisco Spaces license packages, you can choose the license option that best aligns with your deployment needs and use cases.

For advanced Cisco Spaces deployments, choose Cisco Spaces **PREMIER** or Cisco Spaces **PREMIER (CW)** based on the capabilities your organization requires. These license options support higher-tier use cases beyond Cisco Spaces **ADVANTAGE**.

For deployments that require the next level of Cisco Spaces capabilities, you can choose Cisco Spaces **ADVANTAGE** or Cisco Spaces **UNLIMITED**. Cisco Spaces **ADVANTAGE** is available as a per-device license, while Cisco Spaces **UNLIMITED** provides comparable capabilities using a per-square-foot licensing model.

If your deployment requires only specific capabilities, you can choose subset license options such as **SMART_OPERATIONS** or **SMART_VENUES**, based on the use cases you want to enable.

Cisco Spaces also supports Smart License actions such as registration, license detail retrieval, renewal, deregistration, license updates, and license usage checks as part of the current feature workflow.

Depending on your account status, license expiration and registration-related guidance details are displayed during sign-in and license management flows.

Licensing Options

The Cisco Spaces licensing options are:

- **ESSENTIAL**: This license provides foundational capabilities within Cisco Spaces but with some restrictions.
- **ADVANTAGE**: This license works based on the number of Access Point (AP) provisioned for the Cisco Spaces account.

  The SPACES ADVANTAGE license is based on per device/year basis. This is also available as an add-on option on Cisco DNA Advantage subscription (Transactional and EA) as well as offered separately.

  The SPACES ADVANTAGE license is recommended for wireless customers who have Cisco DNA Advantage and who want to keep a device licensing model (without significant expansions or increased device density planned).
- **EXTEND**: Cisco Spaces Extend subscription is included with Cisco DNA Advantage subscriptions with Cisco Catalyst Wireless and Cisco Catalyst 9300 Series and 9400 Series Switches.
- **UNLIMITED**: Cisco Spaces accounts with **UNLIMITED** license include all the entitlements similar to an existing **ADVANTAGE** license. It aligns with Spaces Advantage functionality, with the main difference being per-square-foot licensing instead of per-device licensing. It is available in the new Cisco Spaces Unlimited EA and standalone subscription.



Note Cisco Spaces Unlimited license is not available at floor level.

The SPACES UNLIMITED license is available on a per square foot/square meter building unit/year basis and is generally suited for customers planning broader workspace-focused deployments. The SPACES UNLIMITED license is recommended for users with:

- Multiple technologies or have dense deployments with **Cisco Smart Workspaces**
- Do not need other features besides **Cisco Smart Workspaces**
- Hybrid work offers

Note For a **Cisco Smart License**-enabled account with **UNLIMITED** license package, the license count is based on the total square foot area of all the floor locations calculated based on the maps uploaded to the Cisco Spaces platform.

- **SMART_VENUES**: This license works in the same way as the existing **EXTEND** license with some additional entitlements.
- **SMART_OPERATIONS**: This license works in the same way as the existing **EXTEND** license with some additional entitlements. The **SMART_OPERATIONS** license includes all the access privileges under the **EXTEND** license.
- **PREMIER (W)**: This license works as a top-tier package aligned to Cisco Spaces' premium entitlements (including Smart Workspaces). `Premier` includes Cisco Spaces Advantage plus additional offers such as indoor navigation, desk booking, and Cisco Asset Tag.
- **PREMIER (CW)**: This license works as another top-tier premier option; it is also described as including everything in Cisco Spaces from all license types, including Smart Workspaces. The "CW" denotes a specific premier tier variant used for certain commercial/workspaces packaging.

For information about features included in Cisco Spaces, refer to Cisco Spaces License Types and Features Compatibility, on page 14 and the Cisco Spaces Data Sheet.

Note
- The features available for your account depend on the type of Cisco Spaces license package you own.
- In the Cisco Spaces dashboard, apps are shown according to the license type that allows their use.
- Cisco Spaces users can now choose any of these licenses for a location using the **Split License** feature.

Licensing Usage Details for Cisco Smart License Enabled and Non-Enabled Accounts

For Smart License-enabled deployments, the platform also supports license registration, renewal, deregistration, and license update workflows.

The current license details experience can include registration date, expiry date, expiry window, entitlement information, license tag, smart account details, virtual account details, product instance name, and location count.

Note Contact Cisco Spaces support team:

- To enable trial support following Cisco Smart License activation, as trial mode prevents the smart agent from updating license usage to Cisco Smart License Management.
- To enable administrative workflows for Smart License trial management and provisioning, depending on your specific deployment and entitlement setup.

This table provides an overview of how licenses are consumed for **Cisco Smart License** enabled and **Cisco Smart License** non-enabled accounts, detailing the types of devices counted for each license type:

Table 6: License Consumption

Cisco Spaces Account Type	Devices Counted for License
Cisco Smart License Enabled	Multiple appliances such as: Access Points, Camera, Webex Devices, Sensor (Only Portal Beams), Switches
Cisco Smart License Non-Enabled	Only one appliance: Access Points

Note The license counts for both **Cisco Smart License** enabled and **Cisco Smart License** non-enabled accounts will not include Cisco Meraki's MT Sensors.

Cisco Spaces License Types and Features Compatibility

Cisco Spaces offers various license tiers according to your business needs.

This table describes the Cisco Spaces feature compatibility depending on the license types.

Table 7: Feature Compatibility

Features	Cisco Spaces Essential	Cisco Spaces Extend	Cisco Spaces Smart Operations	Cisco Spaces Smart Venues	Cisco Spaces Advantage	Cisco Spaces Unlimited	Cisco Spaces Premier (W)	Cisco Spaces Premier (CW)
Location Hierarchy	Available	Available	Available	Available	Available	Available	Available	Available
Open Roaming (carrier offload)	Available	Available	Available	Available	Available	Available	Available	Available

Features	Cisco Spaces Essential	Cisco Spaces Extend	Cisco Spaces Smart Operations	Cisco Spaces Smart Venues	Cisco Spaces Advantage	Cisco Spaces Unlimited	Cisco Spaces Premier (W)	Cisco Spaces Premier (CW)
Open Roaming (device native)	Available	Available	Available	Available	Available	Available	Available	Available
Live Occupancy	Available	Available	Available	Available	Available	Available	Available	Available
Location Analytics	Available	Available	Available	Available	Available	Available	Available	Available
Detect & Locate	Available	Available	Available	Available	Available	Available	Available	Available
Partner Stream/Local Firehose	-	Available	Available	Available	Available	Available	Available	Available
Firehose API	-	Available	Available	Available	Available	Available	Available	Available
Partner App Center	Available	Available	Available	Available	Available	Available	Available	Available
Data Export	-	Available	Available	Available	Available	Available	Available	Available
CMX On-premise	Base + Partner Stream	Base + Partner Stream	Advanced	Advanced	Advanced	Advanced	Advanced	Advanced
Camera Metrics	Available	Available	Available	Available	Available	Available	Available	Available
Impact Analysis	Available	Available	Available	Available	Available	Available	Available	Available
Behavior Metrics	Available	Available	Available	Available	Available	Available	Available	Available
IoT Explorer/Asset Locator	-	-	Available	-	Available	Available	Available	Available

Features	Cisco Spaces Essential	Cisco Spaces Extend	Cisco Spaces Smart Operations	Cisco Spaces Smart Venues	Cisco Spaces Advantage	Cisco Spaces Unlimited	Cisco Spaces Premier (W)	Cisco Spaces Premier (CW)
Location Analytics Advanced (Path Analytics, Zone)	-	-	Available	Available	Available	Available	Available	Available
Base BLE Gateway	-	-	Available	-	-	-	-	-
IoT Services (Wireless) + Advanced (Path Analytics, Zone level)	-	-	Available	Available	Available	Available	Available	Available
IoT Services (Wireless) +Advanced BLE Gateway	-	-	Available	-	Available	Available	Available	Available
Detect & Locate Advanced (History, Fast Locate, etc)	-	-	Available	-	Available	Available	Available	Available
Captive Portals	-	-	-	Available	Available	Available	Available	Available
Spaces SDK	-	-	-	Available	Available	Available	Available	Available
Engagements	-	-	-	Available	Available	Available	Available	Available
Location Personas	-	-	-	Available	Available	Available	Available	Available
Density Rules	-	-	-	-	Available	Available	Available	Available

Features	Cisco Spaces Essential	Cisco Spaces Extend	Cisco Spaces Smart Operations	Cisco Spaces Smart Venues	Cisco Spaces Advantage	Cisco Spaces Unlimited	Cisco Spaces Premier (W)	Cisco Spaces Premier (CW)
Proximity Reporting	-	-	-	-	Available	Available	Available	Available
Employee Experience	-	-	-	-	Available	Available	Available	Available
Smart Workspaces	-	-	-	-	Available	Available	Available	Available
Standard Rich Maps	Available	Available	Available	Available	Available	Available	Available	Available
Smart Workspaces Data Out	-	-	-	-	Available	Available	Available	Available
Space Utilization	-	-	-	-	Available	Available	Available	Available
Environment Analytics	-	-	-	-	Available	Available	Available	Available

Note If your license status shows **Out of Compliance**, purchase new licenses or remove unlicensed devices to comply.

Log In

Cisco Spaces is now integrated with the Cisco Customer Identity (CCI) application for the login workflow. Cisco Spaces users are now redirected to the CCI application window for login authentication and then proceed to log in to the Cisco Spaces dashboard.

The new workflow is applicable to the following users:

- Cisco domain users
- Customer domain non-SSO users

With the introduction of CCI integration, you can now use the **Switch Users** option to switch between different email addresses in the Cisco Spaces login window.

Note

- Customer domain SSO users can continue to use the existing login workflow.
- The domain specific URLs to log in to Cisco Spaces:
  - European Union (EU): dnaspaces.eu
  - Singapore: ciscospaces.sg
  - Unified: dnaspaces.io
- When you open one of these URLs, Cisco Spaces redirects you to the unified sign-in page at spaces.cisco.com/login.

For more information about CCI, refer to Login and Account Help.

Procedure

Step 1 Go to Cisco Spaces.

Note During the login process, a pop-up window is displayed for Cisco Spaces users who were on board before April 2022 to update their country information. You can either provide the required information or click **Skip & Continue** to skip and proceed to the Cisco Spaces **Home** window. Once you provide the information, the pop-up window is not prompted again during subsequent logins.

When you open the URL, Cisco Spaces redirects you to the unified sign-in page at spaces.cisco.com/login.

Step 2 In the **Email** field, enter your Cisco Spaces account email ID and click **Login**.

You will be redirected to the CCI pop-up window.

Step 3 In the CCI pop-up window, enter your Cisco Spaces account email ID and click **Next**.

You can use the following options in the pop-up window as required:

- **Unlock account**: Use to unlock the Cisco Spaces account if the account gets locked because of incorrect password attempts. Your account will be automatically locked if you make four failed attempts.
- **Forgot email address**: Use to retrieve your Cisco Spaces account email address.

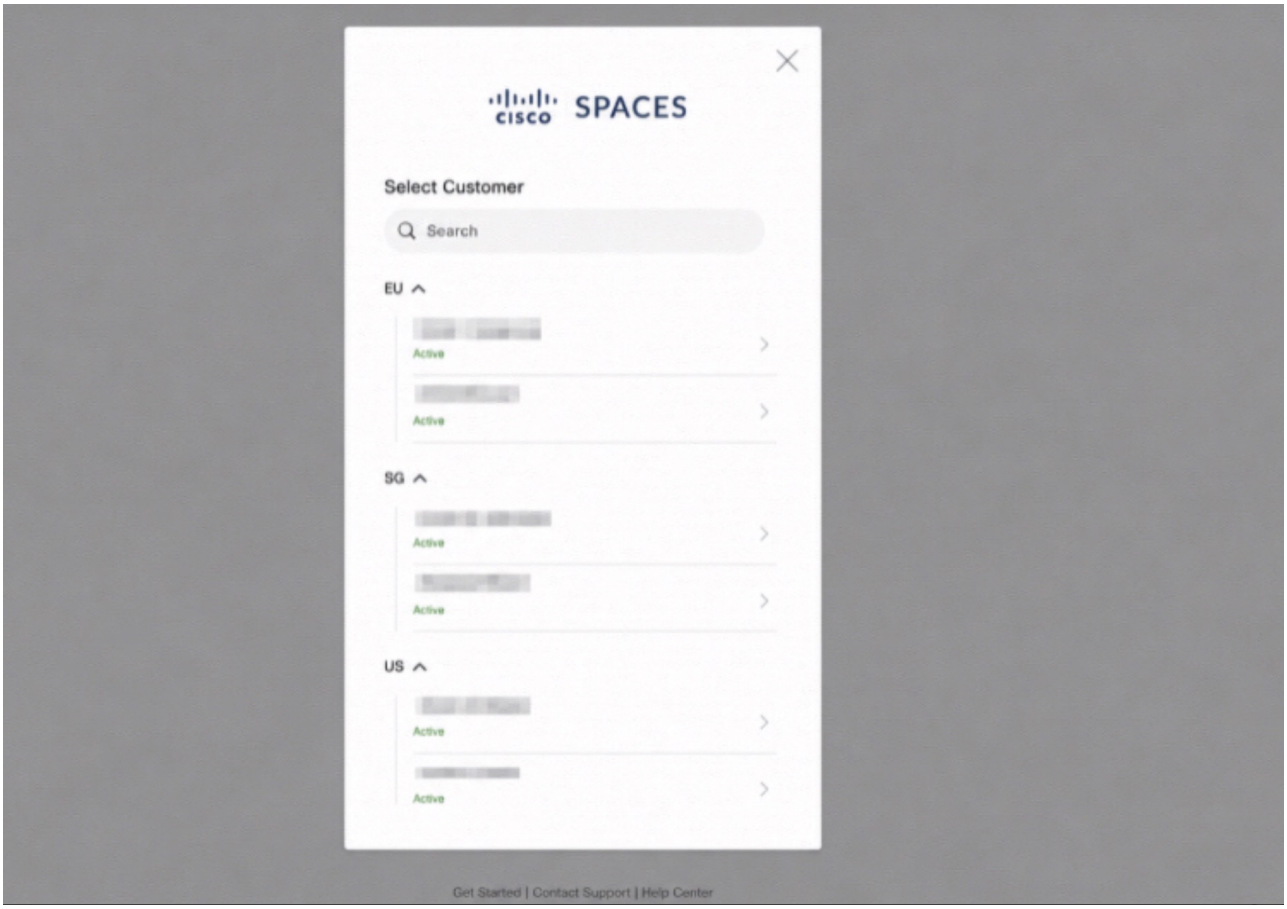
Step 4 In the **Password** field, enter your password.

Use **Forgot password** to retrieve or reset your password.

Step 5 Click **Log In**.

Step 6 In the **Select Customer** window, enter a customer name in the **Search** field to locate a specific customer account.

Figure 3:



If you have access to customer accounts in multiple regions, Cisco Spaces groups the accounts by region.

Step 7 Click the required customer account.

Cisco Spaces dashboard Home page is displayed.

Note To log out, click the profile icon ( ) and choose **Logout**.

Cisco Federation Process

The Cisco Federation Process enables Single Sign-On (SSO) integration with external partner organizations, allowing seamless authentication while maintaining security boundaries. This system uses Cisco's CCI-Okta infrastructure to federate with external Identity Providers (IdPs).

Key benefits

- **Enhanced Security**: Passwords remain with the partner domain; Cisco never stores or accesses them
- **Seamless User Experience**: Single sign-on across Cisco applications
- **Just-in-Time Provisioning**: Automatic user provisioning with minimal required attributes
- **Flexible Authentication Flow**: Multiple entry points for user authentication

Cisco Customer Identity integration

Cisco Customer Identity (CCI) is a unified authentication platform that enhances security and accessibility for users across Cisco Spaces applications. It serves as a common authentication layer, replacing individual application-specific identity providers (IDPs) to streamline user access and improve streamline user access and improve security management.

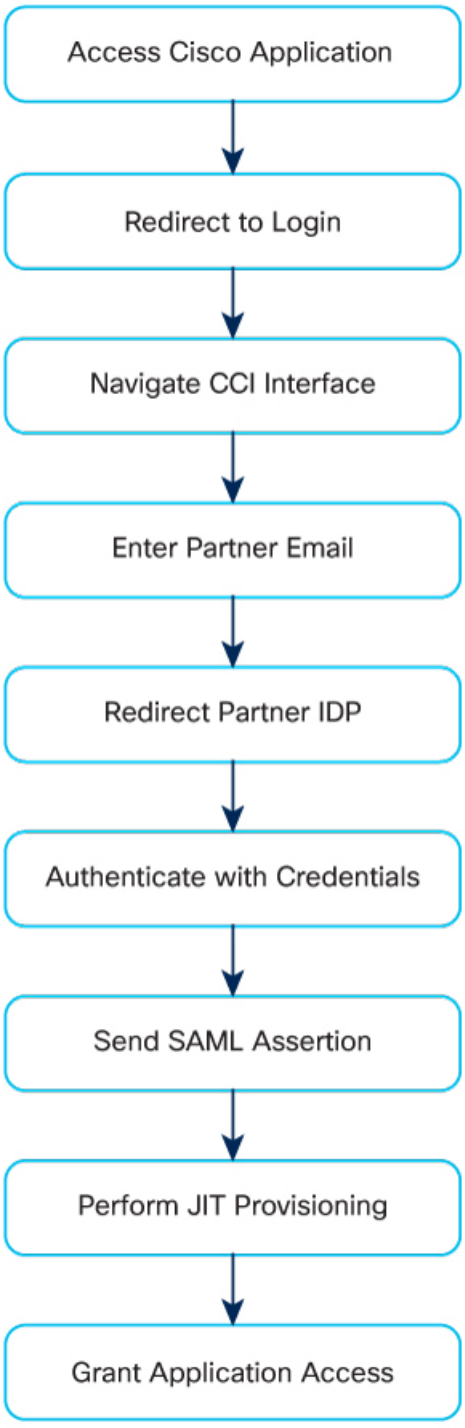
Legacy onboarding used separate IDPs for Cisco Spaces, which created challenges when enabling other applications. Cisco Customer Identity (CCI) provides a common authentication interface that prevents future integration issues for non-CCI customers. To ensure compatibility with the evolving Cisco product ecosystem, users are being transitioned to CCI integration.

CCI integration centralizes user authentication for all Cisco applications, ensuring consistent security policies and simplifying user management. This approach supports future scalability, enabling seamless activation of additional Cisco products that rely on CCI for authentication.

Key attributes:

- Provides a single sign-on (SSO) experience across all Cisco URLs for users with authorized email domains (e.g., @abc.com).
- Replaces legacy or individual application IDPs to avoid fragmentation and complexity.
- Supports SAML-based authentication with metadata exchange between customer IDPs and Cisco.
- Requires mandatory user attributes in SAML responses, such as firstName, lastName, email, company, and countryCode.
- Facilitates both authentication-only and combined authentication and authorization workflows.

Figure 4: Authentication workflow



Set Up SSO for Cisco Spaces with Cisco Customer Identity

Enable Single Sign-On (SSO) across all Cisco applications for users in specified domains by integrating your organization's identity provider with Cisco Customer Identity (CCI). This unified authentication enhances user experience and strengthens application security.

Cisco Spaces uses Cisco Customer Identity (CCI) as its centralized authentication platform. CCI provides secure Single Sign-On (SSO) across Cisco applications by federating with your organization's Identity Provider (IdP).

SSO federation for Cisco Spaces is enabled and configured by the Cisco Customer Identity (CCI) team. Cisco Spaces does not configure SSO independently. Federation is configured at the Cisco domain level so users from the federated domain can authenticate with their corporate credentials across CCI-protected Cisco applications.

Use this task when you need centralized authentication for Cisco applications. The SSO setup is performed at the Cisco domain level, not at the individual application level, to provide consistent, secure access for all users in your organization. You will work with Cisco's SSO enablement team to exchange required metadata and certificates, ensuring that SSO functions reliably and meets organizational security requirements.

Before you begin

Ensure that these requirements are met:

- **CCI-Okta**: Cisco's Identity Provider
- **Federated Partner Domain**: External organization's Identity Provider
- **Protected Applications**: Cisco applications requiring authentication
- **SAML Protocol**: Secure authentication messaging

Ensure that your organization can provide these SAML metadata and configuration details:

Table 8: Metadata

Required information	Description
`SubjectNameID`	Account-linking attribute, typically the user's email address.
Remote IdP Issuer URI	SAML EntityID of your organization's IdP.
Remote IdP Single Sign-On URL	Authentication endpoint for your organization's IdP.
Remote IdP Signature Certificate	Public key certificate in PEM or DER format, used to verify SAML signatures.

Note In this model, the customer Identity Provider (IdP) authenticates the user. CCI acts as Cisco's federated service provider and validates the SAML assertion. Cisco Spaces trusts CCI for authentication validation.

Your SAML assertion must include these mandatory user attributes:

- `firstName`

- `lastName`
- `email`
- `company`
- `countryCode`

  The `countryCode` value must use a two-character country code, such as `US`, `UK`, or `BE`.

Follow these steps to configure SSO.

Procedure

Step 1 Contact the Cisco Customer Identity team, your Cisco account representative, or Cisco Spaces Support to request SSO enablement for Cisco Spaces.

Step 2 Provide the required SAML metadata and configuration details for your organization's IdP to enable SSO integration.

- **SubjectNameID**: Key account linking attribute (usually the user's email).
- **Remote IDP Issuer URI**: SAML Metadata EntityID of the customer's IdP.
- **Remote IDP Single Sign-On URL**: Endpoint receiving SAML authentication requests from CCI.
- **Remote IDP Signature Certificate**: Public key certificate (PEM or DER) to verify SAML signatures.

Step 3 In return, Cisco provides these details so that your IdP can be configured:

- **Assertion Consumer Service URI**: Endpoint where CCI receives SAML assertions after authentication.
- **Audience URI**: Cisco EntityID used by your IdP.
- **SP Signature Certificate**: Public key certificate used to verify authentication request signatures.

After metadata is exchanged, the CCI team validates the trust relationship and enables the customer domain for SSO. After the domain is enabled, users from that domain can sign in to Cisco Spaces using their corporate credentials.

Standard Federation User Journey

When Single Sign-On (SSO) is enabled, you sign in to Cisco Spaces through Cisco Customer Identity (CCI). CCI identifies your federated domain and redirects you to your organization's Identity Provider (IdP) for authentication.

1. Log in to Cisco Spaces.

   Cisco Spaces redirects you to the CCI login page.

2. In the CCI login window, enter your corporate email address. Use the email address that belongs to your organization's federated domain, for example, `username@PartnerDomain.com`.

Note Your email domain must be preconfigured in the federation setup. CCI uses the email domain to identify your organization's IdP.

3. CCI redirects you to your organization's IdP login page.
4. Enter your corporate username and password. Use the same credentials that you use to sign in to your organization's systems.
5. Complete any additional authentication requirements, such as MFA, if configured by your organization.
6. After successful authentication, your organization's IdP sends a secure SAML assertion to CCI.
7. CCI validates the SAML assertion received from the customer IdP. After successful validation, CCI redirects the user back to Cisco Spaces and access is granted.
8. Access is granted and your authentication is complete. You successfully land on the application front page. Full access to the application is now available based on your permission settings.



Note Cisco does not store or manage customer passwords. Passwords remain within the customer domain.

Enable Authentication and Authorization

Cisco Spaces also supports an Authentication and Authorization model. In this model, authentication is handled by CCI, and authorization is enforced in Cisco Spaces through role-based access control.

Use this model when you want your corporate IdP to manage centralized access control and automatically assign Cisco Spaces roles to users.

To enable Authentication and Authorization:

Procedure

Step 1 Configure a `role` attribute in your organization's IdP.

Step 2 Include the `role` attribute in the SAML assertion sent to CCI.

Step 3 Create custom roles in the IdP application and map them to user groups.

Step 4 Create corresponding roles in the Cisco Spaces dashboard.

Step 5 Ensure that the role name in the IdP exactly matches the role name in Cisco Spaces.

The role attribute must use this format:

```
dnaspaces:<AccountNumber>:<Role_Name>
```

For example,

```
dnaspaces:507829691528:Dashboard_Admin
```

Where:

- `<AccountNumber>` is the Cisco Spaces account number.

- `<Role_Name>` is the role created in Cisco Spaces.

Note The role name is case-sensitive and must match exactly.

What to do next

To configure roles in Cisco Spaces, log in to the Cisco Spaces dashboard, go to **Admin Management** > **Roles**, create a role if required, assign the required permissions, and verify that the role name matches the value configured in the IdP.

Role-based access control is required only if you enable the Authentication and Authorization model. If you enable Authentication only, role configuration is not required.

Single Sign-On for Cisco Spaces

Cisco Spaces supports Single Sign-On (SSO) so that users can login to Cisco Spaces using their SSO credentials. For example, if the Cisco domain is SSO-enabled, Cisco employees, who have a Cisco Spaces account, can access Cisco Spaces using their Cisco e-mail address and password. Additionally, if a Cisco employee is already logged in to the Cisco domain through any other Cisco website or application, that Cisco employee can access Cisco Spaces by simply specifying the Cisco e-mail address.

When you click the **Login** button, only the **e-mail ID** field will appear in the **Login** window along with a **Continue** button. If the user is already logged into the SSO-enabled domain, then the user will be directly taken to the Cisco Spaces Dashboard after clicking the **Continue** button. If the Cisco Spaces account supports multiple customer names, then the **Select Customer** window will be displayed. If the user has not logged into the domain, then the user will be redirected to the IDP page for login authentication, and user can login by specifying the SSO credentials.

For SSO enablement or federation-related configuration, contact the Cisco Customer Identity (CCI) team. You can also work through your Cisco account representative or Cisco Spaces Support for assistance.

To enable SSO for your Cisco Spaces account, contact the Cisco Spaces support team and provide the following information:

- Account name
- Domain name (for which SSO needs to be enabled)
- Application Name
- SSO type: Currently, only SAML is supported.
- If only authentication is needed or both authentication and authorization needs to be enabled. This is done by setting the **authenticateOnly** flag to True or False.
  - True: Only authentication is enabled for the user.
  - False: Both authentication and authorization is enabled for the user.



Note

- If you set **authenticateOnly** to `False`:
  - You need to pass additional information from the IDP while sending the user details. For example, **role**=dnaspaces:174923535949:Dashboard_Admin.
  - The value for **role** is mandatory and must be available in the IDP while sending the user details.
  - You need not invite individual users from the **Cisco Spaces dashboard** > **Admin Management**. User invitation and activation is based on both authentication and authorization process by the specific customer IDP & Cisco Spaces.

    You can use the Cisco Spaces dashboard existing default roles or create a new role in the Cisco Spaces dashboard and use that specific role name.

    The Cisco Spaces dashboard default roles are:

    Under **Dashboard Admin Role**: Provides full admin permission to the List user for the selected account
    bullet
    5
    Under **Dashboard Admin Read**: Provides read permission to the user List for the selected account
    bullet
    5

    If you use the Cisco Spaces dashboard default roles, you must pass the **role** string value in the specified format:

    ```
    role": "dnaspaces:<account number>:Dashboard Admin Role",

    role": "dnaspaces:<account number>:Dashboard Admin Read",
    ```

    If you use custom roles, create these custom roles in **Cisco Spaces** > **Admin Management** > **Roles** and pass the role name as the **role** string value in the IDP response.

- When authentication and authorization is enabled, authentication continues to be handled by CCI, while authorization is enforced in Cisco Spaces through role-based access control. Use this model when you want access control to be managed through your corporate IdP and roles to be assigned automatically in Cisco Spaces.

The following information from the metadata.xml file:

- SSO Details
- Entity

- Entry point

Once you provide the above details, the Cisco Spaces support team will send you the following so that you can configure your application:

- Entity ID
- Reply URL (also known as Assertion Consumer Service URL)
- Cisco metadata file with the following information:
  - Depending on the location of your application, either the US or EU Cisco Spaces IDP metadata
  - Identifier: https://dnaspaces.io
  - Sign On URL: https://dnaspaces.io/api/tm/v1/account/login
  - Sign out URL: https://dnaspaces.io/api/tm/v1/account/logout
  - CallBack URL from your IDP to Cisco Spaces: https://dnaspaces.io/api/tm/v1/account/login/callback

Configure your IdP metadata or SAML response to return these mandatory attributes: `firstName`, `lastName`, `email`, `company`, and `countryCode`.

For example,

```
nameid-format:"emailAddress","firstName":"Jane","lastName":"Doe","phone":"9876543210","level":"info","
```

Start Working with Cisco Spaces

Before starting working with Cisco Spaces ensure that you have the prerequisites mentioned in System Requirements, on page 1.

Note Initially, you must contact the Cisco Spaces support team for creating a Cisco Spaces account. You will get an invite to activate your Cisco Spaces account through e-mail. Click the **Accept Activate** button, and in the window that displays configure the log in credentials, and click **Activate Account**. You are now logged into Cisco Spaces. If you are a **Dashboard Admin**, you can now invite other Cisco Spaces users.

For more information, refer to Activation requests reminder emails, on page 29.

To start working with Cisco Spaces, perform the following steps:

Procedure

Step 1 Log in to Cisco Spaces.

Note You can enable Single Sign-On for Cisco Spaces. For more information, refer to Single Sign-On for Cisco Spaces, on page 25.

Step 2 Connect to your wireless network and configure the wireless network for Cisco Spaces referring to the instructions in the **Setup** section of the Cisco Spaces dashboard.

The setup instructions are also available in the following sections of this guide:

- **Meraki**: For configuring a Cisco Meraki network, refer to Configuring Cisco Meraki for Cisco Spaces.
- **Cisco Unified Wireless Network with Cisco CMX**: For connecting Cisco Spaces with Cisco AireOS Controller through Cisco CMX, refer to Connecting Cisco Spaces to Cisco Wireless Controller through Cisco CMX, on page 74.
- **CiscoAireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller (without Cisco CMX)**.

Note Connecting through the Cisco Wireless Controller Direct Connection method is only recommended for small scale deployments. All large-scale production deployments require a Cisco Spaces: Connector.

- **Using Cisco Wireless Controller Direct Connect**: For configuring Cisco Spaces with Cisco Wireless Controller using Wireless Controller Direct Connect, refer to the Connecting Cisco Catalyst 9800 Series Wireless Controller or Cisco Wireless Controller to Cisco Spaces Using WLC Direct Connect or Cisco Spaces: Connector, on page 89section.
- **Using Cisco Spaces Connector**: For configuring a Cisco Spaces with Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller using Cisco Spaces: Connector, refer to Connecting Cisco Spaces to Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller using Cisco Spaces: Connector, on page 110.
- **Using Cisco Embedded Wireless Controller**: For configuring a Cisco Unified Wireless Network using Cisco Embedded Wireless Controller, refer to Configuring Mobility Express to work with Cisco Spaces, on page 111.

Note Cisco Spaces provides a universal account so that you can connect Cisco Spaces to multiple wireless networks.

Step 3 Add your team members, and assign them roles and permissions. For more information about adding Cisco Spaces users, refer to Manage Cisco Spaces Users, on page 303.

Step 4 Import the location hierarchy defined in your wireless network to Cisco Spaces. For more information on configuring the location hierarchy, refer to Location Hierarchy in Cisco Spaces and Overview of Location Hierarchy 2.0.

The following steps are optional and depend on the apps that you want to use and the activities that you want to perform.

Step 5 To use the Captive Portals app, import SSIDs to Cisco Spaces. For more information on importing the SSIDs, refer to the “SSIDs” section.

Step 6 Define Location Personas Rules to tag customers. For more information on creating a Location Personas Rule, refer to the “Creating or Modifying Tags Using a Location Persona App” section.

Step 7 Configure supporting features such as SMS Gateways. Refer to the respective topic in this guide for configuration.

Step 8 If required, create Captive Portals. For more information on creating the captive portals, refer to the “Creating and Managing Portal” section .

Step 9 If required, create Captive Portal Rules to display the appropriate captive portal to various customers. For more information on creating Captive Portal Rules, refer to the “Captive Portal Rule” section.

Step 10 If required, create Engagement Rules to send appropriate notifications to the customers. For more information on creating Engagement Rules, refer to the “Creating an Engagement Rule” section.

Step 11 Analyze the Cisco Spaces performance, and your business performance using apps such as Behavior Metrics, Location Analytics, and Impact Analysis. For more information on these apps, refer to the respective section..

Step 12 Monitor the Cisco Spaces domain and apps using the Monitor section.

Profile Information

Cisco Spaces supports adding the profile information such as first name, last name, and mobile number of the Cisco Spaces dashboard user.

- A tab, **My Profile**, is available in the **Account Preferences** window to add the profile information. You can specify the first name, last name, and mobile number in this window, where mobile number and its verification are optional. When you specify the mobile number, a **Verify Mobile Number** link appears, which allows you to verify the mobile number using One Time Password. Once the mobile number is verified, the status **Verified** is shown. The **Verify Mobile Number** link will appear again when you change your mobile number.
- The Login workflow for Cisco Spaces displays the **Update Profile Information** dialog box as part of the login process if the Profile Information is not available for the particular Cisco Spaces user. You can skip this step, and can proceed to log in. You can then add the profile details through the Account Preferences window any time later. However, the **Profile Information** dialog box is shown as part of the Login workflow till the time information is provided.



Note The SSO users will not be able to edit the profile information or verify the mobile number. Also, the **Update Profile Information** dialog box will not be shown to SSO users during login.

Activation requests reminder emails

The Cisco Spaces platform now automatically sends a sequence of reminder emails if you are newly invited and have not yet activated your account. If you do not activate your account with the initial invitation, you will receive additional reminders on day 2, day 4, and day 5, so you have more opportunities to complete activation before the link expires.

Additionally, you can now request a resend of your activation link directly through the Cisco Spaces platform. Your request immediately generates and delivers a new activation email, so you do not need support assistance or manual processing.

These improvements make onboarding easier for you, provide faster responses to activation requests, and reduce support delays. With this enhancement, you receive timely reminders and can easily obtain a new activation link whenever you need, making the activation process simple.

Cisco Spaces Dashboard GUI Enhancements

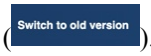
Cisco Spaces has introduced a new Beta version of the existing dashboard. The new beta dashboard exclusively offers all new features and enhancements, retaining the functionalities of the current one while providing an improved experience. We encourage you to try the beta version for an enhanced experience and better performance.

To highlight few updates in the new beta version:

- The **Location Hierarchy** feature is available in the previous version of the Cisco Spaces dashboard. In the beta UI, experience the features of **Location Hierarchy 2.0** that includes features to import the locations in the same structure in which you have defined in your wireless network such as Cisco AireOS Wireless Controller, Cisco Catalyst 9800 Series Wireless Controller, or Cisco Meraki.
- Instead of the **Map Service** (**Set Up** > **Map Service**) feature available in the previous version, use the **Locations and Maps** (**Setup** > **Locations and Maps**) feature to import, normalize and unify network hierarchies from various sources such as Cisco Meraki, Catalyst Center, and Cisco Prime Infrastructure into a single business oriented hierarchy.
- The **Room Occupancy Reports** feature is available under the Cisco Spaces: Space Utilization App application.

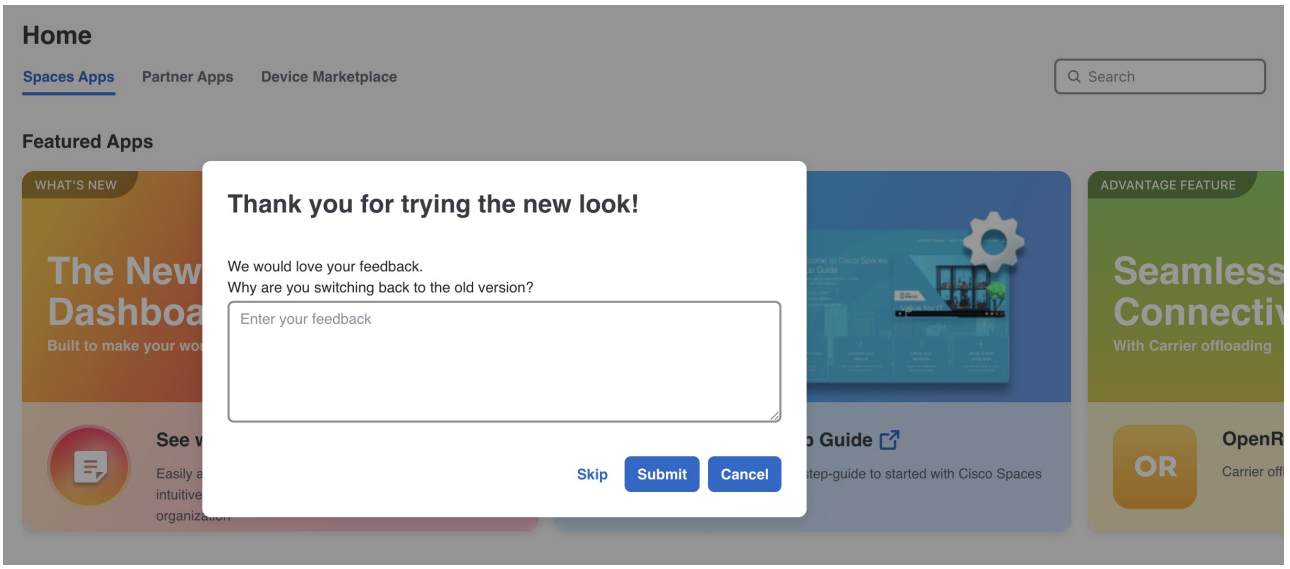
To access the new beta Cisco Spaces dashboard, click the **Try new version (Beta)** (

) toggle option that is available on the top-right corner of the Cisco Spaces dashboard window.

To go back to the old version, click **Switch to old version** (

). Use the **Feedback** pop-up window to share your feedback and valuable suggestions to improve the user experience.

Figure 5:



Cisco Spaces: Licenses

Cisco Spaces new dashboard UI (React dashboard) includes these license updates:

- The **SEE** and **ACT** licenses are renamed as **ESSENTIAL** and **ADVANTAGE**, respectively.
- The location-level license is now shown beside each location in the **Location Hierarchy** tree for Cisco Spaces accounts registered with smart licensing.

Verticals overview

Cisco Spaces apps supports various verticals to provide tailored solutions for different industries.

Currently, **Behavior Metrics** App and **Space Utilization** App supports verticals.

These are the four verticals supported:

- Generic: Provides insights into behavior patterns, monitors and locates assets in real-time to optimize operations.
- Workspaces: Utilizes Wi-Fi-associated devices and room sensors to provide accurate occupancy data. Campus-level computation is implemented for the Workspaces vertical.
- Retail: Uses Wi-Fi probing, cameras, and sensors to gather data.
- Education: Smart campus solutions, attendance tracking, and wayfinding.

Verticals for apps are defined at the backend level. Currently, Cisco Spaces does not support a GUI to select verticals for apps.

Cisco Spaces supports associating verticals to the Cisco Spaces account. Verticals are added with the Cisco Spaces account when the account is onboarded to Cisco for the first time.

If you want to update the vertical for your account, contact Cisco Spaces support team.

Note By default, for workspaces and education vertical accounts, Wi-Fi metrics data will be displayed.

For more information, refer to Cisco Spaces: Behavior Metrics App and Cisco Spaces: Space Utilization App Guide.

Cisco Meraki Integration Workflow

You can onboard Cisco Spaces through the Cisco Meraki Dashboard. The new seamless integration flow eliminates the need for multiple manual steps in establishing a mapping between the Cisco Meraki Dashboard and Cisco Spaces. This eliminates the need to manually copy and paste the API key and post URLs from one platform to the other. With the new integration, you can easily initiate the integration from the Meraki dashboard with just a few clicks.

For more information, refer to Seamless Meraki Integration with Cisco Spaces.

For setup instructions, refer to Cisco Meraki Integration with Cisco Spaces.

These integrations options are available:

- **Native Integration**: Simple and seamless flow to enable Cisco Spaces integration via Cisco Meraki dashboard

- **Bundled Licensing**: Cisco Spaces Licenses are now bundled with Cisco Meraki Enterprise and Advanced licenses.
  - If you already have a Cisco Spaces account with Smart Licensing, you must create a new Cisco Spaces account when integrating Cisco Meraki Organization with Cisco Spaces. Otherwise, the bundled Cisco Meraki licenses are not displayed in Cisco Smart Software Manager (CSSM), and the Smart Licensing dashboard displays the status as Out of Compliance.
  - If you already have a Cisco Spaces account with Legacy Licensing, and the existing licensing tier matches the Cisco Meraki Organization being integrated, we recommend that you use the existing account when integrating Cisco Meraki Organization.

    For example, if the existing Cisco Spaces account is Spaces EXTEND licensing and the Cisco Meraki licensing is MR Enterprise, that would be the same Cisco Spaces licensing tier.
  - If you already have a Cisco Spaces account with Cisco Spaces Legacy Licensing, and the existing licensing tier is higher than the Cisco Meraki Organization being integrated, we recommend that you create a new Cisco Spaces account when integrating Cisco Meraki Organization.

    For example, if the existing Cisco Spaces account is Spaces ADVANTAGE licensing and the Cisco Meraki licensing is MR Enterprise, that would be a higher Cisco Spaces licensing tier.

Manage Networks in Cisco Meraki Dashboard

Cisco Spaces offers **Manage Networks** capability for Cisco Meraki integration users. This enhancement gives users direct control over which Cisco Meraki networks are synchronized with Cisco Spaces.

Key details include:

- **Availability**: Once the Meraki integration is completed, the **Manage Networks** option becomes available on the Meraki integration details page.
- **Network Selection**: All networks are selected and synced by default. Users can now explicitly choose which Meraki networks should be synchronized with Cisco Spaces.
- **Selected Networks**: Networks chosen for synchronization are imported into the Cisco Spaces Dashboard and kept automatically in sync.
- **Ability to Deselect Networks**: Any network that is deselected is removed from the Locations Hierarchy, and further synchronization for that network is stopped. Existing data associated with the unselected network is also removed, unless there are active app-specific configurations or rules attached to that node.

  In such cases, you must remove those associations before the network can be completely deleted from Cisco Spaces.

Cisco Magnetic Design

Cisco Spaces - Partner Dashboard user experience is enhanced by adhering to the Cisco Magnetic Design guidelines for a consistent and intuitive graphical user interface (GUI) across the Cisco Spaces - Partner Dashboard ecosystem.

The enhancements include:

- Faster load times and smoother interactions
- Improved usability and accessibility

Cisco Spaces: Connector 3.0

Cisco Spaces: Connector (referred to as Connector in all subsequent references in this document) is a fully redesigned version of the Connector with the capability to efficiently manage multiple services that connect to different network devices such as Cisco Wireless controller and switches for data. The Connector platform makes it easy to add/remove new services from the cloud. It enables enhanced troubleshooting with debugging, log upload, and restart functionalities from the cloud. Connector also provides detailed metrics for each service with CPU, Memory, Connectivity and Up/Down status.

Connector is the next generation connector of Cisco Spaces that provides an enhanced user experience, architecture to support multiple services, simplicity, modularity, seamless upgrade and High Availability. Connector supports an active-active High Availability setup. Unlike the earlier releases of Connector 2.x, you can specifically configure and monitor the High Availability pair. All services and device configurations are managed at the Connector level to make it easy to pair with High Availability.

The Connector and device status is also aggregated at the Connector level from each instance for easy monitoring. Connector provides full visibility to each instance of a High Availability pair. You can view how the services are running on each instance, their upgrade status and so on. You can also perform actions on a particular instance, such as restarting of services.

Idle Timeout for Cisco Spaces

A user who is logged in to the Cisco Spaces dashboard can remain idle only for a specific time period. If inactive for 20 minutes, the user is automatically logged out of the dashboard. A notification is displayed 5 minutes before the idle timeout and the title of the browser window where the Cisco Spaces application is open changes to `INACTIVE: You will be logged out in 5 mins`. Any action performed on the corresponding window extends the user's session.

Migrate Data from Cisco Prime Infrastructure to Catalyst Center

In the Cisco Spaces Location Hierarchy, if you have previously imported map data using Cisco Prime Infrastructure's import feature, you can now perform the same map data import using Catalyst Center's import feature.

This migration from Cisco Prime Infrastructure import to Catalyst Center import is considered as the source data migration in Cisco Spaces Location Hierarchy. After the migration, the import type source is considered as Catalyst Center import.

Before proceeding with map import or data migration, we strongly recommend that you reach out to the Cisco Spaces support team for assistance and guidance.

Contact Cisco Spaces Support

The process for requesting support for Cisco Spaces is enhanced. To contact Cisco Spaces support, you now need to raise a case using the Support Case Manager, based on the account types: **Paid** and **Non-Paid**.

Note All the support contact email addresses are decommissioned.

Follow these steps to raise a support case.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces Dashboard, click the (**Support**) icon displayed at the top-right.

Step 3 Click **Support**. The **Support** slide-in pane displays.

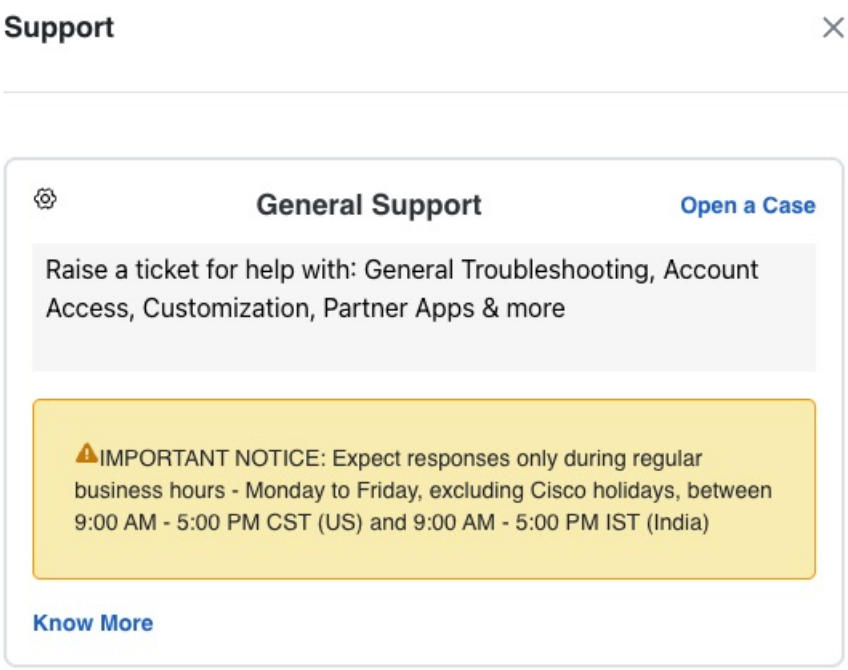
Step 4 Depending on the account types, the following support options are available:

- **Paid**: There are two different SCM links for **Paid** accounts.
  - For General Support, raise a case with Moderate Impact (S3) severity.
  - For Configuration & Deployment Support, raise a case with Ask a Question / Warranty (S4) severity.

Figure 6: Paid Account Support Options

- **Non-Paid**: Use the General Support link to raise both general support and onboarding/use case deployment assistance cases.

Figure 7: Non-Paid Account Support Options



Step 5 Click **Open a Case** to raise a case using SCM.

Cisco Spaces Documentation

You can access the documentation for Cisco Spaces including Configuration Guides and Release Notes using the **Cisco Spaces Support** icon ( ) displayed at the top-right of the Cisco Spaces dashboard.

Access these documentation support resources.

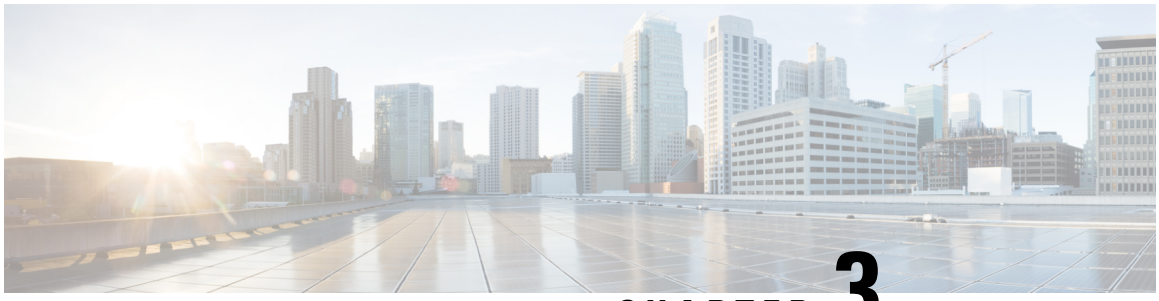
- Help Center
- Documentation
- Support
- Latest Release Notes
- Release Notes History



PART III

Cisco Spaces Home

- Cisco Spaces Dashboard, on page 39
- Cisco Spaces: Apps, on page 59
- Partner App Management, on page 67
- Configuring Cisco Wireless Controllers and Cisco Catalyst 9800 Series Controllers for Cisco Spaces, on page 71
- Configuring Cisco Meraki for Cisco Spaces, on page 123



CHAPTER 3

Cisco Spaces Dashboard

- Cisco Spaces Navigation, on page 39
- Cisco Spaces Dashboard, on page 43
- Cisco Spaces Features, on page 44
- User Profile, on page 49
- Viewing Cisco Spaces Account Details, on page 51
- Cisco Smart License, on page 51

Cisco Spaces Navigation

When you log in to the Cisco Spaces dashboard, the **Home** page is displayed.

You can navigate to the **Home** page by clicking **Cisco Spaces** logo displayed at the top-left of the dashboard or using the **Home** option.

All Cisco Spaces apps are accessible from the Home page. Click **Dashboard** to view and open the available apps.

Use the menu icon displayed at the top-left of the **Home** page to expand and collapse the left navigation pane.

Use the left navigation pane to access these features of Cisco Spaces.

- **Location Hierarchy**
- **Integrations**
- **Configure**
- **Monitor**
- **Admin Management**
- **IoT Services**
- **Setup**

Cisco Spaces Home

The new and improved Cisco Spaces dashboard - **Home** page introduces these changes to enhance user experience and navigation:

- A new tab structure for Spaces Apps, Partner Apps, and Device Marketplace streamlines navigation and improves accessibility.
- App overviews now highlight the value, key personas, and provide quick setup guidance.
- You can mark apps as favorites. Click the heart-shaped **Add to Favorites** icon on an app tile to mark the app as a favorite. After you mark one or more apps as favorites, the **Favorite Apps** section appears.

Note A Favorite Apps section appears after you mark one or more apps as favourites.

Note While the dashboard and apps feature a more organized design for better performance, the functionality and features remain the same. Your data, instance, and access will not change.

Click the info icon displayed on the app tile to view the app summary in the slide-in window.

Figure 8: Spaces Apps

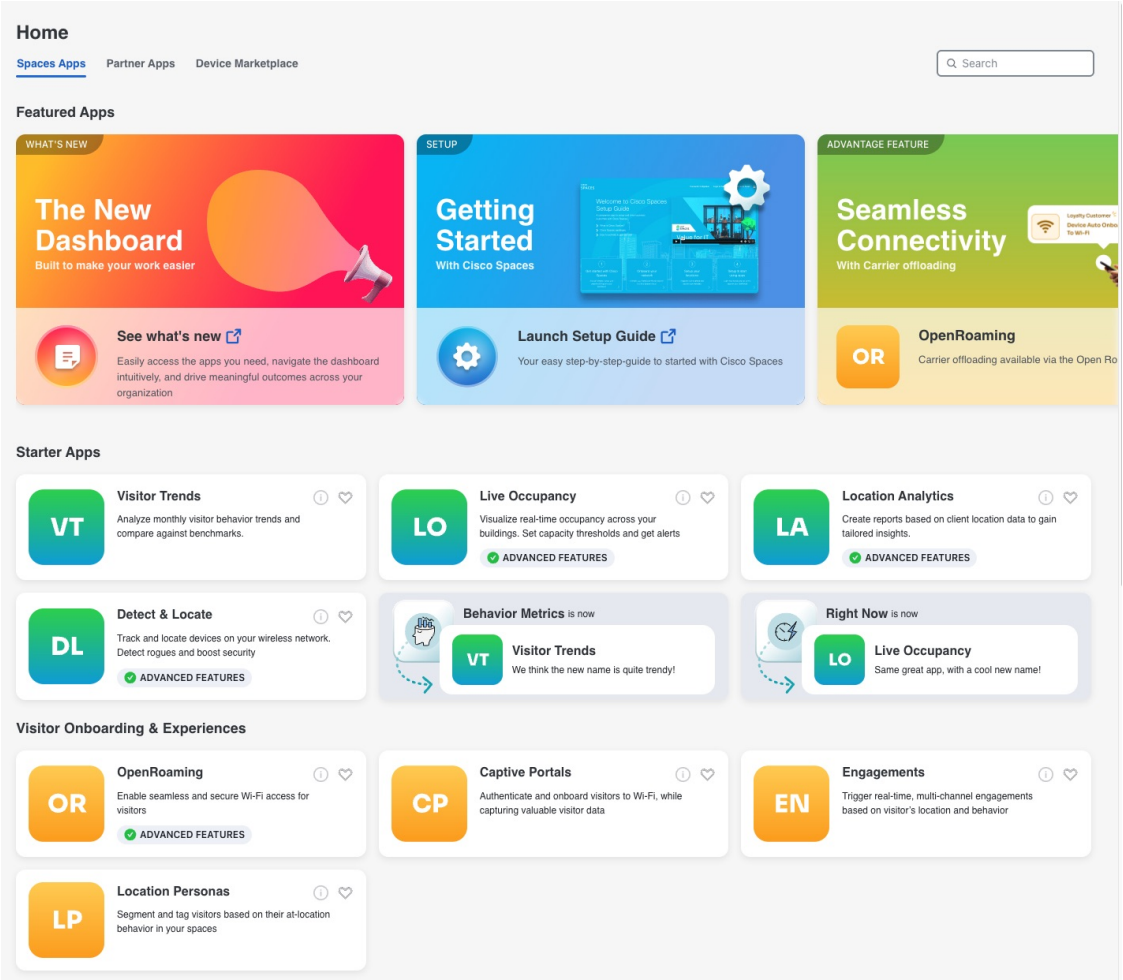


Figure 9: Partner Apps

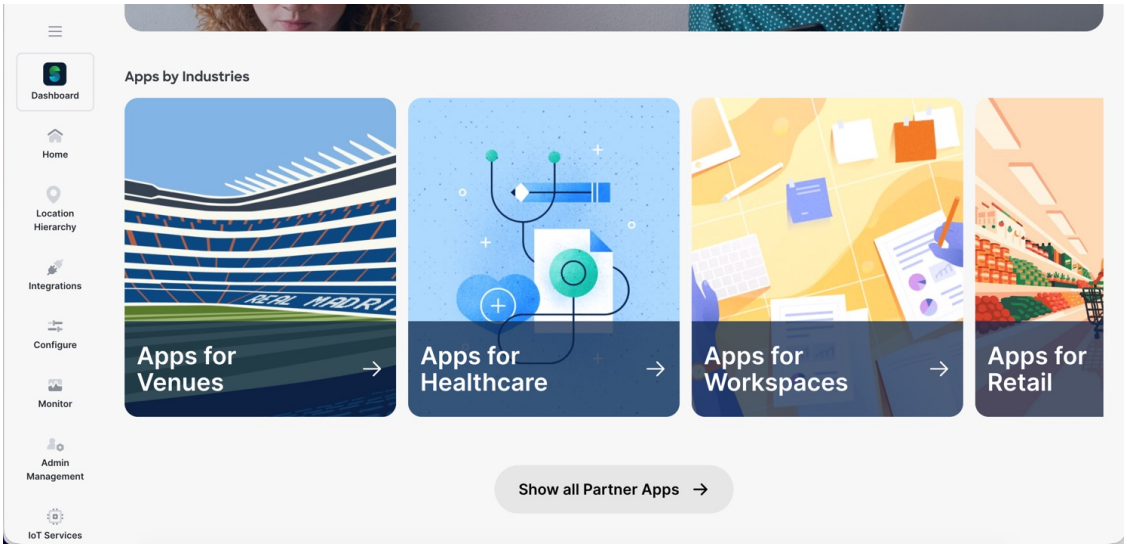


Figure 10: Device Marketplace

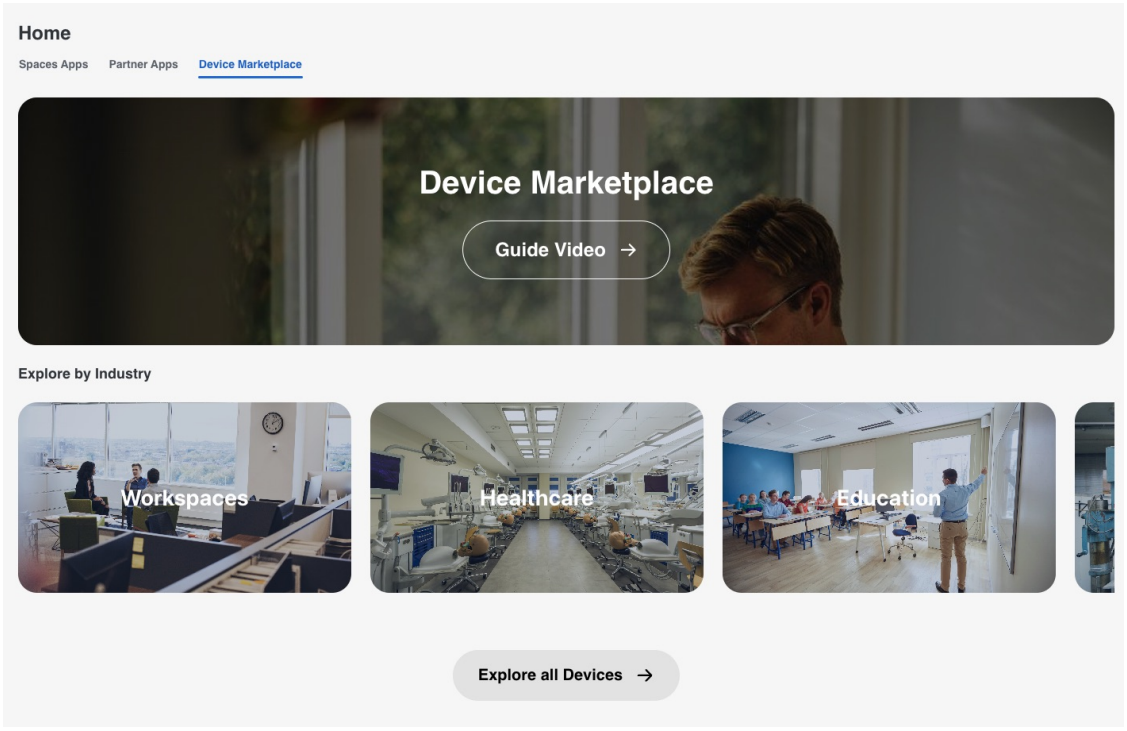


Figure 11: Favorite Apps

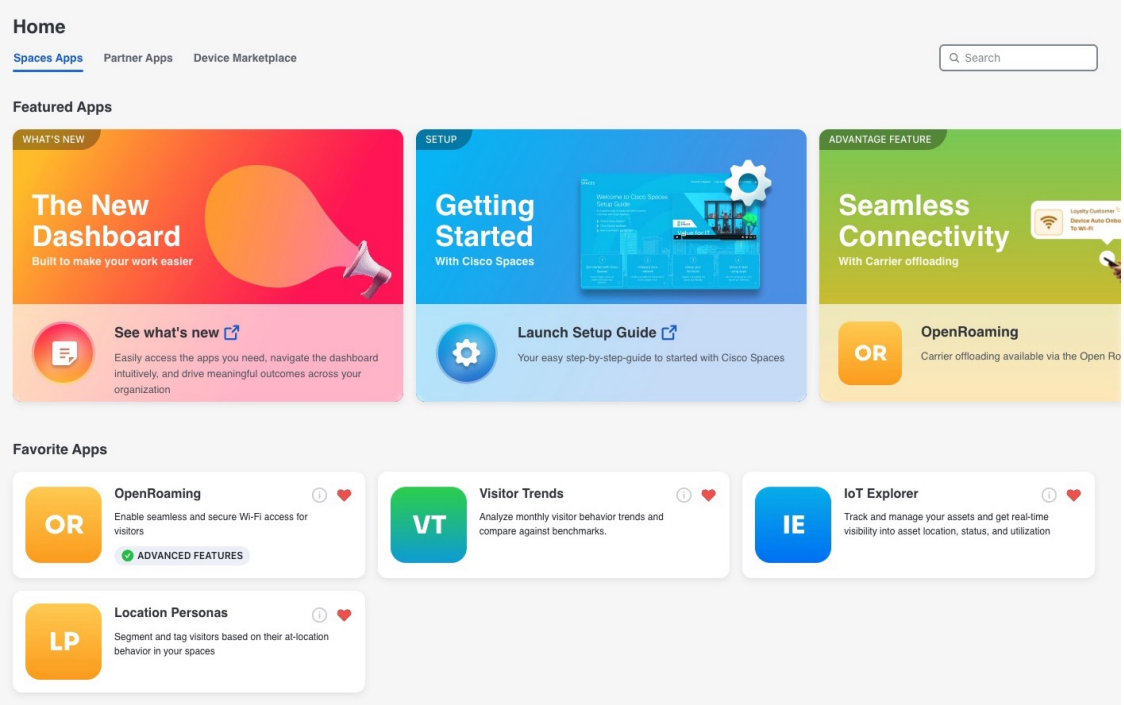
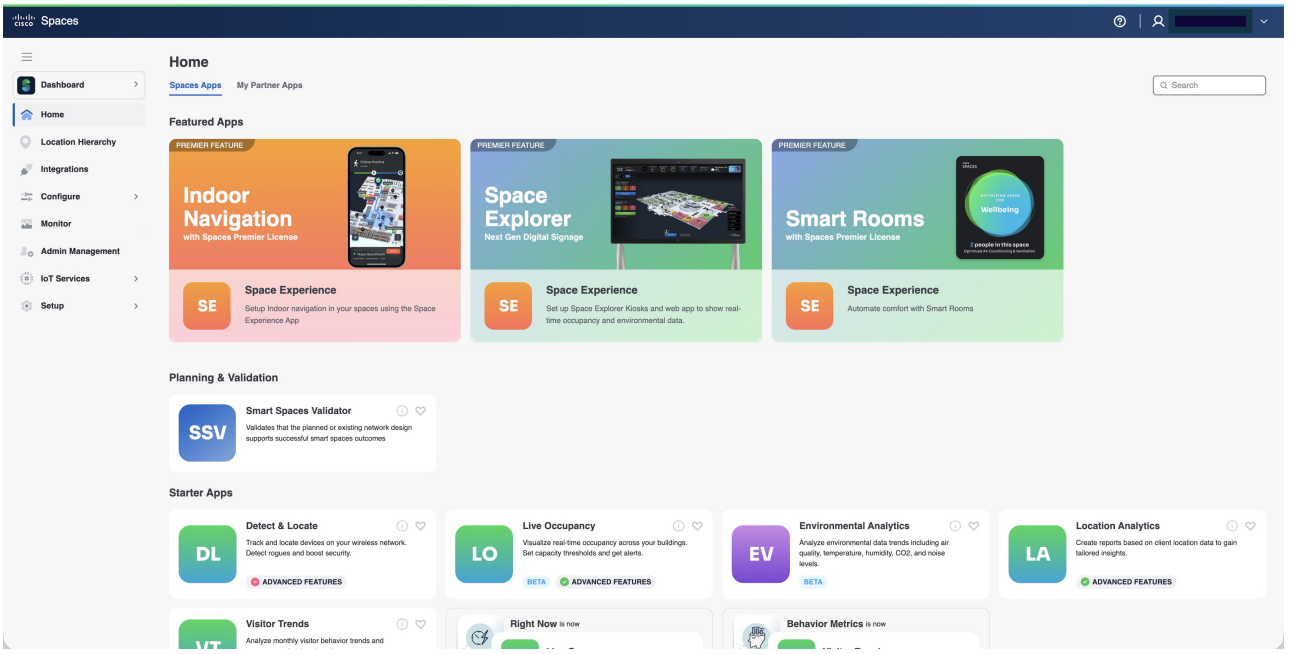


Figure 12: Home

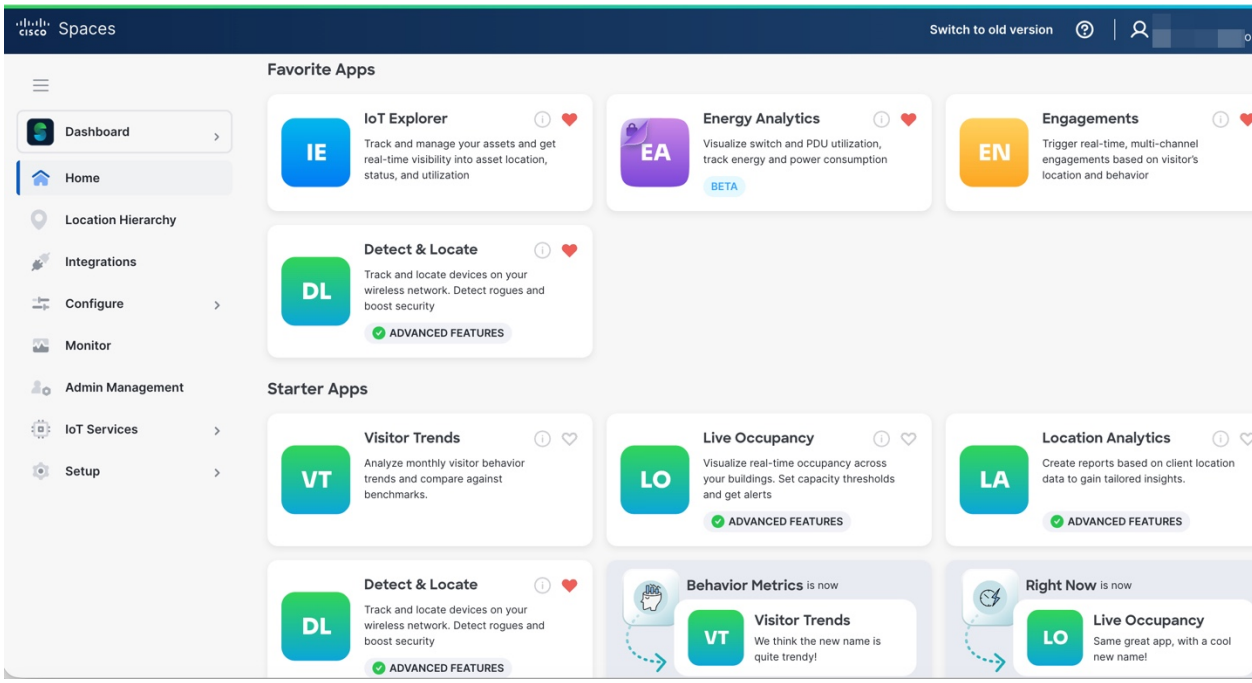


Cisco Spaces Dashboard

Cisco Spaces dashboard is the default home page of Cisco Spaces application. The Cisco Spaces GUI adopts the Magnetic design implementation. Magnetic design follows a persistent header and collapsible left navigation pane.

After you log in to Cisco Spaces, the **Home** window is displayed as shown in the following image:

Figure 13: Cisco Spaces Home



The Cisco Spaces **Home** window includes the **Dashboard** drop-down list (in the left navigation pane) which allows you to search and view the available apps associated with your Cisco Spaces license.

Use the **Dashboard** drop-down list to choose and navigate to any selected app. To navigate back to the Cisco Spaces **Home** window, choose **Dashboard** option from the drop-down list.

The dashboard has the following main areas: Menu Bar, Information icon, Profile icon, and various applications available as per your subscription.

Left Navigation Pane

Use the left navigation pane to access these features.

- Home
- Location Hierarchy
- Integrations
- Configure
- Monitor

- Admin Management
- IoT Services
- Setup

Icons

Click the icons on the right side of the menu bar to perform common tasks:

Icon	Description
	Support: Displays help center, support and documentation links.
	User Profile: Displays account, smart licenses and logout options. The license information is available under **My Account** > **License Info** > **License Units Consumed**. For more information, refer to User Profile, on page 49.

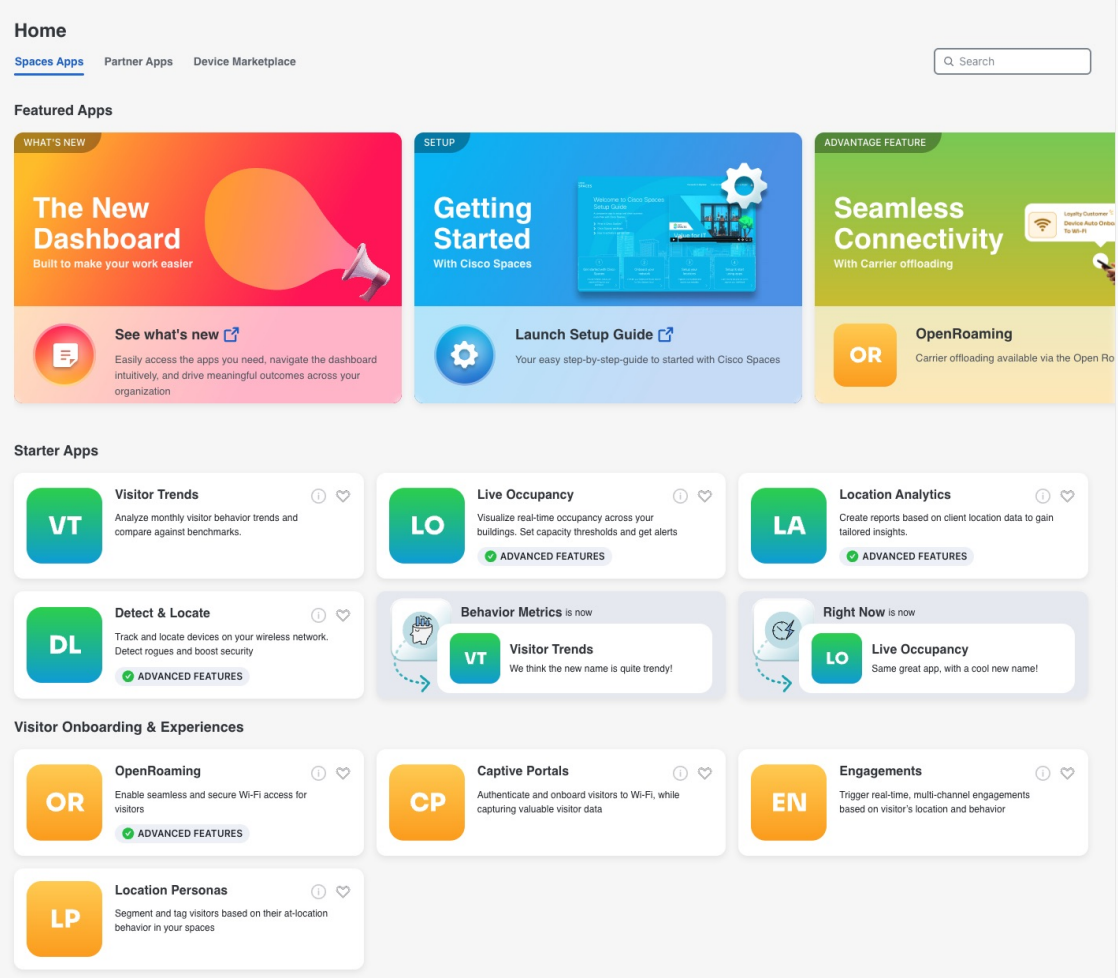
Cisco Spaces Features

The major features of Cisco Spaces dashboard includes:

Cisco Spaces Apps

- Log in to **Cisco Spaces**.
- In the left navigation pane, click **Dashboard** to view the apps.
- On the Home page, click the **Spaces Apps** tab.
- Use the Search field to search for apps and features.
- Check the app tiles. If a tile displays a lock icon, the app cannot be accessed with the current account or license.
- Click a **featured app** card to open the overview drawer.
- In the overview drawer, click **Open App** to launch the app.

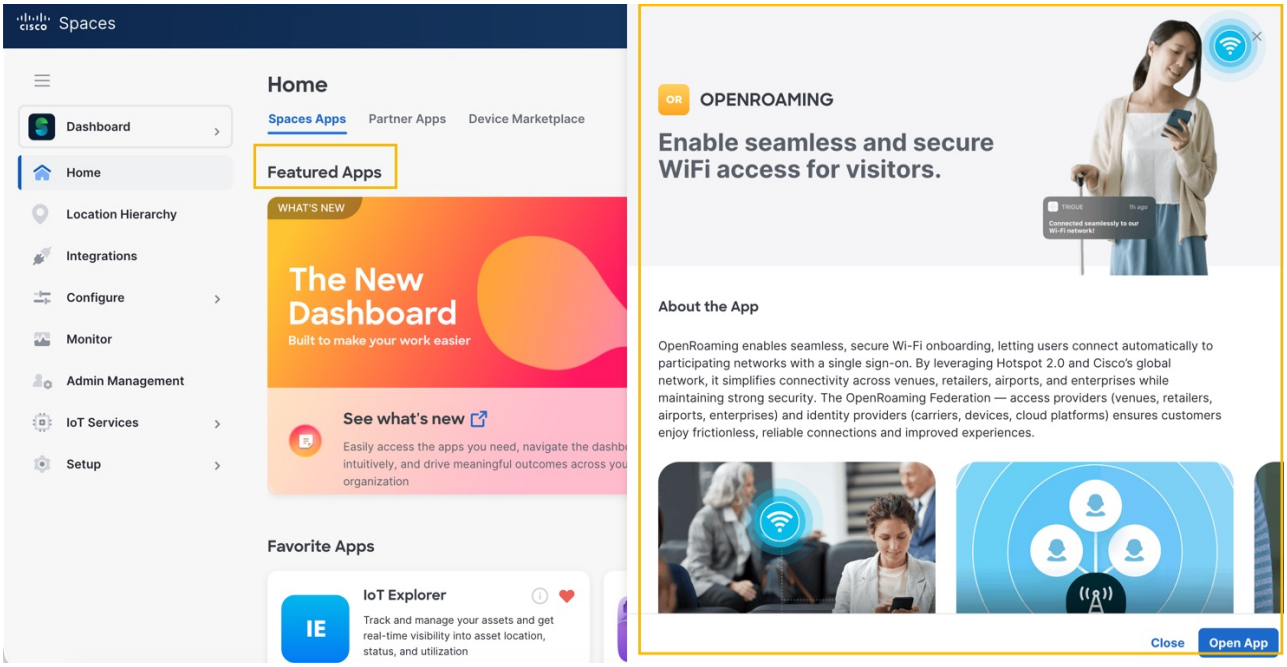
Figure 14: Spaces Apps



Note **Right Now** is now called **Live Occupancy**, and **Behavior Metrics** is renamed **Visitor Trends**.

- Log in to **Cisco Spaces**.
- In the left navigation pane, click **Dashboard**.
- On the **Home page**, click the **Spaces Apps** tab.
- In the **Featured Apps** section, click a featured app card.
- The app overview drawer opens.
- Click **Open App** to launch the app, or click **Close** to return to the **Home page**.

Figure 15: Featured App Cards



Location Hierarchy

Location Hierarchy enables you to define and organize the business locations used by Cisco Spaces. You can import or add locations from supported wireless networks and maintain them in a hierarchy that reflects your organization's structure, such as networks, campuses, buildings, floors, and zones.

Apps such as **Engagements**, **Captive Portals**, and **Location Personas** use the locations defined in **Location Hierarchy**.

Cisco Spaces maintains the location hierarchy at the account level, so locations from multiple wireless networks can be added to the same hierarchy. The APs and locations available for use can vary based on the Cisco Spaces license associated with your account.

1. Log in to Cisco Spaces.
2. In the left navigation pane, click **Location Hierarchy**.
3. Use the hierarchy tree or search option to find the required location.
4. Expand the hierarchy nodes, such as network, campus, building, floor, or zone.
5. Select the required location to view or manage its details.

Integrations

The **Integrations** feature enables you to connect Cisco Spaces with Cisco and third-party applications, such as Catalyst Center, Office 365, Google Calendar, ServiceNow, and Hamina.

These **integrations** help extend Cisco Spaces data and workflows into other systems. Depending on the integration, Cisco Spaces can synchronize maps, provide device location updates, share location, occupancy, space utilization, or footfall data, and synchronize meeting room booking information. This helps improve workspace operations and maximize the value of your Cisco Spaces deployment.

- Log in to **Cisco Spaces**.
- In the left navigation pane, click **Integrations**.
- Select the required integration, such as **Catalyst Center, Office 365, Google Calendar, ServiceNow,** or **Hamina**.
- Click **Connect or Manage** depending on the integration status.
- For more information click **More details**.
- Complete the configuration steps shown for the selected integration.

Configure

The **Configure** feature enables you to configure Cisco Spaces options such as **SDK, Notifications,** and **Location Compute**.

- Log in to Cisco Spaces.
- In the left navigation pane, expand **Configure**.
- Select **SDK, Notifications,** or **Location Compute**.
- Configure the required settings and save the changes.

Monitor

The **Monitor** feature enables you to view the operational status of Cisco Spaces and related services. It displays summary information for connectivity, anomalies, connectors, controllers, location updates, Cisco Spaces apps, enterprise integrations, partner integrations, Meraki networks, and support tickets.

- Log in to Cisco Spaces.
- In the left navigation pane, click **Monitor**.
- Review the **Summary, Connectivity, Anomaly,** and **status sections**.
- Use the available tables or **See All links** to view more details.

Admin Management

The **Admin Management** feature enables you to invite and manage Cisco Spaces admin users. You can create and edit roles, assign permissions, and restrict user access to specific locations based on their role.

- Log in to Cisco Spaces.
- In the left navigation pane, click **Admin Management**.
- Use the **Admins** tab to invite, edit, resend invitations, or remove users.

- Use the **Roles** tab to create, edit, or remove roles.
- Assign permissions and location access, then save the changes.

IoT Services

Cisco Spaces: IoT Services enables you to activate, claim, manage, monitor, and configure IoT devices using Cisco wireless and wired infrastructure. It supports IoT device management across vendors, form factors, and technology protocols. Bluetooth Low Energy (BLE) is supported for IoT device management, with additional device and gateway workflows available through IoT Services.

IoT Services uses Cisco Spaces, Cisco Spaces Connector, Cisco Catalyst 9800 Series Wireless Controllers, compatible Cisco access points, and supported switches to enable wireless and wired gateway activation, device onboarding, inventory management, monitoring, and device configuration.

- Log in to Cisco Spaces.
- In the left navigation pane, expand **IoT Services**.
- Use **About** to review IoT Services status and activation guidance.
- Use **Inventory** to view APs, wired devices, and claimed devices.
- Use **Manage** to onboard or manage devices and policies.
- Use **Monitoring** to monitor device and gateway status.
- Use **Settings** to configure options such as device filtering or sensor history.

For more information, refer to Cisco Spaces: IoT Service Configuration Guide (Wireless).

Setup

Use Setup > Locations & Maps to manage location information, network maps, and digital maps in Cisco Spaces. You can import locations, upload or manage network maps, and add digital maps for supported use cases.

To manage an existing **CMX Tethering** configuration.

1. Go to **Setup > Wireless Networks**.
2. Choose **Cisco Catalyst > CMX Tethering**.
3. In the **Wireless Networks** window, locate the existing **CMX Tethering** connection and use the available options to view or manage the configuration.

.

Note **CMX Tethering** is supported only for legacy customers who already use this connection method. New customers must use the currently supported wireless network onboarding methods. **CMX Tethering** is deprecated for new deployments.

For legacy customers, use **CMX Tethering** only to manage an existing CMX-based deployment. The **Cisco Catalyst > CMX Tethering** option may not be displayed for new customers or accounts that are not enabled for this legacy workflow.

To manage an existing **CMX Tethering** configuration, click the **Menu** icon and choose **Setup > Wireless Networks**. In the **Wireless Networks** window, locate the existing **CMX Tethering** connection and use the available options to view or manage the configuration.

The **Setup** menu features are categorized into:

- **Network Connectivity:**
  - Wireless Networks
  - Wired Network
- **Location and Physical Monitoring:**
  - Locations & Maps
  - Sensors
  - Camera
- **Integrations and Management:**
  - Webex
  - pxGrid Cloud
  - Data Export
  - Plugins
  - Device Placement

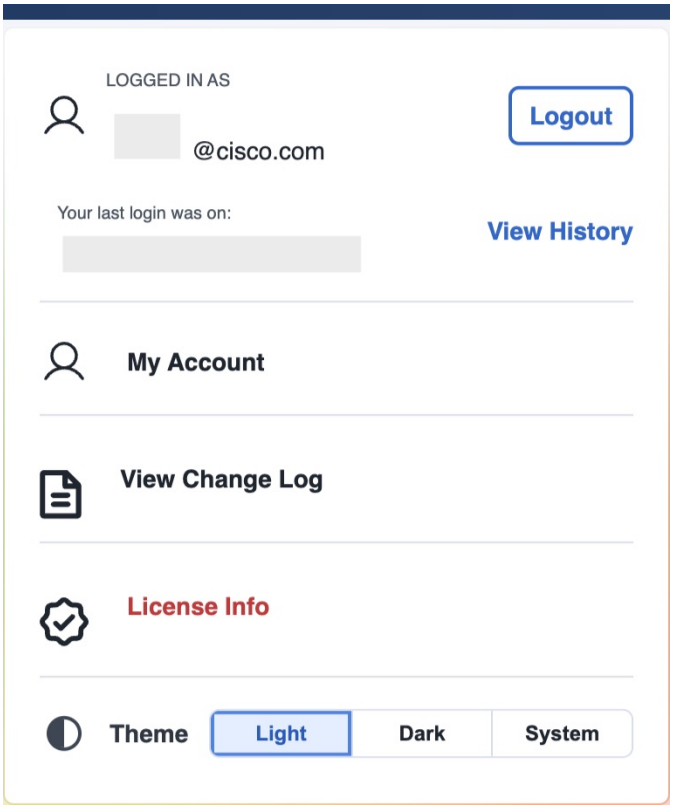
Locations & Maps

Use Locations & Maps to upload and manage location maps in Cisco Spaces. Navigate to **Setup > Locations & Maps > Network Maps**or **Digital Maps** to manage maps and configure CMX Tethering.

User Profile

The **User Profile** icon ( ) in the top-right of the Cisco Spaces dashboard lets you view account details, smart licenses and logout options.

Figure 16: User Profile



You can view the last login and timestamp details. Click **View History** to view the recent login attempts.

The **User Profile** feature includes the following options:

- **My Account**: Click to display the **My Account** window. For more information, refer to Viewing Cisco Spaces Account Details, on page 51.
- **View Change Log**: Click to open the **Change Log** tab in the **My Account** window that displays the activity details of all the users in a particular account. For more information, refer to Viewing Cisco Spaces Account Details, on page 51.
- **Activate Smart License**: Click to activate Smart License. For more information, refer to Activate Smart License, on page 52.
- **Logout**: Click to log out from Cisco Spaces.
- **License Info**: Opens license usage and Smart Software License details.
- **Theme**: Displays the **Light**, **Dark**, and **System** options. Choose a theme to change the appearance of the Cisco Spaces dashboard. The selected theme persists across sign-ins until you choose a different theme.

  The **Theme** feature (**Profile icon** > **Theme**) allows you to select the appearance of the Cisco Spaces dashboard.

Note The **Light** theme is applied by default the first time a user signs in. If the user chooses **Dark** or **System**, Cisco Spaces retains the selection after sign-out. When the user signs in again, the previously selected theme is applied.

Viewing Cisco Spaces Account Details

Use the **My Account** window to view Cisco Spaces profile details, account activity, licence information, preference, and change log details. The **My Account** window has the following tabs:

- **My Profile**: Displays the basic profile information such as first name, last name, email and mobile number.
- **Account Activity**: Displays Recent Login details in a searchable table with columns for IP Address, Date, and Browser, with pagination controls at the bottom.
- **License Info**: Displays the Cisco Spaces account information, access points limit and Smart Software License details. Click **Link your Smart Account** to activate Cisco Smart License.
- **Preferences**: This tab includes the following options:
  - **Add new domain**: Click to add a new domain for SSO authentication.
  - **Enable Support Access**: Click this option to enable or disable access to their account to the Cisco Spaces support team. Enabling this option helps the Cisco Spaces support team to detect and debug issues under exceptional situations.

Note
- By default, the **Enable Support Access** option is enabled.
- When access is enabled, the Cisco Spaces support team gets access to the customer's Cisco Spaces account.

- **Change Log**: Displays a filterable table with Activity, Time, App, Section, and User columns. Click an activity to view detailed information, including Time, Activity, App, Section, Email, Old Value, and New Value.

  The **View Change Log** feature (**Profile icon** > **My Account** > **Change Log**) helps you to track audit trail activities for the Cisco Spaces apps.

Cisco Smart License

Smart License support in Cisco Spaces allows you to view and manage the Cisco Spaces software license associated with your Cisco Smart Account. To enable Smart Licensing in Cisco Spaces, you must have a Smart Account configured in Cisco Smart Software Manager (CSSM).

In Cisco Spaces, choose **Profile icon** > **Activate Smart License** to start the activation workflow. You can also go to **Profile icon > My Account > License Info** and click **Link Your Smart Account** or **Register for Smart Licensing**, if shown.

Cisco Spaces can now display more detailed Smart License states during registration and post-registration review, including progress, completed, and unavailable statuses while the back end processes the entitlement lifecycle.

Note To enable Smart Licensing in Cisco Spaces, you must have a Cisco Smart Account configured in CSSM. For more information, refer to Smart Software Licensing.

Verify Cisco Smart License Status

The purpose of this task is to verify the Cisco Smart License Status in the Cisco Smart Software Manager (CSSM).

Use this procedure to verify the Cisco Smart License status in Cisco Smart Software Manager (CSSM).

Procedure

Step 1 Log in to CSSM.

Step 2 Identify the Smart Account and Virtual Account used for Cisco Spaces.

Step 3 In CSSM, navigate to the selected **Virtual Account** and verify that the required Cisco Spaces license SKUs are available.

Step 4 Confirm that the available SKUs match the intended Cisco Spaces base license level.

Step 5 If a downgrade or license-level change is required, contact the Cisco Spaces support team.

Activate Smart License

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, choose **Profile Icon (** **)** > **My Account > License Info**.

Step 3 In **Smart Software License** area, click **Link Your Smart Account**.

The **Terms and Conditions** window is displayed.

Step 4 Read the terms and conditions, and click **Accept Terms and Conditions**.

The **Smart Licensing Configuration** window is displayed.

Step 5 If you already have a Cisco Smart Software Manager (CSSM) account, choose **Yes, I have**. If you do not have a CSSM account, choose **No, I don't have** and complete the account-creation flow before returning to this registration process.

Step 6 Click **Next**.

Step 7 Follow the on-screen instructions to create a token in the CSSM tool.

Note Ensure that you copy the generated token to use the same in step 7.

Make sure the Product Instance Token is copied exactly as generated in CSSM. This token is used by Cisco Spaces to start Smart License registration against the selected Smart Account and Virtual Account.

Step 8 Click **Next** after you have generated the token.

Step 9 In the **Product Instance Token** field, paste the generated token.

Step 10 Click **Register** to register Cisco Spaces with your CSSM account.

A success notification message is displayed. You can view the Smart License Software registration details and license compliance information in the **Profile icon > My Account > License Info**

Note

- After the Cisco Smart License activation, contact the Cisco Spaces support team to enable the trial support. If trial mode is enabled, the smart agent will not update the license usage to Cisco Smart License Management.
- After you activate your Cisco Smart License, you can upgrade the base license level to match the licenses present in the linked Smart Account. To do this, choose **Profile Icon** > **License Info** > **Select License**. For more information, refer to Update License Information, on page 53.
- After the Cisco Smart License activation, contact the Cisco Spaces support team to downgrade the base license level.

Update License Information

Use **License info** tab to manage onboarding, renewals/extensions, or to troubleshoot activation and entitlement visibility issues.

Use the **License Info** tab in the **My Account** window to view and manage Cisco Spaces license details, Smart Software License registration, compliance status, account details, and license usage.

These licenses are available:

- **ESSENTIAL**
- **ADVANTAGE**
- **EXTEND**
- **SMART VENUES**
- **SMART OPERATIONS**
- **UNLIMITED**

- **PREMIER (W)**
- **PREMIER (CW)**

Note

- For **UNLIMITED**, **PREMIER**, and **PREMIER_CW**, floor area can increase the calculated license quantity. If floor area is not defined, device counts are converted by the configured building-unit threshold instead.
- ESSENTIAL is the base license available for Cisco Spaces. You can upgrade from ESSENTIAL to any higher-tier license.
- After a location is upgraded to a higher-tier license, it can be downgraded only up to the base license that was purchased during onboarding. If the base license for that location is ESSENTIAL, then downgrading back to ESSENTIAL is supported.
- Downgrades are allowed only down to the base license purchased during onboarding; you cannot downgrade to any license tier lower than that base license.

Procedure

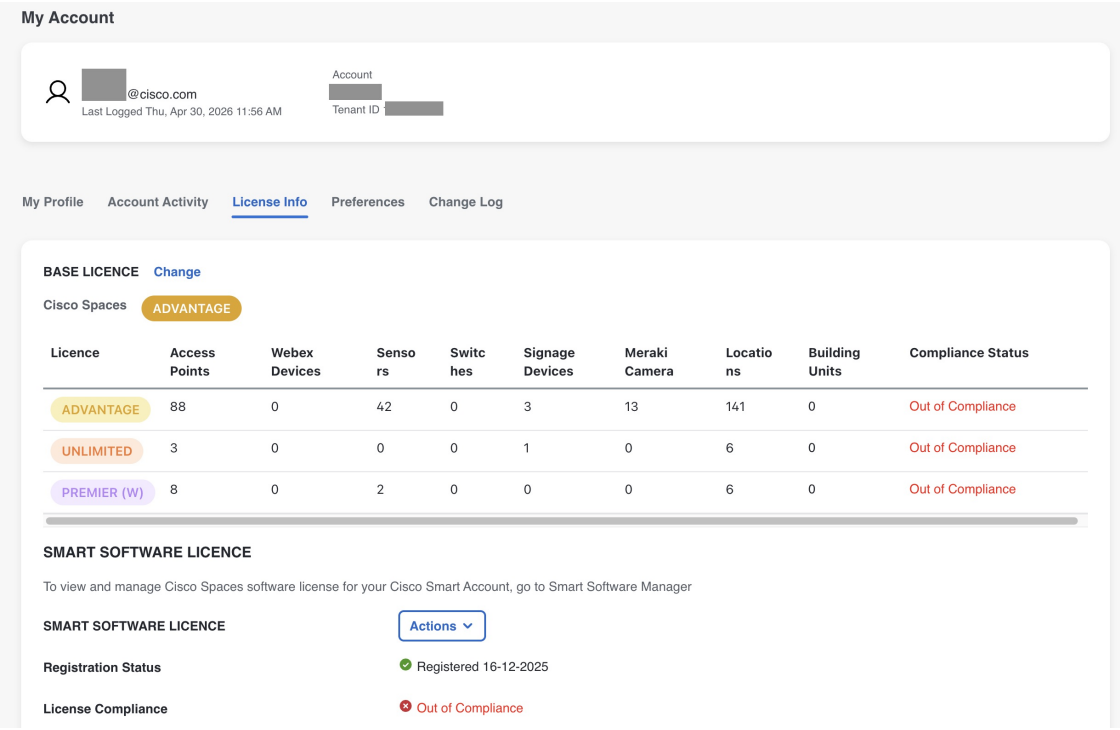
Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, choose **Profile Icon ( )** > **My Account**.

Step 3 In the **My Account** window, click the **License Info** tab.

The **LICENSE USAGE** area displays the Cisco Spaces license details and compliance status.

Figure 17: License Usage



Step 4 To upgrade or change the license for your Cisco Spaces account, click **Change**.

The **Select License** window is displayed. The current license detail is displayed in the top right of the window. The upgrade possibilities are enabled in the **Select License** window.

a) Select the plan you would like to upgrade.

A warning message is displayed with license upgrade information.

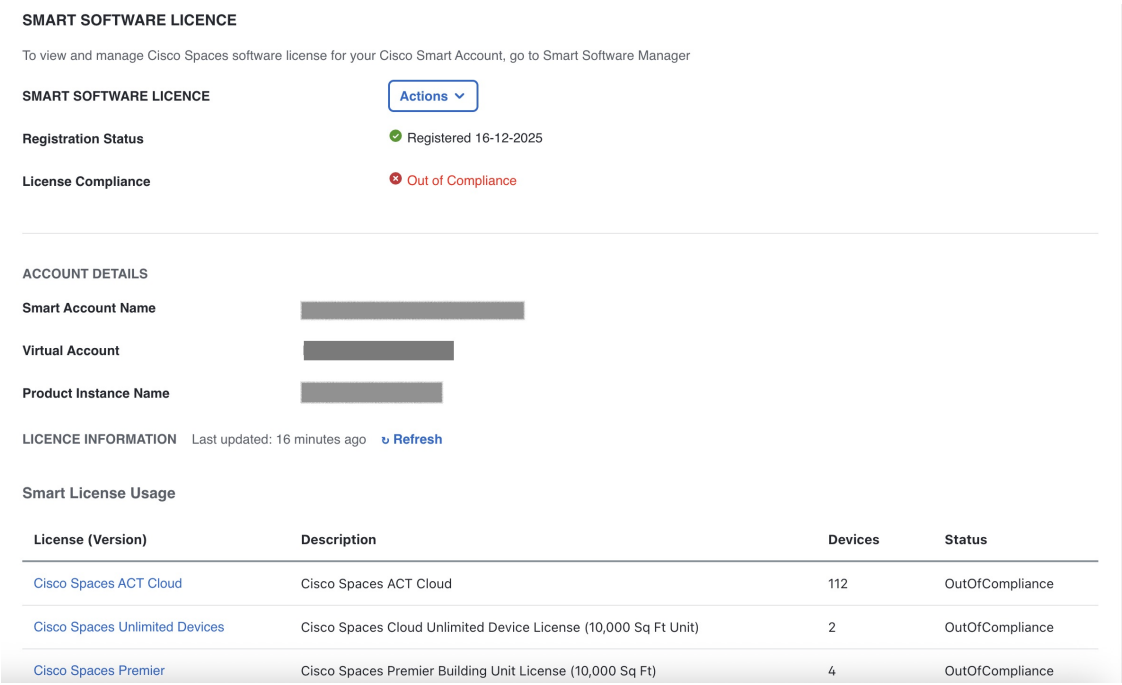
b) Check the **I accept the terms and conditions** checkbox to proceed.

c) Click **Change Plan**.

Cisco Spaces displays a success notification message. You need to log out, and then log back in to Cisco Spaces to use the new license privileges.

Step 5 In the **Smart Software License** area, the following information is displayed:

Figure 18: Smart Software License



- **Registration Status**: Displays the Cisco Spaces smart license registered status.
- **License Compliance**: Displays the Cisco Spaces smart license compliance details. The compliance statuses available are: **Init** (Initiated), **In Compliance** and **Out of Compliance**.

Note If the status indicates **Out of Compliance**, you cannot access the Cisco Spaces dashboard once the Smart Account licenses expire. However, Cisco Spaces will still allow access to the Cisco Spaces dashboard if the number of access points exceeds the license limit or the account is in an **Out of Compliance** status.

In addition to the compliance states listed above, you can also track unavailable, deregistered, failed, and retry conditions during the registration lifecycle. The **Smart Software License** window also shows **Refresh** and **Last updated** information.

Step 6 Click **Actions** drop-down list to view these options:

- **Renew Authorization**: Click to renew Cisco Spaces smart license authorization. Use **Renew Authorization** when you want Cisco Spaces to refresh the authorization view against CSSM after recent Smart Account changes.

Note

- This action is optional as renew authorization is performed automatically when Cisco Spaces communicates with CSSM. Alternatively, Smart License agent performs renew authorization automatically after every 30 days from backend.
- We recommend that you perform this action if you want to troubleshoot or renew authorization manually if status is `Out of Compliance`. You also can renew authorization manually to reflect any recent Smart Account updates in Cisco Spaces.

- **Renew Smart License**: Click to renew Cisco Spaces smart license registration. Use **Renew Smart License** when you want to renew the registration identity and certificate.

Note

- This action is optional as renew registration is performed by Cisco Spaces automatically in backend at the time of registration.
- This action renews the Registration ID and Certificate with CSSM. Cisco Spaces performs this action automatically every 6 months from backend.

- **Re-register**: Click to re-register Cisco Spaces smart license in the CSSM. Use **Re-register** only when you are ready to replace the existing registered instance.

Note

- This action forcefully re-registers Smart License and overrides any existing registered instance. This action results in reported data loss of that particular instance in Smart Account.
- We recommend that you perform this action to troubleshoot Smart License.

- **Deregister**: Click to deregister Cisco Spaces smart license from CSSM.

Note We recommend that you perform this action if Cisco Spaces is not in use and you want to deregister the instance from CSSM.

Step 7 In the **Account Details** area, the following information is displayed:

- **Smart Account Name**: Displays the Cisco Spaces smart license account name.
- **Virtual Account**: Displays the Cisco Spaces virtual account name.
- **Product Instance Name**: Displays the Cisco Spaces product instance name.

Use **Refresh** option to refresh the account details.



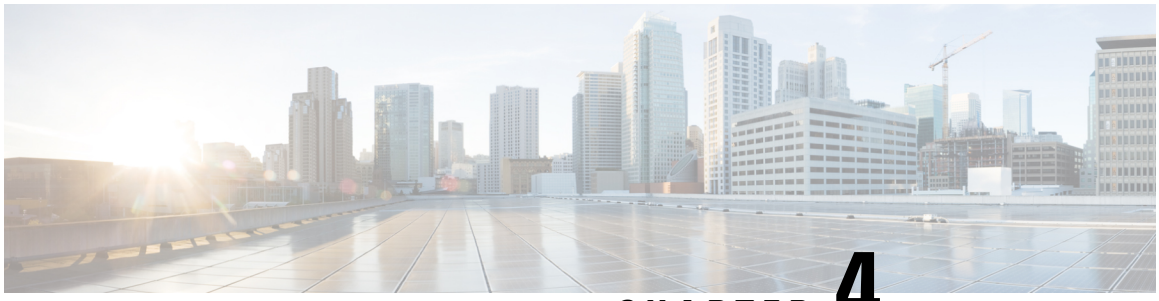
Note **Smart Account Name**, **Virtual Account**, and **Product Instance Name** remain the key account-identification fields for the linked CSSM registration.

Step 8 In the **Access Points** area, the following information is displayed:

- **Active APs**: Displays the number of active access points.

Step 9 In the **Smart License Usage** area, the following information is displayed:

- **License (Version)**: Displays the license version.
- **Description**: Displays the license description.
- **Devices**: Displays the device counts.
- **Status**: Displays the license status.



CHAPTER 4

Cisco Spaces: Apps

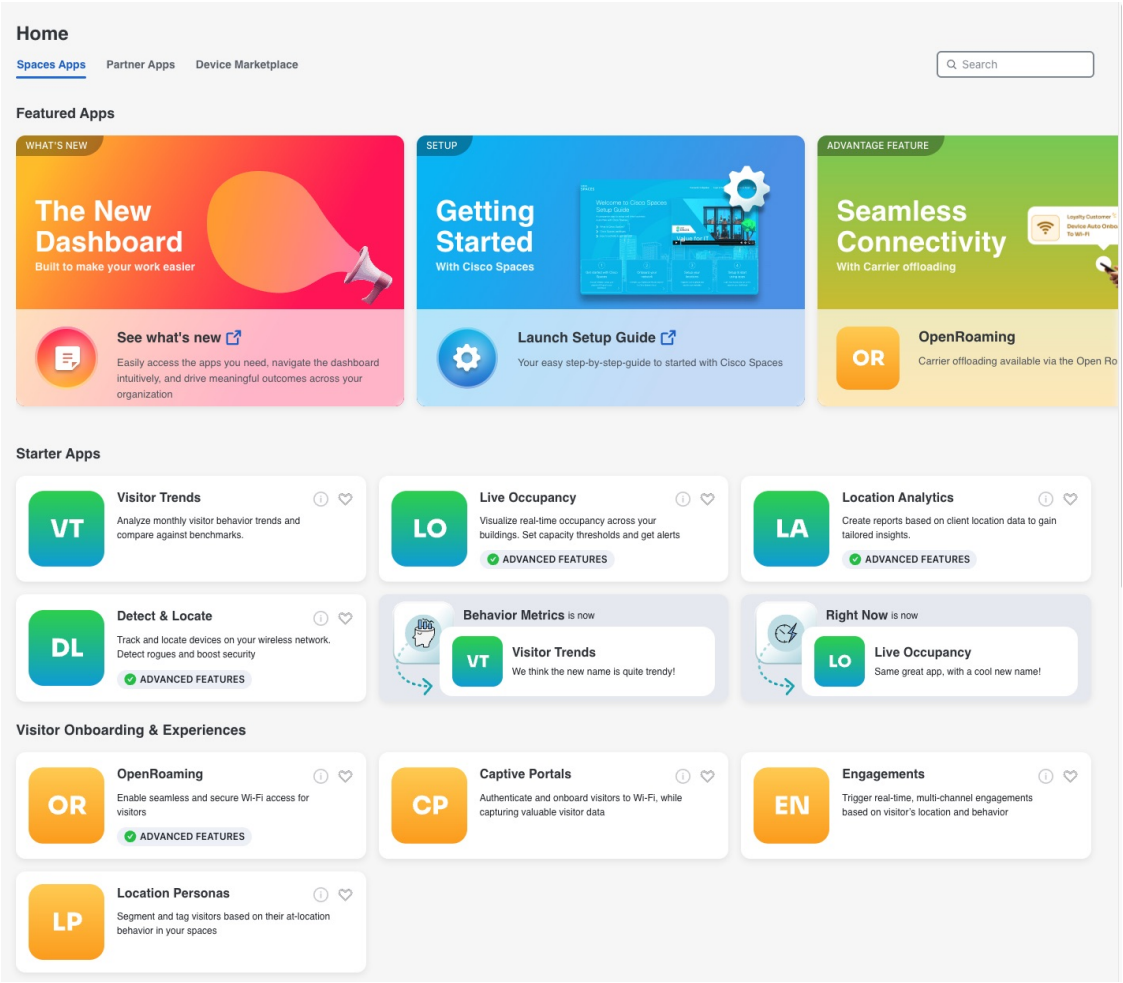
Cisco Spaces provides various use case-oriented apps. You can also add partner apps to Cisco Spaces.

- Cisco Spaces Apps, on page 59
- Apps, on page 61
- Partner Apps, on page 63
- IoT Device Marketplace Application, on page 63
- Contact sales team, on page 64

Cisco Spaces Apps

- Log in to **Cisco Spaces**.
- In the left navigation pane, click **Dashboard** to view the apps.
- On the Home page, click the **Spaces Apps** tab.
- Use the Search field to search for apps and features.
- Check the app tiles. If a tile displays a lock icon, the app cannot be accessed with the current account or license.
- Click a **featured app** card to open the overview drawer.
- In the overview drawer, click **Open App** to launch the app.

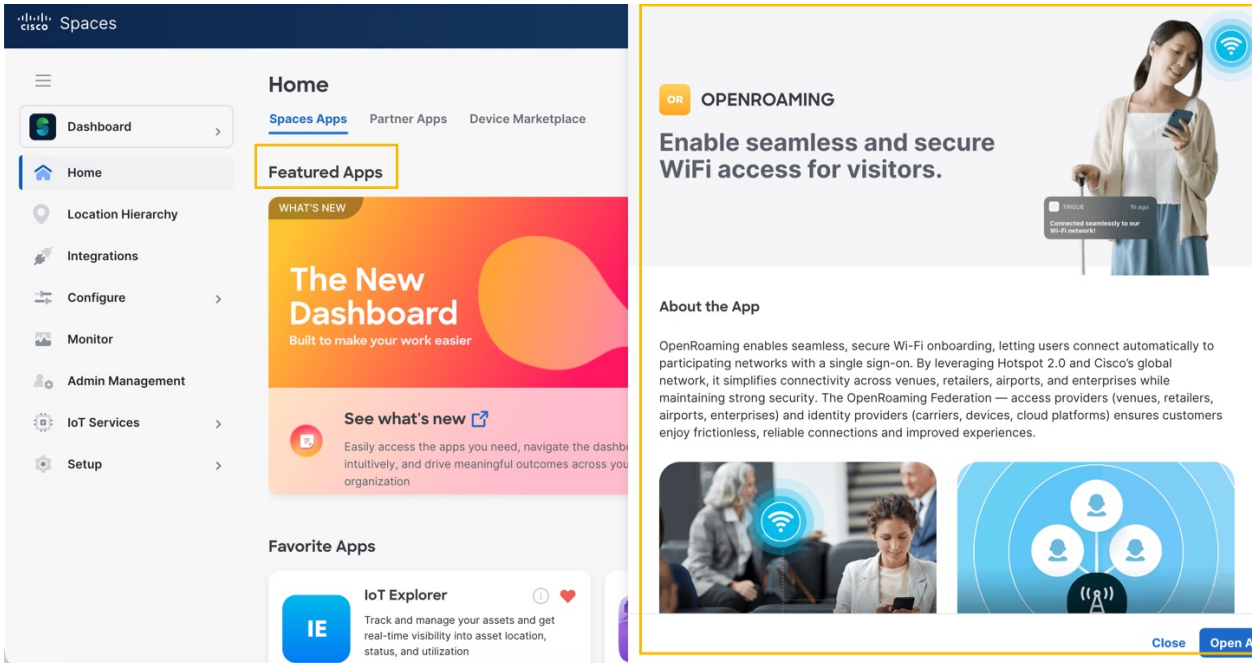
Figure 19: Spaces Apps



Note **Right Now** is now called **Live Occupancy**, and **Behavior Metrics** is renamed **Visitor Trends**.

- Log in to **Cisco Spaces**.
- In the left navigation pane, click **Dashboard**.
- On the **Home page**, click the **Spaces Apps** tab.
- In the **Featured Apps** section, click a featured app card.
- The app overview drawer opens.
- Click **Open App** to launch the app, or click **Close** to return to the **Home page**.

Figure 20: Featured App Cards



Apps

The apps available are:

- **Visitor Trends**: The **Visitor Trends** app enables you to view various reports that provide insights about the performance of your business. You can compare your business performance with the industry performance. By default, the report includes the data from the date of installation of Cisco Spaces. The report is displayed for all the locations for which you have access. You can filter to view the report for a particular location, month, or tag.
- **Live Occupancy**: The **Live Occupancy** app provides you the Right Now report that shows the details of visitors currently present at your locations. Using the **Live Occupancy** app, you can also create **Density Rules**. Use these **Density Rules** to sent notifications to the business users such as employees based on the visitor density or device count in the business locations.
- **Location Analytics**: The **Location Analytics** app enables you to view reports of visits in your locations.
- **Detect and Locate**: Cisco Spaces: **Detect and Locate** app enables you to view the current and historic location of Wi-Fi devices in your deployment. The tracked devices count is displayed on the **Detect and Locate** app tile. For more information on the **Detect and Locate** app, refer to Cisco Spaces Detect and Locate Configuration Guide.
- **OpenRoaming**: The **OpenRoaming** app enables secure, seamless, and automatic network connectivity by eliminating tedious Wi-Fi guest onboarding processes and the risk of connecting to rogue SSIDs.
- **Captive Portals**: The **Captive Portal** app enables you to create captive portals, and display them to your customers based on Captive Portals rules.
- **Engagements**: The **Engagements** app enables you to reach out to your customers individually.

- **Location Personas**: Cisco Spaces enables you to create tags by grouping the customers. You can create the tags using the **Location Personas** app. You can also use the Location Personas app to add another customers to an existing tag, or remove certain customers from an existing tag.

  For more information on creating tags, refer to Create or Modify Tags, on page 223.

- **IoT Explorer**: Cisco Spaces: **IoT Services** is a platform service within Cisco Spaces that enables you to claim, manage, and monitor IoT devices using Cisco's wireless infrastructure. IoT Services is designed to enable management of IoT devices across vendors, form factors, and technology protocols. Bluetooth Low Energy (BLE) is the first technology available for management using IoT services. For more information on **IoT Services**, refer to Cisco Spaces IoT Services Configuration Guide.

- **Space Manager**: The **Space Manager** app allows you to configure various devices, sensors, and workspaces and to provide access to real-time occupancy data and environment telemetry (heat map, indoor air quality, temperature, humidity, and noise levels) rendered on rich maps for a specific building, floor, or meeting room.

- **Space Experience**: The app **Space Experience** enables you to create and manage signage for **Cisco Smart Workspaces**, onboard new signage for a Cisco Webex device or a non-Webex device and configure the telemetry parameters and publish the signage.

- **Space Utilization**: The **Space Utilization** app offers historical insights into the usage of your physical spaces, helping in their effective optimization. These insights are derived from data collected through sensors integrated into your networking and Wi-Fi infrastructure.

  For more information, refer to Cisco Spaces: Space Utilization App Guide.

- **Environmental Analytics**: The **Environmental Analytics** app enables you to optimize the performance of buildings by leveraging indoor environment insights and metrics. These insights are derived from sensors integrated into the networking and collaboration infrastructure throughout your buildings within your network.

  For more information, refer to Cisco Spaces: Environmental Analytics App Configuration Guide.

- **Camera Metrics**: The **Camera Metrics** app enables you to view a metrics report based on the data captured using Meraki Camera. The report is displayed for a particular month.

- **Impact Analysis**: The **Impact Analysis** app is a way of measuring the effect of any action that you made based on before and after analytics.

- **Proximity Reporting**: The **Proximity Reporting** app enables you to generate Proximity Reports. The **Proximity Reporting** app helps the workplace administrators to create a safe environment for employees who are returning to work during the COVID-19 pandemic. The wireless devices of the reporting users (people to be monitored) must be associated with the wireless networks and mapped to physical locations. The Proximity Reporting app enables you to trace the movement of a person tested positive for COVID-19. The count of proximity reports created is displayed on the **Proximity Reporting** app tile. For more information on the **Proximity Reporting** app, refer to Cisco Spaces Proximity Reporting Configuration Guide.

- **Asset Locator**: The **Asset Locator** app enables you to monitor assets and optimize the performance of your assets, sensors, alerting system, and operational work flows. The app provides a range of tags and sensors to continually integrate, monitor, and manage your connected operations. Using its cloud-based interface, you can define the profile, category, and ownership of each assets. You can establish business rules to define work flows, and the expected operating range of your assets and sensors. For more information on the **Asset Locator** app, refer to Cisco Spaces Asset Locator Configuration Guide.

Captive Portals

The **Captive Portal** refers to the portal that appears for a user who accesses your Wi-Fi from a particular location with a specific Wi-Fi network ID (SSID). The customers of this captive portal are internet users who connect to the Wi-Fi from your business locations. It offers a range of customization options to improve user experience, including welcome messages, notices, promotions, apps, videos, and a help line. These features can be implemented through the use of different portal modules available in Cisco Spaces.

Captive Portal Rules

Cisco Spaces enables you to create Captive Portal Rules to display the captive portals based on various parameters. You can configure to display a captive portal based on the location, number of visits made by the customer, type of customer, app status of the customer, and so on. You can also use this rule to manage the internet provisionings for the customers, and to send customer information to an external API.

Engagements App

Cisco Spaces also functions as a Wi-Fi-based beacon that facilitates you send appropriate notification to your customers, who has a Wi-Fi enabled device, when the customer is in and around your business premises.

The **Engagements** app enables you to reach out to your customers individually with different promotions and offers. You can remind the customers about the offers available for them and their membership details. You can also set to provide offers only in certain outlets. You can configure to send the notifications using the **Engagement Rule** app. Cisco Spaces enables you to send the notification when a customer connects to a Wi-Fi.

Cisco Spaces enables you to send the notifications in the following ways:

- SMS
- E-mail
- API notifications
- Cisco Webex Teams

For more information, refer to Creating an Engagement Rule.

Partner Apps

Cisco Spaces enables you to integrate third party apps to it. The third party apps are listed as partnership apps in the Cisco Spaces dashboard.

IoT Device Marketplace Application

A new app **IOT Device Marketplace** is now available in the Cisco Spaces dashboard. This app is available only for the **ADVANTAGE** license users. For the ESSENTIAL and EXTEND accounts, the **IOT Device Marketplace** tile is shown in the disabled mode.

The **IOT Device Marketplace** app enables you to learn about devices tailored to your industry and use cases and order them.

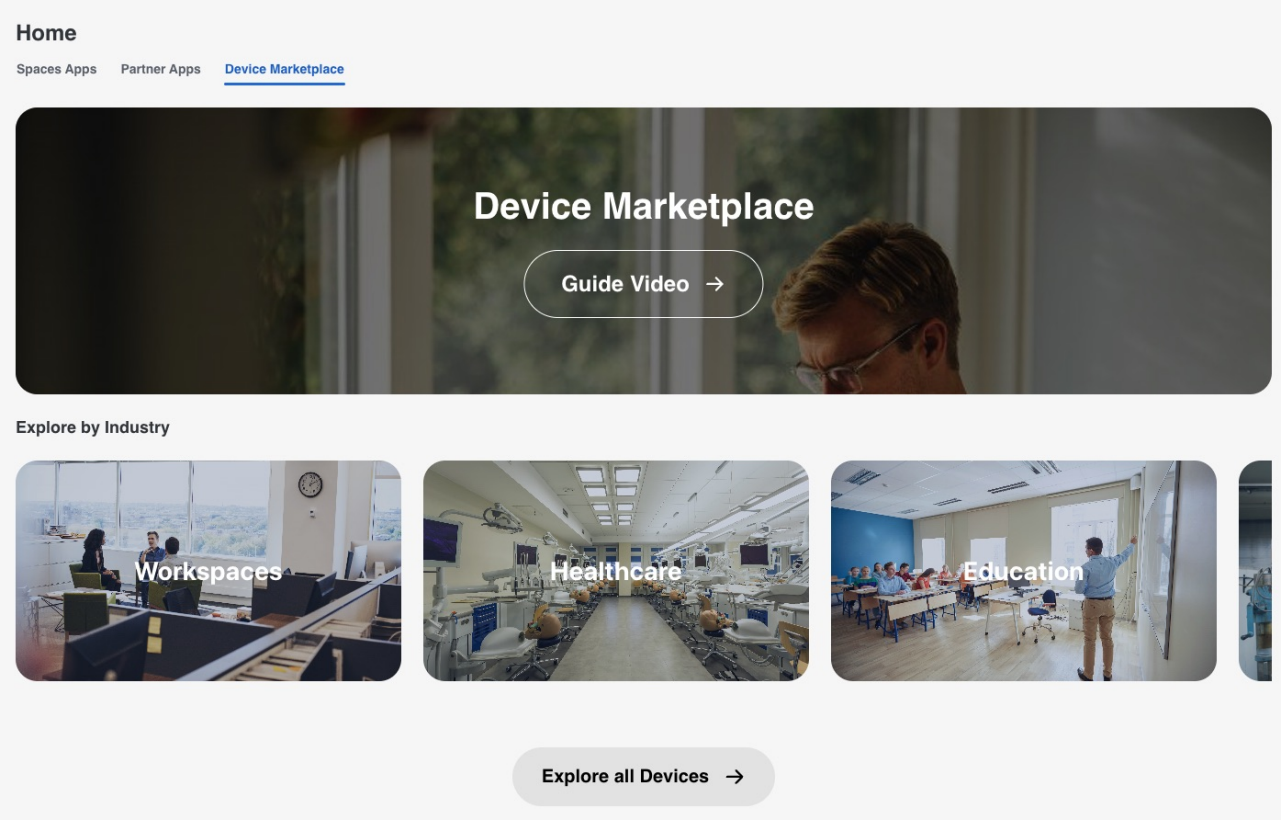
When you click the **IoT Device Marketplace** tile on the Cisco Spaces dashboard, it automatically redirects you to the IoT Device Marketplace application. Before this enhancement, you had to provide the login credentials again to log in to the **IoT Device Marketplace** application.

After you login, you can proceed further to select your industry and the usecase, and can view the IoT devices available for the selected use case. You can then view the device details and can request a quote. Once the quote request is submitted, it will be redirected to the respective vendor along with your contact details. The remaining purchase procedures will be directly between you and the vendor where there will be no involvement of Cisco Spaces.

A device marketplace is an online platform that

- lists IoT devices from Cisco and multiple third-party vendors with detailed specifications and use cases,
- enables customers to filter devices by use case, directly contact vendors, and request quotes in a streamlined workflow, and
- provides Cisco-validated devices alongside multi-vendor offerings for flexible deployment options.

Figure 21: Device Marketplace



Contact sales team

These steps provides step-by-step instrction to contact sales team to order IoT Devices.

- In the Cisco Spaces - Homepage, click the **Device Marketplace** tab.

- The **Device Marketplace** window displays the industries.
- (Optional) Select the Industries.
- Click **Explore All Industries**, select **Industries** and **Use Cases** from the dropdown menu.
- (Optional) Use the options in the **Filter By** section, to filter the **Price Range, Battery Life, Technology, Certifications, Mounting Options.**
- Click on the device that you want to buy.
- The product windows displays **Product Details, Technical Specification, Similar devices, About the Vendor.**
- In the **Contact Vendor** section fill all the mandatory details:

  Customer Name: Enter your name

  Email: Enter your e-mail address

  Purpose of Request: Select the purpose of request from the drop down menu.

  Expected Volume Needs: Enter the number

  County: Enter the country.

  Industry: Select the industry from the drop down menu.

  Company Name: Enter your company name.

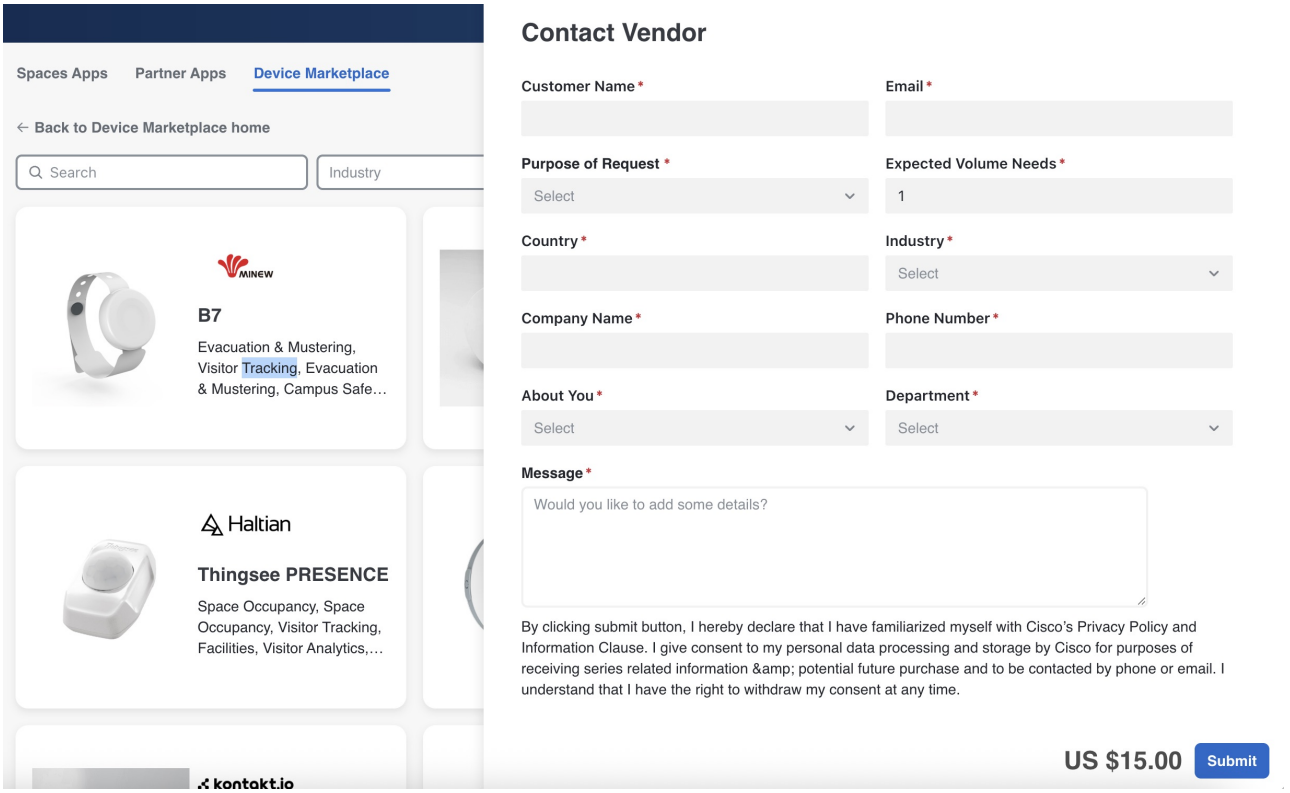
  Phone Number: Enter your phone number.

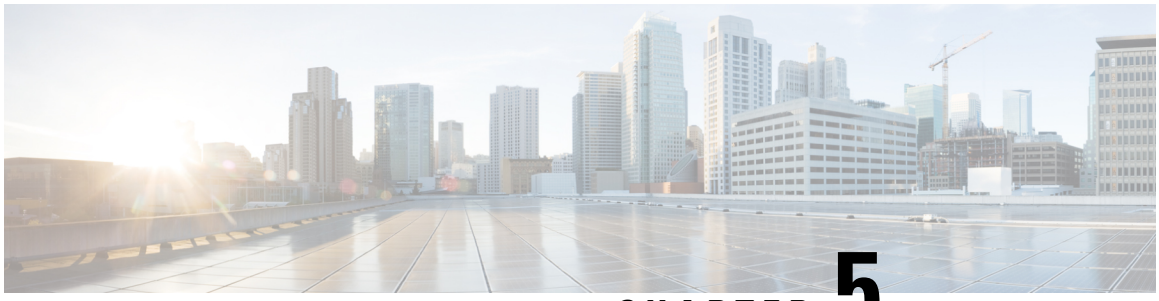
  About You: Select from the drop down menu.

  Department: Select the department from the drop down menu.

  Message: Enter the message.
- Click **Submit**.
- Respective vendor will contact you.

Figure 22: Contact Vendor





CHAPTER 5

Partner App Management

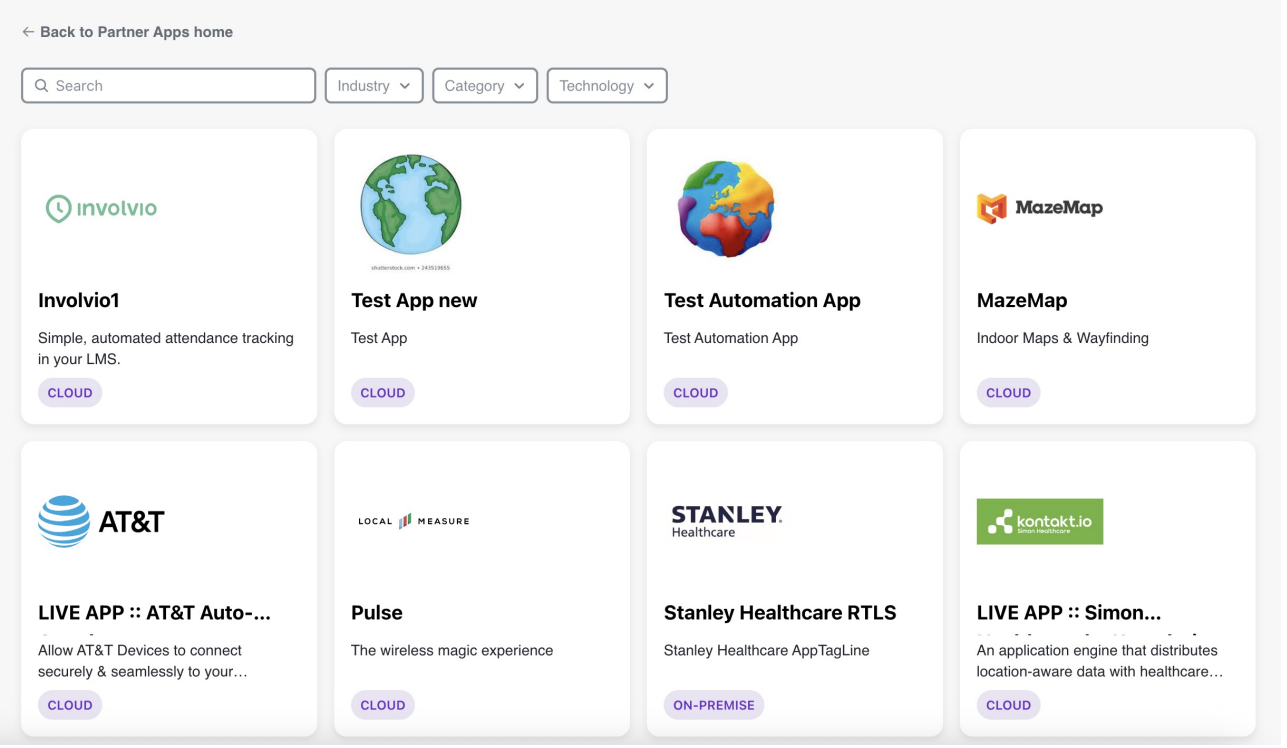
- Overview of Partner App Center, on page 67
- Activate an App, on page 69

Overview of Partner App Center

The Cisco Spaces - Partner Dashboard offers Cisco Spaces partners, a single location to view, update, add, and test their application. Cisco Spaces is seamlessly integrated with the Cisco Spaces - Partner App Center. As a partner, you can access location data that the access points collect and use this data to extend your business apps. Log in to the Cisco Spaces - Partner Dashboard to create and integrate your applications.

Note This feature is available from Cisco Spaces Extend licenses.

Figure 23: App Center



The combination of the Cisco Spaces platform plus the Partner-led ecosystem provides the ability to work with third-party application developers, to build customized applications for individual businesses and customers, by leveraging the power of Cisco Spaces and the Cisco Spaces - Partner Firehose API.

Application developers use the Partner APIs, also called the Cisco Spaces - Partner Firehose API to create and publish their Apps. The Partner ecosystem allows independent software vendors to enable vertical-relevant, pre-validated, and tested location-based solution applications and to publish their live applications on the Cisco Spaces - Partner App Center. As a registered partner, you can access the Cisco Spaces - Partner App Center.

Your customers can view and activate the applications from the Cisco Spaces - Partner App Center. For example, your customer can click on any available App from the Cisco Spaces - Partner App Center and choose to activate the App for their business use cases. After the app is approved and made live in the Cisco Spaces - Partner App Center, it is available for all the customers of Cisco Spaces for activation. When a customer activates the app, the customer's data starts flowing to your app as events over the Cisco Spaces - Partner Firehose API.

For more information about Partner App Management, refer to Overview of the Cisco Spaces - Partner Ecosystem online help.

Partner Firehose event data and filter scope

For Cisco Meraki-connected customers, `IOT_TELEMETRY` events can include PM2.5 mass-concentration data when it is available from the source device.

Device-level Firehose events can also include `occupancyAnalytics` metadata for devices evaluated against Live Occupancy exclusion filters. The metadata indicates whether Cisco Spaces evaluated the device as `INCLUDE` or `EXCLUDE`. This behavior applies to the these events:

- DEVICE_LOCATION_UPDATE
- DEVICE_PRESENCE
- DEVICE_ENTRY
- DEVICE_EXIT
- DEVICE_ASSOCIATION

Firehose filter APIs support independent event-type scope for MAC, MAC OUI, iBeacon, and Eddystone filters through these optional fields:

- macFilterEventTypes
- macOuiFilterEventTypes
- iBeaconFilterEventTypes
- eddystoneFilterEventTypes

If a field is omitted or contains an empty list, Cisco Spaces retains the default event scope. GET returns the effective event-type scope for each filter. DELETE clears the configured filters and resets the event-type scopes to their default behavior.

Activate an App

Cisco Spaces partners uses Partner Dashboard to create and publish apps. After app creation and publishing, those customer apps are listed in Cisco Spaces - Partner Dashboard. Cisco Spaces the administrator must approve the new applications and once the app is approved it is listed under **Partner Apps** tab in Cisco Spaces - Homepage.

You must activate the app from **Partner Apps** so that your customers can use them. These apps can be activated for selected locations as per the customer requirement. App includes multiple events and partner enable the events for these apps and activate them.

Events are triggered through Firehouse APIs. These APIs checks for the device status and then events are triggered accordingly. For more information, refer to Firehose API.

When a Cisco Spaces partner adds a new event to an already activated app, it will be sent through Firehose APIs only when the customer subscribes to the new event by accepting the permissions. Prior to this enhancement, customer permission was not required for new events.

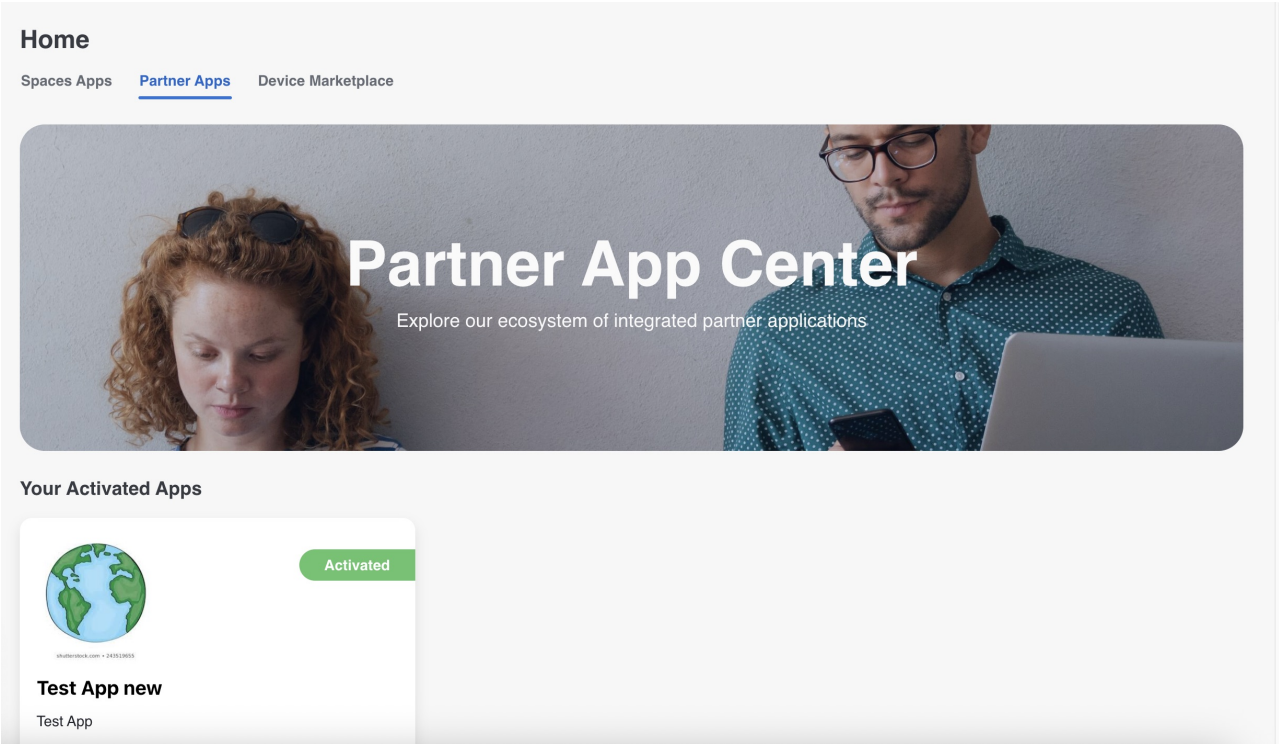
You are prompted with the following notification message `New Permission Required` on the app tile and you must click and accept the new app permission to subscribe to these new app events. An email notification is also sent to the customer indicating that a new event is added to the app.

Procedure

Step 1 In the Cisco Spaces - Homepage, click the **Partner Apps** tab.

The Partner Apps window displays the published apps. The app title displays the name of the application, a brief description and whether the app is hosted on **Cloud** or **On-prem**.

Figure 24: App Center



Step 2 (Optional) Use the options in the **Filter By** section, to filter the applications.

Step 3 Click on the app that you want to activate.

Step 4 Click **Activate**.

The corresponding app activation window is displayed. Each application will have different activation instructions as per the customer authentication configuration.

Step 5 Complete the **Sign Up & Onboarding** configurations.

Step 6 Click **Continue**.

Step 7 In the **Permissions** section, read location data requirements.

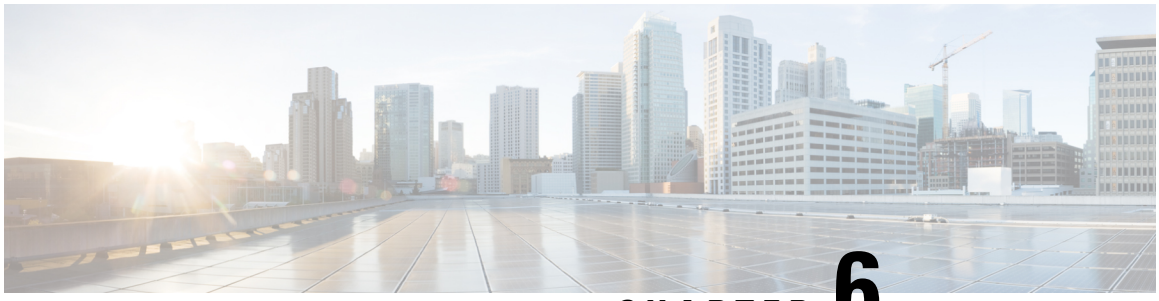
Step 8 Click **Accept Permission**.

Step 9 Choose the locations you would like to activate the app for. You can select **Enable for all locations** checkbox to select all location.

Step 10 Click **Next**.

The specific customer website displays and you must complete the required customer authentication to proceed.

Step 11 Follow the on-screen instructions and complete the app activation steps.



CHAPTER 6

Configuring Cisco Wireless Controllers and Cisco Catalyst 9800 Series Controllers for Cisco Spaces

This chapter describes the configurations to be done in the CiscoWireless Controller (Cisco AireOS) or Cisco Catalyst 9800 Series Controllers to work with Cisco Spaces. The configurations required differ based on the wireless controller type and connector you use.

Note

- You cannot connect a Cisco Wireless Controller with hyper location with Cisco Spaces and Cisco CMX simultaneously.
- If you want to connect a Cisco Wireless Controller with both Cisco CMX and Cisco Spaces simultaneously, you must use a Cisco Spaces: Connector. Check the limitations for the number of NMSP connections your Cisco Wireless Controller can support, and ensure that your Cisco Wireless Controller can support the addition of a new connection to Cisco Spaces: Connector, especially if there are existing connections to multiple Cisco CMX servers.
- You cannot use a Cisco Wireless Controller simultaneously with Cisco WLC Direct Connect and Cisco Spaces: Connector. Disable the Cisco WLC Direct Connect before using the Cisco Spaces: Connector.
- It is recommended to use Cisco Spaces: Connector rather than Cisco WLC Direct Connect, especially when you are using a lower version of Cisco Wireless Controller.Also, certain apps such as Operation Insights, Detect and Locate, and so on are supported only by Cisco Spaces: Connector.
- It is not recommended to compare the data displayed in your wireless network with the data shown in Cisco Spaces reports as it is expected to defer as per the design.

Note The configurations are done in the external applications that are not a part of Cisco Spaces, and the menu path and names specified for the tabs, windows, options, and so on in this documentation are subject to change.

The features supported by various connector types, and the configurations for various combinations of wireless controllers and connectors are as follows:

- Features Supported by Various Connectors, on page 72
- Connecting Cisco Spaces to Cisco Wireless Controller through Cisco CMX, on page 74

- Connecting Cisco Catalyst 9800 Series Wireless Controller or Cisco Wireless Controller to Cisco Spaces Using WLC Direct Connect or Cisco Spaces: Connector, on page 89
- Cisco Spaces Scale Benchmark, on page 121

Features Supported by Various Connectors

The following table lists the features supported by each type of connector. You can opt the connector based on the feature or app that you want to use. Cisco Spaces: Connector is recommended if you want to use the apps such as Operational Insights and Open Roaming.

Table 9: Connectors-Feature Support

Features/Apps	Cisco Spaces Connector	Cisco WLC Direct Connect (Recommended only for small scale deployments)[1] Cisco Wireless Controller Cisco Catalyst 9800 Controller	CMX Tethering Connector	Wired Devices	Cisco Meraki
Cisco Spaces Dashboard	Supported	Supported	Supported	Not Supported	Supported
Captive Portals	Supported	Supported	Supported	Not Supported	Supported
Engagements	Supported	Supported	Supported	Not Supported	Supported
Location Personas	Supported	Supported	Supported	Not Supported	Supported
Location Analytics	Supported	Supported	Supported	Not Supported	Supported
Impact Analysis	Supported	Supported	Supported	Not Supported	Supported
Camera Metrics	Not Supported	Not Supported	Not Supported	Not Supported	Supported
Behavior Metrics	Supported	Supported	Supported	Not Supported	Supported
Live Occupancy WiFi	Supported	Supported	Supported	Supported	Supported

Features/Apps	Cisco Spaces Connector	Cisco WLC Direct Connect (Recommended only for small scale deployments)[1] Cisco Wireless Controller Cisco Catalyst 9800 Controller	CMX Tethering Connector	Wired Devices	Cisco Meraki
Live Occupancy Video	Not Supported	Not Supported	Not Supported	Not Supported	Supported
Open Roaming[2]	Supported	Not Supported	Not Supported	Not Supported	Supported
IoT Services	Supported[3]	Not Supported	Not Supported	Supported	—
Detect and Locate	Supported	Limited Support (Associated Clients only)	Supported	Not Supported	—
Hyperlocation	Supported	Not Supported	Supported	Not Supported	Not Supported
Fastlocate	Supported	Not Supported	Supported	Not Supported	Not Supported
Scale Support For more details, see the scale summary in Cisco Spaces Scale Benchmark, on page 121.	Best suited for scaling	Scale supported for AireOS Controller 8.8 MR2 and Cisco Catalyst 9800 Series 16.12.1.	Supports the scale that Cisco CMX can handle.	Not Supported	Best suited for scaling
AireOS Controller Platform Support	Supported	Supported	Supported	Not Supported	Not applicable
Cisco Catalyst 9800 Platform Support	Supported	Supported	Supported	Not Supported	Not applicable

1 Connecting through the Cisco Wireless Controller Direct Connection method is only recommended for small scale deployments. All large scale production deployment require a Cisco Spaces: Connector.
2 As the **Open Roaming** app is in Beta, currently documentation is not available for this app. For any information related to **Open Roaming**, contact the Cisco Spaces support team.
3 Currently, support for IoT services is only available for Cisco Catalyst 9800 Controller.

Note

- Connecting through the Cisco Wireless Controller Direct Connection method is only recommended for small-scale deployments. All large-scale production deployments require a Cisco Spaces: Connector.
- For more information about **Cisco Spaces:OpenRoaming**, refer to Cisco Spaces: OpenRoaming Configuration Guide.

Location Service compatibility

Location Service 3.2.3.33 supports the UWN TDOA TDL for Cisco Catalyst 9800 Series Wireless Controllers running version 17.18.2.

Location Service 3.2.4.42 supports TLS 1.3 for Location NMSP connections to Cisco Catalyst controllers running Cisco IOS XE 26.x.

Application compatibility for IoT Services

Cisco Catalyst 9800 Series Wireless Controllers running Cisco IOS XE 26.1.x or later require the 64-bit IOx Application version 1.8.x for Cisco Spaces IoT Services. IOx Application version 1.7.x is not supported on these controller releases and does not function.

IOx Application 1.8.x also improves stream-configuration status and payload-identification messages, supports an exclusion list of MAC-address prefixes for BLE scanning, buffers Cisco Spaces requests through a priority queue during high load, supports additional UWB tags, and includes Kontakt firmware upgrade and configuration fixes.

Connecting Cisco Spaces to Cisco Wireless Controller through Cisco CMX

To connect Cisco Spaces with Cisco Wireless Controllers through Cisco CMX, you must have Cisco CMX 10.6 or later.

For Cisco Unified Wireless Network with Cisco CMX, the following configurations are required to work with Cisco Spaces:

Note

- The configuration for internet provisioning and RADIUS authentication is required only if you need RADIUS authentication. This configuration is required only if you need social authentication for your portals.

Configuring Access Point Mode, SSIDs, ACLs, Splash URLs, and Virtual Interface in the WLC

To create a Captive Portal rule, you must initially define the mode for access points, and create the SSIDs and ACLs in the Cisco Wireless Controller. You must also ensure that the splash URL for the SSID is configured in the Cisco Wireless Controller.

Note The SSIDs and ACLs are created in the Cisco Wireless Controller and not in the Cisco CMX.

The Cisco Wireless Controller configurations for the local and flexconnect modes are different.

Note The configurations are done in the Cisco Wireless Controller that is not a part of Cisco Spaces, and the menu path and names specified for the tabs, windows, options, and so on in this documentation are subject to change.

Local Mode Configurations for Using Cisco Spaces

To configure the Cisco Wireless Controller to use with Cisco Spaces in the local mode, perform the following steps:

Configure the Local Mode for an Access Point

To configure a local mode for an access point, perform the following steps:

Procedure

Step 1 Log in to the Cisco Wireless Controller with your Wireless Controller credentials.

Step 2 In the Cisco Wireless Controller main window, click the **Wireless** tab.

All of the access points are listed.

Step 3 Click the access point for which you want to configure the mode to local.

Step 4 Click the **General** tab.

Step 5 From the **AP Mode** drop-down list, choose **Local**, and click **Apply**.

Create SSIDs in Cisco Wireless Controller

Note The SSIDs are created in the Cisco Wireless Controller, not in the Cisco CMX.

To create the SSIDs in the Cisco Wireless Controller, perform the following steps:

Procedure

Step 1 In the Cisco Wireless Controller main window, click the **WLANs** tab.

Step 2 To create a WLAN, choose **Create New** from the drop-down list at the right side of the window, and click **Go**.

Step 3 In the **New** window that appears, enter the WLAN details like Type, Profile Name, SSID, and so on.

Step 4 Click **Apply**.

The **Edit <SSID Name>** window appears.

Step 5 Add the SSID to the Cisco Spaces dashboard.

Step 6 In the Cisco Wireless Controller main window, on the **General** tab, uncheck the **Broadcast SSID** check box.

Note The SSID Broadcasting is interrupted to avoid any customer accessing the SSID before completing the configurations.

Step 7 Choose **Security** > **Layer 2**, and check the **MAC Filtering** check box.

Step 8 In the **Layer 3** tab, do the following configurations:

a) From the **Layer 3 security** drop-down list, choose **Web Policy**.

Note **Web Policy** is the Layer 3 security option that enables you to configure captive portal in the Cisco Wireless Controller.

b) Choose the **On Mac Filter Failure** radio button.

c) In the **Preauthentication ACL** area, from the **IPv4** drop-down list, choose the ACL previously defined.

d) Check the **Enable** check box for the Sleeping Client.

Note Enabling sleeping client is not mandatory. But if enabled, the customer who is in sleeping mode after authentication gets connected without authentication if is waken up within the specified time. The clients with guest access that had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which the sleeping clients are to be remembered for before re-authentication becomes necessary. The valid range is 1 hour to 720 hours (30 days), with the default being 12 hours. Ideally, this should be similar to session timeout.

e) Check the **Enable** check box for the Override Global Config.

Note Enabling **Override global config** allows you to redirect the customer to the Cisco Spaces URL, which is an external URL.

f) From the **Web Auth Type** drop-down list, choose **External (Redirect to External Server)**.

Note The **Web Auth Type** must be **External** as the Cisco Spaces page is hosted in the external server, and not in the controller.

g) In the **URL** field that appears, enter the Cisco Spaces splash URL.

To view the splash URL for your CUWN or AireOS account, in the Cisco Spaces dashboard, the **Configure Manually** link for a AireOS SSID in the **SSIDs** window. The Configure Manually link appears only after adding a Cisco AireOS SSID.

Note You must configure the splash page for the customer to be redirected to the Cisco Spaces web page during on-boarding.

h) Click **Apply**.

Step 9 Click the **Advanced** tab.

Step 10 In the **Enable Session Timeout** field, enter the required session timeout value in seconds. For example, for session timeout of 30 minutes, enter 1800.

Step 11 Click **Apply**.

Step 12 In the **General** tab, check the **Enabled** check box for the **Status** and **Broadcast SSID** options, to enable the SSID.

Step 13 Execute the following command in the command prompt to disable captive bypassing. Then, restart the Cisco Wireless Controller.

config network web-auth captive-bypass disable Management > HTTP-HTTPS

Note If captive bypassing is enabled, the CNA will not pop up for iOS devices.

Step 14 In the **HTTP-HTTPS configuration** window that appears, do the following:

a) From the **HTTP Access** drop-down list, choose **Disabled**.
b) From the **HTTPS Access** drop-down list, choose **Enabled**.
c) From the **WebAuth SecureWeb** drop-down list, choose **Disabled**.
d) Click **Apply**.

Step 15 Choose **Security** > **Web Auth** > **Web Login Page**, and ensure that the Redirect URL after login field is blank.

Note The redirect URL field must be blank so that it won't override the Cisco Spaces splash URL configured in **Layer 3**.

What to do next



Note If you have made any changes to the **Management** tab, then restart your Cisco Wireless Controller for the changes to take effect.

Create Access Control Lists

To restrict the Internet access for customers, and to allow access only to Cisco Spaces splash page URL when connected to the SSID, the Cisco Spaces IPs (wall garden ranges) must be configured in the ACL. Now when a customer connects to the SSID, the splash page appears for the customer.

If ACL is not configured with all the required IPs, the system considers the Cisco Spaces as an external URL, and results into multiple redirection for customer.

To create the access control list, perform the following steps:

Procedure

Step 1 Log in to the Cisco Wireless Controller with your Wireless Controller credentials.

Step 2 Choose **Security** > **Access Control Lists** > **Access Control Lists**.

Step 3 To add an ACL, click **New**.

Step 4 In the **New** window that appears, enter the following:.

a) In the **Access Control List Name** field, enter a name for the new ACL.



Note You can enter up to 32 alphanumeric characters.

b) Choose the ACL type as **IPv4**.

c) Click **Apply**.

Step 5 When the **Access Control Lists** window reappears, click the name of the new ACL.

Step 6 In the **Edit** window that appears, click **Add New Rule**.

The **Rules** > **New** window appears.

Step 7 Configure a rule for this ACL with the required wall garden ranges.

To view the wall garden ranges, in the **Cisco Spaces** dashboard, click the **Configure Manually** link for a Cisco Unified Wireless Network SSID in the **SSIDs** window. The wall garden ranges are listed under the caption **Creating the Access Control List**. The **Configure Manually** link appears only after adding a Cisco AireOS SSID.

When defining the ACL rule, ensure to configure the values as follows:

- **Direction**: Any
- **Protocol**: Any
- **Source Port Range**: 0-65535
- **Destination Port Range**: 0-65535

- **DSCP**: Any
- **Action**: Permit

Step 8 If you want to provide social authentication for your portal, you must also configure the wall garden ranges for social authentication.



Note The wall garden ranges configured for social authentication allows the customers to access all the HTTPS web sites directly after connecting to your SSID, without using the captive portal.

Configure the Virtual Interface

To configure the virtual interface, perform the following steps:

Procedure

Step 1 Choose **Controller** > **Interfaces**.

Step 2 Click the **Virtual** link.

Step 3 In the **Interfaces** > **Edit** window that appears, enter the following parameters:

a) In the **IP address** field, enter the unassigned and unused gateway IP address, if any.

b) In the **DNS Host Name** field, enter the DNS Host Name, if any.



Note Ideally this field must be blank.



Note To ensure connectivity and web authentication, the DNS server must always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then you must configure the same DNS host name on the DNS servers used by the client.

c) Click **Apply**.



Note If you have made any changes to the virtual interface, restart your Cisco Wireless Controller for the changes to take effect.

FlexConnect Mode Configurations for Using Cisco Spaces

You can configure FlexConnect for central switch or local switch mode.

FlexConnect Central Switch Mode

To configure the Cisco Wireless Controller to use the Cisco Spaces in the FlexConnect central switch mode, perform the following steps:

Configure the FlexConnect Mode for an Access Point

This configuration is applicable for FlexConnect central switch and local switch mode. To configure a FlexConnect Central switch mode for an access point, perform the following steps:

Procedure

Step 1 In the Cisco Wireless Controller main window, click the **Wireless** tab.

All of the access points are listed.

Note For more details on the access points, see the Cisco Wireless Controller user guide.

Step 2 Click the access point for which you want to configure the mode to FlexConnect.

Step 3 Click the **General** tab.

Step 4 From the **AP Mode** drop-down list, choose **FlexConnect**.

Step 5 Click **Apply** to commit your changes and to cause the access point to reboot.

Create SSIDs in the Cisco Wireless Controller for FlexConnect Central Switch Mode

Create the SSID using the same steps as outlined for the local mode. For more information, refer to the Create SSIDs in Cisco Wireless Controller , on page 75.

Create Access Control Lists for FlexConnect Central Switch Mode

Create the Access Control List using the same steps as outlined for the local mode. For more information, refer to the Create Access Control Lists, on page 78.

Configure the Virtual Interface

To configure the virtual interface, perform the following steps:

Procedure

Step 1 Choose **Controller** > **Interfaces**.

Step 2 Click the **Virtual** link.

Step 3 In the **Interfaces** > **Edit** window that appears, enter the following parameters:

a) In the **IP address** field, enter the unassigned and unused gateway IP address, if any.
b) In the **DNS Host Name** field, enter the DNS Host Name, if any.



Note Ideally this field must be blank.



Note To ensure connectivity and web authentication, the DNS server must always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then you must configure the same DNS host name on the DNS servers used by the client.

c) Click **Apply**.



Note If you have made any changes to the virtual interface, restart your Cisco Wireless Controller for the changes to take effect.

FlexConnect Local Switch Mode

To configure the Cisco Wireless Controller to use the Cisco Spaces in the FlexConnect local switch mode, perform the following steps:

- Configure the FlexConnect Mode for an Access Point, on page 80

Configure the FlexConnect Mode for an Access Point

This configuration is applicable for FlexConnect central switch and local switch mode. To configure a FlexConnect Central switch mode for an access point, perform the following steps:

Procedure

Step 1 In the Cisco Wireless Controller main window, click the **Wireless** tab.

All of the access points are listed.



Note For more details on the access points, see the Cisco Wireless Controller user guide.

Step 2 Click the access point for which you want to configure the mode to FlexConnect.

Step 3 Click the **General** tab.

Step 4 From the **AP Mode** drop-down list, choose **FlexConnect**.

Step 5 Click **Apply** to commit your changes and to cause the access point to reboot.

Create SSIDs in the Cisco Wireless Controller for the FlexConnect Local Switch Mode

Note The SSIDs are created in the Cisco Wireless Controller, not in the Cisco CMX.

To create the SSIDs in the CUWN for the FlexConnect local switch mode, perform the following steps:

Procedure

Step 1 In the Cisco Wireless Controller main window, click the **WLANs** tab.

Step 2 To create a WLAN, choose **Create New**from the drop-down list at the right side of the window, and click **Go**.

Step 3 In the **New** window that appears, enter the WLAN details such as, Type, Profile Name, SSID, and so on.

Step 4 Click **Apply**.

The **Edit <SSID Name>** window appears.

Step 5 Add the SSID to the Cisco Spaces dashboard.

Step 6 In the Cisco Wireless Controller main window, on the **General** tab, uncheck the **Broadcast SSID** check box.

Note The SSID Broadcasting is interrupted to avoid any customer accessing the SSID before completing the configurations.

Step 7 Choose **Security** > **Layer 2**, and check the **MAC Filtering** check box.

Step 8 In the **Layer 3** tab, do the following configurations:

a) From the Layer 3 security drop-down list, choose **Web Policy**.

Note **Web Policy** is the **Layer 3** security option that enables you to configure captive portal in the Cisco Wireless Controller.

b) Choose the **On Mac Filter Failure** radio button.

c) In the **Preauthentication AC**L area, from the **WebAuth FlexAC**L drop-down list, choose the ACL previously defined.

d) Check the **Enable** check box for Sleeping Client.

Note Enabling sleeping client is not mandatory. But if enabled, the customer who is in sleeping mode after authentication gets connected without authentication if is waken up within the specified time. The clients with guest access that had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login window. You can configure the duration for which the sleeping clients are to be remembered for before re-authentication becomes necessary. The valid range is 1 hour to 720 hours (30 days), with the default being 12 hours. Ideally, this should be similar to session timeout.

e) Check the **Enable** check box for Override Global Config.

Note Enabling **Override Global Config** enables you to redirect the customer to the Cisco Spaces URL, which is an external URL.

f) From the **Web Auth Type** drop-down list, choose **External**.

Note The **Web Auth Type** must be **External** as the Cisco Spaces page is hosted in the external server, and not in the controller.

g) In the URL field that appears, enter the Cisco Spaces Splash URL.

To view the splash URL for your CUWN account, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in the **SSIDs** window. The **Configure Manually** link appears only after adding a Cisco AireOS SSID.

Note You must configure the splash page for the customer to be redirected to the Cisco Spaces web page during on-boarding.

h) Click **Apply**.

Step 9 Click the **Advanced** tab.

Step 10 In the **Enable Session Timeout** field, enter the required session timeout value in seconds. For example, for session timeout of 30 minutes, enter 1800.

Step 11 In the **FlexConnect** area, check the **Enabled** check box for FlexConnect Local Switching, and click **Apply**.

Step 12 In the **General** tab, select the **Enabled** check box for the Status and Broadcast SSID options, to enable the SSID.

Step 13 Execute the following command in the command prompt to disable captive bypassing. Then, restart the Cisco Wireless Controller.

config network web-auth captive-bypass disable

Note If captive bypassing is enabled, the CNA will not pop up for iOS devices.

Step 14 Choose **Management** > **HTTP-HTTPS**.

Step 15 In the **HTTP-HTTPS Configuration** window that appears, perform the following:

a) From the **HTTP Access** drop-down list, choose **Disabled**.
b) From the **HTTPS Access** drop-down list, choose **Enabled**.
c) From the **WebAuth SecureWeb** drop-down list, choose **Disabled**.
d) Click **Apply**.

Step 16 Choose **Security** > **Web Auth** > **Web Login Page**, and ensure that the **Redirect URL after login** field is blank.

Note The redirect URL field must be blank so that it will not override the Cisco Spaces splash URL configured in Layer 3.

Create Access Control Lists for FlexConnect Local Switch Mode

To restrict the Internet access for customers, and to allow access only to Cisco Spaces splash page URL when connected to the SSID, the Cisco Spaces IPs (wall garden ranges) must be configured in the ACL. Now when a customer connects to the SSID, the splash page appears for the customer.

If ACL is not configured with all the required IPs, the system considers the Cisco Spaces as an external URL, and results into multiple redirection for customer.

To create the access control list for the FlexConnect local switch mode, perform the following steps:

Procedure

Step 1 Log in to the Cisco Wireless Controller with your Wireless Controller credentials.

Step 2 Choose **Security** > **Access Control Lists** > **FlexConnect ACLs**.

Step 3 To add an ACL, click **New**.

Step 4 In the **New** window that appears, enter the following:

a) In the **Access Control List Name** field, enter a name for the new ACL.

Note You can enter up to 32 alphanumeric characters.

b) Click **Apply**.

Step 5 When the **Access Control Lists** window reappears, click the name of the new ACL.

Step 6 In the **Edit** window that appears, click **Add New Rule**.

The **Rules** > **New** window appears.

Step 7 Configure a rule for this ACL with the required wall garden ranges.

To view the wall garden ranges, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in the **SSIDs** window.”.

When defining the ACL rule, ensure to configure the values as follows:

- **Direction**: Any
- **Protocol**: Any
- **Source Port Range**: 0-65535
- **Destination Port Range**: 0-65535
- **DSCP**: Any
- **Action**: Permit

Step 8 To provide social authentication for your portal, configure the wall garden ranges for social authentication.

To know the wall garden ranges that you must configure for social authentication, refer to the Configuring the Wireless Network for Social Authentication section.

Note The wall garden ranges configured for social authentication allows the customers to access all the HTTPS web sites directly after connecting to your SSID, without using the captive portal.

Configure the Virtual Interface

To configure the virtual interface, perform the following steps:

Procedure

Step 1 Choose **Controller** > **Interfaces**.

Step 2 Click the **Virtual** link.

Step 3 In the **Interfaces** > **Edit** window that appears, enter the following parameters:

a) In the **IP address** field, enter the unassigned and unused gateway IP address, if any.

b) In the **DNS Host Name** field, enter the DNS Host Name, if any.

Note Ideally this field must be blank.

Note To ensure connectivity and web authentication, the DNS server must always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then you must configure the same DNS host name on the DNS servers used by the client.

c) Click **Apply**.

Note If you have made any changes to the virtual interface, restart your Cisco Wireless Controller for the changes to take effect.

Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication

We highly recommend the use of RADIUS authentication for captive portals.

Note The Cisco Spaces cloud RADIUS server only supports PAP for web RADIUS authentication. CHAP is not supported. To avoid client authentication failure, you will need to configure PAP as the web RADIUS authentication method on the Cisco wireless controller.

The following features work only if you configure RADIUS authentication.

- Seamless Internet Provisioning.
- Extended session duration and Internet bandwidth.
- Deny Internet.

Also, for Customer onboarding by captive portal, internet provisioning configuration is required.

To configure radius authentication and seamless internet provisioning, perform the following steps:

Procedure

Step 1 Log in to Cisco Wireless Controller with your Cisco Wireless Controller credentials.

Step 2 In the **Cisco Wireless Controller** main window, click the **Security** tab.

Step 3 Choose **Radius** > **Authentication**.

The **RADIUS Authentication Servers** window is displayed.

Step 4 From the **Auth Called Station ID Type**e drop-down list, choose **AP MAC Address:SSID**.

Step 5 From the **MAC Delimiter** drop-down list, choose **Hyphen**.

Step 6 Click **New**.

Step 7 In the **New** window that appears, enter the details of the radius server for authentication, such as server IP address, port number, and secret key, select the **Server Status** as **Enabled**, and click **Apply**.

Port Number: 1812

Note You can configure only the Cisco Spaces RADIUS servers. To view the radius server IP address and secret key, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in the **SSIDs** window. The **Configure Manually** link appears only after adding a Cisco AireOS SSID. Configure both the primary and secondary radius server IPs. You can also contact the Cisco Spaces support team.

Step 8 Choose **Radius** > **Accounting**.

The Radius Accounting Servers window appears.

Note Enabling RADIUS Accounting is not mandatory for Captive Portals. The applicable use cases for Accounting are OpenRoaming and Change of Authorisation (CoA).

Step 9 From **Acct Called Station ID** Type, choose **AP MAC Address:SSID**.

Step 10 From the **MAC Delimiter** drop-down list, choose **Hyphen**.

Step 11 Click **New**.

Step 12 In the New window that appears, enter the details of the radius server for accounting, such as server IP address, port number, and secret key, select the Server Status as **Enabled**, and click **Apply**.

Port Number: 1813

Note You can configure only the Cisco Spaces RADIUS servers. You can configure only the Cisco Spaces RADIUS servers. To view the RADIUS server IP address and secret key, in the Cisco Spaces dashboard, click the "Configure Manually" link for a CUWN SSID in the **SSIDs** window.

Step 13 In the Cisco Wireless Controller main window, click the **WLANs** tab.

Step 14 Click the **WLAN** of the SSID for the Captive Portal rule.

Step 15 Choose **Security**.

Step 16 In the **Layer 2** tab, select the **MAC Filtering** check box.

Step 17 In the **Layer 3** tab, ensure that the following is configured.

In the Layer 3 security drop-down list, Web Policy is selected, and the On Mac Filter Failure radio button is selected.

Note These configurations in the Layer 3 are done when creating the SSIDs.

Step 18 In the AAA Servers tab, in the Radius Servers area, do the following:

a) Select the **Enabled** check box for the Authentication Servers.

a) From the **Server 1** drop-down list, choose the radius server you have previously defined.

Step 19 In the Authentication priority order for the web-auth user area, in the Order Used for Authentication box, set **Radius** as first in the order.

Note Use the Up and Down buttons to rearrange the order.

Step 20 Click the **Advanced** tab, and select the **Enabled** check box for Allow AAA Override.

Step 21 Click **Apply**.

Step 22 In the Cisco Wireless Controller main window, click the **Security** tab.

Step 23 Choose **AAA** > **MAC Filtering**.

Step 24 In the **MAC Filtering** window that appears, do the following:

a) From the **RADIUS Compatibility Mode** drop-down list, choose **Cisco ACS**.
b) From the **MAC Delimiter** drop-down list, choose **Hyphen**.
c) Click **Apply**.

Step 25 Ensure that the wall gardens are configured for the ACLs. To view the wall garden ranges, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in the **SSIDs** window.The **Configure Manually** link appears only after adding a Cisco AireOS SSID.

Configuring Cisco Wireless Controller for Social Authentication

For social authentication with Cisco Unified Wireless Network, you must do some configurations in the Cisco Wireless Controller.

To configure the Cisco Unified Wireless Network for social authentication, perform the following steps:

Procedure

Step 1 Log in to Cisco Wireless Controller using your credentials.

Step 2 Choose **Security** > **Access Control Lists** > **Access Control Lists**.

Step 3 In the **Access Control List** window that appears, click the Access Control List configured for Cisco Spaces.

Click **Add New Rule** and add additional two rules with following information. .

No	Action	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Destination Port Range	DSCP	Direction
1	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	HTTPS	Any	Any	Any
2	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	Any	HTTPS	Any	Any

Note This wall garden ranges configured for social authentication will allow the customers to access all the HTTPS web sites directly after connecting to your SSID, without using the captive portal.

Step 4 Add social platform specific domains as ACLs based on the social networks that you want to use for authentication. To add social domains as ACLs, perform the following steps:

a) In the Cisco Wireless Controller dashboard, choose **Security** > **Access Control Lists**.
b) Click **More Actions** for the Access Control List configured for Cisco Spaces.
c) Click **Add Remove URL**.
d) Enter a social URL name, and click **Add**.
e) Repeat steps **c** and **d** for each domain.

Note These domain names are managed by the social networks and can change at any time. Also, these domain names are subjected to change based on country/region. If you are facing any issue, contact the Cisco Spaces support team.

The commonly used domain names for various social platforms are as follows:

Facebook

- facebook.com
- static.xx.fbcdn.net
- www.gstatic.com
- m.facebook.com
- fbcdn.net
- fbsbx.com

LinkedIn

- www.linkedin.com
- static-exp1.licdn.com

Twitter

- abs.twimg.com
- syndication.twitter.com
- twitter.com
- analytics.twitter.com

Connecting Cisco Catalyst 9800 Series Wireless Controller or Cisco Wireless Controller to Cisco Spaces Using WLC Direct Connect or Cisco Spaces: Connector

To import the locations from Cisco 9800 Series Wireless Controller or Cisco Wireless Controller (without CMX) to Cisco Spaces, you must first connect the Controller to Cisco Spaces through one of the connectors.

The connectors, **Cisco WLC Direct Connect** and **Cisco Spaces Connector** can be used for both Cisco Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller.

Note

- If you want to connect a Cisco Wireless Controller with both Cisco CMX and Cisco Spaces simultaneously, you must use a Cisco Spaces: Connector. However, it is not recommended to connect a single Controller to both Cisco Spaces and Cisco CMX simultaneously.
- It is recommended not to compare the data displayed in Cisco Spaces reports such as Behavior Metrics with the data displayed in Cisco Wireless Controller or Cisco CMX, as it is expected to differ as per design.
- For importing a Controller to Cisco Spaces, ensure that at least one AP is connected to that particular Controller.
- In the Controller, if new APs are added to the Controller, those APs get automatically imported during the next Controller synchronization. If an imported AP is deleted from the Controller, the changes will be reflected in Cisco Spaces only after 48 hours. However, an AP without updates will be deleted after 48 hours only if updates are coming from other APs. For example, if there are 10 APs that are configured, and if 2 APs are removed from Controller, these 2 APs will be removed from Cisco Spaces only when updates are received from other 8 APs.
- If an AP is disassociated from the Controller, it is not immediately removed from Cisco Spaces to release the AP count. The APs will be removed from Cisco Spaces only after 48 hours.

The configurations required for various combinations of Wireless Controllers and Connectors are as follows:

Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect

To connect the Cisco Wireless Controller Version 8.3 or later (without Cisco CMX installation) to the Cisco Spaces, and to import the Cisco Wireless Controller and its access points to the Cisco Spaces, perform the following steps:

Before you begin

- You need Cisco Wireless Controller Version 8.3 or later.
- For importing a Cisco Wireless Controller to Cisco Spaces, ensure that at least one AP is connected to that particular Cisco Wireless Controller.
- The Cisco Wireless Controller must be able to reach Cisco Spaces cloud over HTTPS.
- Cisco Wireless Controller must be able to reach out to the internet.
- To use Cisco Spaces with anchor mode, you must have a network deployment with Cisco Wireless Controllers in both anchor controller mode and foreign controller mode. If the network deployment contains Cisco Wireless Controller in Anchor Controller mode and Foreign Controller mode, Cisco WLC Direct Connect must be enabled in both controllers using the commands described in this section. In addition, the Cisco Wireless Controllers in both modes must be able to reach the Cisco Spaces cloud over HTTPS. However, Cisco Spaces does not support Cisco Wireless Controller Version 8.3.102 in anchor mode.

- To connect the Cisco AireOS Wireless Controller Version 8.3 or later successfully to the Cisco Spaces using Cisco WLC Direct Connect, you must have a root certificate issued by DigiCert CA. If the network deployment contains Cisco Wireless Controller in Anchor Controller mode and Foreign Controller mode, you must import the certificate to the Cisco Wireless Controllers in both modes".

Procedure

Step 1 Import the DigiCert CA root certificate.

a) Download your root certificate from the following link:

https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem

b) Copy the root certificate content to a file with .cer extension, and save the file as {your_filename}.cer.

c) Copy the **{your_filename}.cer** file to the default directory on your TFTP.

d) Log in to the Cisco Wireless Controller CLI, and execute the following commands:

```
transfer download datatype cmx-serv-ca-cert
transfer download mode tftp
transfer download filename {your_filename}.cer
transfer download serverip {your_tftp_server_ip}
transfer download start
```

e) Type **Y** to start the upload

f) After the new root certificate has been uploaded successfully, execute the following commands to disable, and then enable your Cisco CMX Cloud Services:

```
config cloud-services cmx disable
config cloud-services cmx enable
```

Note After uploading the root certificate, Cisco Wireless Controller will prompt for reboot. Rebooting is recommended, but not mandatory. The certificate will be installed in either case.

If you try to connect the Wireless Controller to Cisco Spaces using a root certificate not issued by DigiCert CA, you will get the following error:

```
https:SSL certificate problem: unable to get local issuer certificate
```

Step 2 In the Cisco Wireless Controller CLI mode, execute the following commands:

```
config cloud-services cmx disable
 config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}
config cloud-services server id-token <Customer JWT Token>
 config network dns serverip <dns server ip>
 config cloud-services cmx enable
```

Note To view the {Customer Path Key}, {LB Domain}, {LB IP Address}, and {Customer JWT Token}, log in to Cisco Spaces dashboard, and click the three-line menu icon that is displayed at the top-left of the dashboard. Choose **Setup > Wireless Networks**. Then expand **Connect WLC / Catalyst 9800 Directly**, and click **View Token**. Click the **WLC** tab, and you can view the {Customer Path Key}, {LB Domain}, and {LB IP Address} at Step 1b and {Customer JWT Token} at Step 1c.

Step 3 Check the summary using the following command:

```
show cloud-services cmx summary
```

The result appears.

Now in the Cisco Spaces dashboard, when you choose **CUWN-WLC** in the **Add a Wireless Network** window, the WLC will be listed. So, you can import the APs of that WLC to the Cisco Spaces.

Example:

Sample Result

(Cisco Controller) >show cloud-services cmx summary

CMX Service

Server ..... https://$customerpathkey.dnaspaces.io

IP Address..... <Local System IP Address>

Connectivity..... https: UP

Service Status ..... Active

Last Request Status..... HTTP/1.1 200 OK

Heartbeat Status ..... OK

Now the Cisco Wireless Controller will be available for import in the Cisco Spaces location hierarchy. You can import the locations using Map services or Access Point Prefix.

What to do next

For social authentication, radius authentication, and internet provisioning, refer to the following sections:

- Configuring Cisco AireOS for Social Authentication
- Configuring Cisco AireOS for Internet Provisioning and Radius Authentication

Configuring Cisco Wireless Controller (without Cisco CMX) for Notification and Reports

Without Cisco CMX, you can connect Cisco Wireless Controller to Cisco Spaces using the connectors **WLC Direct Connect** and **Cisco Spaces Connector**. In these cases, the configurations required for notifications and reports aredone automatically when you import the Cisco Wireless Controller.

Note If you are using Cisco Spaces with **WLC Direct Connect** or **Cisco Spaces Connector**, the controller must be in **Foreign controller** mode.

Connecting Cisco Spaces to Cisco Catalyst 9800 Series Wireless Controller Using Cisco WLC Direct Connect

Before you begin

- For importing a Cisco Catalyst 9800 Series Wireless Controller to Cisco Spaces, ensure that atleast one AP is connected to that particular Cisco Catalyst 9800 Series Wireless Controller.
- Cisco Catalyst 9800 Series Wireless Controller must be able to reach Cisco Spaces cloud over HTTPS.
- Cisco Catalyst 9800 Series Wireless Controller must be able to reach out to the internet.
- To connect the Cisco Catalyst 9800 Series Wireless Controller successfully to the Cisco Spaces using Cisco WLC Direct Connect, you must have a root certificate trusted by Cisco.

To connect the Cisco Catalyst 9800 Series Controller to Cisco Spaces, and to import that controller and its access points to the Cisco Spaces, perform the following steps:

Procedure

Step 1 Import the Cisco External Trusted Root Store to install the DigiCert Global Root CA on the Controller.

a) Download the root certificate using the following command:

```
(config)#crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b
```

b) verify the certificate installation using the following command:

```
#show crypto pki trustpool | section DigiCert Global Root CA
cn=DigiCert Global Root CA
cn=DigiCert Global Root CA
```

Note You must check the output to verify correct trustpool installation.

Step 2 (Optional) On Cisco Catalyst 9800 Series Controller, enable DNS to resolve the Cisco Spaces URL using the following commands:

```
a. (config)#ip name-server <Primary IP> <Secondary IP>
b. (config)#ip domain lookup
c. (config)#ip route 0.0.0.0 0.0.0.0 <default_gw_ip_addr>
```

Step 3 Enable nmsp cloud-services on Cisco Catalyst 9800 Series Controller to communicate with Cisco Spaces Cloud over HTTPS.

```
a. (config)#nmsp cloud-services server url <URL>
b. (config)#nmsp cloud-services server token <Customer JWT TOKEN>
c. (config)#nmsp cloud-services http-proxy <proxy ip_addr> <proxy port> -This command is optional,
and must be used only if the proxy server needs to reach the internet.
d. (config)#nmsp cloud-services enable
```

Note To view the server URL and token, log in to Cisco Spaces dashboard, and click the three-line menu icon that is displayed at the top-left of the dashboard. Choose **Setup > Wireless Networks**. Then expand **Connect WLC / Catalyst 9800 Directly**, and click **View Token**. Click the **Cisco Catalyst 9800** tab, and you can see the URL at Step 2b and token at Step 2c.

Step 4 Confirm the connection between Cisco Catalyst 9800 Series Controller and Cisco Spaces Cloud by executing the following command:

```
#show nmsp cloud-services summary
```

The result must be as follows.

Example:

Sample Result

Server : https://abc.dnaspaces.io

CMX Service : Enabled

Connectivity : https: UP

Service Status : Active

Last IP Address : <Local System IP Address>

Last Request Status : HTTP/1.1 200 OK

Heartbeat Status : OK

Now the Cisco Catalyst 9800 Series Wireless Controller will be available for import in the Cisco Spaces location hierarchy.

Note The controller connects to the data.dnaspaces.io URL and not the abc.dnaspaces.io URL.

Step 5 To view the breif summary of active/inactive Cisco CMX cloud connections, execute the following command:

```
#show nmsp status
```

Note You can see the state of the connection to Cisco Spaces Cloud connection.

Step 6 To view aggregated subscriptions summary for all active Cisco Spaces cloud connections, execute the following command:

```
# show nmsp subscription summary
```

Note You can view the services that Cisco Spaces Cloud is subscribed to, after the connection is established.

Step 7 Import the locations to the Cisco Spaces dashboard.

For more information on importing the location, refer to Location Hierarchy.

Step 8 If you want to use the **Captive Portals** and **Engagements** apps, do the required configuration from the following:

Configuring Cisco Catalyst 9800 Series Wireless Controller (Local Mode) for Captive Portals and Engagements Apps Using CLI

Note The minimum supported Cisco Catalyst 9800 Series Wireless Controller Version is **16.10.20181030**.

To configure Cisco Catalyst 9800 Series Wireless Controller for Captive Portals and Engagements app , perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, configure a Cisco Catalyst SSID.

For more information on configuring the SSIDs, refer to the Importing the SSIDs for Cisco Unified Wireless Network section.

Note You can define any name for the SSID. You must use the same SSID name when configuring the Cisco Catalyst 9800 Series Wireless Controller .

Step 2 On Cisco Catalyst 9800 Series Wireless Controller , enable HTTP and HTTPS as follows:

ip http server

ip http secure-server

Step 3 Configure parameter maps for client redirection.

parameter-map type webauth <map name>

type consent

timeout init-state sec 600

redirect for-login <splash page URL>

redirect append ap-mac tag ap_mac

redirect append wlan-ssid tag wlan

redirect append client-mac tag client_mac

redirect portal ipv4 <IP Address>

logout-window-disabled

success-window-disable

Note For Splash URL and IP address, in the Cisco Spaces dashboard, click the **Captive Portal** app. Click **SSIDs**, and then click the **Configure Manually** link for the Cisco Catalyst SSID created in Step 1. The splash URL for your CUWN account will be listed in the **Creating the SSIDs in CUWN-WLC** section. The IP address will be listed in the **Creating the Access Control List** section. You must use only any one IP address from the list. You can also contact the Cisco Spaces support team.

Step 4 Configure virtual IP address for client redirection.

parameter-map type webauth global

virtual-ip ipv4 192.0.2.0

intercept-https-enable

Note
- Instead of **ipV4** *192.0.2.0*, you can configure any virtual IP. The virtual-ip should be a non-routable and a not used IP address.
- You must have a valid SSL certificate for the virtual IP/Domain installed in Cisco Catalyst 9800 Series Wireless Controller controller.

Step 5 Configure FQDN URL filtering.

For central switch wlans, the URL filter list is attached to the policy-profile:

urlfilter list social_login_fqdn_central

action permit

url <splash page domain>

Note Configure the domain configured at Step 3 for "redirect for-login".

url *.fbcdn.net

url *.licdn.com

url *.licdn.net

url *.twimg.com

url *.gstatic.com

url *.twitter.com

url *.akamaihd.net

url *.facebook.com

url *.facebook.net

url *.linkedin.com

url ssl.gstatic.com

url *.googleapis.com

url static.licdn.com

url *.accounts.google.com

url *.connect.facebook.net

url oauth.googleusercontent.com

wireless profile policy default-policy-profile

urlfilter list pre-auth-filter social_login_fqdn_central

For flex WLANs the URL filter list is attached to the flex-profile

urlfilter list social_login_fqdn_flex

action permit

url <splash page domain>



Note Configure the domain configured at Step 3 for "redirect for-login".

url *.fbcdn.net

url *.licdn.com

url *.licdn.net

url *.twimg.com

url *.gstatic.com

url *.twitter.com

url *.akamaihd.net

url *.facebook.com

url *.facebook.net

url *.linkedin.com

url ssl.gstatic.com

url *.googleapis.com

url static.licdn.com

url *.accounts.google.com

url *.connect.facebook.net

url oauth.googleusercontent.com

urlfilter list social_login_fqdn_central

wireless profile flex default-flex-profile

acl-policy <WA-sec-<ip>>

urlfilter list social_login_fqdn_flex

description "default flex profile"

Step 6 Configure Radius server.

aaa new-model

aaa group server radius <group name>

server name <radius server name>

subscriber mac-filtering security-mode mac

mac-delimiter hyphen

aaa accounting login <authentication> group <group name>

aaa authorization network <Authorization> group <Group Name>

aaa accounting identity <Accounting> start-stop group <Group Name>

aaa server radius dynamic-author

client <Radius Server IP> server-key <Radius Secret>

aaa session-id common

radius-server attribute wireless accounting call-station-id ap-macaddress-ssid

radius server <Radius Name>

address ipv4 <Radius Server IP> auth-port 1812 acct-port 1813

key <Radius Secret>



Note You can configure only the Cisco Spaces RADIUS servers. To view the IPv4 IP address, secret key, and port for RADIUS server configuration, in the Cisco Spaces dashboard, click the **Captive Portal** app. Click **SSIDs**, and then click the **Configure Manually** link for the Cisco Catalyst SSID created in Step 1. The radius server details will be listed in the **Radius Server Configuration** section. Configure both the primary and secondary RADIUS server IPs. You can also contact the Cisco Spaces support team.

Step 7 Configure Policy Profile.

wireless profile policy default-policy-profile

aaa-override

accounting-list <Accounting Server>

autoqos mode voice

description "default policy profile"

service-policy input platinum-up

service-policy output platinum

urlfilter list pre-auth-filter <url filter>

vlan <id>

no shutdown

Step 8 Configure WLAN.

wlan <WLAN name >

ip access-group web <ACL Name>

no security wpa

no security wpa akm dot1x

no security wpa wpa2 ciphers aes

security web-auth

security web-auth authentication-list default

security web-auth parameter-map <map name>

no shutdown

Note Ensure that the WLAN name you mention here matches with the SSID name you configured in Cisco Spaces at step 1.

Step 9 Enable DNS resolution and make sure you have a default gateway configured on the Cisco Catalyst 9800 Series Wireless Controller .

ip name-server <dns_ip_address>

ip domain-lookup

ip route 0.0.0.0 0.0.0.0 <default_gw_ip_addr>

You can then import the SSIDs to Cisco Spaces, and configure captive portals for SSIDs using the Captive Portal Rule.

Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Local Mode) for Captive Portals and Engagements Apps

Note The minimum supported Cisco Catalyst 9800 Series Wireless Controller Versions are 16.10.1E and 16.10.11.

To configure Cisco Catalyst 9800 Series Wireless Controller for Captive Portals and Engagements apps, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, configure a Cisco Catalyst SSID.

For more information on configuring the SSIDs, refer to the Importing the SSIDs for Cisco Unified Wireless Network section.

Step 2 Create the Parameter Map:

a) Log into Cisco Catalyst 9800 Series Wireless Controller .
b) Choose **Configuration** > **Security** > **Web Auth**.
c) On the **Web Auth Parameter Map** tab, click **Add**.
d) In the **Parameter-map name** field, enter parameter-map name.
e) From the **Type** drop-down list, choose **consent**, and click **Apply to Device**.
The newly created Parameter Map gets listed on the Web Auth Parameter Map tab.
f) Click the newly created **Parameter Map**.
g) On the **General** tab, check the **Disable Success Window** check box, and the **Disable Logout Window** check box.
h) On the **Advanced** tab, do the following:

- In the **Redirect for log-in** field, enter the splash page URL https://<domain>/p2/<customerPathKey>.
- In the **Redirect Append for AP MAC Address** field, enter ap_mac.
- In the **Redirect Append for Client MAC Address** field, enter client_mac.
- In the **Redirect Append for WLAN SSID** field, enter wlan.
- In the **Portal IPV4 Address** field, enter the Cisco Spaces IP to be allowed.



Note To view the IP address to be allowed, in the Cisco Spaces dashboard, click the **Captive Portals** app. Click **SSIDs**, and then click the **Configure Manually** link for the Cisco Catalyst SSID. The IP addresses will be listed in the Creating the Access Control List section. You must use only any one IP address from the list. The remaining IPs are specified when creating the ACL. The **Configure Manually** link appears only after adding a Cisco Catalyst SSID.

i) Click **Update and Apply**.

Step 3 Install the web-auth certificate and configure the global parameter map.

You must have a valid SSL certificate for the virtual IP/Domain installed in Cisco Catalyst 9800 Series Wireless Controller. You can purchase any wild card certificate.

a) Log into Cisco Catalyst 9800 Series Wireless Controller.
b) In the Cisco Catalyst 9800 Series Wireless Controller dashboard, choose **Configuration** > **Security** > **Web Auth**.
c) Click the Parameter map name, **global**.
d) Configure **Maximum Http connections** as **100**
e) Configure **Init-State Timeout(Secs)** as **120**
f) On the **General** tab, from the **Type** drop-down list, choose **Webauth**.
g) Specify virtual IPv4 address (virtual IP) or virtual IPv4 Host name (domain) in the respective field.
h) Configure **Watch List Expiry Timeout(Secs)** as **600**.
i) Check the **Web Auth intercept HTTPS** check box.
j) Click **Update & Apply**.
k) Convert the certificate into pkcs12.
The file format will be .p12.
l) Copy the file into the tftp server.
m) Download the certificate copied to the tftp server using the following steps:

- In the Cisco Catalyst 9800 Series Wireless Controller CLI, enter the following command:

  ```
  crypto pki import <name> pkcs12 tftp://<tftp server ip>:/ password <certificate password>
  ```

- To confirm the **tftp** server IP, enter **yes**.
- Enter the certificate file name. For example, wildcard.wifi-mx.com.p12.

  The certificate gets downloaded.

n) To verify the installed certificate, in the Cisco Catalyst 9800 Series Wireless Controller dashboard, choose **Configuration** > **Web Auth** > **Certificate**.

   The downloaded certificate appears as the last certificate in the list.

o) To map the installed certificate with webauth parameter map, in the Cisco Catalyst 9800 Series Wireless Controller CLI, execute the following commands:

- `Conf t`
- `parameter-map type webauth global`
- `trustpoint <installed trustpool name > ex: trustpool name`
- `end`
- `wr (to save the configuration)`

Reload Cisco Catalyst 9800 Series Wireless Controller .

Step 4 Create the ACL by adding URL filters.

a) Choose **Configuration** > **Security** > **URL Filter**.
b) In the **URL Filters** window, click **Add**.
c) In the **List Name** field, enter the list name.
d) Change the status of **Action** to **Permit**
e) In the **URLs** field, enter the splash page domain configured at Step 2h (Parameter Map).

   Add the following domains, if you want to enable social authentication:

- *.fbcdn.net
- *.licdn.com
- *.licdn.net
- *.twimg.com
- *.gstatic.com
- *.twitter.com
- *.akamaihd.net
- *.facebook.com
- *.facebook.net
- *.linkedin.com
- ssl.gstatic.com

- *.googleapis.com
- static.licdn.com
- *.accounts.google.com
- *.connect.facebook.net
- oauth.googleusercontent.com

f) Choose **Configuration** > **Tags and Profiles** > **Policy**.
g) In the **Policy Profile** window, click **default-policy-profile.**
h) In the **Edit Policy Profile** window, click the **Access Policies** tab.
i) In the **URL Filters** area, from the **Pre Auth** drop-down list, choose the previously created ACL.
j) Click **Update & Apply to Device** .

Step 5 Create the SSID.

a) Choose **Configuration** > **Tags and Profiles** > **WLANs**.
b) Click **Add**.
a) On the **General** tab, in the **Profile Name** field, enter the profile name.
b) In the **SSID** field, enter the SSID name defined at Step 1.
c) Set the status as **Enabled**.
d) Click the **Security** tab, and then click the **Layer2** tab.
e) From the **Layer 2 Security Mode** drop-down list, choose **None**.
f) Click the **Layer3** tab.
g) Check the **Web Policy** check box.
h) From the **WebAuth Parameter Map** drop-down list, choose the Web Auth Parameter Map created at step 2.
i) Click **Save & Apply to Device**.

Step 6 Configure the RADIUS server.

Note We highly recommend to use RADIUS authentication for captive portals. The following features work only if you configure RADIUS authentication.

- Seamless Internet Provisioning.
- Extended session duration.
- Deny Internet.

a) Choose **Configuration** > **Security** > **AAA**.
b) In the **Authentication Authorization and Accounting** window, click the **Servers/Groups** tab.
c) Choose **Radius** > **Servers**, and click **Add**.
d) In the **Name** field, enter a name for the radius server.
e) In the **IPv4 / IPv6 Server Address** field, enter the radius server address.



Note You can configure only the Cisco Spaces RADIUS servers. To view the radius server IP address and secret key, in the Cisco Spaces dashboard, click the **Captive Portal** app. Click **SSIDs**, and then click the **Configure Manually** link for the Cisco Catalyst SSID created at Step 1.In the window that appears, the radius server details will be listed in the **Radius Server Configuration** section. Configure both the primary and secondary RADIUS server IPs.You can also contact the Cisco Spaces support team.

f) In the **Key** field, enter the key, and confirm it in the **Confirm Key** field.
g) In the **Auth Port** field, enter 1812.
h) In the **Acct Port** field, enter 1813.
i) Click **Save & Apply to Device**.

   The server added will be available in **Servers** list.

j) Choose **Radius** > **Server Groups**, and click **Add**.
k) In the **Name** field, enter a name.
l) From the **MAC-Delimiter** drop-down list, choose **hyphen**.
m) From the **MAC-Filtering** drop-down list, choose **mac**.
n) Move the radius server previously created from "Available Servers" to "Assigned Servers" using the arrow button.
o) Click **Save & Apply to Device**.
p) In the **Authentication Authorization and Accounting** window, click the **AAA Method List** tab.
q) Click **Authentication**, and click **Add** and specify the following details:

   1. In the **Method List Name** field, enter the method list name.
   2. From the **Type** drop-down list, choose **Login**
   3. From the **Group Type** drop-down list, choose **Group**.
   4. Move the server group created earlier (step j to Step o) from **Available Server Groups** to **Assigned Servers Groups**, and click **Save & Apply to Device**.

r) On the **AAA Method List** tab, click **Authorization**, and click **Add**, and specify the following details:

   1. In the **Method List Name** field, enter the method list name.
   2. From the **Type** drop-down list, choose **Network**.
   3. From the **Group Type** drop-down list, choose **group**.
   4. Move the server group previously created (step j to Step o) from **Available Servers** to **Assigned Servers** using the arrow button, and click **Save & Apply to Device**.

s) On the **AAA Method List** tab, click **Accounting**, and click **Add**, and specify the following details:

   1. In the **Method List Name** field, enter the method list name.
   2. From the **Type** drop-down list, choose **Identity**.
   3. From the **Group Type** drop-down list, choose **group**.
   4. Move the server group previously created (step j to Step o) from **Available Servers** to **Assigned Servers** using the arrow button, and click **Save & Apply to Device**.

Step 7 Enable L3 and L2 authentication (Mac Filtering).

Make sure **Type** is selected as **webauth** in parameter-map for RADIUS Authentication.

Note To configure L3 and L2 authentication, ensure that you have created the SSIDs and have done all the configurations at step 5. You can then import the SSIDs to Cisco Spaces, and configure captive portals for SSIDs using the Captive Portal Rule.

a) Choose **Configuration** > **Tags and Profiles** > **WLANs**.
b) Click the SSID for which you want to configure L2 and L3 Authentication.
c) In the **Edit WLAN** window, click the **Security** tab.
d) On the **Layer3** tab, from the **Authentication** drop-down list, choose the radius authentication configured previously(step 6q).
e) On the **Layer2** tab, to enable Mac Filtering, check the **MAC Filtering** check box.
f) From the **Authorization List** drop-down list that appears, choose the authorization server created previously(step 6r).
g) Click **Show Advanced Settings**.
h) Check the **On Mac Filter Failure** check box.
i) Click **Update & Apply to Device**.
j) Choose **Configuration** > **Tags and Profiles** > **Policy**.
k) Click **default-policy-profile**.
l) On the **Advanced** tab, in the **AAA Policy** area, check the **Allow AAA Override** check box.
m) Ensure that default **aaa** policy is selected from the **Policy Name** drop-down list.
n) Click **Update & Apply to Device**.

Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Flex Mode or Mobility Express) for Captive Portals and Engagements Apps

Note The minimum supported Cisco Catalyst 9800 Series Wireless Controller Versions are 16.10.1E and 16.10.11.

To configure "Cisco Catalyst 9800 Series Wireless Controller in Flex mode" or "Cisco Catalyst 9800 Series Wireless Controller with Mobility Express" for Captive Portals and Engagements apps, perform the following steps:

Procedure

Step 1 To configure the Cisco Catalyst 9800 Series Wireless Controller in Flex mode, ensure that the following configurations are done:

This configuration is not required for Mobility Express.

a) Log into Cisco Catalyst 9800 Series Wireless Controller .
b) Choose **Configuration** > **Tags** > **Site.**

c) Select the required site name.
d) Uncheck the **Enable Local Site** check box.
e) Click **Update & Apply to Device.**
f) Choose **Configuration** > **Policy**.
g) Select the required policy name.
h) Disable **Central Switching**.
i) Click **Update & Apply to Device.**.

Note AP might reboot and rejoin the wireless controller on changing from **Local Mode** to **Flex mode**.

Step 2 In the Cisco Spaces dashboard, configure a Cisco Catalyst SSID.

For more information on configuring the SSIDs, see the Importing the SSIDs for Cisco Unified Wirelesss Network section.

Step 3 Create the Parameter Map:

a) Log into Cisco Catalyst 9800 Series Wireless Controller .
b) Choose **Configuration** > **Security** > **Web Auth**.
c) On the **Web Auth Parameter Map** tab, click **Add**.
d) In the **Parameter-map name** field, enter parameter-map name.
e) From the **Type** drop-down list, choose **consent**, and click **Apply to Device**.
The newly created Parameter Map gets listed on the **Web Auth Parameter Map** tab.
f) Click the newly created **Parameter Map**.
g) On the **General** tab, check the **Disable Success Window** check box, and the **Disable Logout Window** check box.
h) On the **Advanced** tab, do the following:

- In the **Redirect for log-in** field, enter the splash page URL https://<domain>/p2/<customerPathKey>.
- In the **Redirect Append for AP MAC Address** field, enter ap_mac.
- In the **Redirect Append for Client MAC Address** field, enter client_mac.
- In the **Redirect Append for WLAN SSID** field, enter wlan.
- In the **Portal IPV4 Address** field, enter the Cisco Spaces IP to be allowed.

Note To view the IP address to be allowed, in the Cisco Spaces dashboard, click the **Captive Portals** app. Click **SSIDs**, and then click the **Configure Manually** link for the CUWN/Catalyst SSID. The IP addresses will be listed in the **Creating the Access Control List** section. You must use only any one IP address from the list. The remaining IPs are specified when creating the ACL. The **Configure Manually** link appears only after adding a Cisco Catalyst SSID.

i) Click **Update and Apply**.

Step 4 Install the web-auth certificate and configure the global parameter map.

You must have a valid SSL certificate for the virtual IP/Domain installed in Cisco Catalyst 9800 Series Wireless Controller. You can purchase any wild card certificate.

a) Log into Cisco Catalyst 9800 Series Wireless Controller.
b) In the Cisco Catalyst 9800 Series Wireless Controller dashboard, choose **Configuration** > **Security** > **Web Auth**.
c) Click the Parameter map name, **global**.
d) Configure **Maximum Http connections** as **100**
e) Configure **Init-State Timeout(Secs)** as **120**
f) On the **General** tab, from the **Type** drop-down list, choose **Webauth**.
g) Specify virtual IPv4 address (virtual IP) or virtual IPv4 Host name (domain) in the respective field.
h) Configure **Watch List Expiry Timeout(Secs)** as **600**.
i) Check the **Web Auth intercept HTTPS** check box.
j) Click **Update & Apply**.
k) Convert the certificate into pkcs12.

   The file format will be .p12.

l) Copy the file into the tftp server.
m) Download the certificate from the tftp server using the following steps:

   - In the Cisco Catalyst 9800 Series Wireless Controller CLI, enter the following command:

     ```
     crypto pki import <name> pkcs12 tftp://<tftp server ip>:/ password <certificate password>
     ```

   - To confirm the **tftp** server IP, enter **yes**.
   - Enter the certificate file name. For example, wildcard.wifi-mx.com.p12.

     The certificate gets downloaded.

n) To verify the installed certificate, in the Cisco Catalyst 9800 Series Wireless Controller dashboard, choose **Configuration** > **Web Auth** > **Certificate**.

   The downloaded certificate appears as the last certificate in the list.

o) To map the installed certificate with webauth parameter map, in the Cisco Catalyst 9800 Series Wireless Controller CLI, execute the following commands:

   - `Conf t`
   - `parameter-map type webauth global`
   - `trustpoint <installed trustpool name > ex: trustpool name`
   - `end`
   - `wr (to save the configuration)`

   Reload Cisco Catalyst 9800 Series Wireless Controller .

Step 5 Create the ACL by adding URL filters.

a) Choose **Configuration** > **Security** > **URL Filter**.
b) In the **URL Filters** window, click **Add**.
c) In the **List Name** field, enter the list name.
d) Change the status of **Action** to **Permit**
e) In the **URLs** field, enter the splash page domain configured at Step 3h (Parameter Map).

   Add the following domains, if you want to enable social authentication:

   - *.fbcdn.net

- *.licdn.com
- *.licdn.net
- *.twimg.com
- *.gstatic.com
- *.twitter.com
- *.akamaihd.net
- *.facebook.com
- *.facebook.net
- *.linkedin.com
- ssl.gstatic.com
- *.googleapis.com
- static.licdn.com
- *.accounts.google.com
- *.connect.facebook.net
- oauth.googleusercontent.com

f) Choose **Configuration** > **Tags and Profiles** > **Policy**.
g) In the **Policy Profile** window, click **default-policy-profile.**
h) In the **Edit Policy Profile** window, click the **Access Policies** tab.
i) In the **URL Filters** area, from the **Pre Auth** drop-down list, choose the previously created ACL.
j) Click **Update & Apply to Device** .
k) Choose **Configuration** > **Tags and Profiles** > **Flex**.
l) Click the Profile in use.
m) In the **Edit Flex Profile** window that appears, click **Policy ACL** tab.
n) Click **Add**.
o) From the **ACL Name** drop-down list, choose **WA-sec-<ip>**.
p) From the **Pre Auth URL Filter** drop-down list, choose URL filter ACL created previously(Step 5a to 5e).
q) Click **Save**.
r) Click **Update & Apply to Device**.

Step 6 Create the SSID.

a) Choose **Configuration** > **Tags and Profiles** > **WLANs**.
b) Click **Add**.
a) On the **General** tab, in the **Profile Name** field, enter the profile name.
b) In the **SSID** field, enter the SSID name defined at Step 2.
c) Set the status as **Enabled**.
d) Click the **Security** tab, and then click the **Layer2** tab.
e) From the **Layer 2 Security Mode** drop-down list, choose **None**.
f) Click the **Layer3** tab.
g) Check the **Web Policy** check box.

h) From the **WebAuth Parameter Map** drop-down list, choose the Web Auth Parameter Map created at step 3.
i) Click **Save & Apply to Device**.

Step 7 Configure the RADIUS server.

Note We highly recommend to use RADIUS authentication for captive portals. The following features work only if you configure RADIUS authentication.

- Seamless Internet Provisioning.
- Extended session duration.
- Deny Internet.

a) Choose **Configuration** > **Security** > **AAA**.
b) In the **Authentication Authorization and Accounting** window, click the **Servers/Groups** tab.
c) Choose **Radius** > **Servers**, and click **Add**.
d) In the **Name** field, enter a name for the radius server.
e) In the **IPv4 / IPv6 Server Address** field, enter the radius server address.

Note You can configure only the Cisco Spaces RADIUS servers. To view the RADIUS server IP address and secret key, in the Cisco Spaces dashboard, click the **Captive Portal** app. Click **SSIDs**, and then click the **Configure Manually** link for the Cisco Catalyst SSID created at Step 2. In the window that appears, the RADIUS server details will be listed in the **Radius Server Configuration** section. Configure both the primary and secondary RADIUS server IPs.You can also contact the Cisco Spaces support team.

f) In the **Key** field, enter the key, and confirm it in the **Confirm Key** field.
g) In the **Auth Port** field, enter 1812.
h) In the **Acct Port** field, enter 1813.
i) Click **Save & Apply to Device**.
The server added will be available in **Servers** list.
j) Choose **Radius** > **Server Groups**, and click **Add**.
k) In the **Name** field, enter a name.
l) From the **MAC-Delimiter** drop-down list, choose **hyphen**.
m) From the **MAC-Filtering** drop-down list, choose **mac**.
n) Move the radius server previously created from “Available Servers” to “Assigned Servers” using the arrow button.
o) Click **Save & Apply to Device**.
p) In the **Authentication Authorization and Accounting** window, click the **AAA Method List** tab.
q) Click **Authentication**, and click **Add** and specify the following details:

1. In the **Method List Name** field, enter the method list name.
2. From the **Type** drop-down list, choose **Login**
3. From the **Group Type** drop-down list, choose **Group**.

4. Move the server group created earlier (step j to Step o) from **Available Server Groups** to **Assigned Servers Groups**, and click **Save & Apply to Device**.

r) On the **AAA Method List** tab, click **Authorization**, and click **Add**, and specify the following details:

1. In the **Method List Name** field, enter the method list name.
2. From the **Type** drop-down list, choose **Network**.
3. From the **Group Type** drop-down list, choose **group**.
4. Move the server group previously created (step j to Step o) from **Available Servers** to **Assigned Servers** using the arrow button, and click **Save & Apply to Device**.

s) On the **AAA Method List** tab, click **Accounting**, and click **Add**, and specify the following details:

1. In the **Method List Name** field, enter the method list name.
2. From the **Type** drop-down list, choose **Identity**.
3. From the **Group Type** drop-down list, choose **group**.
4. Move the server group previously created (step j to Step o) from **Available Servers** to **Assigned Servers** using the arrow button, and click **Save & Apply to Device**.

Step 8 Enable L3 and L2 authentication (Mac Filtering).

Make sure **Type** is selected as **webauth** in parameter-map for RADIUS Authentication.

Note To configure L3 and L2 authentication, ensure that you have created the SSIDs and have done all the configurations at step 6. You can then import the SSIDs to Cisco Spaces

Step 9 , and configure captive portals for SSIDs using the Captive Portal Rule.

a) Choose **Configuration** > **Tags and Profiles** > **WLANs**.
b) Click the SSID for which you want to configure L2 and L3 Authentication.
c) In the **Edit WLAN** window, click the **Security** tab.
d) On the **Layer3** tab, from the **Authentication** drop-down list, choose the radius authentication configured previously(step 7q).
e) On the **Layer2** tab, to enable Mac Filtering, check the **MAC Filtering** check box.
f) From the **Authorization List** drop-down list that appears, choose the authorization server created previously(step 7r).
g) Click **Show Advanced Settings**.
h) Check the **On Mac Filter Failure** check box.
i) Click **Update & Apply to Device**.
j) Choose **Configuration** > **Tags and Profiles** > **Policy**.
k) Click **default-policy-profile**.
l) On the **Advanced** tab, in the **AAA Policy** area, check the **Allow AAA Override** check box.
m) Ensure that default **aaa** policy is selected from the **Policy Name** drop-down list.
n) Click **Update & Apply to Device**.

Connecting Cisco Spaces to Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller using Cisco Spaces: Connector

Cisco Wireless Controller with Cisco Spaces Connector

To connect Cisco AireOS Wireless Controller to Cisco Spaces using a Cisco Spaces: Connector, and to configure captive portal authentication or notifications, do the following:

- Connect Cisco AireOS Wireless Controller to Cisco Spaces using a Cisco Spaces: Connector refering the procedure mentioned in Cisco Spaces: Connector Configuration Guide.
- After connecting Cisco AireOS Controller to Cisco Spaces, configure RADIUS authentication and internet provisioning as described in Configuring Cisco AireOS for Internet Provisioning and Radius Authentication.
- If Captive Portal Authentication is required, import SSIDs, create captive portal with the required authentication type, and configure Captive Portal rule based on the procedure mentioned in chapter Captive Portal Rule.
- If social authentication is required for captive portal, configure social authentication as described in Configuring Cisco Wireless Controller for Social Authentication, on page 88
- If you want to send notifications using Cisco Spaces, configure the engagement rules based on the procedure mentioned in Creating an Engagement Rule, on page 202.

Cisco Catalyst 9800 Series Wireless Controller with Cisco Spaces Connector

To connect Cisco Catalyst 9800 Series Wireless Controller to Cisco Spaces using a Cisco Spaces: Connector, and to configure captive portal authentication or notifications, do the following:

- To connect Cisco Catalyst 9800 Series Wireless Controller to Cisco Spaces using a Cisco Spaces: Connector, see Cisco Spaces: Connector Configuration Guide"
- After connecting Cisco Catalyst 9800 Series Wireless Controller to Cisco Spaces, for social authentication, RADIUS authentication, and internet provisioning (for using the **Captive Portals** app and **Engagements** app), see the following:
  - Configuring Cisco Catalyst 9800 Series Wireless Controller (Local Mode) for Captive Portals and Engagements Apps Using CLI , on page 95
  - Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Local Mode) for Captive Portals and Engagements Apps, on page 99
  - Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Flex Mode or Mobility Express) for Captive Portals and Engagements Apps, on page 104.
- To configure Captive Portal Authentication, import SSIDs, create captive portal with the required authentication type, and configure Captive Portal rule based on the procedure mentioned in chapter Captive Portal Rule.
- If you want to send notifications using Cisco Spaces, configure the engagement rules based on the procedure mentioned in chapter Creating an Engagement Rule, on page 202.

Configuring Mobility Express to work with Cisco Spaces

This section describes the configurations to be done in the Mobility Express Controller for using Cisco Spaces.

The configurations required for various Mobility Express versions are different. The configurations for various Mobility Express versions are as follows:

Configuring Mobility Express 8.7 or Later for Cisco Spaces

To configure the Mobility Express 8.7 or later for Cisco Spaces, perform the following steps:

Creating SSIDs in the Mobility Express

To create SSIDs in the Mobility Express, perform the following steps:

Procedure

Step 1 Log in to **Mobility Express** with your credentials.

Step 2 In the main window, click **Wireless Settings** in the left pane.

Step 3 Click **WLANs**.

Step 4 To create a WLAN, click **Add new WLAN/RLAN**.

Step 5 In the window that appears, in the **General** tab, enter the WLAN details like Type, Profile Name, SSID, and so on.

Step 6 Click **Apply**.

The **Add new WLAN/RLAN** window appears.

Step 7 Click **WLAN Security**.

Step 8 Enable the **Guest Network** toggle switch.

Step 9 Enable the **Captive Network Assistant** toggle switch.

Step 10 From the Captive Portal drop-down list, choose **External Splash Page**.

Step 11 From the Access Type drop-down list, choose **Web Consent**.

Step 12 In the Captive Portal URL field that appears, enter the Cisco Spaces splash URL.

To view the splash URL for your ME account, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in the **SSIDs** window.

Step 13 Click **Apply**.

Step 14 To enable and broadcast the SSID, in the **General** tab, from the Admin drop-down list, choose “Enabled”, and enable the “Broadcast SSID” toggle switch.

Step 15 Execute the following command in the command prompt to disable the secure webauth mode. Then, restart the ME.

```
config network web-auth secureweb disable
```

Step 16 Execute the following command in the command prompt to change the webauth login success page from **Default** to **None**.

config custom-web webauth-login-success-page none

Configuring RADIUS Authentication in Mobility Express 8.7 or Later

To configure radius authentication in the Mobility Express 8.7 or later, perform the following steps:

Procedure

Step 1 Log in to **Mobility Express** with your credentials.

Step 2 In the ME main window, click **Switch to Expert View** in the top right of the window.

Step 3 In the pop up window that appears, select **OK**.

Step 4 In the left pane, click **Management** > **Admin Accounts**.

Step 5 In the window that appears, click the **Radius** tab.

Step 6 Click **Add RADIUS Authentication Server**.

In the **Add/ Edit Radius Authentication Server** window appears, enter the following radius server details:

a) In the **Server IP Address** field, enter the IP address of the radius server.
b) In the **Shared Secret** field, enter your radius secret key.
c) In the **Confirm Shared Secret** field, re-enter the radius secret key.



Note You can configure only the Cisco Spaces RADIUS servers. To view the IP address and secret key for radius server configuration, in the Cisco Spaces dashboard, click the **Captive Portal** app. Click **SSIDs**, and then click the **Configure Manually** link for a Cisco Unified Wireless Network (Cisco AireOS) SSID. Click the **Configure SSID in CUWN-WLC** tab. The RADIUS server details will be listed in the **Radius Server Configuration** section. Configure both the primary and secondary RADIUS server IPs.You can also contact the Cisco Spaces support team.

Step 7 Click **Apply**.

Step 8 In the **Mobility Express** main window, click **Wireless Settings** in the left pane.

Step 9 Click **WLANs** .

The **WLAN/RLAN Configuration** window appears with the SSIDs list.

Step 10 Click the **Edit** icon for the SSID created previously.

Step 11 In the **Edit WLAN** window that appears, click the **WLAN Security** tab.

Step 12 From the **Access Type** drop-down list, choose **Radius**.

Step 13 Click the Radius Server tab, and click **Add RADIUS Authentication Server**.

Step 14 From the **Server IP Address** drop-down list, select your Radius Server, and click **Apply**.

Step 15 In the **Edit WLAN** window, click **Apply**.

Now the Mobility Express 8.7 or later is configured for radius server authentication.

Creating Access Control Lists in Mobility Express 8.7 or Later

To create Access Control Lists in the Mobility Express 8.7 or later, perform the following steps:

Procedure

Step 1 Log in to **Mobility Express** with your credentials.

Step 2 In the **Mobility Express** main window, click the Wireless Settings in the left pane.

Step 3 Click **WLANs**.

The WLAN/RLAN Configuration window appears with the SSIDs list.

Step 4 Click the **Edit** icon for the SSID created previously.

In the **Edit WLAN** window that appears, click the **WLAN Security** tab.

Step 5 Click the **Pre Auth ACLs** tab.

Step 6 Click **Add IP Rules**.

Step 7 In the Add/Edit IP ACLs, create rules with the following configuration:

Action	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Dest Port Range	DSCP
Permit	34.252.248.212/255.255.255.255	0.0.0.0/0.0.0.0	Any	Any	Any	Any
Permit	0.0.0.0/0.0.0.0	34.252.248.212/255.255.255.255	Any	Any	Any	Any
Permit	52.52.35.39/255.255.255.255	0.0.0.0/0.0.0.0	Any	Any	Any	Any
Permit	0.0.0.0/0.0.0.0	52.52.35.39/255.255.255.255	Any	Any	Any	Any

Note For EU region, `34.235.248.212, 52.55.235.39` must be replaced with `54.77.207.183,34.252.175.120`.

When defining the ACL rule, ensure to configure the values as follows:

- **Protocol**: Any
- **DSCP**: Any
- **Action**: Permit

Step 8 Click **Apply**.

Configuring Mobility Express 8.7 or Later for Social Authentication

To configure the Mobility Express for Social Sign authentication for captive portals, perform the following steps:

Procedure

Step 1 Log in to Mobility Express with your credentials.

Step 2 In the **Mobility Express** main window, click the **Wireless Settings** in the left pane.

Step 3 Click **WLANs**.

The **WLAN/RLAN Configuration** window appears with the SSIDs list.

Step 4 Click the **Edit** icon for the SSID created previously.

In the **Edit WLAN** window that appears, click the **WLAN Security** tab.

Step 5 Click the **Pre Auth ACLs** tab.

Step 6 Click **Add IP Rules**.

Step 7 In the Add/Edit IP ACLs, configure the following two rules in addition to the existing ACL rules:

Action	Source IP Address/Netmask	Destination IP Address/Netmask	Protocol	Source Port Range	Dest Port Range	DSCP
Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	HTTPs	Any	Any
Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	Any	HTTPS	Any

Allowing the URLs in the Mobility Express 8.7 or Later

To allow a URL in the Mobility Express 8.7 or later, perform the following steps:

Procedure

Step 1 Log in to **ME** with your credentials.

Step 2 In the **ME** main window, click the **Wireless Settings** in the left pane.

Step 3 Click **WLANs**.

The **WLAN/RLAN Configuration** window appears with the SSIDs list.

Step 4 Click the **Edit** icon for the SSID created previously.

Step 5 In the **Edit WLAN** window that appears, click the **WLAN Security** tab.

Step 6 Click the **Pre Auth ACLs** tab.

Step 7 Click **Add URL Rules**.

Step 8 In the **Add/Edit URL ACLs** window that appears, configure the URL that you want to include in the allowed list.

When defining the URL rule, ensure to configure the values as follows:

- **URL**: domain
- **Action**: Permit

Step 9 Click **Update**.

Configuring Mobility Express for Notifications and Reports

If you are using Mobility Express with WLC connect, to configure for location updates, perform the following steps:

Procedure

Step 1 In the **Cisco Wireless Controller CLI**, execute the following commands:

a. config cloud-services cmx disable

b. config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}

c. config cloud-services server id-token {Customer JWT Token}

d. config network dns serverip <dns server ip>

e. config cloud-services cmx enable



Note To view the {Customer Path Key}, {LB Domain}, {LB IP Address}, and {Customer JWT Token}, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in SSIDs window. You can also contact the Cisco Spaces support team. Ensure that there are no trailing or leading spaces.

Step 2 Check the summary using the following command:

show cloud-services cmx summary

The result appears.

Now in the Cisco Spaces dashboard, when you choose **CUWN-WLC** in the **Add a Wireless Network** window, the WLC will be listed. So, you can import the APs of that WLC to the Cisco Spaces.

Sample Resultt

(Cisco Controller) >show cloud-services cmx summary

CMX Service

Server ..... https://$customerpathkey.dnaspaces.io

IP Address..... 50.16.12.224

Connectivity..... https: UP

Service Status ..... Active

Last Request Status..... HTTP/1.1 200 OK

Heartbeat Status ..... OK

What to do next

Now the Cisco Wireless Controller will be available for importing to the CiscoCisco Spaces location hierarchy. For more information on importing the Cisco Wireless Controller and its access points, follow from Step 4 of the procedure mentioned in Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect , on page 90.

Configuring Mobility Express 8.6 or Earlier for Cisco Spaces

To configure Mobility Express 8.6 or earlier for Cisco Spaces:

Creating SSIDs in Mobility Express 8.6 or Earlier

The steps to create SSIDs in Mobility Express 8.6 or earlier are same as that for Mobility Express 8.7 or later. To know the configuration steps, see the Creating SSIDs in the Mobility Express, on page 111.

Configuring RADIUS Authentication for Mobility Express 8.6 or Earlier

In Mobility Express 8.6 or earlier, you cannot configure RADIUS servers individually.

To configure Mobility Express 8.6 or earlier for RADIUS authentication, perform the following steps:

Procedure

Step 1 Log in to **Mobility Express** with your credentials.

Step 2 In the **Mobility Express** main window, click **Wireless Settings** in the left pane.

Step 3 Click **WLANs**.

The **WLAN/RLAN Configuration** window appears with the SSIDs list.

Step 4 Click the **Edit** icon for the SSID created previously.

Step 5 In the **Edit WLAN** window that appears, click the WLAN Security tab.

Step 6 From the **Access Type** drop-down list, choose **Radius**.

Step 7 To add the radius server, click **Add**.

Step 8 In the window that appears, enter the following radius server details:

a. In the **Server IP Address** field, enter the IP address of the radius server.

b. In the **Shared Secret** field, enter your radius secret key.

c. In the **Confirm Shared Secret** field, re-enter the radius secret key.

d. Click **Apply**.

Note You can configure only the Cisco Spaces RADIUS servers. To view the IP address and secret key for radius server configuration, in the Cisco Spaces dashboard, click the **Captive Portal** app. Click **SSIDs**, and then click the **Configure Manually** link for a Cisco Unified Wireless Network (Cisco AireOS) SSID. Click the **Configure SSID in CUWN-WLC** tab. The RADIUS server details will be listed in the **Radius Server Configuration** section. Configure both the primary and secondary RADIUS server IPs.You can also contact the Cisco Spaces support team.

Step 9 In the **Edit WLAN** window, click **Apply**.

Now, the Mobility Express is configured for radius server authentication of Cisco Spaces captive portals.

Creating ACLs for Mobility Express 8.6 or Earlier

Mobility Express 8.6 or earlier does not provide user interface to configure Access Control Lists. So for creating ACLs, and configuring social authentication, you must use the command prompt. For the commands to use for these ACL configurations, see the " Mobility Express Command Reference Guide".

Now the Cisco Wireless Controller will be available for import in Cisco Spaces location hierarchy. For more information on importing the Cisco Wireless Controller and access points to the Cisco Wireless Controller, follow from Step 3 of the procedure mentioned in Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect , on page 90.

Configuring Mobility Express for Notifications and Reports

If you are using Mobility Express with WLC connect, to configure for location updates, perform the following steps:

Procedure

Step 1 In the **Cisco Wireless Controller CLI**, execute the following commands:

a. config cloud-services cmx disable

b. config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}

c. config cloud-services server id-token {Customer JWT Token}

d. config network dns serverip <dns server ip>

e. config cloud-services cmx enable

Note To view the {Customer Path Key}, {LB Domain}, {LB IP Address}, and {Customer JWT Token}, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in SSIDs window. You can also contact the Cisco Spaces support team. Ensure that there are no trailing or leading spaces.

Step 2 Check the summary using the following command:

show cloud-services cmx summary

The result appears.

Now in the Cisco Spaces dashboard, when you choose **CUWN-WLC** in the **Add a Wireless Network** window, the WLC will be listed. So, you can import the APs of that WLC to the Cisco Spaces.

Sample Resultt

(Cisco Controller) >show cloud-services cmx summary

CMX Service

Server ..... https://$customerpathkey.dnaspaces.io

IP Address..... 50.16.12.224

Connectivity..... https: UP

Service Status ..... Active

Last Request Status..... HTTP/1.1 200 OK

Heartbeat Status ..... OK

What to do next

Now the Cisco Wireless Controller will be available for importing to the CiscoCisco Spaces location hierarchy. For more information on importing the Cisco Wireless Controller and its access points, follow from Step 4 of the procedure mentioned in Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect , on page 90.

Configuring Aironet 4800 Series Mobility Express Controller 8.10.150.0 for Cisco Spaces

To configure AireOS 4800 Series Mobility Express Controller 8.10.150.0 for Cisco Spaces:

Configuring Mobility Express 8.10.150.0

To configure Mobility Express 8.10.105.0 for Cisco Spaces, perform the following steps:

Procedure

Step 1 Log in to **Mobility Express** with your credentials.

Step 2 Go to **Advanced** > **Security Settings**.

Step 3 Click **Add New ACL**.

Step 4 In the **Add ACL Rule** window, enter the ACL details:

a) From the **ACL Type** drop-down list, choose **IPv4**.

b) In the **ACL** name field, enter a name for the ACL.

c) Click **Add URL Rules**.

The **Add /Edit URL ACLs** window appears.

d) In the **URL** field, enter splash page URL domain.

e) From the **Action** drop-down list, choose **Permit**.

f) To enable social authentication, add the following domains in the ACL:

- *.facebook.com
- *.facebook.com
- ssl.gstatic.com
- static.licdn.com
- *.fbcdn.net

- *.akamaihd.net
- *.twitter.com
- *.twimg.com
- oauth.googleusercontent.com
- *.googleapis.com
- *.accounts.google.com
- *.gstatic.com
- *.linkedin.com
- *.licdn.net
- *.licdn.com

This step is required only of you want to enable social authentication.

g) Click **Update**.

Step 5 To add radius server configuration, perform the following steps:

a) Create an ACL.
b) Enable **Expert** view.
c) Go to **Managenent** > **Admin Accounts** > **Radius**
d) From the **Authentication Call Station ID Type** drop-down list, choose **AP MAC Address:SSID**.
e) From the **Authentication MAC Delimiter** drop-down list, choose **Hyphen**.
f) From the **Accounting Call Station ID Type** drop-down list, choose **AP MAC Address:SSID**.
g) From the **Accounting MAC Delimiter** drop-down list, choose **Hyphen**.
h) From the **Fallback Mode** drop-down list, choose **Off**.
i) Click **Apply**.

Step 6 Click **Add Radius Authentication Server**, and in the **Add/Edit Radius Authentication Server** that appears, enter the following details:

a) Disable **CoA**.
b) In the **Server Ip Address** field, enter the radius server IP address.
c) In the **Shared Secret** field, enter the secret key.
d) In the **Confirm Shared Secret** field, enter the secret key to confirm
e) Click **Apply**.

Added radius server will be listed under the Radius Servers list.

Note You can configure only the Cisco Spaces RADIUS servers. To view the IP address and secret key for the radius server configuration, in the Cisco Spaces dashboard, click the **Captive Portals**app. Click **SSIDs**, and then click the **Configure Manually** link for a Cisco Unified Wireless Network (Cisco AireOS) SSID. The RADIUS server details will be listed in the RADIUS Server Configuration section. Configure both the primary and secondary RADIUS server IPs. You can also contact the Cisco Spaces support team.

Step 7 To configure **WLAN** for radius server, perform the following steps:

a) In the Cisco Aironet ME dashboard, choose **Wireless Settings** > **WLAN**.
b) Click the **General** tab.
c) In the **Profile Name** field, enter the SSID name.
d) From the **Admin State** drop-down list, choose **Enabled**.
e) From the **Radio Policy** drop-down list, choose **ALL**.
f) Click the **WLAN Security** tab.
g) Enable **Guest Network**.
h) Enable **Captive Network Assistant**.
i) In the **Captive Portal URL** field, enter the captive portal URL.



Note To view the Captive Portal URL, in the Cisco Spaces dashboard, click the **Captive Portals**app. Click **SSIDs**, and then click the **Configure Manually** link for a Cisco Unified Wireless Network (Cisco AireOS) SSID. Go to the **Creating the SSIDs in WLC Direct Connect** section. The URL is displayed at Step 7g.

j) From the **Access Type**, choose **RADIUS**.
k) In the **ACL Name (IPV4)**, choose the ACL name configured at Step 4b.
l) For radius server, click **Add Radius Authentication Server**
m) Select Radius server IP added at Step 6b from the list.

Step 8 For Radius L2 Authentication, enable **MAC Filtering** and **ON MAC Filter failure**.

Step 9 Click **Apply**.

Configuring Mobility Express for Notifications and Reports

If you are using Mobility Express with WLC connect, to configure for location updates, perform the following steps:

Procedure

Step 1 In the **Cisco Wireless Controller CLI**, execute the following commands:

a. config cloud-services cmx disable

b. config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}

c. config cloud-services server id-token {Customer JWT Token}

d. config network dns serverip <dns server ip>

e. config cloud-services cmx enable



Note To view the {Customer Path Key}, {LB Domain}, {LB IP Address}, and {Customer JWT Token}, in the Cisco Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in SSIDs window. You can also contact the Cisco Spaces support team. Ensure that there are no trailing or leading spaces.

Step 2 Check the summary using the following command:

show cloud-services cmx summary

The result appears.

Now in the Cisco Spaces dashboard, when you choose **CUWN-WLC** in the **Add a Wireless Network** window, the WLC will be listed. So, you can import the APs of that WLC to the Cisco Spaces.

Sample Resultt

(Cisco Controller) >show cloud-services cmx summary

CMX Service

Server ..... https://$customerpathkey.dnaspaces.io

IP Address..... 50.16.12.224

Connectivity..... https: UP

Service Status ..... Active

Last Request Status..... HTTP/1.1 200 OK

Heartbeat Status ..... OK

What to do next

Now the Cisco Wireless Controller will be available for importing to the CiscoCisco Spaces location hierarchy. For more information on importing the Cisco Wireless Controller and its access points, follow from Step 4 of the procedure mentioned in Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect , on page 90.

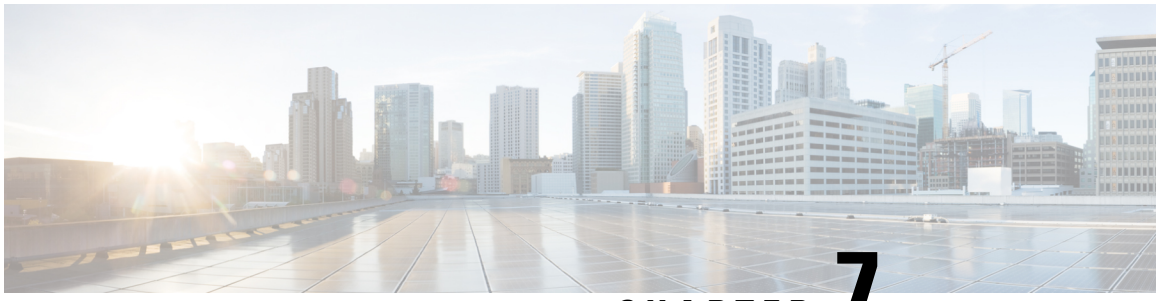
Cisco Spaces Scale Benchmark

Table 10: Scale Summary

SNO	Cisco Spaces: Connector	Cisco WLC Direct Connect		CMX Tethering Connector
Platforms	Cisco AireOS	Cisco AireOS	Cisco Catalyst 9800 Series	Cisco AireOS
Max Scale on supported appliance.	12.5K APs, 250K clients Incoming NMSP should not be more than 10.5K messages/sec.	50 APs and 50 Clients	50 APs and 50 Clients	60K clients, 5K APs, and 50k RFID tags Maps with 1BLDG-100 Floors and each floor with 50 APs

SNO	Cisco Spaces: Connector	Cisco WLC Direct Connect		CMX Tethering Connector
Scale supported releases	Connector version 2.1.1 with docker v2.0.204	8.8MR2	16.12, 17.1	8.8MR2 with CMX 10.6 (high end)

Note Currently, scaling is not available for Mobility Express.



CHAPTER 7

Configuring Cisco Meraki for Cisco Spaces

This chapter describes the configurations required in Cisco Meraki for using Cisco Spaces.

- Enabling SSIDs in Cisco Meraki, on page 123
- Configuring Cisco Meraki for RADIUS Authentication, on page 124
- Configuring Cisco Meraki for Notifications and Reports, on page 126
- Configuring Cisco Meraki for Social Authentication, on page 127
- Manually Configuring SSIDs for Cisco Meraki, on page 127
- Configuring Scanning API in Cisco Meraki, on page 128
- Bluetooth Low Energy Device Support, on page 129

Enabling SSIDs in Cisco Meraki

To import the SSIDs to the Cisco Spaces to configure them for the Captive Portal Rules, you must enable those SSIDs in Cisco Meraki.

Note As Cisco Meraki is not a part of the Cisco Spaces, the menu path and menu names are subject to change.

To enable the SSIDs in Cisco Meraki, perform the following steps:

Procedure

Step 1 Go to https://meraki.cisco.com.

Step 2 Log in to the application using the login credentials for your Cisco Meraki account.

Step 3 Click the **Cisco Merkai Organization** in which you want to enable the SSIDs, and choose the required network.

Step 4 Choose **Wireless** > **Configure** > **SSIDs**.

The SSIDs available for the network appears.

Step 5 Rename the SSID and enable it.

Step 6 Click **Edit Settings**, and in the Splash page option, click the **Click-Through** radio button.

Step 7 Click **Save Changes**.

The SSID is successfully enabled in Cisco Meraki.

Configuring Cisco Meraki for RADIUS Authentication

To provide more security to your portals, the Cisco Spaces provides radius-authentication for the portals. Also, certain configurations are required in Cisco Meraki to manage the seamless internet provisioning that can be configured using the Captive Portal Rule.

The Radius Server Configurations required when configuring for the seamless internet provisioning is different from that of the standard radius server configuration.

Configuring Cisco Meraki for RADIUS Authentication (Without Seamless Internet Configurations)

To configure Cisco Meraki for RADIUS authentication, perform the following steps:

Procedure

Step 1 Log in to Cisco Meraki with your Meraki credentials.

Step 2 Choose **Wireless Access Control**.

Step 3 Choose the SSID for the captive portal rule.

Step 4 In the **Association requirements** area, choose **Open**.

Step 5 In the **Splash page** area, choose **Sign-on with**, and from the drop-down list select **my RADIUS server**.

Step 6 In the **Radius servers**area, click **Add a server**, and in the fields that appear mention the radius server details for authentication.

- Port:1812

Note You can configure only the Cisco Spaces RADIUS servers.To view the RADIUS server IP address and secret key, in the Cisco Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the SSIDs page.

Step 7 From the **Radius accounting** drop-down list, choose **Radius Accounting is enabled**.

Note Enabling RADIUS Accounting is not mandatory for Captive Portals. The applicable use cases for Accounting are OpenRoaming and Change of Authorisation (CoA).

Step 8 In the **Radius accounting servers** area, click **Add a server**, and in the fields that appear mention the radius server details for accounting.

- Port:1813

Note You can configure only the Cisco Spaces RADIUS servers. You can configure only the Cisco Spaces RADIUS servers. To view the RADIUS server IP address and secret key, in the Cisco Spaces dashboard, click the Configure Manually link for a Meraki SSID in the SSIDs page.

Step 9 Configure the Wall Garden ranges. To view the wall garden ranges, in the Cisco Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the SSIDs page.

Step 10 Save the changes.

Configuring Cisco Meraki for RADIUS Authentication and Seamless Internet Provisioning

To configure Cisco Meraki for RADIUS authentication and Seamless Internet Provisioning, do the following configurations in Cisco Meraki:

Procedure

Step 1 Log in to Cisco Meraki with your Meraki credentials.

Step 2 Choose **Wireless** > **Access** > **Control**.

Step 3 Choose the SSID for the captive portal rule.

Step 4 In the Association requirements area, choose **Mac-based access control (no encryption)**.

Step 5 In the Splash page area, choose **Click-through**.

Step 6 In the Radius servers area, click **Add a server**, and in the fields that appear mention the radius server details for authentication.

- Port:1812

Note You can configure only the Cisco Spaces RADIUS servers. To view the RADIUS server IP address and secret key, in the Cisco Spaces dashboard, click the **Configure Manually**link for a Meraki SSID in the SSIDs page.

Step 7 From the **Radius accounting** drop-down list, choose **Radius Accounting is enabled**.

Note Enabling RADIUS Accounting is not mandatory for Captive Portals. The applicable use cases for Accounting are OpenRoaming and Change of Authorisation (CoA).

Step 8 In the **Radius accounting servers** area, click **Add a server**, and in the fields that appear mention the radius server details for accounting.

- Port :1813

Note You can configure only the Cisco Spaces RADIUS servers. To view the RADIUS server IP address and secret key, in the Cisco Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the SSIDs page.

Step 9 From the **Radius attribute specifying group policy name** drop-down list, choose **Filter-Id**.

Step 10 Save the changes.

Step 11 In the Cisco Meraki dashboard, click **Network-wide Group Policies**.

Step 12 Click **Add a Group**.

Step 13 In the **New group** window that appears, enter a name for the group.

Note You have to configure this name as the policy name in the Cisco Spaces dashboard. If you are specifying the group name as **CaptiveBypass**, this policy name will act as the default policy name for all the Captive Portal rules. That is, if you are not specifying a policy name for a Captive Portal rule for which the "Seamlessly Internet Provision" is opted, the policy name **CaptiveBypass** will be applied for that rule.

Step 14 From the **Bandwidth** drop-down list, choose the required option, and specify the Internet bandwidth to be provisioned for the customers.

Step 15 From the Splash drop-down list, choose **Bypass**.

Step 16 Click **Apply**.

Step 17 Configure the Wall Garden ranges. To view the wall garden ranges, in the Cisco Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the SSIDs page.

Configuring Cisco Meraki for Notifications and Reports

To send notifications using the Cisco Spaces and to view the Cisco Spaces reports, you must do certain configurations in Cisco Meraki.

Note When you import a Meraki network location to Location Hierarchy, the Notification URL automatically gets configured in Cisco Meraki. This support is not applicable for the Meraki networks added using Meraki API Key.

To manually configure Cisco Meraki for sending notifications using the Cisco Spaces or to view the Cisco Spaces reports, perform the following steps:

Procedure

Step 1 Log in to Cisco Meraki using the credentials for your Meraki account.

Step 2 Click the organization in which you want to enable SSIDs, and choose the required network.

Step 3 Choose **Network-wide** > **Configure** > **General**.

Step 4 In the **CMX** area, do the following:

a) From the **Analytics** drop-down list, choose **Analytics is enabled**.

b) From the **Scanning API** drop-down list, choose **Scanning API enabled**.

c) Click **Add a Post URL**, and enter the post URL details in the respective fields.

To view the post URL details, in the Cisco Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the **SSIDs** window.

Step 5 Click **Save Changes**.

Configuring Cisco Meraki for Social Authentication

For social authentication with Cisco Meraki, you must do some configurations in meraki.cisco.com.

To configure Cisco Meraki for social-authentication, perform the following steps:

Procedure

Step 1 In the Cisco Meraki dashboard, choose **Wireless** > **Configure** > **Access Control** .

The **Access Control**window appears.

Step 2 From the **SSID** drop-down list, choose the SSID for which you want configure the social authentication.

Step 3 In the **Wall Garden Ranges** field, enter the social networking domain names listed in the following table, and click **Save Changes**.

Social Authentication for Cisco Meraki is successfully configured.

Table 11: Social Networking Domain Names

Facebook	Twitter	LinkedIn	
*.facebook.com *.fbcdn.net *.akamaihd.net *.connect.facebook.net	*.twitter.com *.twimg.com	*.linkedin.com *.licdn.net *.licdn.com	

Manually Configuring SSIDs for Cisco Meraki

To manually configure an SSID in Cisco Meraki, you have to initially import that SSID in the Cisco Spaces. For more information, see the "Importing the SSIDs for Cisco Meraki section .

To configure the SSID manually in Cisco Meraki, perform the following steps:

Procedure

Step 1 Log in to Cisco Meraki using the credentials for your Meraki account.

Step 2 Choose the required Cisco Meraki organization and network from the respective drop-down list.

Step 3 Choose **Wireless** > **Access Control**.

Step 4 From the SSID drop-down list, choose the SSID that you want to configure for the Cisco Spaces.

Step 5 In the splash page area, choose **Click-through**.

Step 6 From the Wall garden drop-down list, choose **Wall garden is enabled**.

Step 7 In the **Wall garden ranges** field, enter the required wall garden ranges.

To view the wall garden ranges, in the Cisco Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the **SSIDs** window.

Step 8 Click **Save Changes**.

Step 9 Choose **Wireless** > **Splash page**.

Step 10 For the previously selected SSID, in the **Custom Splash URL** area, choose **Or provide a URL where customers will be redirected**, and in the adjacent field enter the splash URL.

To generate and view the splash page URL for a Meraki SSID, follow the steps given below:

a) Click **Home** > **Captive Portals** > **SSIDs** to import the Meraki SSID to Cisco Spaces.
A splash page URL is generated in the Cisco Spaces Dashboard.

b) On the **SSIDs** page, click the **Configure Manually** link for the desired Meraki SSID.
The splash page URL for the selected Meraki SSID is displayed.

Step 11 In the **Splash Behavior**area, click the **The URL they were trying to fetch** radio button under **Where should users go after the splash page**.

Step 12 Click **Save Changes**.

Step 13 Repeat steps 3-12 for all the SSIDS that you want to use in the Cisco Spaces.

What to do next

Configuring Scanning API in Cisco Meraki

For using Meraki Camera, you must configure Scanning API in Cisco Meraki.

To configure a Scanning API in Cisco Meraki, perform the following steps:

Procedure

Step 1 Log in to the https://meraki.cisco.com using the login credentials for your Cisco Meraki account.

Step 2 Choose **Networkwide** > **General**.

Step 3 In the **Location and Scanning** area, do the following:

a) From the **Analytics** drop-down list, choose **Analytics enabled**.

b) From the **Scanning API** drop-down list, choose **Scanning API enabled**.

c) Add a post URL.

- In the **Post URL** field, enter the post URL .
- In the **Secret Key** field, enter the secret key that is used by your HTTP server to validate that the JSON posts that are coming from the Cisco Meraki cloud.

Note You can copy the post URL and secret key from the **Connect your Meraki Camera** window for **Setup** > **Camera** in Cisco Spaces dashboard.

- From the **API Version** drop-down list, choose the Location API version your HTTP server is prepared to receive and process.

Step 4 Configure and host your HTTP server to receive JSON objects.

Step 5 During the first connection, the Cisco Meraki cloud will verify the organization's identity as the Cisco Meraki customer.

The Cisco Meraki cloud will then begin performing JSON posts.

Bluetooth Low Energy Device Support

Support for Bluetooth Low Energy (BLE) devices are available on the Cisco Meraki network, in addition to the existing support on the Cisco Catalyst Wireless network.

This enhancement allows the Cisco Spaces platform to seamlessly integrate with BLE devices using Cisco Meraki. With this enhancement, Cisco Meraki BLE devices can now be accessed in various Cisco Spaces applications, including Firehose IoT Telemetry events, IoT Explorer, Signage, and Live Occupancy.

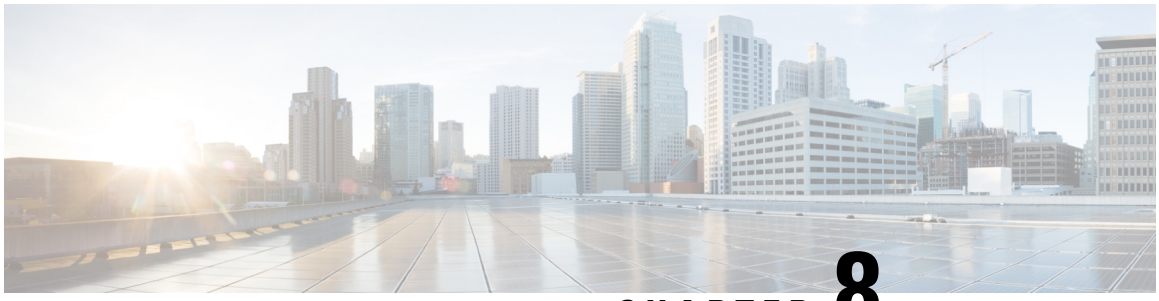
Note For this feature to work, you must perform specific configurations on the Cisco Meraki network to enable the data transmission to Cisco Spaces. We recommend that you contact Cisco Spaces support team for further assistance.



PART IV

Cisco Spaces: Apps

- Cisco Spaces: Visitor Trends App, on page 133
- Cisco Spaces: **Live Occupancy** App, on page 145
- Cisco Spaces: Camera Metrics App, on page 161
- Cisco Spaces: OpenRoaming App, on page 165
- Cisco Spaces: Location Analytics App, on page 167
- Cisco Spaces: Impact Analysis App, on page 181
- Cisco Spaces: Space Utilization App, on page 185
- Cisco Spaces: Smart Workspaces App, on page 187
- Cisco Spaces: Environmental Analytics App, on page 189
- Cisco Spaces: Asset Locator App, on page 191
- Cisco Spaces: IoT Explorer App, on page 193
- Cisco Spaces: Captive Portal App, on page 199
- Cisco Spaces: Engagements App, on page 201
- Cisco Spaces: Location Personas App, on page 223
- Cisco Spaces: Asset Tracker App, on page 235



CHAPTER 8

Cisco Spaces: Visitor Trends App

This chapter describes the Visitor Trends app and reports.

- Overview of Visitor Trends, on page 133
- View the Visitor Trends Report, on page 133
- Benchmarks, on page 135
- Report Tabs, on page 136
- Visitor Trends (Business Metrics), on page 136
- Workspaces Vertical (Visitor Trends), on page 139
- Education Vertical (Visitor Trends), on page 141
- Pin a Location, on page 143
- Location-Based RBAC, on page 143

Overview of Visitor Trends

The **Visitor Trends** app enables you to view various reports that provide insights about the performance of your business. By default, the report includes the data for the previous month. You can filter to view the report for a particular location and month. You can also filter the report based on tags.

After installing Cisco Spaces, it will take a month to show the initial report. You can view the sample report during this period. You can also see how your report is building up by switching to the “My Data” option during this period. A notification is sent once the report is ready.

Note The **Visitor Trends** is enhanced to show **Sub Vertical** level benchmark metrics. This is applicable for category average metrics and accounts where a sub-vertical is defined.

If a sub-vertical is not defined, category average metrics are computed based on the vertical level benchmark.

View the Visitor Trends Report

In the **Visitor Trends** app, a minimum of 100 visits at each location level is required to display the chart data. Hence, only those locations with a significant amount of visit data are considered for visualisation in the charts.

To view the various reports in the **Visitor Trends** app, perform the following steps:

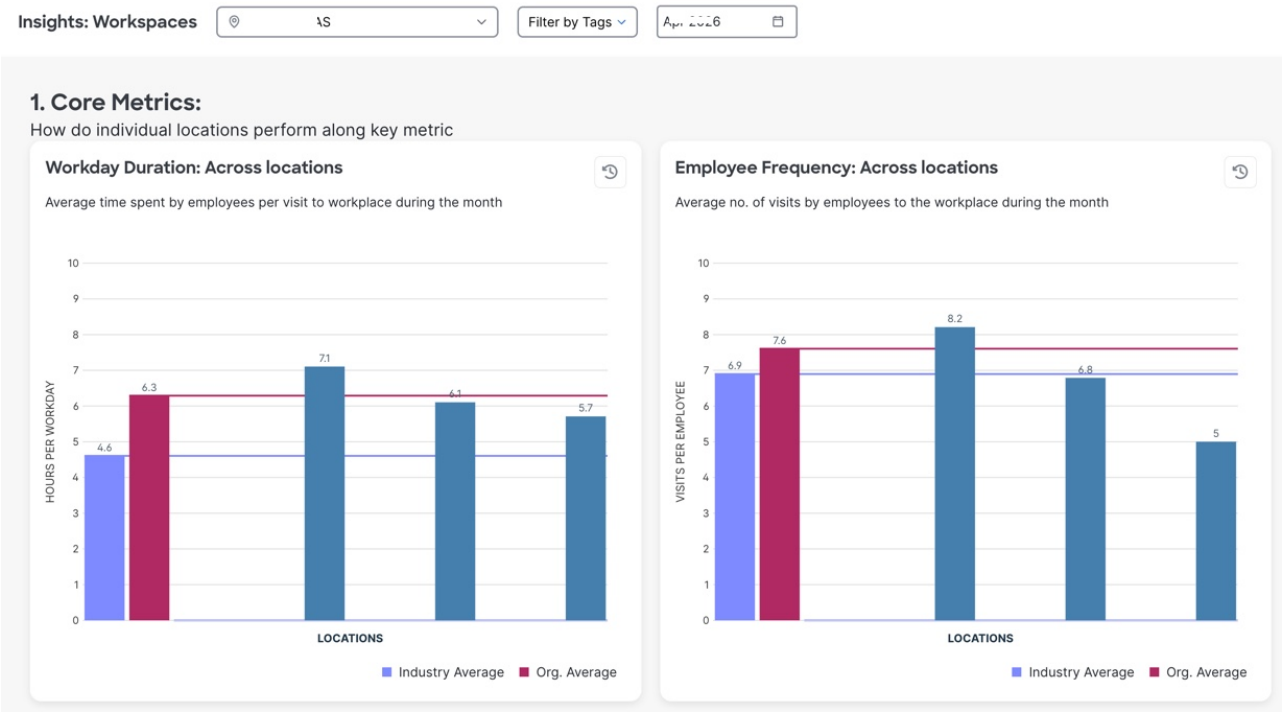
Procedure

Step 1 From the **Dashboard** drop-down list (left navigation pane of the Cisco Spaces **Home** page), choose **Visitor Trends**.

Step 2 In the left navigation pane, click **Monthly Insights**.

The Visitor Trends report is displayed.

Figure 25: Visitor Trends Report



Step 3 Specify the location, tag, and month for which you want to view the report in the corresponding drop-down list at the top of the window.

Note

- By default, the report is displayed for the entire organization. If you do not have access at the organization level, the report is shown for the top-level location to which you have access. You can filter the locations up to the network level.
- The percentage or count described in the report for a filtered location is the total or average of all its child locations. For example, if the filtered location is a network, the number of visits shown for the network will be the total of number of visits for all the floors in that network.
- If the customer has a retail business, the title **Retail** displays along with **Visitor Trends** at the top of the **Visitor Trends** window. For the **Workspaces** vertical, the title **Workspaces** displays along with **Visitor Trends**. For other businesses, **Generic** is displayed.

Benchmarks

Organization Benchmark: Displays the average value for the entire organization. For example, if the organization is Cisco, the Organization Benchmark for "Average Visit Duration" shows the "average visit duration" for Cisco.

Industry Benchmark: Displays the average value for the industry to which your business belongs. For example, if you are in the retail sector, in the **Visit Duration Distribution** graph, the average visit duration for retail is displayed. The industry benchmark average value is restricted to the data obtained from other clients who have installed Cisco Spaces.

Country Benchmark: Displays the average value for the locations tagged under the particular country. For example, if you choose the U.S. as the tag in the **Average Visit Duration** graph, a bar corresponding to the U.S. is displayed which is the average visit duration for all the locations tagged under the U.S. Besides this, the total number of locations associated with the country tag is also displayed. If the locations under the particular country tag are associated with any other tag, in certain graphs such as **Average Visit Duration**, the average value for that tag is also shown.

State Benchmark: Displays the average value for the locations tagged under that particular state. In certain reports, if you select a state tag, two additional bars are displayed. One bar displays the average value with the state name, and the other bar displays the same average value with the total number of locations in the state. For example, the **Average Visit Duration** graph.

Brand Benchmark: Displays the average value for the brand name. A brand name can be used as metadata only for the locations of a particular state. In certain graphs such as **Average Visit Duration**, if you choose a brand the average value for the state to which the brand is tagged is also displayed.

Filtered Location Benchmark: Displays the average value for the filtered location. It appears only if you filter a particular location. For example, if "Cisco San Fransisco" is filtered in the location hierarchy, the "Average Visit Duration" for Cisco San Fransisco is shown along with the organization average. Besides this, the total number of locations under the filtered location is also displayed.

Top and Bottom 3 locations: Displays the top tree and bottom three child locations.

Important Locations: Displays the child locations that are top in the overall ranking for various parameters such as intent rate, acquisition rate, visit distribution, visit frequency, and so on. The top five important locations are shown in the graphs.

Note

- The country, state and brand benchmarks are displayed based on the data for the particular customer.
- When you filter the report for a brand, do not filter a state name that is not associated with it.
- Do not filter the report for two brands simultaneously.
- By default, the report is shown for the top and bottom three locations. You can view the report for the important locations by clicking the toggle switch at the top right of the page.
- You can tag the locations under country, state, and brand benchmarks by defining metadata for the locations.

Report Tabs

The Visitor Trends report includes the following tabs:

- **Group Tab**: By default, the report is shown for Group View and displays the report for the entire organization.
- **Historical Tab**: Displays the report that shows the average values for the last twelve months. In most of the reports, average of the last twelve months is shown along with the average for each month. The industry and organization average are also shown based on the report. You can access the historical view, by clicking the **Toggle Historical View** button at the far right of the Visitor Trends window.
- **Comparative Tab**: When you filter a location, the Comparative tab displays and the report is displayed for that particular location along with the organization benchmark.

Visitor Trends (Business Metrics)

Performance Benchmarking: Performance on Core Metrics related to Peers

Note The Visitor Trends report for the **Workspaces** vertical is different from the following one. For information on theVisitor Trends report for the **Workspaces** vertical, refer to Workspaces Vertical (Visitor Trends), on page 139.

Visit Duration

Visit Duration: Across Locations

Displays a line graph showing the average visit duration for all your business locations. This report enables you to identify the time that visitors are spending at various locations. Besides this, the average visit duration for the industry and organization is also displayed in the graph.

Visit Duration: Key Locations

Displays a bar graph showing the average duration of visits in key locations. The top and bottom three locations or important locations are shown in this report along with the industry and organization benchmark. If you are filtering a location, the average value for the filtered location is also shown in the report.

Visit Duration: By Sub-brand

Displays a bar graph showing the average visit duration for various brands in your business. Besides this, the industry and organization benchmarks are also displayed in the graph.

Visit Duration: Distribution

Displays a bar graph showing the total number of visits for various Visit Duration ranges. Organization and industry averages are shown in the report.

Visit Frequency

Visit Frequency represents the “number of visits made by the visitors” by the “number of visitors”.

Visit Frequency: Across Locations

Displays a line graph showing the average visit frequency for all your business locations. This report enables you to identify how often visitors are visiting your locations. Besides this, the average visit frequency for the industry and organization is also displayed in the graph.

Visit Frequency: Key Locations

Displays a bar graph showing the average visit frequency in key locations. The top and bottom three locations in visit frequency or important locations with the highest visit frequency are shown in this report along with the industry and organization benchmarks. If you are filtering a location, the average value for the filtered location is also shown in the report.

Visit Frequency: By Sub-brand

Displays a bar graph showing the average visit frequency for various brands in your business. This report enables you to identify which brand is more often visited. Besides this, the industry and organization benchmarks are also displayed in the graph.

Visit Frequency: Distribution

Displays a bar graph showing the total number of visits for various visit frequency ranges. Organization and industry averages are shown in the report.

Diagnostics: Factors that Impact or are impacted by the Core Metrics

Visit Duration by Visit Number

Displays a bar graph showing the time that the visitors spent in the locations for various numbers of visits. This report helps you to identify the change that happens to the visit duration based on the visit count.

Each bar represents the average visit duration of the visitors for various visit numbers. For example, the bar for seven represents the average visit duration of the visitors who have visited the locations seven times during the specified month.

Repeat Visitors: Across Locations

Displays a line graph showing the percentage of repeat visitors for all the locations. The organization and industry benchmark for repeat visitors is also shown in the report.

Repeat Visitors: Key Locations

Displays a bar graph showing the repeat visitor percentage for key locations. The top and bottom three locations in repeat visitors or important locations with the highest repeat visitors are shown in this report along with the industry and organization benchmarks for repeat visitors. If you are filtering a location, the average value for the filtered location is also shown in the report.

Visit Recency: Across Locations

Displays a line graph showing the gap between the visits of the repeat visitors for various locations. The visit recency is shown in the number of days. Besides this, the industry and organization benchmark for visit recency is also shown in the report.

Visit Recency: Key Locations

Displays a bar graph showing the gap in the number of days between the visits of the repeat visitors for key locations. The top and bottom three locations in visit recency or important locations are shown in this report along with the industry and organization benchmarks.

Repeat Visitors: By Sub-brand

Displays a bar graph showing the percentage of repeat visitors for various brands in your business. This report enables you to identify the location with which the brand is repeatedly visited the most. Besides this, the industry and organization benchmark for repeat visitors is also displayed in the graph.

Visit Recency- By Sub-Brand

Displays a bar graph showing the visit recency (gap in days between the two visits of a repeat visitor) for various brands in your business. The industry and organization benchmark for visit recency is also displayed in the graph.

Visit Distribution: Hour of the Day

Displays a bar graph showing the daily visits in the organization (average of all the locations of the organization) during various hours of the day. This report enables you to identify at what hour of the day there are more visits to the locations.

Each bar in the graph represents “the percentage of visits that occurs at that particular hour of the day” among “the total daily visits”. For example, the bar for 2:00 PM represents the percentage of visits that occurs at 2:00 PM among the average total daily visits.

Visit Distribution: Day of the Week

Displays a bar graph showing the average daily visits in the organization during various days of the week. This report enables you to identify on which day of the week there are more visits.

Each bar in the graph represents “the percentage of visits that occurs on that particular day of the week” among “the average total weekly visits”. For example, the bar for “THU” represents the “percentage of visits that occurs on Thursdays” among “the total number of weekly visits”.

Size of the Store and Visit Duration

Displays a graph showing the visit duration based on the square foot area of the locations. This report enables you to identify the influence the size of a location has on the time spent by visitors in the location.

In the graph, the blue dot in the graph represents the three child locations that have the highest visit duration and the three child locations that have the lowest visit duration. The grey dot in the graph represents other

child locations. Each dot represents the total square foot area of that particular child location and its average visit duration.

Size of the Store and No. of Visits

Displays a graph showing the number of visits based on the square foot area of the locations. This report enables you to identify the influence the size of a location has on repeat visits to the location.

In the graph, the blue dot in the graph represents the three child locations that have the highest number of visits and the three child locations that have the lowest number of visits. The grey dot in the graph represents other child locations. Each dot represents the total square foot area of that particular child location and its average number of visits.

Retail Experience Grid

Displays a graph showing a consolidated report of the visit duration and visit frequency for the entire month from all the locations. The graph displays only root locations and group locations. The visit duration is displayed on the X-axis and the visit frequency is displayed on the Y-axis. **Retail Experience Grid** is available only for the retail vertical.

Workspaces Vertical (Visitor Trends)

Campus-level computation is implemented for the **Workspaces** vertical. Earlier, network nodes in the location hierarchy were used to derive metrics. To improve the quality of the data reported for the **Workspaces** vertical, campus nodes are used to track visits and derive insights. In most real-time deployments for enterprises and universities, people move between multiple buildings that are close by within a campus. This behavior of people moving between networks is the motivation behind moving to the campus node as the single contiguous space to track visits and derive insights.

Note

- If you select a campus node from the **Location** option, campus average displays for the following charts: **Workday Duration**, **Employee Frequency**, **Density Index**, **Entry Time** and **Exit Time** charts.
- By default, the campus and group location data are displayed at the root-level view. Network location data displays when no campus location is defined in the location hierarchy.

The **Visitor Trends** window for **Workspaces** vertical displays the following information:

Core Metrics: How do individual workspace locations perform along key metric

Workday Duration

- **Workday Duration**: The average number of hours the employees spent in the workplace is shown in this report.
- **Workday Duration: Distribution**: The time spent by an employee at the workplace as a percentage of visits is shown in this report.

Employee Frequency

- **Employee Frequency**: The average frequency at which the employees visited the workspaces are shown in this report.

- **Employee Frequency: Distribution**: The number of visits by each employee to the workplace is shown in this report.

Employees

- **Employees: %Share By floor**: The number of employee visits to a particular floor as a percentage is shown in this report. This information displays for location view.
- **Employees: %Share By zone**: The number of employee visits at various zones as a percentage is shown in this report. This information displays for location view.

Presence

- **Presence: By floor**: The employee presence in manhours by floor is shown in this report. This information displays for location view.
- **Presence: By zone**: The employee presence in manhours by zone is shown in this report. This information displays for location view.

Visit Duration

- **Visit Duration: By floor**: The time spent by an employee on each floor during a workday is shown in this report. This information displays for location view.
- **Visit Duration: By zone**: The time spent by an employee at each zone during a workday is shown in this report. This information displays for location view.

Density

- **Density: By floor**: The employee presence per 1000 squarefoot on each floor in the workplace is shown in this report. This information displays for location view.
- **Density: By zone**: The employee presence per 1000 squarefoot at each zone in the workplace is shown in this report. This information displays for location view.
- **Density Index**: The monthly employee presence (man-hours) per 1000 squarefoot at the workspace is shown in this report.

Diagnostics: Analysis of factors that impact or are impacted by the core metrics

Entry Time

- **Entry Time**: The average time at which employees enter the workspaces are shown in this report.
- **Entry Time: Distribution**: The percentage of employees who entered the locations at various hours of the day along with the industry and organization average percentage for each hour of the day is shown in this report.

Exit Time

- **Exit Time**: The average time at which employees exit the workspaces are shown in this report.
- **Exit Time: Distribution**: The percentage of employees who exited the locations at various hours of the day along with the industry and organization average percentage for each hour of the day is shown in this report.

Employee Presence

- **Employee Presence: Hour of Day**: The percentage of employees present at the workspaces at various hours of the day along with the industry and organization average percentage for each hour of the day is shown in this report.
- **Employee Presence: Day of the Week**: The percentage of employees that were present at the workspaces on various days of the week along with the industry and organization average percentage for each day of the week is shown in this report.

Guest Presence

- **Guest Presence: Hour of Day**: The percentage of guests present at the workspaces at various hours of the day along with the industry and organization average percentage for each hour of the day is shown in this report.
- **Guest Presence: Day of the Week**: The percentage of guests present at the workspaces on various days of a week along with the industry and organization average percentage for various days of a week is shown in this report.

Education Vertical (Visitor Trends)

Cisco Spaces supports a new vertical called **Education** in the **Visitor Trends** app. All the key charts reflect information based on student metrics. The **Education** vertical chart resembles all the metrics similar to the **Workspaces** vertical.

The Visitor Trends window for **Education** vertical will have the following information:

Core Metrics: How do individual locations perform along key metric

Visit Duration

- **Visit Duration: Across Locations**: The average time spent by students per visit to the university during the month is shown in this report.
- **Visit Duration: Distribution**: The time spent by a student at university as a percentage of visits is shown in this report.

Student Frequency: Across Locations

- **Student Frequency: Across Locations**: The average number of visits by students to the university during the month is shown in this report.
- **Student Frequency: Distribution**: The number of visits by a student at university as a percentage of visits is shown in this report.

Student

- **Student: %Share By floor**: The number of students visits at a particular floor as a percentage is shown in this report. This information displays for location view.
- **Student: %Share By zone**: The number of students visits at various zones as a percentage is shown in this report. This information displays for location view.

Presence

- **Presence: By floor**: The student presence in man-hours by the floor is shown in this report. This information displays for location view.
- **Presence: By zone**: The student presence in man-hours by zone is shown in this report. This information displays for location view.

Visit Duration

- **Visit Duration: By floor**: The time spent by a student on each floor during a workday is shown in this report. This information displays for location view.
- **Visit Duration: By zone**: The time spent by a student at each zone during a workday is shown in this report. This information displays for location view.

Density

- **Density: By floor**: The student presence per 1000 square feet on each floor is shown in this report. This information displays for location view.
- **Density: By zone**: The student presence per 1000 square feet at each zone is shown in this report. This information displays for location view.
- **Density Index**: The monthly students' presence (man-hours) at the university area per 1000 square feet is shown in this report.

Diagnostics: Analysis of factors that impact or are impacted by the core metrics

Entry Time

- **Entry Time: Across Locations**: The average entry time of students across locations is shown in this report.
- **Entry Time : Distribution**: The number of students in university at a specific entry time (hour of the day) as a percentage is shown in this report.

Exit Time

- **Exit Time: Across Locations**: The average exit time of students across locations is shown in this report.
- **Exit Time : Distribution**: The number of students in university at a specific exit time (hour of the day) as a percentage is shown in this report.

Student Presence

- **Student Presence: Hour of Day**: The number of students present during each hour of the day as a percentage is shown in this report.
- **Student Presence: Day of the Week**: The number of students present during each day of the week as a percentage is shown in this report.

Guest Presence

- **Guest Presence: Hour of Day**: The number of guests present during each hour of the day as a percentage is shown in this report.
- **Guest Presence: Day of the Week**: The number of guests present during each day of the week as a percentage is shown in this report.

Pin a Location

If you want to add certain locations as favorites, you can pin those locations. You can pin a maximum of three locations at a time. By default, all graphs display the value for the pinned locations, if you have added pin locations. In the bar chart, each pin location is represented by a bar.

To pin a location, perform the following steps:

Procedure

Step 1 In the **Visitor Trends** window, click the **Pin Locations**.

Step 2 In the **Pin Locations** window, select the locations that you want to pin.

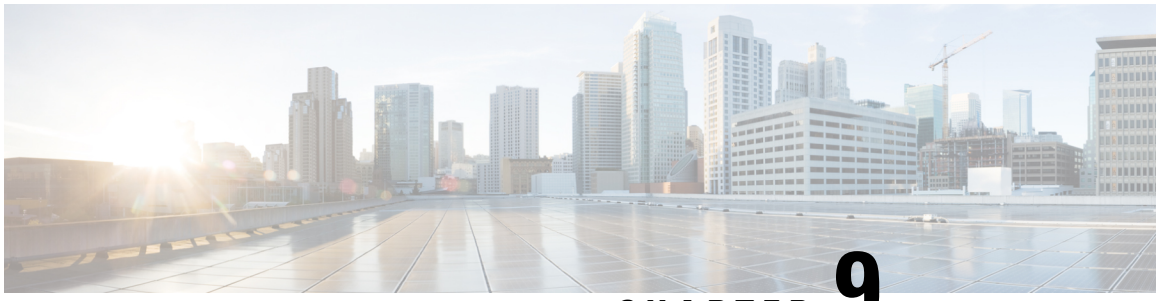
Step 3 Click **Apply**.

Location-Based RBAC

A location-based RBAC role is a user access control setting that

- restricts a user's access to data and features based on assigned physical locations,
- enables administrators to specify which locations a role applies to during role creation or user invitation, and
- ensures that users can view only the data for the locations to which they are invited.

For more information, refer to Location-Based RBAC (Role-Based Access Control) in Cisco Spaces, on page 310.



CHAPTER 9

Cisco Spaces: Live Occupancy App

This chapter describes about the **Live Occupancy** app.

- **Live Occupancy** Overview, on page 145
- WiFi Occupancy, on page 146
- Camera Occupancy, on page 148
- Density Rules, on page 150
- Settings, on page 157
- Location-Based RBAC, on page 159

Live Occupancy Overview

The **Live Occupancy** app provides you the **Live Occupancy** report that shows the details of visitors currently present at your locations. Using the **Live Occupancy** app, you can also create **Density Rules** through which you can send notifications to business users such as employees based on the visitor density or device count in the business locations.

The **Live Occupancy** app is enhanced to address issues with counts when there are any changes in the **Location Hierarchy**. Prior to this enhancement, changes in **Location Hierarchy** such as adding new locations, removing existing locations or updating vital parameters such as **TimeZone** introduced stale or incorrect counts for Wi-Fi.

With this enhancement, the **Presence** chart count gets reset (removes all existing numbers until the current time) for the present day because the counts are invalid after the **Location Hierarchy** changes.

The **Live Occupancy** app is available for these license types:

- ESSENTIAL
- EXTEND
- SWITCH_EXT
- SMART_VENUES
- SMART_OPERATIONS
- SMART_OPERATIONS_BASE
- ADVANTAGE
- UNLIMTED

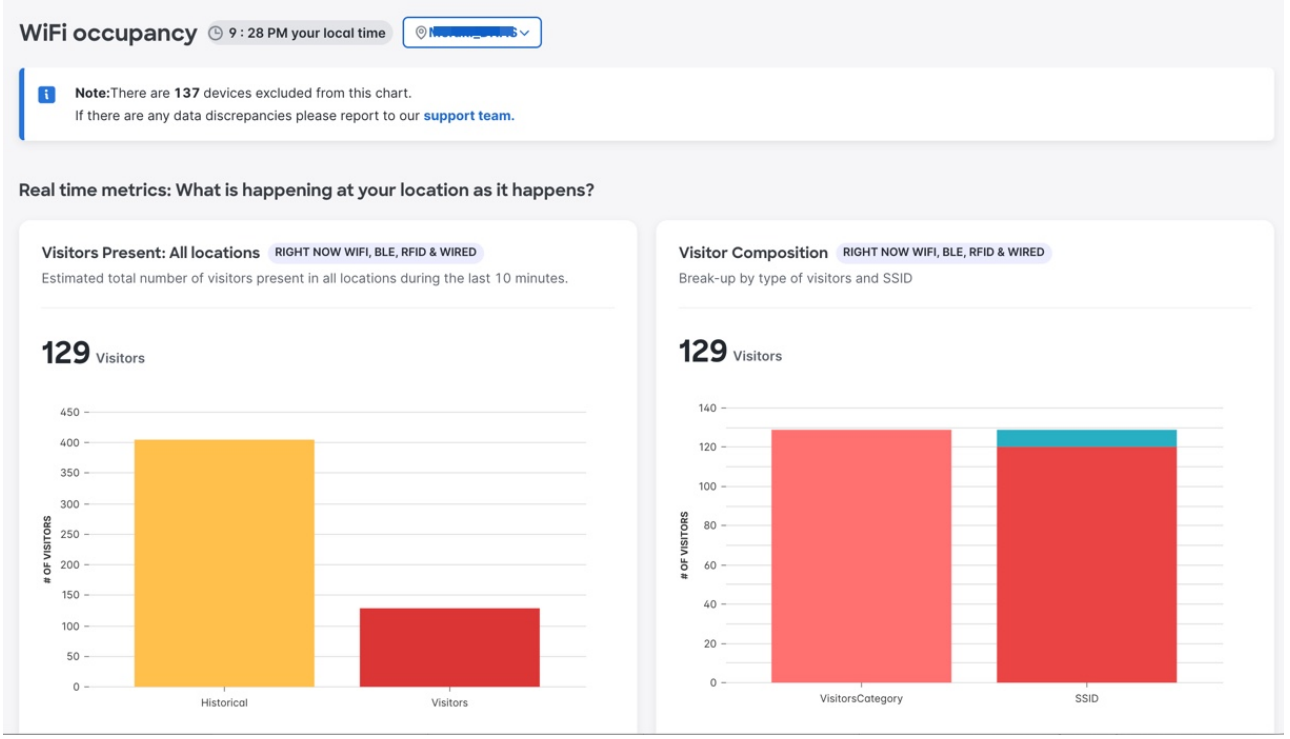
- PREMIER_W
- PREMIER_CW

WiFi Occupancy

The **WiFi occupancy** report displays the details of the visitors currently present at your locations. By default, the report shows the details of visitors currently present at all locations. You can filter upto the floor level.

The **WiFi occupancy** is enhanced to show the count of excluded devices that are not considered as visitors or filtered during data processing. The excluded device count is displayed as a message in the **Note** section of the **WiFi occupancy**.

Figure 26: Live Occupancy App



Note

- If a location is removed or modified in the location hierarchy or timezone is changed, the existing **Presence** chart count is reset.
- For BLE processing:
  - BLE group information should be received as part the IoT updates
  - RSSI value should be greater than -85
- For probing devices:
  - **Cisco Connector** and other device types: RSSI value should be greater than -70
  - **Cisco Meraki**: RSSI value should be greater than -100.

  Only those probing devices meeting the specified signal strength thresholds are allowed to share the device location update events as part of the Firehose data stream.

Viewing the Live Occupancy Report

To view the **Live Occupancy** report, perform these steps:

Procedure

Step 1 In the Cisco Spaces Dashboard, choose **Live Occupancy**.

The **Live Occupancy** app is displayed.

Step 2 From the **Location** drop-down list, select the desired network location.

The **Live Occupancy** report for the selected network location is displayed.

The local time of your system is displayed under the **Live Occupancy** section at the top of the report.

The **Live Occupancy** report displays these charts:

- **Visitors Present: All locations**: Displays an estimated total number of visitors, during the last 10 minutes, in the filtered location including its child location.
- **Visitor Composition**: Displays the composition of active visitors, in percentage, by SSID category (employee, guest, etc.) and by SSID (top 5 SSIDs).
- **Visitors Present: All Locations**: Displays a trend of the total number of visitors during the last 10 minutes for the filtered location.
- **Visitors Present: Map View**: Displays the location-wise count of active visitors in the child locations of the filtered location.
  - **Map View**: The child locations of the filtered location are shown in the world map along with the total number of visitors in each of those child locations.
    - **Floor map view**: Select a specific floor to refer to the chosen floor map view as well.

If the selected location has a map, imported from Cisco CMX, which is uploaded to Cisco Spaces, you can view the floor and the total number of visitors on the displayed floor.

- **List View**: The child locations of the filtered location are listed, and the number of current visitors for each child location is shown against that location.

Note

- An "active visitor" can be any visitor who is present at the location during the last 10 minutes and is connected to the network (WLAN or SSID).
- If a device has a dwell time lesser than a minute, during the 10-minute window, it is excluded from the Live Occupancy report.
- The average value for the last 51 weeks is shown as historical data for each chart in the report.

Camera Occupancy

The Camera occupancy option shows the camera occupany report for your locations based on the data captured by the Meraki Cameras installed in your locations. This report is available only if you have configured Meraki Camera for Cisco Spaces using the **Camera** option in **Setup**.

For more information on configuring Meraki Camera, refer to the Set up Cisco Spaces to Work with Cisco Meraki Camera, on page 355.

When a person comes under the vicinity of the Meraki Camera, an OID is assigned and the user movement is tracked. Meraki Camera then sends the respective coordinates to Cisco Spaces. Cisco Spaces compares the coordinates with the trip wire coordinates and calculates the corresponding entry/exit points.

The **Camera occupancy** app is refreshed every 30 seconds and takes approximately three minutes to update the latest count on the report window.

Note The camera occupancy report supports Cisco Meraki MV93 Cloud-Managed Smart Camera.

View Camera occupancy report for meraki camera

To view the Camera occupancy report for Meraki Camera, perform these steps:

Procedure

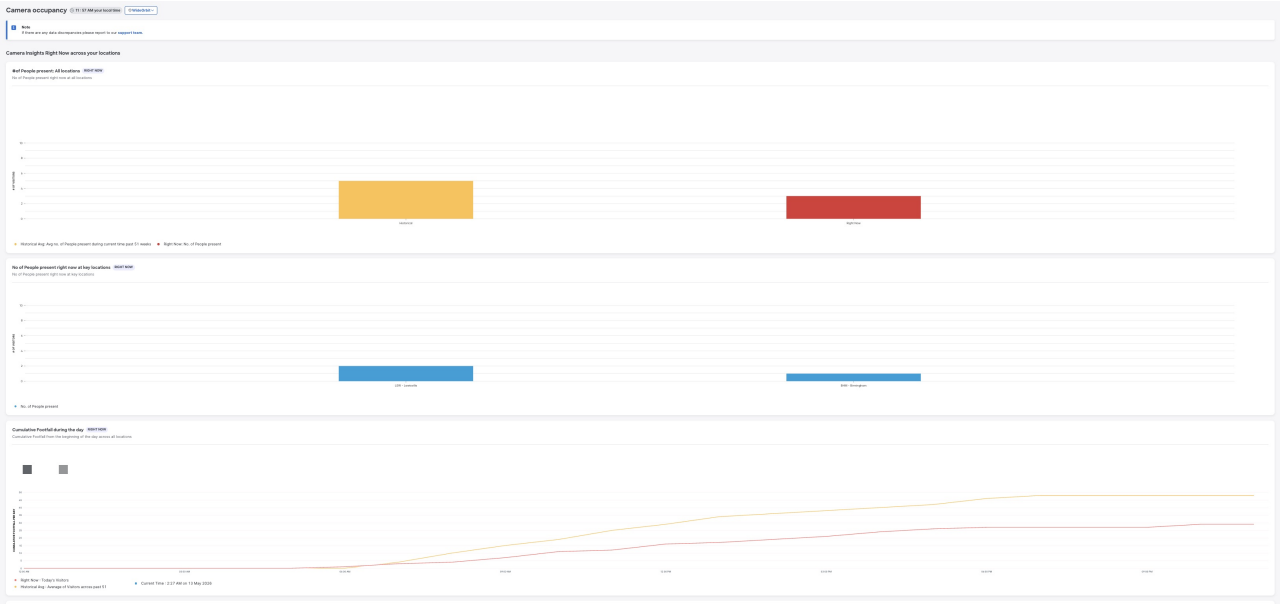
Step 1 In the Cisco Spaces dashboard, choose **Live occupancy**.

The **Live occupancy** window appears.

Step 2 Click the three-line menu icon displayed at the top-left of the window, and choose **Camera occupancy**.

The **Camera occupancy** window appears with the Live Occupancy report for Meraki Camera.

Figure 27: Camera occupancy report



Step 3 If required, from the **Location** drop-down list, select the location for which you want to view the report.

Note By default, the report will be show for the root location.

The report will be having these details:

- Your local time will be displayed at the top of the window, and the data in the report will be shown for this time.
- **No of people present: All locations**: Displays a bar graph that shows the total number of people currently present at the selected location and its child locations. The average number of people that were present at this time during the last 51 weeks at the selected location and its child locations is shown as Historical Average. The total number of people currently present will "Total number of people entered during the last 15 minutes through the tripwire entry for the cameras in the location" - "Total number of people exited during the last 15 minutes through the tripwire exit for the cameras in the location".
- **No of People present right now at key locations**: Displays a bar graph that shows the total number of people currently present at each of the child locations. If the total number of locations are more than or equal to 15, it will display the count for top and bottom three locations. This graph will appear only for the locations other than Network, Floor and Zone. The total number of people currently present will "Total number of people entered during the last 15 minutes through the tripwire entry for the cameras in the child locations" - "Total number of people exited during the last 15 minutes through the tripwire exit for the cameras in the child locations".
- **# of the people present: Key Cameras**: Displays a bar graph that shows the total number of people currently present for each Camera in the filtered location. If the total number of Cameras are more than Six, it will display the count for top and bottom three Cameras. This graph will appear only for network, floor and zone level locations.

- **# of the people present: Key Cameras Zones**: Displays a bar graph that shows the total number of people currently present for each camera zones defined for the cameras in the filtered location. If the total number of Camera Zones are more than Six, it will display the count for top and bottom three Camera Zones. This graph will appear only for network, floor and zone level locations.
- **Cumulative Footfall during the day**: Displays a line graph that shows the total footfall during each hour of the day on which the Live Occupancy report is viewed, in a cumulative manner. For example, the total number of footfall at 3 am will be total number of footfall that occurred from 00 am to 3 am.



Note The graph is shown based on the time zone of the Network, Floor and Zone level locations. For example, if the root location XYZ has network locations in California, Tokyo and Bangalore, the report will display the data for these networks based on their curent time. When it is 8.am at India, Japan will be at 11.30 am on the same day and California will still be on previous day 7.30 pm. So if your are viewing the **Camera occupancy** report at 8 am IST, two graphs will be shown in the **Cumulative Footfall during the day** section. One with cumulative footfall count for Bangalore at 8.am and Tokyo at 11.30 am (as both are on same day), and another graph with cumulative footfall count for California at 7.30 pm on 19/07/2020.

- **Map View**: The location selected for the report, and its child locations are displayed in the Global Map, along with the count of visitors currently present at these locations in the **Map View**. You can also know the present visitor count as a hierarchy using the **List View**.



Note The **# of the people present: Key Cameras Zones** chart will be based on the people on camera's vicinity, and all the remaining charts will be based on entry and exit of people through tripwire line drawn for the cameras.

What to do next

You can go back to the **Camera occupancy** report using the **WiFi occupancy** option in the three-line menu that appears at the top-left of the window.

Density Rules

Density Rule enables you to track the density of unique devices or visitors in your business locations.

The **Density Rule** option allows you to create rules that trigger notifications to the business users such as building administrators based on the density of visitors, count of unique devices, or occupancy in the business locations. You can configure notifications to send through SMS, email, Cisco Webex Teams, or using Trigger API.

This rule can be used to monitor the visitors in your locations to maintain the COVID 19 protocols, and can also be used to measure the impact of COVID 19 in your locations.

The **Density Rules** option also allows you to create rules that trigger notifications to business users based on the number of people captured by the Meraki Camera located in the business location.

To create a Density Rule, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, choose **Live Occupancy**.

The **Live Occupancy** window appears.

Step 2 Click the three-line menu icon displayed at the top-left of the window, and choose **Density Rules**.

Step 3 In the **Density Rule** window that appears, click **Create New Rule** displayed at the top-right of the window.

The **Create Density Rule** window is displayed.

Step 4 In the **Rule Name** field, enter a name for the Density Rule.

Step 5 In the **Sense** area, choose the required filter criteria from the **When a user is connect to WiFi and** drop-down list:

- **density**: Choose this option if you want to send the notifications based on the visitors density in a particular area. You can configure the area in square feet or square meters. If you choose this option, do the following configurations.
  - Set the density limit using the adjacent drop-down lists. You can configure the density limit as "more than" or "less than" a particular value, or as a value range using "between". You can choose "more than", "less than" or "between" from the first drop-down list, and manually enter the "value" or can choose the "value" from the drop-down list in the second field.
  - In the **per** field, specify the area of which the density limit is to be considered by manually entering the value or using the drop-down list. Then, from the adjascent drop-down list, choose the measurement scale. You can specify the measurement in square feet or square meter.
- **count**: Choose this option if you want to send the notifications based on the unique device count in a particular location type such as campus, building (network), floor, or zone. If you choose this option, do the following configurations.
  - Set the device count limit using the adjacent drop-down lists. You can configure the device count limit as "more than" or "less than" a particular value, or as a value range using "between". You can chooose "more than", "less than" or "between" from the first drop-down list, and you can manually enter the "value" or can choose the "value" from the drop-down list in the second field.
  - From the **at any** drop-down list, choose the location type of which the device count limit is to be considered.

  Note Cisco Meraki network and Cisco AireOS/ Cisco Catalyst connected through **Cisco Spaces Connector** or **WLC Direct Connect** will not have **Campus** as a location type. So for these networks, if you are selecting **Campus** as location type, the rule will not be executed.
- **occupancy**: Choose this option if you want to send the notifications based on the occupancy in a particular location.

  You can define the occpancy limit for each location in **Location Hierarchy**.

You can configure to trigger the notification when the occupancy in a location reaches a certain percentage of the occupancy limit defined for that location. If you choose this option, do the following configurations.

- Set the occupancy limit percentage at which the notification is to be triggered using the adjacent drop-down lists. You can configure the occupancy limit percentage as "more than" or "less than" a particular value, or as a percentage range using "between". You can chooose "more than", "less than" or "between" from the first drop-down list, and you can manually enter the "percentage" or can choose the "pertcentage" from the **percent** drop-down list.

Step 6 In the Locations area, specify the locations for which you want to apply the rule.

You can configure to apply the rule for the entire location hierarchy, or a single or multiple locations such as group, floor, or zone. You can add the locations of multiple network types such as Cisco Meraki, Cisco AireOS or Cisco Catalyst in a Density rule.

You can again filter the locations based on the metadata defined for the selected location, or its parent or child locations.

You can either apply the rule for the locations with a particular metadata or exclude the locations with a particular metadata.

Step 7 In the **Schedule** area, specify the period for which you want to apply the rule.

a) Check the **Set a date range for the rule** check box, and in the fields that appear, specify the start date and end date for the period for which you want to apply the Density rule.
b) Check the **Set a time range for the rule** check box, and in the fields that appear, specify the time range for which you want to apply the Density rule.
c) If you want to apply the rule only on particular days, check the **Filter by days of the week** check box, and from the list of days that appears, click the days on which you want to apply the rule.

Step 8 In the **Actions** area, specify the notification frequency and notification mode.

a) From the Notify drop-down list, choose any of the following:

- Only Once: The notification is sent only once to the business user.
- Once In: The notification is sent more than once based on the interval specified. If you choose this option, from the **every** drop-down list choose the interval value, and from the adjascent drop-down list, choose any of the following interval duration:
  - Hour(s): To send the notification once in the number of hours specified.
  - Day(s): To send the notification once in the number of days specified.
  - Week(s): To send the notification once in the number of weeks specified.
  - Month(s): To send the notification once in the number of months specified.

b) Specify the mode for sending notification.

You can send the notification to the customers through Cisco Webex Teams, e-mail, SMS, or to an external API.

For more information on notification types, refer to Notification Type for a Business User, on page 217.

The summary of the rule is shown in the right side of the window.

Note

- If you are using the **Via Email** option, you must ensure to add the e-mail ID entering in the **From** field in the allowed list of e-mail IDs.
- To include the e-mail ID in the allowed list, contact the Cisco Spaces support team.
- If you do not want to use a specific e-mail ID, you can use the default allowed e-mail ID **no-reply@dnaspaces.io**. However, the default ID is not displayed in the dashboard automatically. So, you have to enter it manually.

Step 9 Click **Save and Publish**.

The rule gets published, and is listed in the **Density Rules** window.

If you do not want to publish the rule now, you can click the **Save** button. You can publish the rule at any time later by opening the rule, and clicking the **Save and Publish** button. Also, you can publish the rule by clicking the **Make Rule Live** icon at the far right of the rule in the **Density Rules** window.

What to do next

You can go back to the **Live Occupancy** report using the **Live Occupancy on WiFi** option in the three-line menu that appears at the top-left of the window.

Viewing a Density Rule Report

The Density Rule report enables you to view the report for each Density Rule.

To view a Density Rule report, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click **Live Occupancy**.

The **Live Occupancy** window appears.

Step 2 Click the three-line menu icon that appears at the top-left of the window.

Step 3 Choose **Density Rules**.

The **Density Rules** window appears with all the existing Density rules listed.

Step 4 Click the **Density Rule** for which you want to view the report.

The Density Rule report for that particular rule is displayed.

The **Density Rule** report will have the following details:

- **Rule Summary**
  - **# of times triggered**: Displays the total number of times the notification is triggered for the particular rule.

- **Top 3 locations**: Displays the details of top three locations with highest number of notifications.
  - **Location**: The location name along with its location hierarchy.
  - **# of times triggered**: Total number of times the notifications have been trigered for this location for the particular Density Rule.
  - **most recent**: The date and time at which notification has been triggered recently for this location for the particular Density Rule.

- **Recent Activity**: Lists all the activities occurred for the particular rule. The recent activities will be listed at the top.
  - **Location**: The location name along with its location hierarchy for which the activity has occurred.
  - **time**: The date and time at which the activity has occured.
  - **count of people**: Total number of people that were available in the location when the activity occured
  - **result**: The result of the activity. For example, if a Density Rule is configured to trigger a notification every one hour if the count of people in a location exceeds 10, and at a particular hour the notification is skipped as the count of people is less than 10, the result for the activity will be "Skipped notification due to the interval set".

- **Trigger History**: Shows the notification details for each day of a particular month in the calendar.
  - **Location**: Report will be for **All Locations**.
  - **Month**: Select the month for which you want to view the report using the arrow keys. By default, it will show the month for which the notifications are triggered recently along with the cumulative notification count.
  - **Calendar**: The notifications for various location types (Campus, Building, Floor, Zone) for each date are shown in the calendar. When you click on a date in the calendar, the notification details such as location, time, count of people and result is shown for that particular day.

Testing a Density Rule

To test a Density Rule, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click **Live Occupancy**.

The **Live Occupancy** window appears.

Step 2 Click the three-line menu icon that appears at the top-left of the window.

Step 3 Choose **Density Rules**.

The **Density Rules** window appears with all the existing Density rules listed.

Step 4 Click the three-dot icon that appears at the far right of the Density Rule that you want to test.

Step 5 Choose **Test Rule**.

The **Test Rule** window displays.

Step 6 Click **Yes** to trigger a notification on the selected channels.

A notification is triggered and a success message is displayed.

Step 7 Click **Continue**.

Modifying a Density Rule

To modify a Density rule, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click **Live Occupancy**.

The **Live Occupancy** window appears.

Step 2 Click the three-line menu icon that appears at the top-left of the window.

Step 3 Choose **Density Rules**.

The **Density Rules** window appears with all the existing Density rules listed.

Step 4 Click the three-dot icon that appears at the far right of the Density Rule that you want to test.

Step 5 Choose **Edit Rule**.

The **Edit Rule** window displays.

Step 6 Make necessary changes.

Step 7 To save the changes, click **Save** or to publish the changes, click **Save and Publish**.



Note A live rule will have only the **Save and Publish** button. When you click the **Save and Publish** button, the rule gets published with the changes.

Pausing a Density Rule

To pause a Density rule, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click **Live Occupancy**.

The **Live Occupancy** window appears.

Step 2 Click the three-line menu icon that appears at the top-left of the window.

Step 3 Choose **Density Rules**.

The **Density Rules** window appears with all the existing Density rules listed.

Step 4 Click the three-dot icon that appears at the far right of the Density Rule that you want to test.

Step 5 Choose **Pause Rule**.

The **Pause Rule** window displays.

Step 6 In the window that appears, confirm pausing.

The Density rule is paused.

What to do next

Note To pause multiple Density rules, check the check box for the Density rules that you want to pause, and click the **Pause** button that appears at the bottom of the page.

Restarting a Density Rule

To restart an Density rule, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click **Live Occupancy**.

The **Live Occupancy** window appears.

Step 2 Click the three-line menu icon that appears at the top-left of the window.

Step 3 Choose **Density Rules**.

The **Density Rules** window appears with all the existing Density rules listed.

Step 4 Click the three-dot icon that appears at the far right of the Density Rule that you want to test.

Step 5 Choose **Make Rule Live**.

Note By default the icon name will be **Pause Rule** for all rules. Only for those rules that are paused the icon name changes to **Make Rule Live** .

The Density rule is restarted.

What to do next

Note To restart multiple Density rules, check the check box for the Density rules that you want to restart, and click the **Make Live** button that appears at the bottom of the window.

Deleting a Density Rule

To delete a Density rule, perform the following steps

Procedure

Step 1 In the Cisco Spaces dashboard, click **Live Occupancy**.

The **Live Occupancy** window appears.

Step 2 Click the three-line menu icon that appears at the top-left of the window.

Step 3 Choose **Density Rules**.

The **Density Rules** window appears with all the existing Density rules listed.

Step 4 Click the three-dot icon that appears at the far right of the Density Rule that you want to test.

Step 5 Choose **Delete Rule**.

The **Delete Rule** window displays.

Step 6 In the dialog box that appears, click **Delete Rule**.

The Density Rule gets deleted.

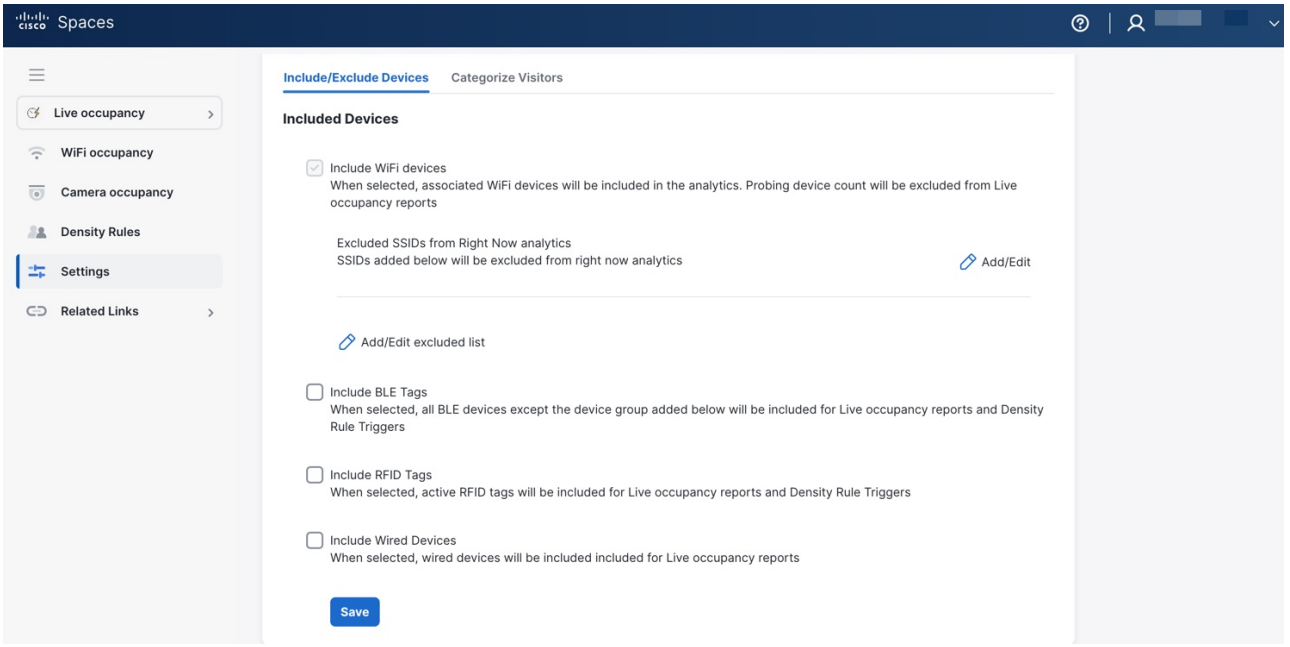
What to do next

Note To delete multiple Density rules, check the check box for the Density rules that you want to delete, and click the **Delete** button that appears at the bottom of the window.

Settings

The **Settings** menu helps you manage devices, SSIDs, and visitors in the **Live Occupancy** app reports. The **Settings** menu includes the **Include/Exclude Devices** and **Categorize Visitors** tabs.

Figure 28: Live Occupancy - Settings



Including or Excluding Devices

Use the **Include/Exclude Devices** tab to select among the following options for Wi-Fi, BLE, and RFID devices for the **Live Occupancy** reports:

- Wi-Fi devices option is included by default and you cannot deselect the same.

  To exclude devices connected to specific SSIDs from the **Live Occupancy** analytics, click **Add/Edit** or **Add/Edit excluded list** and select the desired SSIDs from the **Exclude SSIDs** list.

  If you configure an SSID for exclusion here, clients connected to that SSID are excluded not only from Live Occupancy but also from other applications that receive data from Live Occupancy, such as Partner Firehose Wi-Fi data (except for the Wi-Fi events `DEVICE_LOCATION_UPDATE`, `DEVICE_PRESENCE`, `DEVICE_ENTRY`, `DEVICE_EXIT`, and `DEVICE_ASSOCIATION`), Space Utilisation floor occupancy metrics, Signage Occupancy Count, and Density rules.

- BLE Tags: To include BLE tags in the **Live Occupancy** reports, select **Include BLE Tags**.

  To exclude specific device groups from the **Live Occupancy** analytics, click **Add/Edit** or **Add/Edit excluded list** and select the desired BLE devices from the **Exclude BLE devices** list.

- RFID Tags: To include RFID tags in the **Live Occupancy** reports, select **Include RFID Tags**.

- Wired Devices: To include wired devices as part of active visitors in the **Live Occupancy** reports, select **Include Wired Devices**. By default, wired devices are excluded.

Note

- If you select RFID and BLE tags, then the corresponding device count is displayed in the **Live Occupancy** report.
- If you configure an SSID to be excluded here, it not only excludes the clients connected to that SSID from **Live Occupancy** but also excludes them from other applications that receive data from **Live Occupancy** such as Partner Firehose Wifi data, Space Utilisation Floor occupancy metrics, Signage Occupancy Count, and Density rules.

Categorizing Visitors

Use the **Categorize Visitors** tab to automatically or manually classify visitors, based on the visitor type, that have joined an SSID. The options available are:

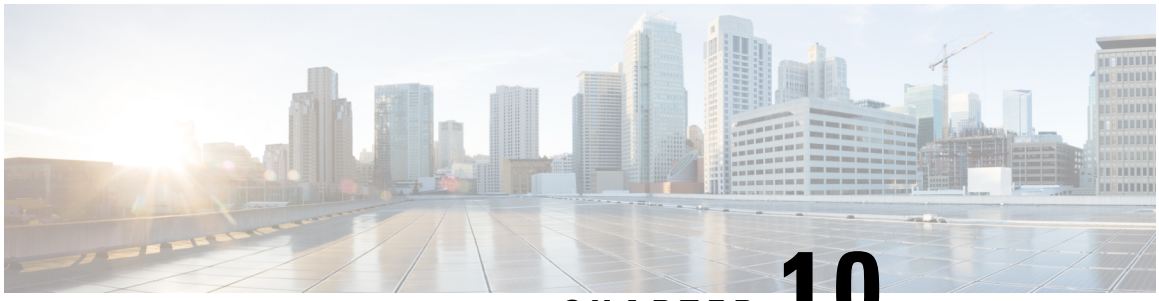
- Auto
- Guest
- Employee
- Custom

Location-Based RBAC

A location-based RBAC role is a user access control setting that

- restricts a user's access to data and features based on assigned physical locations,
- enables administrators to specify which locations a role applies to during role creation or user invitation, and
- ensures that users can view only the data for the locations to which they are invited.

For more information, refer to Location-Based RBAC (Role-Based Access Control) in Cisco Spaces, on page 310.



CHAPTER 10

Cisco Spaces: Camera Metrics App

This chapter describes the Camera Metrics app.

- Camera Metrics, on page 161
- Viewing the Camera Metrics Report, on page 162
- Location-Based RBAC, on page 163

Camera Metrics

The **Camera Metrics** app enables you to view a Metrics report based on the data captured using Meraki Camera. The report is displayed for a particular month.

The **Camera Metrics** app also supports the Cisco Meraki MV93 Cloud-Managed Smart Camera along with the existing Meraki Camera.

Note

- The **Camera Metrics** app provides report only if you have configured Meraki Camera in Cisco Spaces using the **Camera** option in **Setup**. For more information about configuring Meraki Camera, see Set up Cisco Spaces to Work with Cisco Meraki Camera, on page 355.
- For Cisco Spaces user accounts that have not yet configured Meraki Camera or have no data for Meraki Camera, a sample report is shown.
- For Cisco Spaces user accounts that have not yet configured Meraki Camera, a notice "Looks like you haven't setup your Meraki Camera" displays along with the Setup Guide link to navigate to the Meraki Camera configuration window.
- The **Camera Metrics** data is not real-time data and the footfall data takes approximately two hours to reflect in the Cisco Spaces dashboard. The **Presence** and **Peak Presence** charts are updated once the day completes.
- The **Camera Metrics** location filter is available for network and building locations and displays data for the selected location. You can view **Camera Metrics** data at the building or network level by selecting a location.

Authentication Support for Camera Message Queuing Telemetry Transport (MQTT) Brokers

Cisco Spaces cloud is updated to support password-based authentication for receiving MQTT updates from Cisco Meraki cameras. The background network synchronization process will automatically update the authentication details to the Cisco Meraki dashboard.

Viewing the Camera Metrics Report

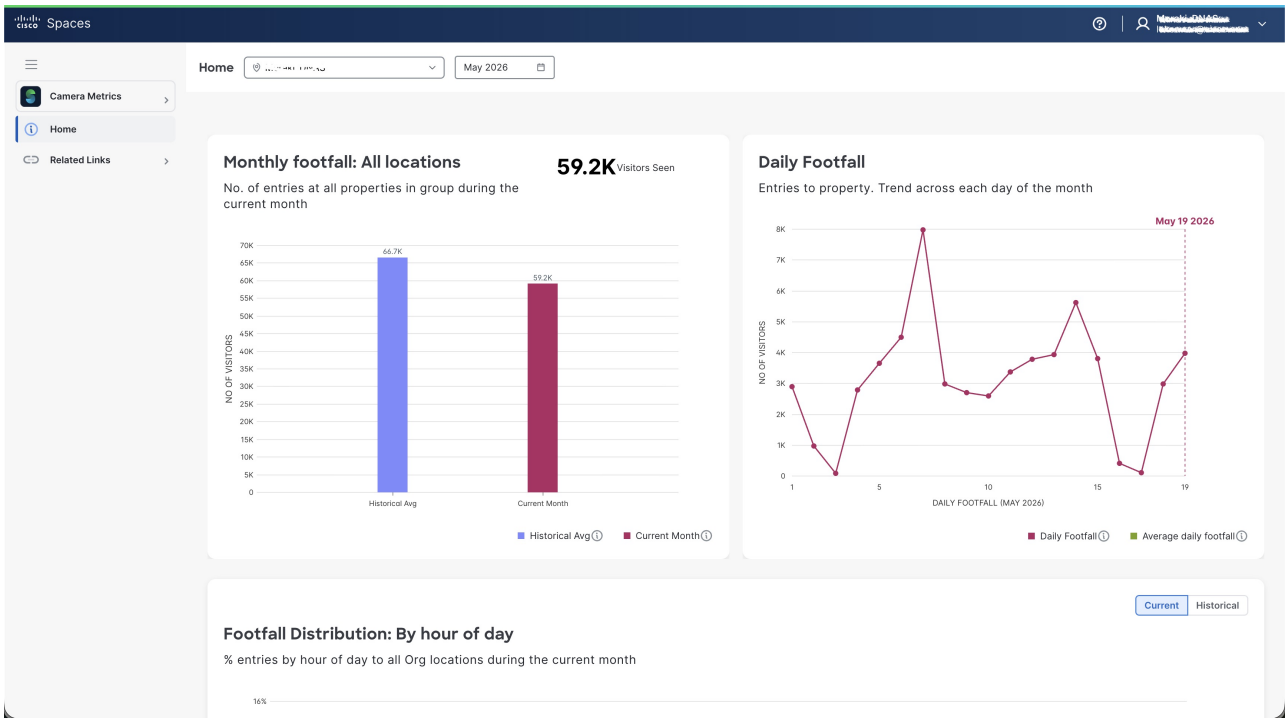
To view the Camera Metrics report, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click **Camera Metrics**.

The Camera Metrics report for the current month is displayed.

Figure 29: Camera Metrics Report



Step 2 (Optional) From the **Location** drop-down list, choose the location for which you want to view the report.

Note By default, the report for the root location is displayed.

Step 3 From the **Month** drop-down list, choose the year and month for which you want to view the report.

The report gets filtered for the selected location and month.

Note As Cisco Spaces has introduced the **Camera** option on 2020, you can select the year starting from 2020 only.

The report includes the following charts:

- **Monthly Footfall: All Locations**: Displays the total footfall count in the filtered location and its child locations during the selected month. Average footfall for the last twelve months in the select location and its child locations is shown as historical average.
- **Daily Footfall**: Displays the total footfall count in the filtered location and its child locations for each day of the selected month. Average daily entries for all the days of the selected month in the selected location and its child locations is shown as Average Daily Footfall.
- **Footfall Distribution : By hour of day**: Displays the average footfall for each hour of the day on the selected month for the filtered location and its child locations as "percentage of the total footfall". You can view the historical average for each hour of the day by clicking the **Toggle Historical View** icon at the top-right of the chart. Historic Average for each hour of the day(average number of people present at the hour of the day in the filtered location and its child locations during the past 12 months) is shown as percentage of total historical average (average number of people present in the filtered location and its child locations during the past 12 months).
- **Presence by hour of day**:Displays the average number of the people present for each hour of the day for the selected month for the filtered location and its child locations. Average number of people that were present on each hour of the day in the filtered location and its child locations during the past 12 months is shown as historical average.
- **Peak Presence : By hour of day**: This graph will be available only for network locations. This graph displays the average number of the people present for each hour of a day on the selected month in a cumulative manner to show the hour of the day with peak count.

Note Ideally, the historical average is shown for charts for last 12 months. However, if you have installed the camera within the last 12 months, the data from the month of installation of camera is considered for historic average.

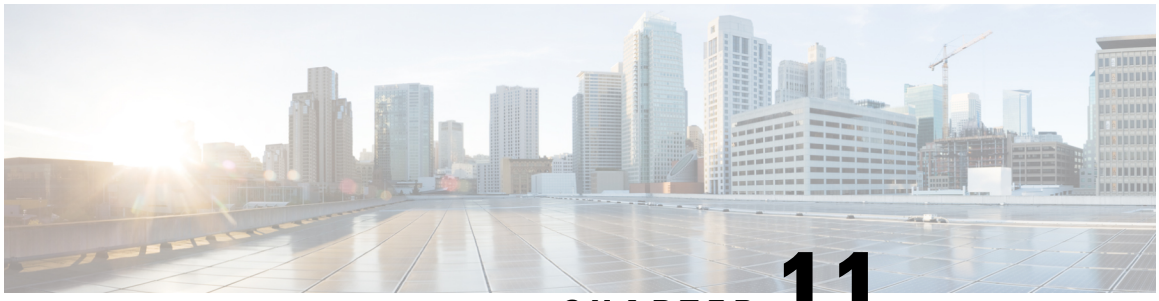
All the charts are based on the entry and exit of visitors through tripwire line drawn for the cameras.

Location-Based RBAC

A location-based RBAC role is a user access control setting that

- restricts a user's access to data and features based on assigned physical locations,
- enables administrators to specify which locations a role applies to during role creation or user invitation, and
- ensures that users can view only the data for the locations to which they are invited.

For more information, refer to Location-Based RBAC (Role-Based Access Control) in Cisco Spaces, on page 310.



CHAPTER 11

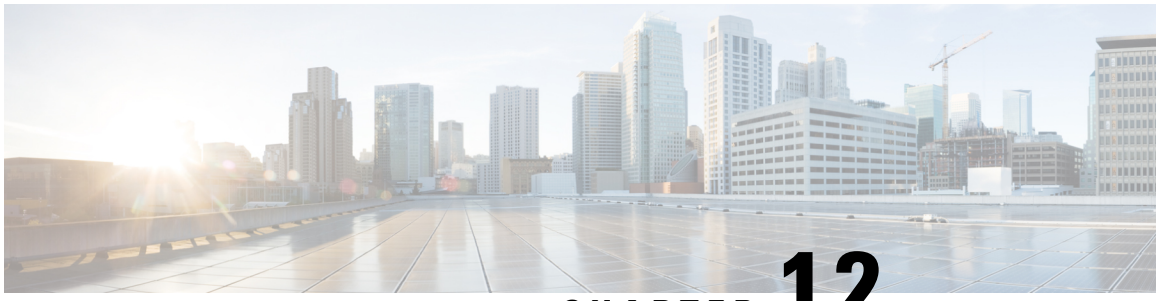
Cisco Spaces: OpenRoaming App

• Overview of OpenRoaming App, on page 165

Overview of OpenRoaming App

OpenRoaming enables secure, seamless, and automatic network connectivity by eliminating tedious Wi-Fi guest onboarding processes and the risk of connecting to rogue SSIDs. This is especially helpful for a mobile device user trying to access the internet because OpenRoaming removes the need to choose between multiple SSIDs, or enter insecure, shared credentials on poorly designed captive portals. With OpenRoaming, user mobility is enhanced by enabling users to connect to the guest network by signing in using a trusted identity provider.

For more information, refer to Cisco Spaces: OpenRoaming Configuration Guide.



CHAPTER 12

Cisco Spaces: Location Analytics App

This chapter describes the Location Analytics Report.

- Overview of Location Analytics App, on page 167
- View Location Analytics Report, on page 169
- Compare Reports, on page 172
- Create Custom Report, on page 173
- Add Widget, on page 177
- Location-Based RBAC, on page 179

Overview of Location Analytics App

The Location Analytics app enables you to understand and analyze footfall, visitors, visit patterns and dwell time distribution across various areas in your building, across regions and different locations. The visits of your employees are also included in the report.

Use the Location Analytics app to view the reports with visits, visitor insights and dwell time distribution data and also create custom reports as per your preferred filter criteria.

The Location Analytics app has two options on the main menu: **Reports** and **Custom Reports**.

Reports

Click **Reports** on the left panel to expand the list and click **Overview** to view the reports. The **Overview** window displays visits, visitor details and dwell time distribution data in both tile and graphical format. You can click the arrow icon on the tile to view the details in graphical format.

Custom Reports

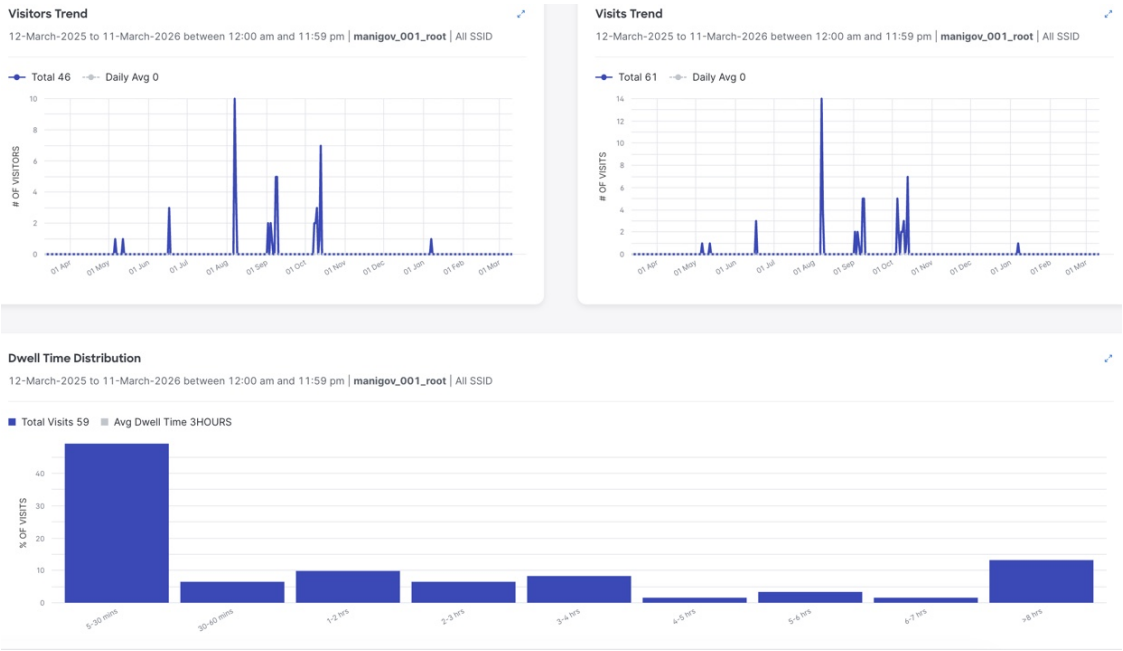
Choose **Location Analytics App** > **Custom Reports** to view and save custom reports. You can create custom reports with the available report type and also with **Path** widget included in the report.

In the Location Analytics app, choose **Reports** > **Overview** to view Location Analytics reports with visitor/visit trends/dwell time distribution in both tile and graphical format. You can also compare reports based on the available filter parameters. For more information, refer to Compare Reports, on page 172.

Note

- Read-only user cannot modify custom reports.

Figure 30: Location Analytics Overview



Note

- By default, a report for all locations, all SSIDs and for the last 365 days is displayed. Use the filters available on top of the window to modify the report as needed.
- If you are new to the Location Analytics app with no data, click **Location Analytics** in the left menu to view the sample reports and understand how visitor details are displayed.

The **Overview** window displays the information related to **Visitors**, **Visits**, **Daily Average Visitors** and **Daily Average Visits** as per the selected parameters.

- **Visitors** are defined as the total number of unique visitors based on the selected criteria.
- **Visits** are defined as the total number of visits for a specific location.
- **Daily Average Visitors** are defined as the daily average calculated by adding the total number of daily visitors for the selected period and then dividing that by the number of days.
- **Daily Average Visits** are defined as the daily average calculated by adding the total number of daily visits for the selected period and then dividing that by the number of days.

The **Overview** window displays the following information in tile format:

- Visitors: Daily Average Visitors
- Visitors: New vs Repeat Visitors
- Visits: Daily Average Visitors
- Visits: Average Dwell Time

The **Overview** window displays the following information in graphical format.

- Visitors Trend
- Visits Trend
- Dwell Time Distribution

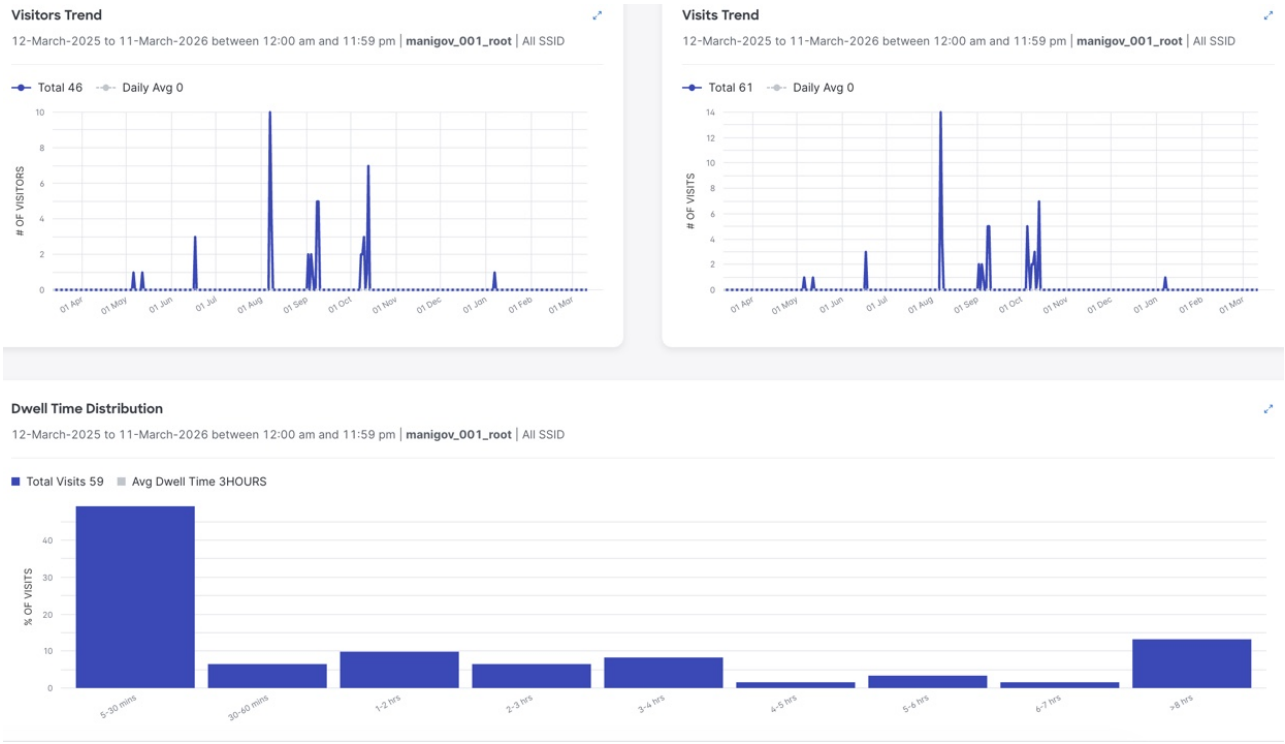
View Location Analytics Report

Procedure

Step 1 In the Cisco Spaces **Home** page, click **Dashboard** and choose **Location Analytics**.
The **Location Analytics Home** page is displayed.

Step 2 From the left panel, choose **Reports** > **Overview**.

The **Overview** window in the Reports menu is displayed.



Note

- By default, the report is displayed for the root location, all SSIDs and for the last 365 days. You can filter the report by location, date range, and SSID.
- The SSID filter option is available only to ADVANTAGE license users; it is not available to the ESSENTIAL and EXTEND license users. However, they can use the date range filter, and filter the locations except the group, floor and zone locations.

Step 3 From the **All Locations** drop-down list, select the location for which you want to view the report.

Note ADVANTAGE license users can view the report for floors and zones. The ESSENTIAL and EXTEND license users can filter only network locations.

Step 4 From the **Date** drop-down list, select the date range for which you want to view the report.

The following options are available:

Table 12: Date Range Options

Date Range	Description
Today	Total number of visits every hour of the current date
Yesterday	Total number of visits every hour of the previous day
Current Week	Total number of visits on each day of the current week
Previous Week	Total number of visits on each day of the previous week
Current Month	Total number of visits on each day of the current month
Previous Month	Total number of visits on each day of the previous month
Current Year	Total number of visits on each day of the current year
Custom	Total number of visits on each day of the time range specified. In the **Custom Date Range** pop-up window, specify the start and end date and click **Apply**.

Note To view the visit details for a particular day, hover over that day on the graph.

Step 5 From the **All SSID** drop-down list, select the SSID for which you want to view the report.

The **Overview** window displays the Location Analytics report as per the selected filter options.

Step 6 View the following information in the Location Analytics report in the tile format:

Table 13: Location Analytics Report Information

Report Item	Description
Visitors	Total number of visitors and the daily average visitors as per the selected filter parameters
Visitors	Total number of visitors as per the selected filter parameters. The count for **New Visitors** and **Repeat Visitors** are displayed separately with percentage information
Visits	Total number of visits and daily average visits as per the selected filter parameters. The count for **Total Visits** and **Daily Avg Visit** are displayed separately with percentage information **Note** • Visits having a duration of less than five minutes are excluded. This helps to exclude transient and transitory visitors, who contribute to inflating the visitor and visits count. • Visits having a duration of more than 1440 minutes are excluded. This helps to exclude devices that are always on, and contribute to inflating the average duration metric.
Dwell Time Distribution	The dwell time break-up for the visits occurred in the filtered location during the period specified for selected SSIDs
Path widget	The visitor traverse pattern between locations and also the percentage of visits at various floors or zones within the same **Network**. In your custom report, hover the mouse over any floor or zone in the **Path widget** to view the exact visit count. You can filter using only the locations available below the **Network** to view the path analytics. The **Path widget** is available only to the ADVANTAGE license users.



Note You can view the **Visitors Trend**, **Visits Trends** and **Dwell Time Ditribution** information in graphical format also.

Compare Reports

You can compare Location Analytics reports based on various filter parameters and thereby analyze the trends and visitor pattern. To compare reports, choose **Location Analytics** > **Reports**. The Reports menu has the following three options: **Compare Locations**, **Compare Dates** and **Compare SSIDs**.

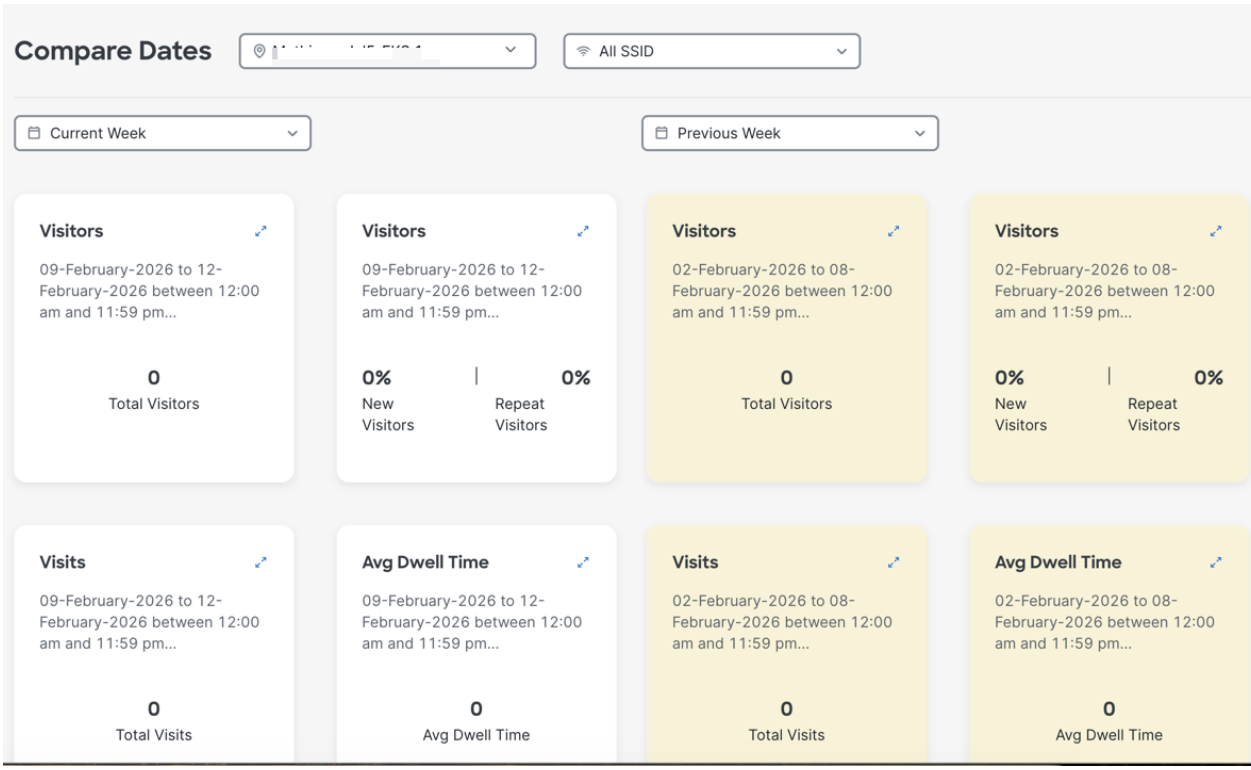
- **Compare Locations**: Use this tab to compare two location reports and view the visitors' trend. By default, two locations with most number of visitors are considered for the report. Visitor data must be available for atleast two network locations to display as charts. In the **Compare Locations** window, from the **Locations** drop-down list displayed at the top, select the locations to compare and view the reports.
- **Compare Dates**: Use this tab to choose two specific dates or date range and view the report. By default, the current week is selected as date range for the first report and previous week for the second report. In the **Compare Dates** window, from the **Date** drop-down list displayed at the top, select the required date range options to compare and view the reports.
- **Compare SSIDs**: Use this tab to compare two different SSIDs and view the visitors' trend. By default, two SSIDs with most number of visitors are considered for the report. In the **Compare SSIDs** window, from the **SSIDs** drop-down list displayed at the top, select the required SSIDs to compare and view the reports.

Depending on the selected compare options, the Location Analytics reports are displayed on the left and right side of the Location Analytics window. You can compare the Location Analytics report displayed on the left side (white background) aganist the report displayed on the right side (yellow background).



Note You can also use the filter parameters available on the top of the window to view the Location Analytics report.

Figure 31: Compare Report Options



Create Custom Report

Use the **Custom Reports** option to create custom location analytics reports based on filters that you can apply to the default report types.

You can create custom reports based on the following default report types that are available:

The **Custom Reports** feature helps to view the default location reports and also create custom-tailored reports. The **Custom Reports** window displays all available reports, default overview reports and reports with compare options along with the number of reports in each category.

The three categories are:

- All Reports
- Overview
- Compare Reports (reports with all categories)

Use the **Custom Reports** feature in the Location Analytics app to create a report with the default filter parameters and save this as the default Location Analytics report for reference. While creating the default Location Analytics report, default filter parameters are considered such as all locations, last 365 days date range and all available SSIDs. The filter parameters at a global level are not available to filter this default Location Analytics report.

In addition to the default Location Analytics report, you can create custom reports by including any one available report type and multiple widget filters.

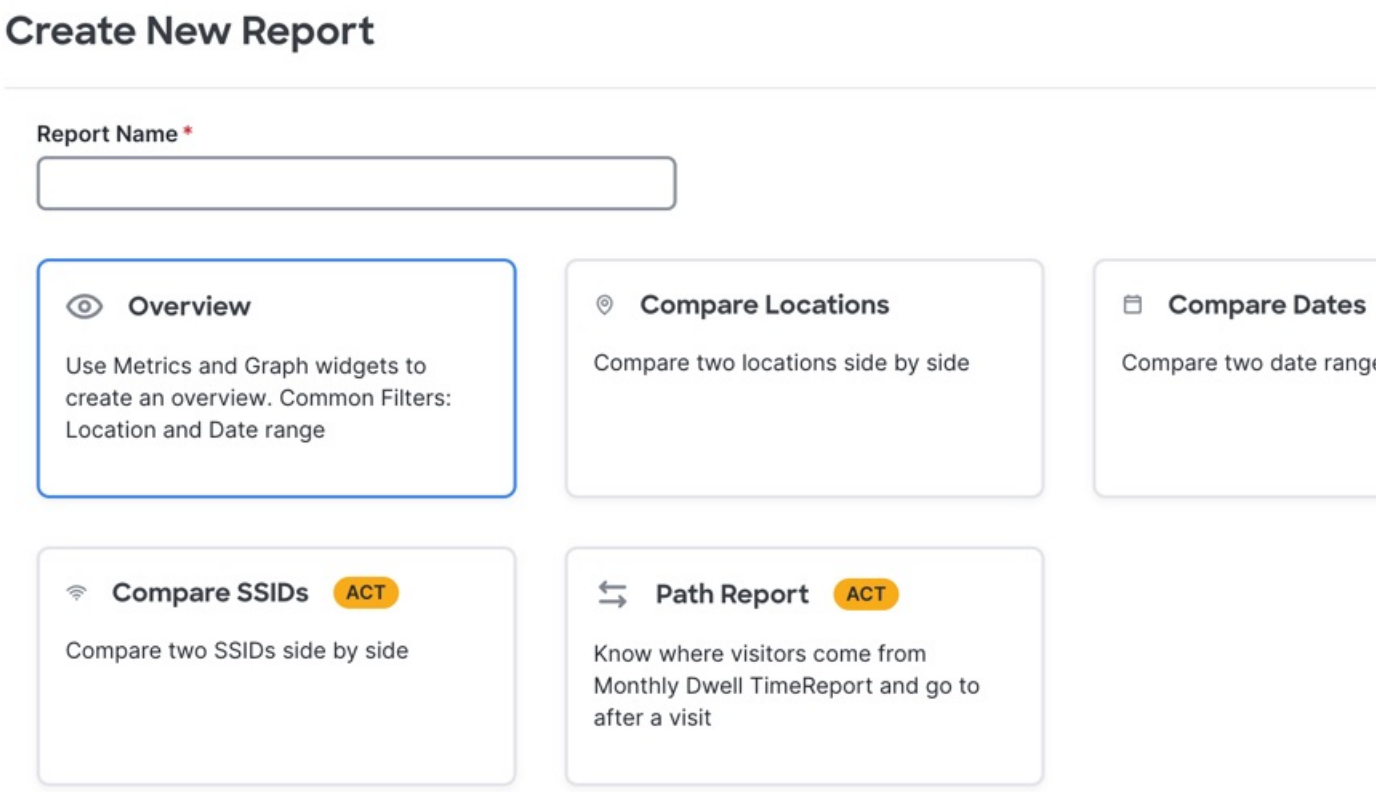
Each custom report can include multiple widgets. You can create widgets with different combinations of report types, locations, time period, SSIDs, visit ranges, and view by options. You can add more than one widget with same report type in a custom report.

Procedure

Step 1 In the Cisco Spaces dashboard, choose **Location Analytics** > **Custom Reports**.

Step 2 Click **Create New Report**.

The **Create New Report** window is displayed.



Step 3 In the **Report Name** field, enter the name for the new report.

Step 4 Select a report type.

The available options are:

- **Overview**
- **Compare Locations**
- **Compare Dates**
- **Compare SSIDs** (Available only for ADVANTAGE license users)

- **Path Report**: This report type is available for ADVANTAGE license. The report filters available for **Path Report** report type are **Location** and **Date**.



Note In the **Path Report**, the visits count displayed on the focus area represents the total number of visits made by visitors who have come from various locations. This count is independent on the visits shown on the home page widget and should not be compared against them.



Note You can select only one report type for a custom report.

You can also create a custom report without adding any report type or selecting any one report type. If you choose to create a custom report without any report type, all default report filter values are considered while creating the report.

The default values are:

- **Location**: Root location
- **Date Range**: 365 days
- **SSID**: All SSIDs

Step 5 Click **Next**.

Step 6 (Optional) Click **Skip & Create** to create the custom report without selecting any report filters.

Step 7 To select the required report filters, click the slide button.

The available options are:

- **Location**
- **Date**
- **SSID**

Use the **Search** option availble to search and select the required report filters.



Note ADVANTAGE (Advanced) subscription customers are allowed to apply all filters (Location, SSID, Time Range and Visit Range) in the widgets. ESSENTIAL and EXTEND subscription customers are restricted to apply SSID and Visit Ranges filters, and cannot filter group, floor and zone locations.

Step 8 Click the **Date** report filter and from the **Choose Date Range value** drop-down, select the date range filter to view the report.

Step 9 Click the **SSID** report filter and from the right panel, select the SSID to filter the report.

The following SSID options will be available for selection:

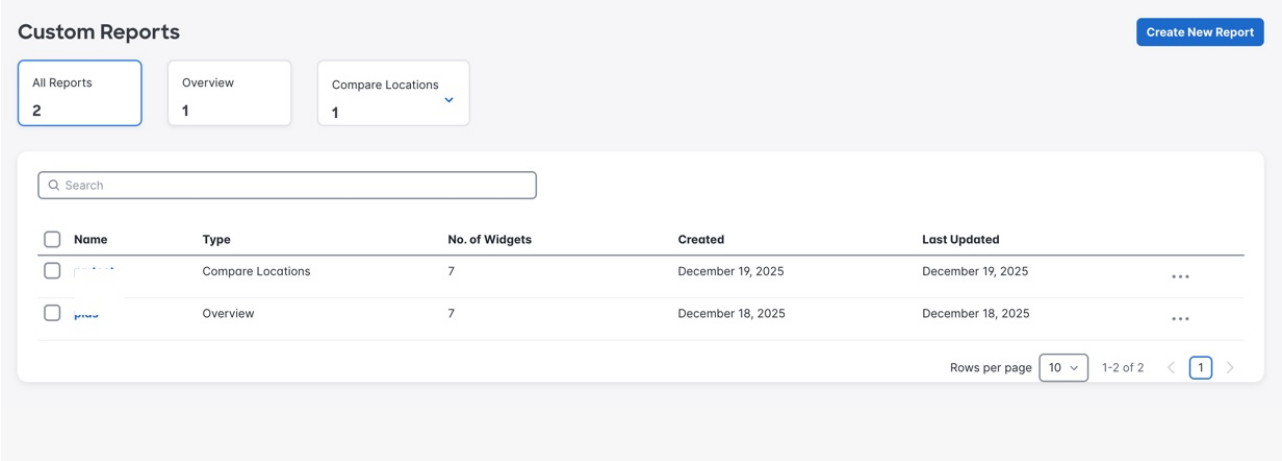
- **All SSIDs**: Displays the visit data in the filtered locations for the specified period captured using the SSIDs in those locations.

- **Custom SSID configured in Cisco Spaces**: Displays the visit data in the filtered locations for the specified period captured using the particular SSID.

Note You can apply the filters only if you are an **ADVANTAGE** license user. The ESSENTIAL license users cannot use the SSID filter. However, they can use the date range filter, and filter the locations except the group, floor and zone locations.

Step 10 Click **Create**.

The new custom report created is displayed in the **Custom Reports** window. You can view the report name, type, number of widgets, created date and last updated date. The **Custom Reports** window also displays the selected report filters available at a global level at the top of the window.



Note

- To delete a report, click the three dots icon (•••) on its row and click **Delete**.
- Check the **Name** check box to select all reports and click **Delete** at the top right of the **Custom Reports** window to delete them.

Step 11 (Optional) Click any custom report to open and view the report.

a) Click the three dots icon (•••) and click **Edit Report** to edit the report.

The available edit options are:

- **Clear All**: Click to clear the reports.
- **Add Widget**: Click to add more widgets to the custom report. For more information, refer to Add Widget, on page 177.
- **View Report**: Click to go back to the report preview.

- **Rearrange** option: Click the plus icon ( ) to rearrange the positioning of tiles and charts. The **Rearrange** option is not available for the **Path** widget.

Add Widget

You can add more widgets to your custom reports while editing a report.

Procedure

Step 1 In the **Location Analytics** window, click **Custom Reports** from the left panel.

Step 2 Select the report to edit.

The selected Location Analytics report is displayed.

Step 3 Click the three dots icon on the top-right of the window.

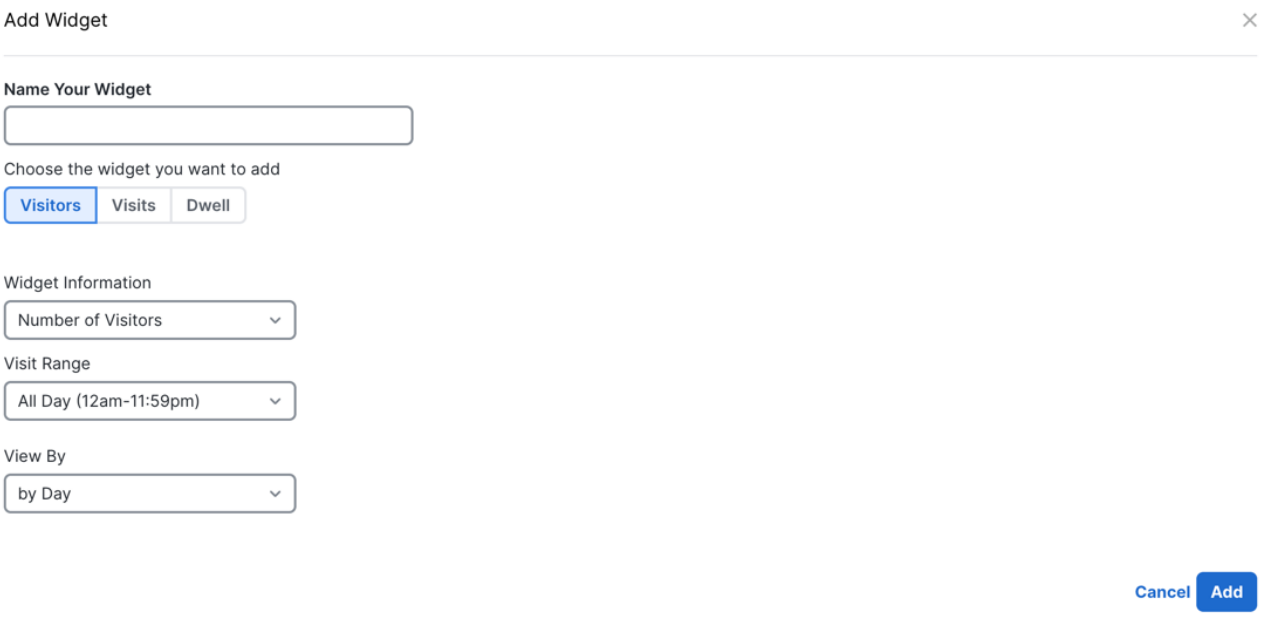
Step 4 Click **Edit Report**.

The report is displayed in edit mode.

Step 5 Click **Add Widget**.

The **Add Widget** pop-up window is displayed.

Figure 32: Add Widget



Step 6 Enter the following information:

a) **Name Your Widget**: Enter the name for the new widget to be added.
b) **Choose the widget you want to add**: Click the widget that you wanted to add. The widget available are **Visitors**, **Visits** and **Dwell**.
c) **Widget Information**: From the **Widget Information** drop-down list, select the information that must be included in the widget. The options vary depending upon the widget selection. The options available are:
   - For **Visitors** widget: **Number of Visitors** and **New vs Repeat**
   - For **Visits** widget: **Number of Visits** and **New vs Repeat**
   - For **Dwell** widget: **Distribution**
d) **Visit Range**: From the **Visit Range** drop-down list, select the date range for the report.

   The following options are available:
   - **All Day**: The visits happened during the entire day (12 am to 11:59 pm) are included in the report.
   - **Mid Night**: Only the visits during mid night (12 am to 2:59 am) are included in the report.
   - **Early Morning**: Only the visits during early morning (3 am to 4:59 am) are included in the report.
   - **Morning**: Only the visits during morning (5 am to 8:59 am) are included in the report.
   - **Business Hours**: Only the visits during business hours (9 am to 4.59 pm) are included in the report.
   - **Evening:**: Only the visits during evening (5 pm to 8:59 pm) are included in the report.
   - **Late Evening**: Only the visits during late evening (9 pm to 11:59 pm) are included in the report.
   - **AM**: Only the visits during early morning (12 am to 11:59 am) are included in the report.
   - **PM**: Only the visits during late evening (12 pm to 11:59 pm) are included in the report.

Step 7 Click **Next**.

The **Add Widget** pop-up is displayed with the following tabs: **Location**, **Date Range** and **SSIDs**. You can click these tabs and choose the required options and add them.

Step 8 Click **Locations** tab.

a) (Optional) In the **Search Location** field, enter the name and search for locations. You must enter a minimum of 3 characters to perform the location search.
b) Select the root location or click to expand and select the required zone or floor.
c) From the **View By** drop-down list, select the time duration for which you want to see the report for selected location.
   - **Day**: The report displays the visit data for each day of the specified period.
   - **Hour of Day**: The report displays the visit data for each hour of the day. The visit count for a particular hour will be total visits occurred during the specified period at that particular hour. For example, in the **Hour of Day** report for November 2022, the visit count displayed at 2:00 PM will be the total of number of visits occurred between 2.00 PM and 2:59 PM during the entire month of November 2022.
   - **Week**: The report displays the visit data for each week in the specified period.
   - **Day of Week**: The report displays the visit data for each week in the specified period with visit count for each day on that particular week.

Step 9 Click **Date Range** tab.

a) From the **Date Range** drop-down list, select the time duration for which you want to see the report.

If you choose **Custom** as the date range, enter the start and end dates in the **Start Date** and **End Date** fields.

b) From the **View By** drop-down list, select the time duration for which you want to see the report.

By default, the **View By** option selected in the **Locations** tab is displayed. You can update the time duration if required and the change is reflected in the **Locations** and **SSIDs** tabs.

Step 10 Click the **SSIDs** tab.

a) From the **SSIDs** drop-down list, select the SSID.

b) From the **View By** drop-down list, select the time duration for which you want to see the report.

By default, the **View By** option selected in the previous tab is displayed. You can update the time duration if required and the change is reflected in the other tabs.

Step 11 Click **Add**.

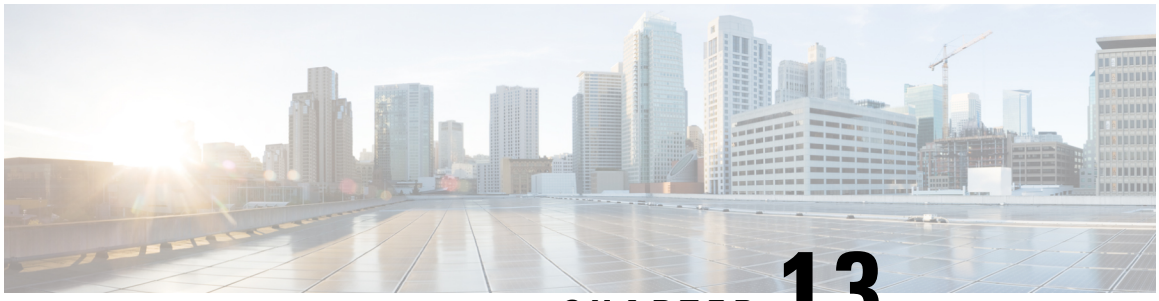
The prompt `Place Widget Here` is displayed and you can click on the blue highlighted area to insert the new widget.

Location-Based RBAC

A location-based RBAC role is a user access control setting that

- restricts a user's access to data and features based on assigned physical locations,
- enables administrators to specify which locations a role applies to during role creation or user invitation, and
- ensures that users can view only the data for the locations to which they are invited.

For more information, refer to Location-Based RBAC (Role-Based Access Control) in Cisco Spaces, on page 310.



CHAPTER 13

Cisco Spaces: Impact Analysis App

This chapter describes how to work with the Impact Analysis app.

- Impact Analysis Overview, on page 181
- Adding an Impact Campaign (Event), on page 182
- Viewing an Impact Analysis Report, on page 183
- Location-Based RBAC, on page 184

Impact Analysis Overview

Impact Analysis is a way of measuring the effect of any action you made based on before and after analytics. The **Impact Analysis** app enables you to do impact analysis. For example, assume that you have provided a discount offer to all the visitors visiting in your location A on November 2019. Now you can measure the impact of this discount offer by comparing the metrics during the offer period with the metrics of the last 365 days.

You can create an event with a particular time period, and can do any of the following:

- Compare the metrics for the event period with the metrics of Daily Average during Past 365 days (Period During EVENT).
- Compare the metrics for same duration before and after the specified event period. (Period AFTER Event)

You can compare the following metrics:

- Visit duration
- Visit Count

Adding an Impact Campaign (Event)

Note

- You cannot add, edit or modify a campaign, if you are a new Cisco Spaces and there is no data for your Cisco Spaces account.
- Event creation is restricted if the visits data that is available for an account is less than 30 days. In this scenario, default data is displayed.
- If you are having only read-only access to a Cisco Spaces account, you can view the Impact Analysis reports for the existing campaigns for that account, but you cannot add, modify, or delete a campaign.

To add an Impact Campaign (Event), perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, choose **Impact Analysis**.

Step 2 In the **Impact Analysis** window that appears, click **Add Impact Campaign**.

The **Add Impact Campaign** window appears.

Step 3 In the **Event Name** field, enter a name for the event.

Step 4 From the **Business Location** drop-down list, choose the location for which the event is created.

You can choose only network locations.

Step 5 In the **Choose the event period that you like to measure** area (**Compared To** drop-down list in the Edit window), choose the event period.

The following options will be available:

- **Period DURING Event**: This option enables you to compare the "data for the event period specified" with the "data for daily average of last 365 days". For example, if you are selecting the event period as December 10, 2019 to December 20, 2019, the graph in the Impact Analysis report displays 2 bar charts, one with "data for December 10, 2019 to December 20, 2019" and the other with "daily average data for December 21, 2018 to December 20, 2019".
- **Period AFTER Event**: This option enables you to compare "the data for the same duration before the date range specified" with "the data for the same duration after the date range specified". For example , if you are specifying the event duration as "January 01, 2020 to January 10, 2020" (10 days), the graph in the Impact Analysis report displays 2 bar charts, one with the "data for the time period December 22, 201 9 to December 31, 2019 (10 days)" and other with the "data for the time period January 10, 2020 to January 19, 2020 (10 Days)".

Note The graphs for Visit Duration and Visit Count are shown separately. In the Visit Duration graph, the difference in visit duration between two bar charts are displayed in minutes. In the Visit Count graph, the difference in visit count between two bar charts are displayed in percentage.

Step 6 In the **EVENT DURATION** area, specify the start date and end date for the event in the **From** and **To** fields respectively.

Step 7 Click **See Impact**.

Now the campaign is added.

- To edit a campaign, from the campaigns listed in the **Impact Analysis** window, click the campaign that you want to edit. Click **Edit Campaign** at the top-right of the window, and make necessary changes. Click **Update** to save the changes.
- To delete a campaign, from the campaigns listed in the **Impact Analysis** window, click the campaign that you want to delete. Click **Delete** displayed at the top-right of the window. In the **Delete Impact Campaign** window, click **Delete** to confirm the deletion. To delete multiple campaigns (events) at a time, in the **Impact Analysis** window, check the check boxes corresponding to the campaigns that you want delete, and click **Delete** that appears at the bottom of the window.

Viewing an Impact Analysis Report

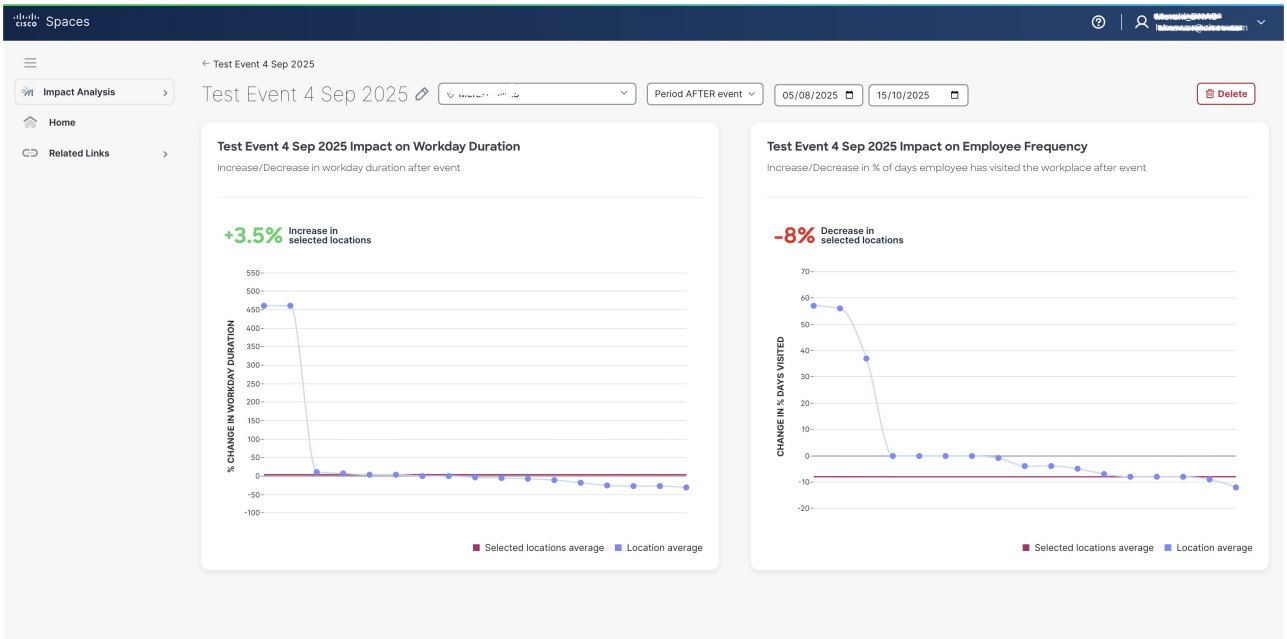
To view an Impact Analysis report, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, choose **Impact Analysis**.

The **Impact Analysis** window appears. All the campaigns created will be listed in the window.

Figure 33: Impact Analysis Report



Step 2 Click the campaign/event for which you want to view the report.

The Impact Analysis report for the selected campaign is displayed. The report will have the following charts:

- **Impact on Visit Duration**: Displays a bar chart with the average visit duration for the event, and the average visit duration for the selected time window, in minutes.
- **Impact on Visit Count:** Displays a bar chart with the average visit count for the event and the average visit count for the selected time window, in percentage.

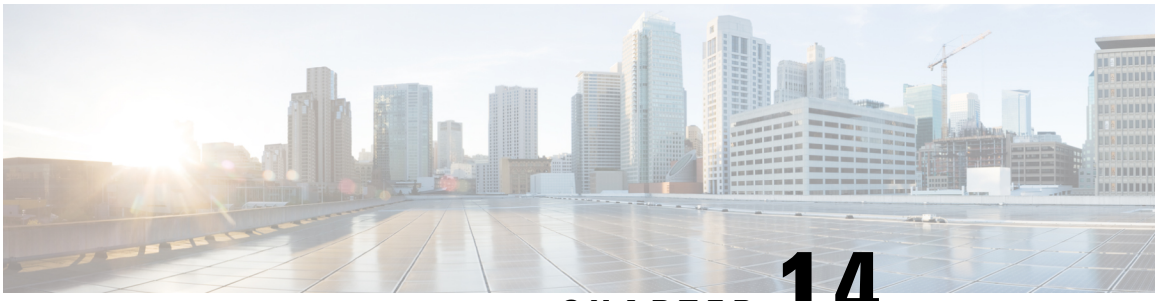
Note Report will be not be displayed if you have created the event for current month or with a future time period.

Location-Based RBAC

A location-based RBAC role is a user access control setting that

- restricts a user's access to data and features based on assigned physical locations,
- enables administrators to specify which locations a role applies to during role creation or user invitation, and
- ensures that users can view only the data for the locations to which they are invited.

For more information, refer to Location-Based RBAC (Role-Based Access Control) in Cisco Spaces, on page 310.



CHAPTER 14

Cisco Spaces: Space Utilization App

- Work with Space Utilization App, on page 185

Work with Space Utilization App

The Cisco Spaces: Space Utilization App offers historical insights into how your physical spaces are used, aiding in space optimization. These insights are gathered from data collected via sensors embedded within your space's networking and collaboration infrastructure.

This app allows you to view the occupancy and utilization for any physical space within a campus, building, or floor. This information includes data such as people count, peak utilization metrics, room utilization metrics and time spent by people in that physical space.

For Cisco Spaces accounts in the Workspace and Education verticals, both Floor Occupancy and Room Occupancy metrics are displayed. By default, for accounts in all other verticals, the following message is displayed: *Occupancy charts are only available to Workspaces / Education vertical*.

Use **Room Occupancy Reports** feature to generate an occupancy report with the data including the number of people present in the room that is aggregated in a window of every 15 minutes. This feature provides the flexibility to download and categorize the people count data based on their preferred reporting time intervals, such as 15, 30, or 60 minutes.

The Glossary enhancements in the **Space Utilization** app provide a consolidated and comprehensive set of definitions for the various metrics and charts available across all views within the **Space Utilization** application. These definitions enhance user understanding and provide clarity on how data is presented and calculated.

You can share a **Space Utilization** report with Cisco Spaces users or external recipients. From the Space Utilization dashboard, open the report, click **Share**, enter the recipient’s email address, optionally enter a message, and send the invitation.

In the Space Utilization dashboard, open the report.

Click **Share**.

Enter the recipient's email address.

(Optional) Enter a message.

Cllick **Send**.

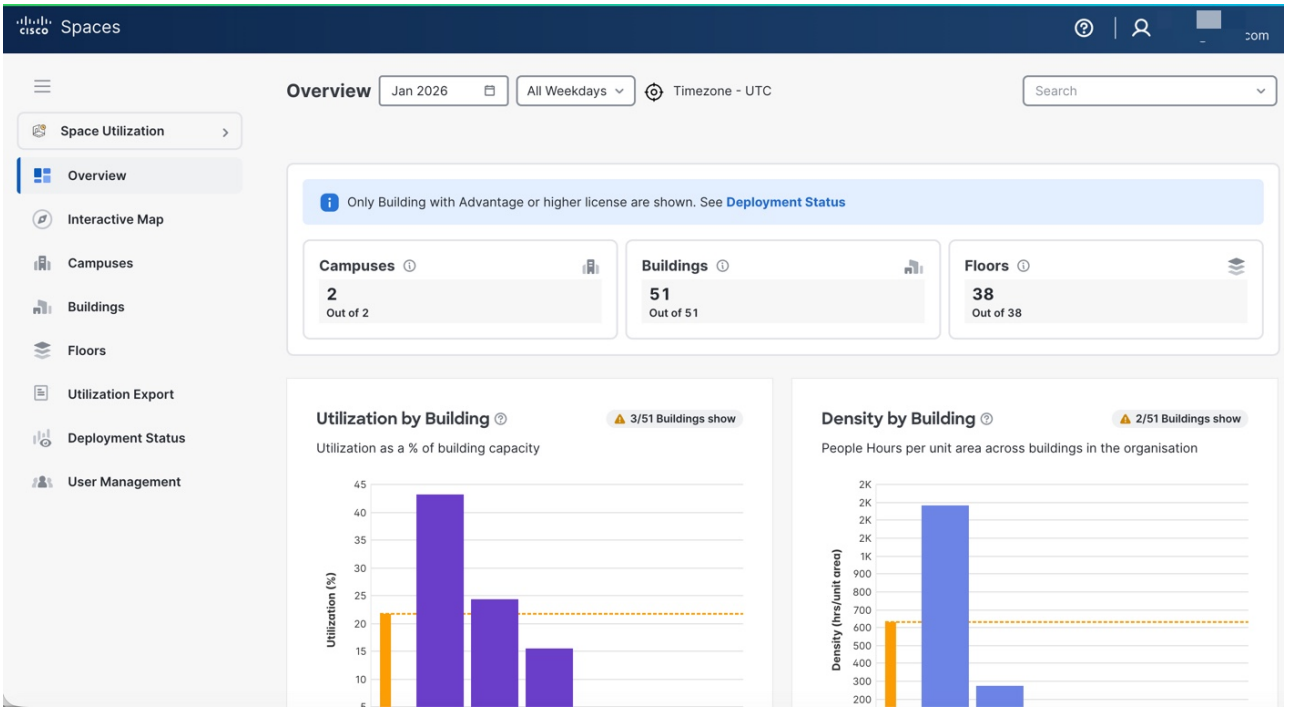
The recipient receives an email containing a report snapshot and a link. A Cisco Spaces user signs in to view the report. An external recipient verifies access by using the PIN generated during authorization.

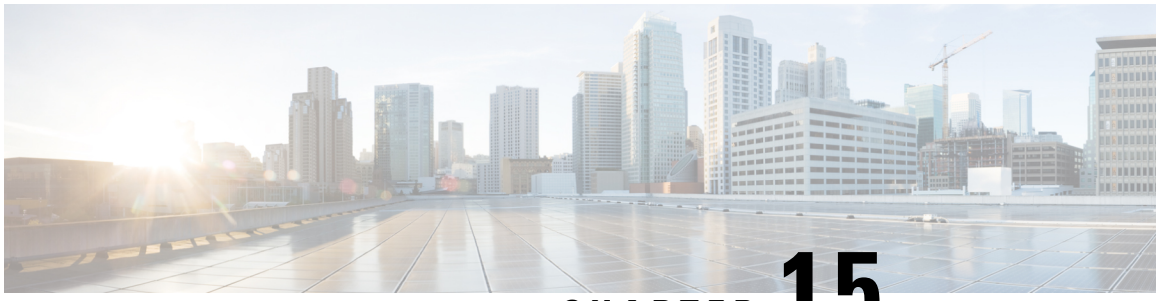
From the shared-access area, the sender can approve or reject access requests, revoke access, and review requests created when a recipient re-shares the report.

For more information, refer to Cisco Spaces: Space Utilization App Guide.

Note The **Space Utilization** app is available to users with **Cisco Spaces ADVANTAGE** and **Cisco Spaces UNLIMITED** licenses.

Figure 34: Space Utilization App





CHAPTER 15

Cisco Spaces: Smart Workspaces App

The Cisco Spaces: **Cisco Smart Workspaces** app offers applications like **Space Manager** and **Space Experience** for your wired, wireless, and WebEx deployments that are used to make your workspace hybrid-work-ready. These applications enhance and provide seamless digital experiences for your employees and visitors through metrics such as occupancy, noise & air quality, and meeting room capacity & availability.

The **Space Manager** app allows you to have a view of real-time occupancy and environment updates like humidity, air quality, and noise levels across buildings, floors, and meeting rooms. Meanwhile, the **Space Experience** app enables signage management through Cisco Spaces.

Note These applications are associated with these types of licenses:

- ADVANTAGE
- UNLIMITED
- PREMIER_W
- PREMIER_CW

• Working with Cisco Spaces: Smart Workspaces, on page 187

Working with Cisco Spaces: Smart Workspaces

To support **Cisco Smart Workspaces** solution, two new apps are available:

- **Space Manager**: Use this app to configure various devices, sensors, and workspaces and to provide access to real-time occupancy data and environment telemetry (heat map, indoor air quality, temperature, humidity, and noise levels) rendered on rich maps for a specific building, floor, or meeting room.
  - In the **Devices** section, you can view the configured devices and their telemetry details on rich maps.
  - The **Manage Rooms** section displays the configured meeting room or workspace and allows you to view, add, or remove devices and sensors to and from the selected workspace.
- **Space Experience**: Use this app to perform these:
  - Create and manage signage for **Cisco Smart Workspaces**

- Onboard new signage for a Cisco Webex device or a non-Webex device.
- Configure the telemetry parameters and publish the signage.

  The configuration updates are auto-notified to the corresponding signage devices.

For more information, refer to Cisco Spaces: Smart Workspaces Solution Guide.

Signage 2.0

Signage 2.0 provides a touch-first kiosk and signage experience with simplified on-screen navigation and improved touch responsiveness.

Floor Occupancy and Environmental widgets appear at the top of the screen with a dial-based design. A sensor widget is displayed only when the corresponding sensor data is available. If Cisco Spaces does not receive data from a sensor, the related widget is hidden.

By default, the kiosk displays the Spaces Explorer branding. To use your organization's logo, choose **Space Experience** > **Settings** and upload the logo. The uploaded logo appears in the upper-left corner of the kiosk application.

Preview signage

When you create or edit signage in Space Experience, use **Preview** to review the configuration before publishing it. The preview displays the signage type, building and floor, latitude and longitude, configured widgets, map-view settings, and Where Am I updates.

Verify the preview and correct any configuration differences before you publish the signage.

Room occupancy source

Signage determines whether a meeting room is occupied from the Webex Room In Use attribute. This replaces occupancy detection based on a combination of People Presence and People Count Out Of Call and provides a more reliable indication of current room use.

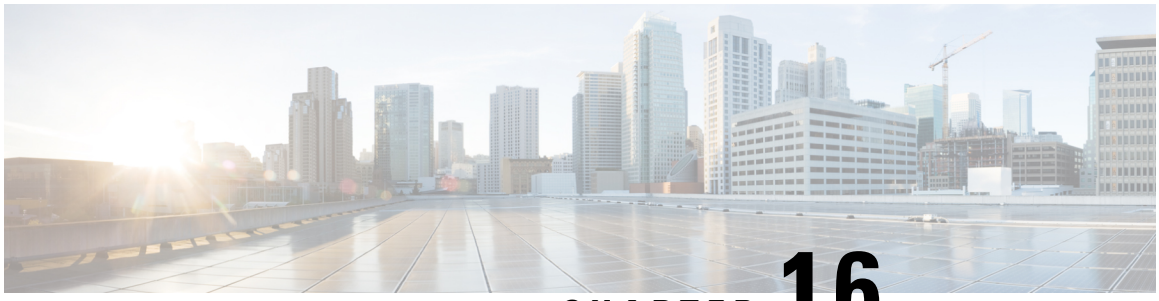
Use a Digital Map default view in signage

New Space Experience signage configurations use the default map view configured for the selected Digital Map. The inherited view includes the map position, pitch, bearing, and zoom.

To configure the default, choose **Setup** > **Locations and Maps** > **Digital Maps**. Locate the required building or floor, open the **More Options** menu, choose **Set default map view**, adjust the view, and click **Save**.

Override the Default Map View is disabled by default for new signage. Enable it only when a signage requires a different map position, pitch, bearing, or zoom.

Existing signage continues to use its saved map view. To make an existing signage inherit the Digital Map default, edit the signage and disable **Override the Default Map View**.



CHAPTER 16

Cisco Spaces: Environmental Analytics App

- Working with Cisco Spaces: Environmental Analytics App, on page 189

Working with Cisco Spaces: Environmental Analytics App

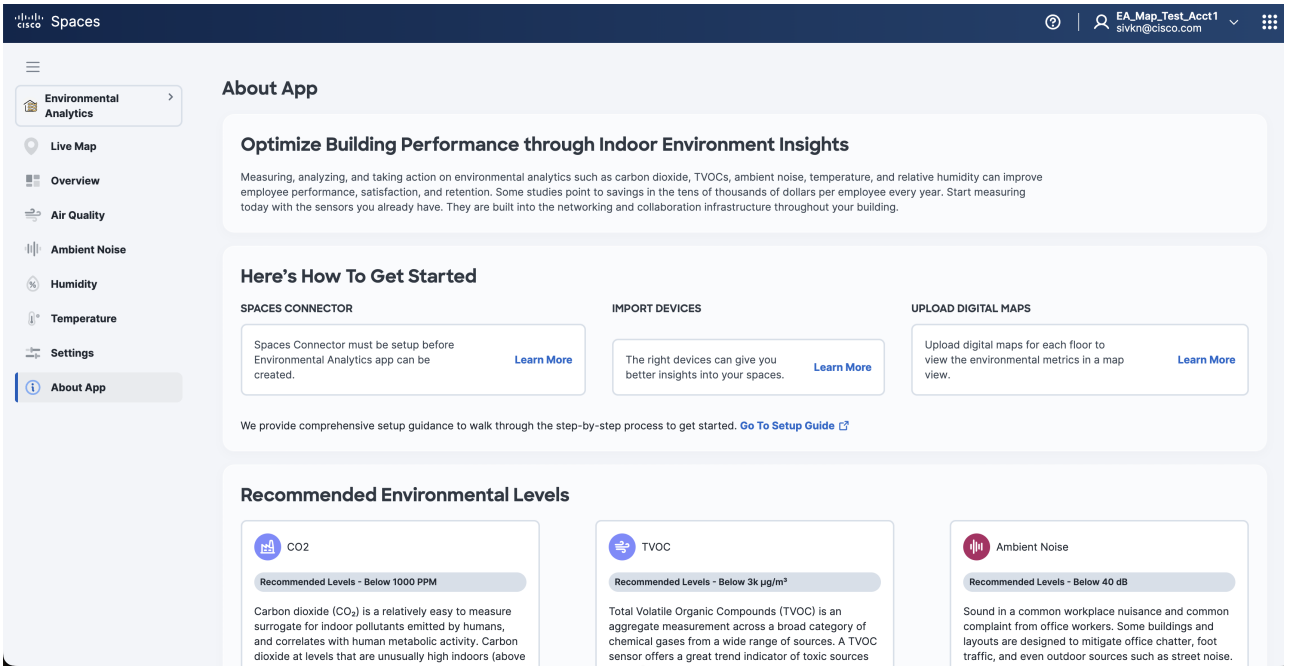
Cisco Spaces: Environmental Analytics App

The Cisco Spaces Environmental Analytics app enables you to optimize the performance of buildings by leveraging indoor environment insights and metrics. These insights are derived from sensors integrated into the networking and collaboration infrastructure throughout your buildings within your network.

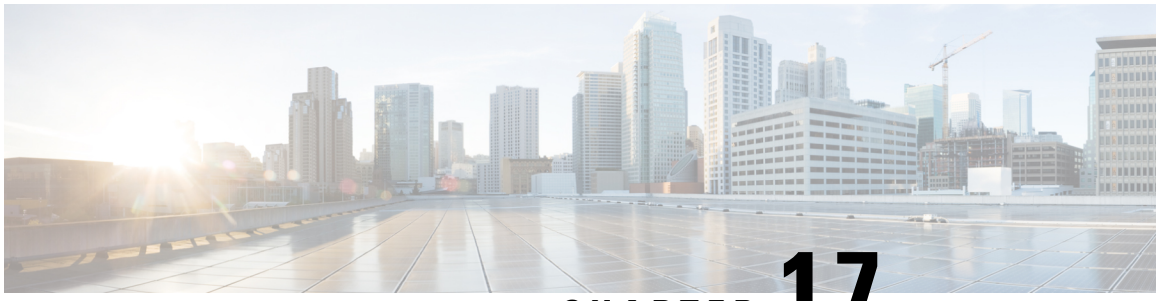
Use the Environmental Analytics app to measure and evaluate critical environmental metrics such as carbon dioxide levels, total volatile organic compounds (TVOCs), ambient noise, temperature, and relative humidity. Leverage this valuable data to take necessary corrective actions to ensure optimal indoor conditions and enhance the overall environmental quality within your facilities.

For more information, refer to Cisco Spaces: Environmental Analytics App Configuration Guide.

Figure 35: Environmental Analytics App



Note Cisco Spaces Environmental Analytics app is tied to the **ADVANTAGE** license.



CHAPTER 17

Cisco Spaces: Asset Locator App

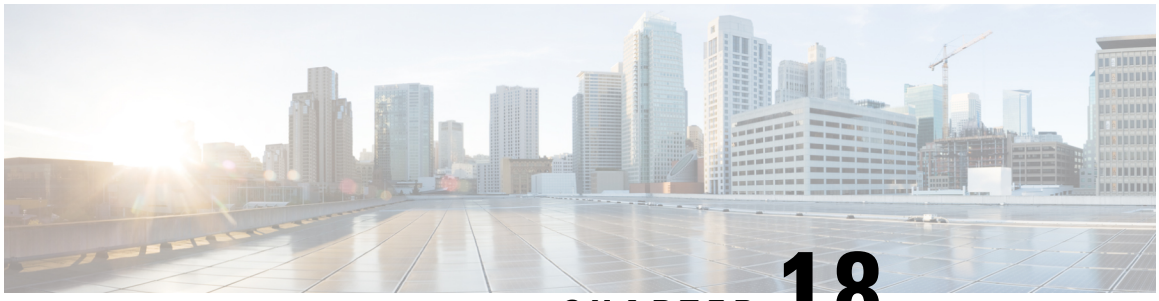
The Cisco Spaces: Asset Locator app enables you to monitor assets and optimize the performance of your assets, sensors, alerting system, and operational workflows.

- Working with the Cisco Spaces: Asset Locator App, on page 191

Working with the Cisco Spaces: Asset Locator App

The Cisco Spaces: Asset Locator app provides a range of tags and sensors to continually integrate, monitor, and manage your connected operations. Using its cloud-based interface, you can define the profile, category, and ownership of each assets. You can establish business rules to define work flows, and the expected operating range of your assets and sensors.

For more information on Cisco Spaces: Asset Locator, see Asset Locator.



CHAPTER 18

Cisco Spaces: IoT Explorer App

- Cisco Spaces: IoT Explorer, on page 193
- Working with Cisco Spaces: IoT Explorer, on page 193
- Temperature Monitoring: Use Case Overview, on page 194
- Asset Tracking: Use Case Overview, on page 195
- Presence Detection: Use Case Overview, on page 196

Cisco Spaces: IoT Explorer

The Cisco Spaces: IoT Explorer app enables you to monitor and optimize the performance of your assets, sensors, alerting system, and workflows.

Working with Cisco Spaces: IoT Explorer

The Cisco Spaces: IoT Explorer app is a comprehensive single resource for managing, monitoring, and optimizing your assets, Internet of Things (IoT) sensors, alerting system, and operational workflows.

IoT Explorer application is the 3rd generation enhanced version of Operational Insights and Cisco Asset Locator applications. The **IoT Explorer** application is designed to bring in quick value to users exploring device driven IoT use cases in Cisco Spaces and to add value to IoT services at the ADVANTAGE licensing level.

This application accomplishes the three use cases listed below:

- Temperature Monitoring: Monitor spaces and receive notifications of changes in temperature
- Asset Tracking: Locate, monitor and set up alerts to gain insight into your asset locations
- Space Occupancy/Presence Detection: Get real-time insights into how your physical spaces are occupied

Within each of these use cases, you can create rules/alerts, view data logs, view the real-time location and status of the device or sensor. The **IoT Explorer** application UI is designed to set up the use case in a simplified way.

The **IoT Explorer** application filters only those devices that comply with the MAC Organisationally Unique Identifier (OUI) standards and the devices which continue to send updates after 24 hours from the initial appearance.

For more information on Cisco Spaces: IoT Explorer, refer to Cisco Spaces: IoT Explorer Configuration Guide.

Temperature Monitoring: Use Case Overview

Use the Temperature Monitoring use case to manage and monitor indoor environments. You can add new temperature sensors with scalable and streamlined onboarding process and create rules to quickly notify team members when a sensor falls or rises below a certain threshold.

In the Temperature Monitoring use case, to trigger a rule or an event, the temperature value of the device must be within the specified condition as defined in the rule. For example, if the device temperature condition in the rule is defined as between 5° Celsius to 10° Celsius, the event is triggered when the device temperature drops down to less than 5° Celsius or goes beyond 10° Celsius and then comes back within the range of 5° Celsius to 10° Celsius.

For more information, see Configure Monitoring of Temperature of Devices.

Cisco Spaces dashboard supports the import of MT Sensor devices in the **Temperature Monitoring** section of the **IoT Explorer** app.

The Temperature Monitoring use case helps you to:

- Get alert when temperature is out of range
- Set up an event log to monitor temperature changes over time
- Gain insight into all the spaces temperature
- Keep assests under compliance

Configure Monitoring of Temperature of Devices

Procedure

Step 1 In the Cisco Spaces dashboard, click the Cisco Spaces: IoT Explorer app tile.

Step 2 Click **Temperature Monitoring**.

Step 3 Click **Get Started**.

Step 4 In the **Use Case Name** field, enter a name for the use case.

Step 5 In the **Description** field, enter a description for the use case.

Step 6 Click **Create Use Case**.
The Temperature Monitoring use case is created with various options to setup sensors, rules and users.

Step 7 Use the following tabs to perform configurations:

- **Configure**: Configure sensors, rules and users.
- **Sensors**: Search and manage the sensors attached to your devices.
- **Rules**: Create rules to monitor the sensors attached to assets. For a rule to work, you need a trigger that activates the rule and an action is performed automatically.

- **Users & Roles**: Add users and manage their roles.
- **Events**: Search and manage events. When the rules you configure trigger events, the events are displayed here.

The new use case is created and displayed in the **Active Use Cases** area.

Asset Tracking: Use Case Overview

Use the Asset Tracking use case to add asset tags to help manage and monitor the location of important objects and search asset on a map. You can add new asset tags with scalable and streamlined onboarding process and create rules to quickly notify team members when an item leaves a zone. All the associated random MAC Wi-Fi devices are displayed in this use case.

The Asset Tracking use case helps you to:

- Configure notifications when an asset leaves a zone, floor, or building
- Locate an asset in real time
- Gain insight into how often a device is used

Configure Tracking and Monitoring of Asset Location

Procedure

Step 1 In the Cisco Spaces dashboard, click the **IoT Explorer** app tile.

Step 2 Click **Asset Tracking**.

Step 3 Click **Get Started**.

Step 4 In the **Use Case Name** field, enter a name for the use case.

Step 5 In the **Description** field, enter a description for the use case.

Step 6 Click **Create Use Case**.
The Asset Tracking use case is created with various options to manage your assets, set up rules, and add users.

Step 7 Use the following tabs to perform configurations:

- **Configure**: Configure sensors, rules and users. See
- **Locator**: Search for a sensor using name or location. You can track all devices on the floor map image in real time.
- **Assets**: Search and manage the sensors.
- **Rules**: Create rules to monitor the sensors. For a rule to work, you need a trigger that activates the rule and an action is performed automatically.
- **Users & Roles**: Add users and manage their roles.
- **Events**: Search and manage events.

The new use cases created are displayed in the **Active Use Cases** area.

Presence Detection: Use Case Overview

Use the Presence Detection use case to manage and monitor live occupancy data for desks, rooms, and offices. You can add new occupancy sensors with scalable and streamlined onboarding process and create rules to quickly notify team members when a space is occupied for a period of time. You can also manually place the sensors on their imported map.

The Presence Detection use case helps you to:

- Gain insight into space utilization by creating a data log rule
- Use the map to quickly see live occupancy status of spaces
- Share historical occupancy data with facilities team members
- Set up a rule to get alerts when a space becomes available

The following sensors are supported by this use case:

- Passive Infrared Sensor (PIR)
- Meraki Camera

Configure Presence Detection

Procedure

Step 1 In the Cisco Spaces dashboard, click the **IoT Explorer** app tile.

Step 2 Click **Presence Detection**.

Step 3 Click **Get Started**.

Step 4 In the **Use Case Name** field, enter a name for the use case.

Step 5 In the **Description** field, enter a description for the use case.

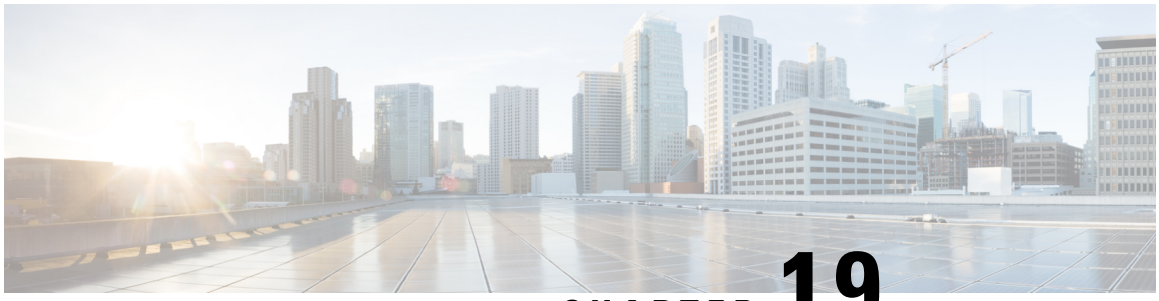
Step 6 Click **Create Use Case**.
The Presence Detection use case is created with various options to manage your assets, set up rules, and add users.

Step 7 Use the following tabs to perform configurations:

- **Configure**: Configure sensors, rules and users.
- **Occupancy View**: Search for a sensor using name or location. You can track occupied and unoccupied spaces from the floor map image.
- **Sensors**: Search and manage the sensors.
- **Rules**: Create rules to monitor the sensors. For a rule to work, you need a trigger that activates the rule and an action is performed automatically.

- **Users & Roles**: Add users and manage their roles.
- **Events**: Search and manage events.

The new use cases created are displayed in the **Active Use Cases** area.



CHAPTER 19

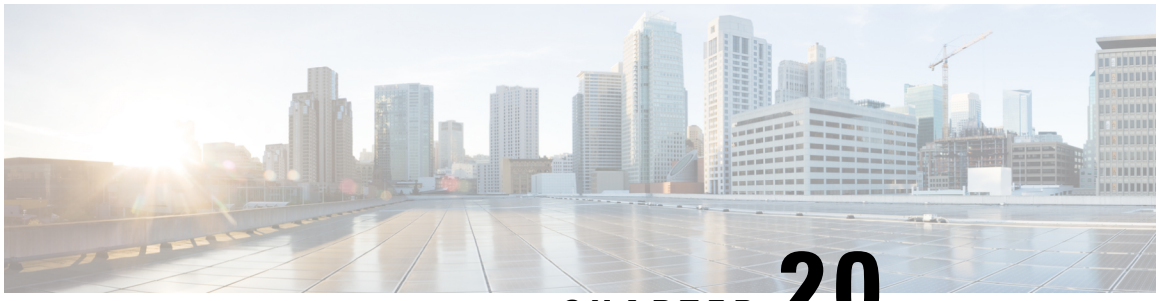
Cisco Spaces: Captive Portal App

• Cisco Spaces: Captive Portal app, on page 199

Cisco Spaces: Captive Portal app

Cisco Spaces: Captive Portal app helps you create Wi-Fi user onboarding portals that:

- appear when users connect to an SSID and can be enhanced with Cisco Spaces portal modules.
- support custom enterprise captive portals for onboarding end users to Wi-Fi, and
- for more information, refer to Cisco Spaces: Captive Portal App Guide.



CHAPTER 20

Cisco Spaces: Engagements App

Cisco Spaces functions as a Wi-Fi Beacon that identifies the customers in a Cisco Spaces enabled premises and sends notifications to the customers and business users, based on the engagement rule defined.

This chapter describes how to create the engagement rules that enable you to send notifications to the customers when they are near your business premises. A customer can be a user who has purchased from your business premises earlier, a potential buyer, or a visitor. You can also configure engagement rules to send notifications to your business users such as employees or to an API end point. For example, you can configure an engagement rule that informs your customer care representative when a privileged customer enters the premises so that the customer care representative can provide value added services to the customer.

You can configure to send the notification based on the customers connectivity to your Wi-Fi.

Note An engagement rule is applied for all the SSIDs defined for the locations specified in the rule.

- Prerequisites for Creating an Engagement Rule, on page 201
- Creating an Engagement Rule, on page 202
- Managing Engagement Rules, on page 210
- Engagement Rule Report, on page 212
- **Visitor Engagement**, on page 212
- Engagement URL, on page 213
- Previous Visit Criteria, on page 213
- Notification Types, on page 214
- Notification Frequency, on page 215
- Location Filter for an Engagement Rule, on page 215
- Notification Type for a Consumer, on page 216
- Notification Type for a Business User, on page 217
- Trigger API Configuration for Notification, on page 220

Prerequisites for Creating an Engagement Rule

- To send notifications, you must do certain configurations in your wireless network system.
  - If your wireless network is Cisco Meraki, do the configurations mentioned in Configuring Cisco Meraki for Notifications and Reports, on page 126.

- If your wireless network is Cisco AireOS or Cisco Catalyst, do the configurations mentioned in Configuring Cisco Wireless Controller (without Cisco CMX) for Notification and Reports, on page 92
- If your wireless network is Cisco Catalyst, do any of the following configurations based on the mode and connector .
  - Configuring Cisco Catalyst 9800 Series Wireless Controller (Local Mode) for Captive Portals and Engagements Apps Using CLI , on page 95
  - Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Local Mode) for Captive Portals and Engagements Apps, on page 99
  - Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Flex Mode or Mobility Express) for Captive Portals and Engagements Apps, on page 104

- To specify the locations for which the engagement rule is applicable, you must define the location hierarchy. For more information on defining the location hierarchy, refer to Location Hierarchy.
- To specify the tags for which the rule is applicable, you must define the tags. For more information on creating the tags, refer to the Create or Modify Tags, on page 223.
- To send to an external API the details such as first name, last name, and so on of the customers who have signed into the captive portal, you must configure the Data Capture form in the captive portal. Without the Data Capture form, only the information such as device mac address will be send to the external API. For more information on configuring a data capture form, refer to the Add a data capture form to a portal.

Creating an Engagement Rule

The Engagement Rule refers to the conditions based on which the notifications are sent to the target users. You can create the engagement rule for your customers and business users such as employees or API endpoints.

You can set the frequency at which the notification is to send. You can also define the criteria that must match to send the notification. You can configure to send the notification to a single user or a group of users in multiple locations.

For customers, you can send the notifications through SMS or e-mail. For business users, you can send the notifications through Cisco Webex Teams, SMS, e-mail, or to an external API. For customers and business users, you can configure to send the notifications based on the connectivity of the customer to an SSID. You can configure more than one notification type for an engagement rule, so that the user gets notification in more than one format. This increases the probability of notifications to be noticed by the user.

Creating an Engagement Rule for a Consumer

You can send notifications to a customer through SMS or e-mail.

You can also send customer notifications through Via App Push Notification if an app channel is configured.

To define an engagement rule to send notifications to the customers, complete these actions.

Procedure

Step 1 In the Cisco Spaces dashboard, choose **Engagements**.

Step 2 In the **Engagements Rules** window, click **Create New Rule**.

Step 3 In the **Rule Name** field, enter a name for the engagement rule.

Step 4 From the **When a user is on WiFi and** drop-down list, choose any of the following:

- **Entering a Location**: Choose this option if you want to send the notification when a visitor connected to the Wi-Fi enters the location.
- **Away from the Location**: Choose this option if you want to send the notification when a visitor connected to the Wi-Fi is away from the location for a specified time. If you are selecting this option, from the **For** scroll list, choose the number of minutes a visitor needs to be away from the location for sending notifications.

Note

- The **Exiting Location** option is no more available. If you are editing an existing Engagement Rule with **Exiting Location** configured, the **Choose User Activity** drop-down list will appear without any selection. You must choose the required option from the **Choose User Activity** drop-down list to save the rule successfully.
- Even if a visitor is physically present in the location, but gets disconnected from the Wi-Fi for the minutes specified in the **For** scroll list, the visitor will be considered for sending notification.

- **Present at Location**: Choose this option if you want to send notifications to a visitor who is connected to the Wi-Fi and is present at the location for a specified duration or at a particular time. If you choose this option, additional fields appear where you can mention the duration or time that needs to be met by the customer to get filtered for this rule.

Step 5 In the **LOCATIONS** area, specify the locations for which you want to send the notifications.

You can configure to send notifications for the entire customer name or a single or multiple locations such as group, floor, or zone. You can add the locations of diffrerent wireless networks such as Cisco Meraki, Cisco Wireless Controller, and so on in an Engagement rule.

You can again filter the locations for which the notification is to send based on the metadata defined for the selected location or its parent or child locations. You can either send the notifications for the locations with a particular metadata or exclude the locations with a particular metadata. For more information on defining the locations for the engagement rue, refer to the #unique_194

Step 6 In the **IDENTIFY** area, specify the type of customers for whom you want to send the notifications.

Note You can filter the customers for whom you want to send the notifications based on whether the customer is an opted in or not opted in user, the tags the customers belong to, and the number of visits made by the customer. You can apply all these filters or any of them based on your requirement.

To specify the customers for whom the notification is to send, perform the following steps:

a) If you want to filter the customers by the Opt In Status, check the **Filter by Opt-In Status** check box, and choose whether you want to send the notifications for opted in users or not opted in users.
b) If you want to filter the customers based on tags, check the **Filter by Tags** check box.

Note You can filter the tags in two different ways. Either you can specify the tags for which the notifications are to send or you can specify the tags for which the notifications must not be sent. You can choose the best filtering method based on your requirement. For example, if you want to send the notifications for all tags expect for one tag, it is easy to opt the exclude

c) If you want to filter the customers based on the number of visits made by the customer in the selected locations, check the **Filter by Previous Visits** check box. Click the **Add Locations** button. In the **Choose Locations** window, specify the locations of which the customer visit needs to consider for filtering. In the following fields, mention the number of visits and duration required to send notifications.

Step 7 In the **SCHEDULE** area, specify the period for which you want to apply the rule.
a) Check the **Set a date range for the rule** check box, and in the fields that appear, specify the start date and end date for the period for which you want to apply the engagement rule.
b) Check the **Set a time range for the rule** check box, and in the fields that appear, specify the time range for which you want to apply the engagement rule, within the date range specified.
c) If you want to apply the engagement rule only on particular days, check the **Filter by days of the week** check box, and from the list of days that appears, click the days on which you want to send the notifications.

Step 8 In the **ACTIONS** area, perform the following steps:
a) From the **Notify** drop-down list, choose **Consumer**, and from the adjacent drop-down list choose any of the following:

- **Only Once**—The notification is sent only once to a customer.
- **Once In**—The notification is sent more than once to a customer based on the notification frequency specified. In the additional fields that appear when you choose this option, specify the notification frequency.

b) Specify the mode of notification. You can send the notification to the customers through push notification, SMS, or e-mail. For more information on the notification types, refer to Notification Type for a Consumer, on page 216.

Note For **Via Email**, the e-mail ID entered in the **From** field must be included in the allowed list for e-mail IDs. To include the e-mail ID in the allowed list, contact Cisco Spaces support team. If you do not want to use a specific e-mail ID, you can use the default allowed e-mail ID **no-reply@dnaspaces.io**. However, the default ID is not displayed in the dashboard automatically. So, you have to enter it manually.

The summary of the rule is shown on the right side of the window.

Step 9 Click **Save and Publish**.
The rule gets published and listed in the Engagement Rules page.

Note If you do not want to publish the rule now, you can click the **Save** button. You can publish the rule at any time later by clicking the **Save and Publish** button. Also, you can publish the rule by clicking the Make Rule Live icon at the far right of the rule in the Engagement Rules page.

Use Case: Engagement Rule for Customers

The retail store ABC has outlets across Europe. As part of its summer sale, ABC has decided to provide some offers to its customers. The offer is only for the customers visiting the ABC outlets at location A and floor 1 at location B. All the customers who had visited any outlet of ABC at least 5 times in the current year are eligible for the offer. ABC wants to send notifications regarding the offers to the customers who had visited any of its outlets minimum 5 times during the current year. The notifications need to send when the customer enters location A or Floor 1 of location B with connected to the Wi-Fi. The notification is to send only on weekends as the offer is only for weekends. The notifications are to send only for a fortnight for the opted-in users. ABC wants to send the notifications during each visit through e-mail.

To meet the preceding scenario, perform the following steps:

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 Create the location hierarchy with all the locations of ABC.

Step 3 In the Cisco Spaces dashboard, click **Engagements**.

Step 4 On the **Engagements** page that appears, click **Create New Rule**.

Step 5 In the **Rule Name** field, enter a name for the engagement rule.

Step 6 From the **When a user is on WiFi and** drop-down list, choose **Entering Location**.

Step 7 In the Locations area, click the **Add Locations** button for choosing the location, and select location A, and Floor 1 of location B.

Step 8 In the **IDENTIFY** area, do the following:

a) Check the **Filter by Opt-In Status** check box, and choose **Only for opted-in Visitor**.

b) Check the **Filter by Previous Visits** check box, and click the **Add Locations**button. Check the customer name (root name) check box to consider the visit to all of the locations of ABC, and click **Done**.

c) From the following drop-down lists, choose **Atleast, 5 Times in This Year**.

Step 9 In the **SCHEDULE** area, do the following:

a) Check the **Set a date range for the rule** check box, and specify the date range for the fortnight for which you want to provide the offer. Set the time also, if required.

b) Check the **Filter by days of the week** check box, and click **Sat** and **Sun**.

Step 10 In the **ACTIONS** area, do the following:

a) From the **Notify** drop-down list, choose **Consumer**.

b) From the adjacent three drop-down lists, choose **Once in, 1**, and **Visits**, respectively.

c) Check the **Via Email** check box.

d) In the **From Name** field, enter the email name that must be displayed to the customer, and in the **From Email** field, enter the email ID that must be displayed to the customer.
e) In the **Subject** field enter a subject for the email. If required, edit the message in the following text box.
f) Check the **Via SMS** check box, specify the SMS gateway. If required, edit the content in the following text box.



Note This configuration is to send the notification even if the app notification fails. In addition, the customers who are not an app user, get the notification through SMS.

Step 11 Click **Save and Publish**.

The rule gets published.

Creating an Engagement Rule for a Business User

Before creating an engagement rule, ensure that the prerequisites are met. For more information on the prerequisites to create an engagement rule, refer to the "Prerequisites for Creating an Engagement Rule" section.

You can send notifications to the business users such as employees through Cisco Webex Teams, SMS, or e-mail. You can also send notifications to an external API.

To define an engagement rule to send notifications to business users or an external API, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, choose **Engagements**.
Step 2 On the **Engagements** window that appears, click **Create New Rule**.
Step 3 In the **Rule Name** field, enter a name for the engagement rule.
Step 4 From the **When a user is on WiFi and** drop-down list, choose any of the following:

- **Entering a Location**: Choose this option if you want to send the notification to the business user, when a visitor connected to the Wi-Fi enters the location.
- **Away from the Location**: Choose this option if you want to send the notification to the business user, when a visitor connected to the Wi-Fi is away from the location for a specified time. If you are selecting this option, from the **For** scroll list, choose the number of minutes a visitor needs to be away from the location for sending notifications.

Note

- The **Exiting Location** option is no more available. If you are editing an existing Engagement Rule with **Exiting Location** configured, the **Choose User Activity** drop-down list will appear without any selection. You must choose the required option from the **Choose User Activity** drop-down list to save the rule successfully.
- Even if a visitor is physically present in the location, but gets disconnected from the Wi-Fi for the minutes specified in the **For** scroll list, the visitor will be considered for sending notification.

- **Present at Location**: Choose this option if you want to send notification to the business user, when a visitor who is connected to the Wi-Fi is present at the location for a specified duration or at a particular time. If you choose this option, additional fields appear where you can mention the duration or time that needs to be met by the customer to get filtered for this rule.

Step 5 In the **LOCATIONS** area, specify the locations for which you want to send the notifications.

You can configure to send notifications for the entire customer name or a single or multiple locations such as group, floor, or zone. You can add the locations of diffrerent wireless networks such as Cisco Meraki, Cisco Wireless Controller, and so on in an Engagement rule.

You can again filter the locations for which the notification is to send based on the metadata defined for the selected location or its parent or child locations. You can either send the notifications for the locations with a particular metadata or exclude the locations with a particular metadata.

Step 6 In the **IDENTIFY** area, specify the type of customers for whom you want to send the notifications to the business users.

Note You can filter the customers for whom you want to send the notifications to the business users based on whether the customer is an opted in or not opted in user, the tags the customers belong to, and the number of visits made by the customer You can apply all these filters or any of them based on your requirement.

To specify the customers for whom the notification is to send to the business user, perform the following steps:

a) If you want to filter the customers by the opt in status, check the **Filter by Opt-In Status** check box, and choose whether you want to send the notifications for opted in users or not opted in users.

b) If you want to filter the customers based on tags, check the **Filter by Tags** check box.

You can filter the tags in two different ways. Either you can specify the tags for which the notifications are to send or you can specify the tags for which the notifications must not be sent. You can choose the best filtering method based on your requirement. For example, if you want to send the notifications to the business users for all tags expect for one tag, it is easy to opt the exclude option, and mention that particular tag for which you do not want to send the notifications.

c) If you want to filter the customers based on the number of visits made by the customer in the selected locations, check the **Filter by Previous Visits** check box.

Click the **Add Locations** button. In the **Choose Locations** window, specify the locations of which the customer visit needs to consider for filtering. In the following fields, mention the number of visits and duration required to send notifications. For more information on the visits and duration you can configure, refer to the “Previous Visit Criteria” section.

Step 7 In the **SCHEDULE** area, specify the period for which you want to apply the engagement rule.

a) Check the **Set a date range for the rule** check box, and in the fields that appear specify the start date and end date for the period for which you want to apply the engagement rule.

b) Check the **Set a time range for the rule** check box, and in the fields that appear specify the time range for which you want to apply the engagement rule, within the date range specified.

c) If you want to apply the rule only on particular days, check the **Filter by days of the week** check box, and from the list of days that appears, click the days on which you want to apply the engagement rule.

Step 8 In the **ACTIONS** area, perform the following steps:

a) From the Notify drop-down list, choose **Business**, and from the adjacent drop-down list choose any of the following:

- **Only Once** —The notification is sent only once to a business user.
- **Once In** —The notification is sent more than once to a business user based on the notification frequency specified. In the additional fields that appear when you choose this option, specify the notification frequency. For more information on the notification frequency, refer to the "Notification Frequency" section.
- Specify the mode of notification. You can send the notification to the customers through Cisco Webex Teams, e-mail, SMS. You can also send the notification to an external API. For more information on notification types, refer to Notification Type for a Business User, on page 217

Note To display the variables such as first name, last name, mobile number, and so on in the notification message, you must configure the data capture form in the portal. For more information on configuring the data capture form in the portal, refer to the Adding a data capture form to a portal section.

Note The summary of the rule is shown in the right side of the page.

Step 9 Click **Save and Publish**.

The rule gets published and listed in the Engagement Rules page.

Note If you do not want to publish the rule now, you can click the **Save** button. You can publish the rule at any time later by opening the rule, and clicking the **Save and Publish** button. Also, you can publish the rule by clicking the **Make Rule Live** icon at the far right of the rule in the Engagement Rules page.

Use Case: Engagement Rule for a Business User

ABC is a hotel group with hotels around the globe. ABC has many privilege customers, mainly business people, who use its hotels. As part of its 25th anniversary, ABC wants to provide some special gifts to its platinum loyalty members who visits its first hotel at location A. ABC considers all the customers who had visited its hotels at location A or location C minimum 10 times in the last 2 years as platinum loyalty members. ABC wants its customer care representative to directly go and meet the customer, and gift the customers.

ABC wants to send notifications to its customer care representative regarding the arrival of the platinum loyalty members through SMS. The notifications need to send for the opted in users when the customer enters the location. The notifications are to send only for the current month. ABC wants to send the notifications only once for a customer.

To meet the preceding scenario, perform the following steps:

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 Create the location hierarchy with all the locations of ABC.

Step 3 Create a tag for the platinum loyalty members, **Platinum**, using the Profile Rule. The rule must be to filter the customers visited the location A or location C at least 10 times in last 2 years.

Step 4 In the Cisco Spaces dashboard, click **Engagements**.

Step 5 On the **Engagements** window that appears, click **Create New Rule**.

Step 6 In the **RULE NAME** field, enter a name for the engagement rule.

Step 7 From the **When a user is on WiFi and** drop-down list, choose **Entering Location**.

Step 8 In the Locations area, click the **Add Locations** button, and select location A, the location where ABC wants to provide the gifts to the customers.

Step 9 In the **IDENTIFY** area, do the following:

a) Check the **Filter by Opt-In** Status check box, and choose **Only for opted-in Visitor**.
b) Check the **Filter by Tags** check box, and click the **Add Tags** button for Include.
c) In the **Choose Tags** window, click the **Include** radio button for **Platinum1**, created at step 3, and click**Done**.

Step 10 In the **SCHEDULE** area, do the following:

a) Check the **Set a date range for the rule** check box, and specify the start date and end date of the current month for which ABC want to provide the offer.

Step 11 In the **ACTIONS** area, do the following:

a) From the Notify drop-down list, choose **Business**.
b) From the adjacent drop-down list, choose **Only Once**.
c) Check the **Via Email** check box. In the From field, specify the From e-mail ID that must appear in the e-mail, in the "To" field, enter the e-mail ID of the business user to whom you want to send the notification, and in the Subject field, enter a subject for the notification e-mail. If required, edit the notification message displayed in the following text editor.

   The e-mail ID entered in the **From** field must be included in the allowed list for e-mail IDs. To include the e-mail ID in the allowed list, contact Cisco Spaces support team.

Step 12 Click **Save and Publish**.

The engagement rule is published.

What to do next

Now, when an opted in platinum loyalty member enters the premises of location A, a notification is sent to the customer care representative of location A.

Managing Engagement Rules

Pausing an Engagement Rule

To pause an engagement rule, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click **Engagements**.

The **Engagements** window appear with all the engagements rules listed.

Step 2 In the **Actions** column, click the three-dot icon.

Step 3 Click **Pause Rule** of the engagement rule that you want to pause.

Step 4 A warning message appears; click **Pause Rule** to confirm.

The engagement rule is paused.

What to do next

To pause multiple engagement rules, check the check box for the engagement rules that you want to pause, and from the **More Actions** drop-down list at the top of the window, select **Pause**. A warning message appears; click **Pause Rule** to confirm.

Restarting an Engagement Rule

To restart an engagement rule, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click **Engagements**.

The **Engagements** window appear with all the engagements rules listed.

Step 2 In the **Actions** column, click the three-dot icon.

Step 3 Click **Play** for a paused rule.

Step 4 A success message appears on the screen.

The engagement rule is restarted.

What to do next

To restart multiple engagement rules, check the check box for the engagement rules that you want to restart, and from the **More Actions** drop-down list at the top of the window, select **Make Live**.

Modifying an Engagement Rule

To modify an engagement rule, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click **Engagements**.

The **Engagements** window appear with all the engagements rules listed.

Step 2 In the **Actions** column, click the three-dot icon.

Step 3 Click **Edit** of the engagement rule that you want to edit.

Step 4 Make necessary changes.

Step 5 To save the changes, click **Save** or to publish the changes, click **Save and Publish**.

Note A live rule will have only the **Save and Publish** button. When you click the **Save and Publish** button, the rule gets published with the changes.

Deleting an Engagement Rule

To delete an engagement rule, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click **Engagements**.

The **Engagements** window appear with all the engagements rules listed.

Step 2 In the **Actions** column, click the three-dot icon.

Step 3 Click **Delete** of the engagement rule that you want to delete.

Step 4 In the window that appears, confirm deletion.

What to do next

To delete multiple engagement rules, check the check box for the engagement rules that you want to delete, and from the **More Actions** drop-down list at the top of the window, select **Delete**. The delete confirmation dialog appears.

Engagement Rule Report

Cisco Spaces allows you to view the report that is specific to each engagement rule. This report displays the details of the rule activity and the user engagement for a specific rule.

To view the Engagement Rule report for an engagement rule, perform these actions:

Procedure

Step 1 In the Cisco Spaces dashboard, choose **Engagements**.

Step 2 Open **Engagements Rules**.

Click the rule name for which you want the Engagement Rule Report.

Step 3 (Optional) In the **Action** column, click three-dot icon to edit, pause, and delete the engagement rules.

Rule Activity

This section displays the details of notifications sent based on the particular engagement rule.

- **Daily Engagements**—Displays the ratio **"**the total number of notifications sent" to **"**the unique customers to whom the notifications are sent", on each day based on the particular engagement rule. X-axis represents the days in the filtered period. Y-axis represents the number of notifications sent. You can view the data for a particular day by hovering the mouse in the graph in the area for the day.
- **Engagements**—This section displays the total number of notifications sent for each of the targeted locations.
- **Engagement by Time of Day**—This bar graph displays the number of notifications sent to the customers during various timings in a day. This helps you to identify at what time the customers filtered for the rule are present in your business premises, and target them accordingly.

Visitor Engagement

The Visitor Engagement report shows the details of engagements with the visitors based on the Engagement Rule you have configured. To access the Visitor Engagement report, in the Engagements window, click the three-line menu icon at the top-left of the window, and then click **Visitor Engagement** .

Engagements

Total Engagements -The total number of engagements (through SMS, e-mail notificationsn, and puch notification) with the visitors, who have visited the selected location, during the specified period. This metrics

for all the locations from the date of installation of the Cisco Spaces is shown at the top of the report for " **Total Engagements with Visitors** ".

Via SMS - The total number of engagements through SMS to the visitors who have visited the selected during the specified period. The percentage of engagements through SMS out of total engagements is also displayed.

Via Email - The total number of engagements through e-mail to the visitors who have visited the selected during the specified period. The percentage of engagements through e-mail out of total engagements is also displayed.

Via Push Notification - The total number of engagements through app push notifications to visitors during the specified period. The percentage of push engagements out of total engagements is also displayed.

Daily Trends of Engagements

This section displays a line graph that shows the number of engagements from the location on each day of the specified period through various notification types such as SMS, e-mail and so on. The color indicators for various notification types are displayed at the top of the graph. Mouse-over the graph to view the engagement details for a particular day.

Engagement Rule Report

This section lists the report for various Engagement Rules. The date on which the rule is published is shown along with the total number of engagements made based on the rule. You can view the detailed report for a particular Engagement rule by clicking the corresponding rule. For more information on Engagement rule report, see Engagement Rule Report, on page 212.

Engagement URL

The Engagement URL refers to the URL that is provided in the SMS and e-mail notification messages that are sent to the customers. For business users, you can add the engagement URL in the SMS notifications. The users can click this URL to view a site page that is relevant to the notification. For example, you can provide a site page with more information on the discounts and offers available to the customer. You can create this site page using any site development application.

Previous Visit Criteria

You can define various criteria for filtering the customers based on their previous visits.

- **Atleast ..Times**— The rule is applied when the number of customer visits meets the number specified.
  - **Last 1 day**—The rule is applied if the number of customer visits in the last one day meets the number specified.
  - **Last 7 days**—The rule is applied if the number of customer visits in the last 7 days meets the number specified.
  - **Last 15 days**—The rule is applied if the number of customer visits in the last 15 days meets the number specified.
  - **Last 30 days**— The rule is applied if the number of customer visits in the last 30 days meets the number specified.

- **Last 90 days**— The rule is applied if the number of customer visits in the last 90 days meets the number specified.
- **This Weekend**— The rule is applied if the number of customer visits in the current week meets the number specified.
- **This Month**— The rule is applied if the number of customer visits in the current month meets the number specified.
- **This Year**—The rule is applied if the number of customer visits in the current year meets the number specified.
- **Date Range**— The rule is applied if the number of customer visits during a particular period meets the number specified. If you choose this option, additional fields appear where you can mention the start date and end date for the period.

- **Between, ..Times**— The rule is applied when the number of customer visits comes within the number range specified.
  - **Last 1 day**—The rule is applied if the number of customer visits in the last one day comes with in the number range specified.
  - **Last 7 days**—The rule is applied if the number of customer visits in the last 7 days comes with in the number range specified.
  - **Last 15 days**—The rule is applied if the number of customer visits in the last 15 days comes with in the number range specified.
  - **Last 30 days**— The rule is applied if the number of customer visits in the last 30 days comes with in the number range specified.
  - **Last 90 days**— The rule is applied if the number of customer visits in the last 90 days comes with in the number range specified.
  - **This Week**— The rule is applied if the number of customer visits in the current week comes with in the number range specified.
  - **This Month**— The rule is applied if the number of customer visits in the current month comes with in the number range specified.
  - **This Year**— The rule is applied if number of customer visits in the current year comes with in the number range specified.
  - **Date Range**— The rule is applied if the number of customer visits during a particular period comes with in the number range specified. If you choose this option, additional fields appear where you can mention the start date and end date for the period.

Notification Types

Cisco Spaces enables you to send the notifications in the following formats:

- **SMS**—To send the notification as an SMS. For business users, you can define the mobile number to which you want to send the notification.

- **Email**— To send the notification as an e-mail. For business users, you can define the e-mail address to which you want to send the notification.
- **API Notifications**—To send an API notification to an external application. Cisco Spaces enables you to send the notification to a third party application. This notification type is not applicable for customers.
- **Cisco Webex Teams**—To send the notification to the Webex Team account of the business user. This notification type is not applicable for customers. To use this notification type, you must have a Cisco Webex account.

Notification Frequency

The frequency at which you want to send the notification for an engagement rule. You can configure the engagement rule for the following notification frequencies:

- Only Once—To send the notification only once to a user.
- Once in— To send the notification once in the interval specified.
  - Visits—To send the notification when the number of customer visits meet the number specified.
  - Days—To send the notification once in the number of days specified.
  - Weeks— To send the notification once in the number of weeks specified.
  - Months— To send the notification once in the number of months specified.

Location Filter for an Engagement Rule

To specify the locations for which you want to send the notifications, perform the following steps:

1. Click the **Add Locations** button.
2. In the **Choose Locations** window that appears, check the check box for the locations for which you want to send the notifications.
3. Click **Done**.

You can again filter the locations using the metadata defined for the locations. Only the metadata defined for the selected locations and their parent or child locations will be available for selection.

To send notifications only for the locations with a particular location metadata, perform the following steps

1. Check the **Filter by Metadata** check box.
2. In the **Filter** area, click the **Add Metadata** button.

   The **Choose Location Metadata** window appears.
3. From the drop-down list, choose the metadata variable, and choose the value for the variable in the adjacent field.
4. Click **Done**. The selected metadata and variable details are displayed in the **Filter by Metadata** area.

To exclude to send notifications for the locations with a particular metadata, perform the following steps:

1. Check the **Filter by Metadata** check box.
2. In the **Exclude** area, click the **Add Metadata** button.

   The **Choose Location Metadata** window appears.
3. From the drop-down list, choose the metadata variable.
4. Click **Done**. The selected metadata is displayed in the **Filter by Metadata** area.

Notification Type for a Consumer

In the Engagement rule, under the Actions area, specify the modes through which you want to send the notifications to the customer.

- If you want to send the notification through SMS, check the “Via SMS” check box. From the “SMS Gateway” drop-down list, choose the SMS gateway through which you want to send the SMS notification. You can use the **Demo Gateway** provided by Cisco, which is chargeable. For information on adding the SMS gateways, see the message content that is sent to the customer is displayed in the following text box. You can enhance the message content using variables. By default, the first name and last name of the customer, and engagement URL are added as variables. You can add more text variables in the message using the variables that lists below the text box when you click the text box. For more information on adding a text variable, see the Smart Links and Text Variables section.

  If required, in the Link field, enter the engagement URL that must appear in the notification. For more information on creating the engagement URL, see the Engagement URL, on page 213 section.
- If you want to send the notification through e-mail, check the **Via Email** check box. In the **From Name** field, specify the name from which the customer receives the e-mail, in the **From Email** field, specify the e-mail ID from which the customer receives the e-mail, and in the **Subject** field, enter the subject for the notification e-mail. The message content that is sent to the customer is displayed in the following text box. You can enhance the message content using the text variables. By default, the first name and last name of the customer, and engagement URL are added as variables. You can add more text variables in the message using the variables that lists below the text box when you click the text box. For more information on adding a text variable, see the Smart Links and Text Variables section.

  If required, in the **Link** field, enter the engagement URL that must appear in the notification. For more information on creating the engagement URL, see the Engagement URL, on page 213 section.

Note

- If you are using the **Via Email** option, you must ensure to add the e-mail ID entering in the **From** field in the allowed list of e-mail IDs. To include the e-mail ID in the allowed list, contact the Cisco Spaces support team. If you do not want to use a specific e-mail ID, you can use the default allowed e-mail ID **no-reply@dnaspaces.io**. However, the default ID is not displayed in the dashboard automatically. So, you have to enter it manually.
- The variable "$firstName" is to display the first name of the customer, "$lastName" is to display the last name of the customer, "$email" is to display the e-mail address of the customer, "$mobile" is to display the mobile number of the customer", "$URL" is to display the engagement URL, "$gender" is to display the gender of the customer", and "locationName" is to display the location from which the message is sent.
- To display the variables such as first name, last name, mobile number, and so on in the notification message, you must configure the data capture form in the portal. For more information on configuring the data capture form in the portal, refer to the Add a data capture form to a portal section.

Notification Type for a Business User

You can send notifications to the business users through Cisco Webex Teams, SMS and e-mail. You can also send the notifications to an API end point.

- If you want to send the notification through Cisco Webex Teams, check the **Via Cisco Webex Teams** check box. From the **Webex Accounts** drop-down list, choose the Webex account to which you want to send the notifications. You can add a Webex account using the **Add Webex Account** option. To add a webex account , you must specify the webex developer account, and you must generate a token for the particular account using the Webex Developer site. Then you must configure the token in the **Add Webex Account** window within the timeout period shown for the token in the developer site. As an alternate to the default token, you can create Bots in the developer site, and can generate tokens without timeout limitations.

  The message content that is sent to the business users is displayed in the **Notification Message** text box.You can enhance the message using the text variables. By default, the first name and last name of the customer, and the engagement URL are added as variables. You can add more text variables in the message using the variables that lists below the text box when you click the text box. For more information on adding a text variable, see the Smart Links and Text Variables section.
- If you want to send the notification through SMS, check the **Via SMS** check box. From the **SMS Gateway** drop-down list, choose the SMS gateway through which you want to send the SMS notification. You can use the **Demo Gateway** provided by Cisco, which is chargeable. In the **To** field that appears, enter the mobile number (with country code) of the business user to whom you want to send the notifications. If required, in the **Link** field, enter the engagement URL that must appear in the notification. For more information on configuring the engagement URL, see the Engagement URL, on page 213.

  The message content that is sent to the business users is displayed in the following text box.You can enhance the message using the text variables. By default, the first name and last name of the customer, and the engagement URL are added as variables. You can add more text variables in the message using the variables that lists below the text box when you click the text box. For more information on adding a text variable, see the Smart Links and Text Variables section.

- If you want to send the notification through e-mail, check the **Via Email** check box. In the **From** field, specify the "From e-mail ID" that must appear in the e-mail, in the **To** field, enter the e-mail ID of the business user to whom you want to send the notification, and in the **Subject** field, enter a subject for the notification e-mail.

Note The e-mail ID entered in the **From** field must be included in the allowed list for e-mail IDs. To include the e-mail ID in the allowed list, contact Cisco Spaces support team. If you do not want to use a specific e-mail ID, you can use the default allowed e-mail ID **no-reply@dnaspaces.io**. However, the default ID is not displayed in the dashboard automatically. So, you have to enter it manually.

The message content that is sent to the business user is displayed in the following text box. By default, the first name and last name of the customer, and the engagement URL are added as variables. You can add more text variables in the message using the variables that lists below the text box when you click the text box. For more information on adding a text variable, see the Smart Links and Text Variables section. If required, in the **Link** field, enter the engagement URL that must appear in the notification. For more information on configuring the engagement URL, see the Engagement URL, on page 213.

- If you want to send the notification to an external API, check the **Trigger API** check box. For more information on the configurations for Trigger API, see the "Trigger API Configuration for Notification" section.

Smark Links and Text Variables for Engagements Rule and Density Rule

In Engagement Rules and Density Rules, you can add text variables in the notification messages sent for all notification types (**Via Cisco Webex Teams**, **Via SMS**, **Via Email**, and **Trigger API**), and can create smart links for **Trigger API** URI. The varilables enable you to display the customer, location and device details in the notification message or Trigger API URI. By default, the notification message will have first name and last name of the customer. You can add additional additional details using the variables.

For example, assume that you have created an engagement rule to send SMS notifications to the customers and have configured the variables "mobile" and "gender" in the message text box for the SMS notification. Now, when a customer receives a SMS message based on this engagement rule, the mobile number and gender details of the customer are also shown in the message.

Note Cisco Spaces captures the personal details of the customers using the Data Capture form. That is, to include the personal details such as first name, last name, gender, and so on in the smart link or as text variable, you must configure the Data Capture form in the portal. For more information on adding a Data Capture form to a captive portal, refer to the Add a data capture form to a portal section.

You can include static and dynamic variables in the notification message and URLs.

The static variables that you can include in the notification message are as follows:

Table 14: Static Variable List

Static Variable Name	Description
$firstName	First name of the customer.
$lastName	Last name of the customer.
$email	E-mail address of the customer.
$mobile	Mobilie number of the customer.
$gender	Gender of the customer.
$URL	URL link value.
$TotalAreaValue	The total area configured for the location in the **Location Info** window in **Location Hierarchy**.
$TotalAreaUnit	The total area unit configured for the location in the **Location Info** window in **Location Hierarchy**.
$TotalCapacity	The total capacity configured for the location in the **Location Info** window in **Location Hierarchy**.
$locationName	Name of the location for which the rule is triggered.,
$buildingName(Only for Density Rules)	Building name of the location for which the notification is triggered.
$floorName(Only for Density Rules)	Floor name of the location for which the notification is triggered.
$zoneName (Only for Density Rules)	Zone name of the location for which the notification is triggered.
$deviceCount (Only for Density Rules)	Device count for the location for which the notification is triggered.
$locationPath (Only for Density Rules)	The location path (parent hierarchy) for the location for which the rule is triggered. The locations in the hierarchy will be separated by '>' (Sample Format: Account>CMXNode>Campus>Building>Floor>Zone).
The **Trigger API** notification type will be having the following additional variables for both Engagements Rules and Density Rules.	
$macaddress	The mac address of the device.
$encryptedMacAddress	The encrypted mac address of the device.
$deviceSubscriberId	The subscriber ID for the device in the database.
$optinStatus-	The opt in status for the customer.

The dynamic variables that you can include in the notification message and URLs for Enagagements Rule and Density Rule are as follows:

Table 15: Dynamic Variable List

Dynamic Variable Name	Description
Business Tags	The business tag to which the customer belongs to. The business tags configured in the Data Capture form are listed as variables. For more information on creating a business tag, refer to the Add a data capture form to a portal section.
Location Metadata	The location metadata for the customer location. The location metadata keys defined in the location hierarchy are listed as variables.or more information on defining the location metadata, refer to Location Hierarchy.

To include a smart link in the URL or text variable in the notification message, perform the following steps:

Procedure

Step 1 To include smart link, click anywhere inside the **URI** field. To include text variable, click anywhere inside the notification message text box. To include text variable for **Via Email**, click the **Smartlinks** drop-down list in the rich text editor.

The variables that you can include get listed.

Step 2 Choose the variables that you want to include.

Trigger API Configuration for Notification

To send notifications to an external API through the rules, in the Create [Rule Name] window, in the Actions area, perform the following steps:

1. Check the **Trigger API** check box.
2. From the **Method** drop-down list, choose the method for triggering API.

Note You can add the customer details in the notification message, by adding the link variables in the API URI or text variables in the method parameters.

- **Get** — To send notification or customer details to the API using the "GET" method. If you choose this method, additional fields appear where you can mention the GET request headers and parameters to include additional details such as first name, last name, mobile number, and so on of the customer in the notification. You can add the request parameter keys defined in your API and mention the values for them using text variables. The value can be a hard-coded value or a variable. You can

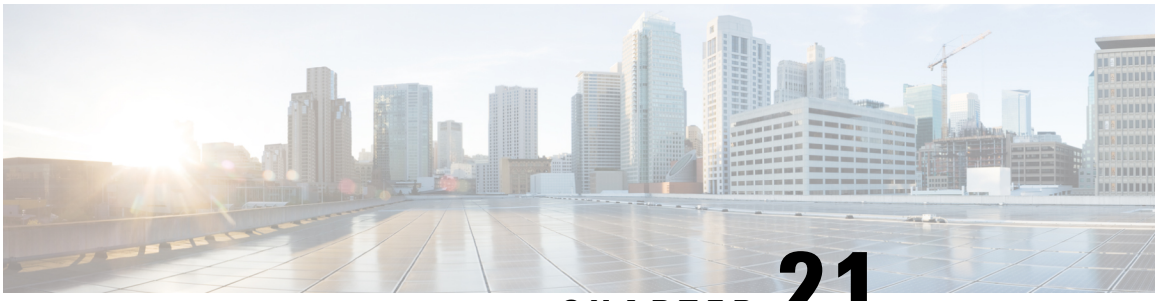
view the variables that you can add by clicking the “Value” field. You can add more **GET** headers and parameters using the corresponding **Add** button.

- **Post Form** — To send notification or customer details to the API using the “POST FORM” method. If you choose this method, additional fields appear where you can mention the POST FORM request headers and parameters to include additional details such as first name, last name, mobile number, and so on of the customer. You can add the form parameter keys defined in your API and mention the values for them.The value can be a hard-coded value or a variable. You can view the variables that you can add by clicking the “Value” field. You can add more “form parameters” using the **Add** button.
- **Post JSON** — To send notification or customer details to the API using the “POST JSON” method. If you choose this method, request header fields appear, along with a text box where you can mention the JSON data that is to send as notification message to the API. You can mention the values for various JSON request header fields defined in your API. The value can be a hard-coded value or a variable. You can view the variables that you can add by clicking the “Value” field. You can view the variables that you can add to the JSON Data by clicking the text box.
- **Post Body** — To send notification or customer details to the API using the "POST BODY" method. If you choose this method, an request header fields appear where you can mention the content that must be included in the notification sent to the API, along with a **Post Body Data** field. You can mention the values for various Body request header fields defined in your API. The value can be a hard-coded value or a variable. You can view the variables that you can add by clicking the “Value” field. You can view the variables that you can add to the **Post Body Data** field when you clicking the field.

Note Only those data that you have configured to capture using the Data Capture form in the portal are included in the notifications.

3. In the URI field, enter the URI for the API. You can include additional details of the customers in the notification message using the smart links. To view the variables that you can include in the URI, click the **URI** field.

   - For information on variables that you can add for the Captive Portal Rule, refer to the Smart Links and text variables for Captive Portals.
   - For information on variables that you can add for the Engagement or Density Rule, see Smark Links and Text Variables for Engagements Rule and Density Rule, on page 218



CHAPTER 21

Cisco Spaces: Location Personas App

Cisco Spaces enables you to group the customers using tags. You can then use these tags in the Cisco Spaces rules such as Engagement Rules. In Cisco Spaces, you can create tags using the Location Personas app.You can also use the Location Personas app to add more customers to the existing tags, or to remove certain customers from an existing tag. You can group a customer under multiple tags.

When you create a tag, you can use the existing tags to filter the customers from the selected locations. For example, if you want to create a tag with location A and location B, but only for android users, you can use the tag filter to remove the tag for iOS.

- Create or Modify Tags, on page 223
- Use Case: Location Personas Rule (Profile Rule), on page 227
- Managing Location Personas Rules, on page 230
- Location Personas Rule Report, on page 232

Create or Modify Tags

To create a tag, or to include the customers to or exclude the customers from an existing tag, perform the following steps:

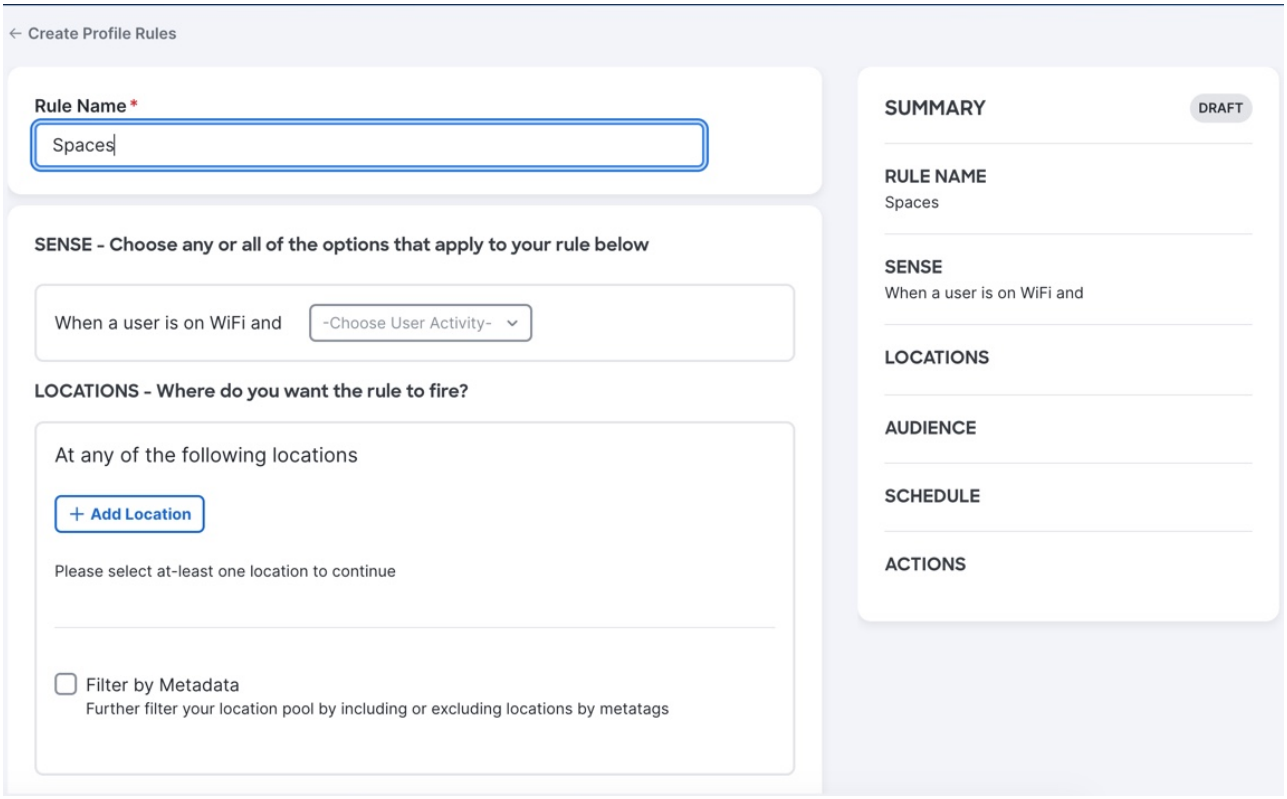
Procedure

Step 1 From the left navigation pane, choose **Dashboard** > **Location Personas**.
The **Location Personas** app is displayed. In the left navigation pane, view three tabs: **Location Personas Rules**, **User Management**, and **Related Links**.

Step 2 In the **Location Personas Rules** tab, click **Create New Rule**.

Step 3 In the **Rule Name** field, enter a name for the Location Personas/Profile rule.

Figure 36: Create Profile Rules



Step 4 From the **When a user is on WiFi and** drop-down list, choose any of the following:

- **Entering a Location**: Choose this option if you want to tag the visitors with Wi-Fi connected, when they enter the location.
- **Away from the Location**: Choose this option if you want to tag the visitors with Wi-Fi connected and are away from the location for a specified time. If you are selecting this option, from the **For** scroll list, choose the number of minutes a visitor needs to be away from the location for tagging based on the this rule.

Note

- The **Exiting Location** option is no more available. If you are editing an existing **Location Personas** rule with **Exiting Location** configured, the **Choose User Activity** drop-down list will appear without any selection. You must choose the required option from the **Choose User Activity** drop-down list to save the rule successfully.
- Even if a visitor is physically present in the location, but gets disconnected from the Wi-Fi for the minutes specified in the **For** scroll list, the visitor will be considered for tagging for this rule.

- **Present at Location**: Choose this option if you want to tag the visitors who are connected to the Wi-Fi and are at present at the location for a specified duration or at a particular time. If you choose this option, additional fields appear where you can mention the duration or time that needs to be met by the visitor to get filtered.

Step 5 In the **LOCATIONS** area, specify the locations of which you want to filter the customers for the rule.

You can choose the entire customer name or single or multiple locations such as group, campus, building, floor, or zone. You can add the locations of both CUWN and Cisco Meraki.

You can again filter the locations based on the metadata defined for the selected location or its parent or child locations. You can either choose the locations with a particular metadata or exclude the locations with a particular metadata. For more information on configuring the location for the profile rule, refer to the Location Filter for a Location Persons Rule, on page 229

Step 6 In the **IDENTIFY** area, specify the type of customers that you want to filter for the rule.

Note You can filter the customers based on whether the customer is an opted in or not opted in user, the tags the customers belong to, the number of visits made by the customer, and the status of the app in the customer's device. You can apply all these filters or any of them based on your requirement.

To specify the customers whom you want to filter for the rule, perform the following steps:

a) If you want to filter the customers by the Opt In Status, check the **Filter by Opt-In Status** check box, and choose whether you want to filter the opted in users or not opted in users for the rule.

Note For more information on opted in users, refer to the Opted In Option for Users, on page 229.

b) If you want to filter the customers based on the tags, check the **Filter by Tags** check box.

Note You can filter the customers by including or excluding existing tags. You can filter the tags in two different ways. Either you can specify the existing tags of which you want to include the customers for the rule or the existing tags of which you want to exclude the customers for the rule. You can choose the best filtering method based on your requirement. For example, if you want to add the customers of all the existing tags expect one tag, it is easy to opt the exclude option, and mention that particular tag of which you want to exclude the customers.

c) If you want to filter the customers based on the number of visits made by the customer in the selected locations, check the **Filter by Previous Visits** check box.

Click the **Add Locations** button. In the **Choose Locations** window, specify the locations of which the customer visit needs to consider for filtering. In the following fields, mention the number of visits and duration required to be met by the customers to be filtered for the rule.

Step 7 In the **SCHEDULE** area, specify the period for which you want to apply the rule for filtering the customers.

Note Only those customers who meet the preceding conditions during the period specified are filtered for the rule.

a) Check the **Set a date range for the rule** check box, and in the fields that appear, specify the start date and end date for the period for which you want to apply the profile rule.

b) Check the **Set a time range for the rule** check box, and in the fields that appear, specify the time range for which you want to apply the profile rule.
c) If you want the rule to be executed only on particular days, check the **Filter by days of the week** check box, and from the list of days that appears, click the days on which you want to apply the rule.

Step 8 In the **ACTIONS** area, specify whether you want to create a new tag by including or excluding the customers filtered based on the preceding conditions, or to include or exclude the filtered customers from an existing tag.

a) Click **Add Tags**.

- If you want to add or remove the filtered customers from the existing tags, mention the tags to which you want to include the filtered customers and the tags from which you want to exclude the filtered customers.
  - To add the customers that are filtered based on this profile rule to an existing tag, choose the Add radio button for the tags to which you want to add the customers.
  - To remove the customers that are filtered based on this profile rule from an existing tag, choose the Remove radio button for the tags from which you want to remove the customers.



Note In the **Choose Tags** window, you can search for a tag using the Search option. The tags selected are displayed on the right side of the window.

- If you want to create a new tag with the rule, click the **Create New Tag** button. In the "Enter the tag name" field that appears, enter a name for the tag, and click **Add**. The newly created tag gets listed in the tag list. Choose whether you want to include or exclude the filtered customers from the tag.

b) Click **Done.**.



Note Using a profile rule, you can create a tag by including or excluding the filtered customers, or you can modify an existing tag by including or excluding the filtered customers, simultaneously. You can also create more than one tag for a rule.



Note The summary of the rule is shown on the right side of the page.

Step 9 Click **Save and Publish**.

The rule gets published and listed in the Profile Rules page.



Note If you do not want to publish the rule now, you can click the Save button. You can publish the rule at any time later by clicking the **Save and Publish** button. Also, you can publish the profile rule by clicking the **Make Rule Live** icon at the far right of the rule on the **Location Personas** window.

Use Case: Location Personas Rule (Profile Rule)

ABC hotel group as part of its 25th anniversary wants to provide some special gifts to its platinum loyalty members. ABC considers all the customers who had visited its hotels at location A or location C minimum 10 times in the last 2 years as platinum loyalty members. All the visitors who have connected to the Wi-Fi at least 45 minutes are to consider as customers. ABC wants to create a tag for its platinum loyalty members. The opted in customers who meet the previous conditions within the end of the current month are to add to the tag.

To meet the preceding scenario, perform the following steps:

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 Create the location hierarchy with all the locations of ABC.

Step 3 From the left navigation pane, choose **Dashboard** > **Location Personas**.

Step 4 In the **Location Personas Rules** tab, click **Create New Rule**.

Step 5 In the **Rule Name** field, enter a name for the profile rule.

Step 6 From the **When a user is on WiFi and** drop-down list, choose **Present at Location,**, and from the drop-down list that appears, choose **45** Minutes.

Step 7 In the **LOCATIONS** area, click the **Add Locations** button, then select location A and location C.

Step 8 Click **Done**.

Step 9 In the **IDENTIFY** area, do the following:

a) Check the **Filter by Opt-In Status** check box, and choose **Only for opted-in Visitor**.
b) Check the **Filter by Previous Visits** check box, and click the **Add Locations** button, and add Location A, and Location C.
c) In the following fields, choose **At least**, **10** times in, and **Date Range**, respectively.
d) In the date range fields, enter the start date and end date for the last two years.

Step 10 In the **SCHEDULE** area, check the **Set a date range for the rule** check box, and specify the start date as today's date and end date as last date of the current month.

Step 11 In the **ACTIONS** area, do the following:

a) Click the **Add Tags** button.
b) In the **Create Tags** window, Click **Create New Tag**.
c) In the **Enter the tag name** field, enter **Platinum1**, and click **Add**. In the Tag list, click the **Include** radio button for Platinum1, and click **Done**.

Step 12 Click **Save and Publish**.

The profile rule is published.

Filter by Tag

You can either opt to include or exclude the tags for filtering.

Including a Tag

To include a tag, perform the following steps:

Procedure

Step 1 In the **Filter by Tags** area of the proximity rule (captive portal rule, engagement rule, profile rule), click the **Add Tags** button for **Include**.

Step 2 In the **Choose Tags** window, click the **Include** radio button for the tag that you want to include.

Step 3 Click **Done**.

Excluding a Tag

To exclude a tag, perform the following steps:

Procedure

Step 1 In the **Filter by Tags** area of the proximity rule (captive portal rule, engagement rule, profile rule), click the **Add Tags** button for **Exclude**.

Step 2 In the **Choose Tags** window, click the **Exclude** radio button for the tag that you want to exclude.

Step 3 Click **Done**.

Search for a Tag

To search for a tag, perform the following steps:

Procedure

Step 1 In the window to create a new rule, in the Filter by Tags area, click the **Add Tags** button for Include or Exclude.

Step 2 In the **Choose Tags** window, enter the name of the tag that you want to search.

The tag list gets filtered with the search results.

Clearing a Tag

If you choose an include or exclude radio button for a tag, you can clear the selection using the **Clear Selection** option for that tag.

Opted In Option for Users

Cisco Spaces enables you to provide an option in the captive portal for the customers to opt out from the notification subscriptions.

In the portal, check the **Allow users to opt in to receive message** check box to provide an option for the customers to opt for the subscriptions. The option **Allow users to opt in to receive message** is available for the authentication types **SMS with password verification** or **Email**.

By default, the customers are opted in for subscription. The customers can opt out from subscription when accessing the captive portal. When a customer accesses the captive portal by connecting to an SSID, the opt in check box is displayed to the customer.

Location Filter for a Location Persons Rule

To specify the locations, perform the following steps:

1. Click the **Add Locations** button.
2. In the **Choose Location** window that appears, select the locations for the profile rule.
3. Click **Done**.

You can again filter the locations using the metadata defined for the locations. Only the metadata defined for the selected locations and their parent or child locations will be available for selection.

To include a locations with a particular meta data, perform the following steps:

Procedure

Step 1 Select the **Filter by Metadata** check box.

Step 2 In the Filter area, click the **Add Metadata** button.

The **Choose Location Metadata** window appears.

Step 3 From the drop-down list, choose the metadata variable, and choose the value for the variable in the adjacent field.

Step 4 Click **Done**.

To exclude a location with a particular metadata, perform the following steps:

Procedure

Step 1 Select the **Filter by Metadata** check box.

Step 2 In the Exclude area, click the **Add Metadata** button.

The **Choose Location Metadata** window appears.

Step 3 From the drop-down list, choose the metadata variable, and choose the value for the variable in the adjacent field.

Step 4 Click **Done**.

Managing Location Personas Rules

You can pause a Location Personas (Profile) Rule and make it live again, whenever required. You can modify a Location Personas rule, and delete it if required. You can create Location Personas rules specific to a location, and view them from the location hierarchy.

Pausing a Location Personas Rule

To pause a Location Personas rule, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click **Location Personas**.

The **Location Personas** window appears with all the existing Location Personas rules.

Step 2 Click the **Pause Rule** icon that appears at the far right of the Location Personas rule that you want to pause.

The Location Personas rule is paused.

What to do next

To pause multiple Location Personas rules, check the check box for the Location Personas rules that you want to pause, and from the **More Actions** drop-down list at the top of the window, select **Pause**.

Restarting a Location Personas Rule

To restart a Location Personas rule, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click **Location Personas**.

The **Location Personas** window appears with all the existing Location Personas rules.

Step 2 Click the **Make Rule Live** icon that appears at the far right of the Location Personas rule that you want to restart.

The Location Personas rule is restarted.

What to do next

To restart multiple Location Personas rules, check the check box for the Location Personas rules that you want to restart, and from the **More Actions** drop-down list at the top of the window, select **Make Live**.

Modifying a Location Personas Rule

To modify a Location Personas rule, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click **Location Personas**.

The **Location Personas** window appears with all the existing Location Personas rules.

Step 2 Click the **Edit Rule** icon for the Location Personas rule that you want to modify.

Step 3 Make necessary changes.

Step 4 To save the changes, click **Save** or to publish the changes, click **Save and Publish**.



Note A live rule will have only the **Save and Publish** option. When you click the **Save and Publish** button, the rule gets published with the changes.

Deleting a Location Personas Rule

To delete a Location Personas rule, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click **Location Personas**.

The **Location Personas** window appears with all the existing Location Personas rules.

Step 2 Click the **Delete Rule** icon that appears at the far right of the Location Personas rule that you want to delete.

What to do next

To delete multiple Location Personas rules, check the check box for the Location Personas rules that you want to delete, and from the **More Actions** drop-down list at the top of the window, select **Delete**.

Viewing a Location Personas Rule for a Location

To view a Location Personas rule for a location such as group, building, floor, and so on, perform the following steps:

Procedure

Step 1 Click the three-line menu icon at the top-left of the Cisco Spaces dashboard.

Step 2 Choose **Location Hierarchy**.

The **Locations** window appears with the location hierarchy.

Step 3 Click the location for which you want to view the Location Personas rule.

Step 4 Click the **Rules** tab.

Step 5 Click the **Profile Rule** tab.

The Location Personas rules for the location gets listed.

What to do next

Note You can also access the **Rules** tab by clicking the **Rules** link that appears for each location in the location hierarchy. The **Rules** link for a location is enabled only if at least one proximity rule exists for that location.

Location Personas Rule Report

The Location Personas Rule report shows the performance of Location Personas rules. It is specific to a Location Personas rule.

To view the Location Personas (Profile) Rule report for a Location Personas rule, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click **Location Personas**.

The **Location Personas** window appears with all the existing Location Personas rules.

Step 2 Click the rule for which you want to the Location Personas Rule Report.

Step 3 In the Filter area, choose the period for which you want to view the report.

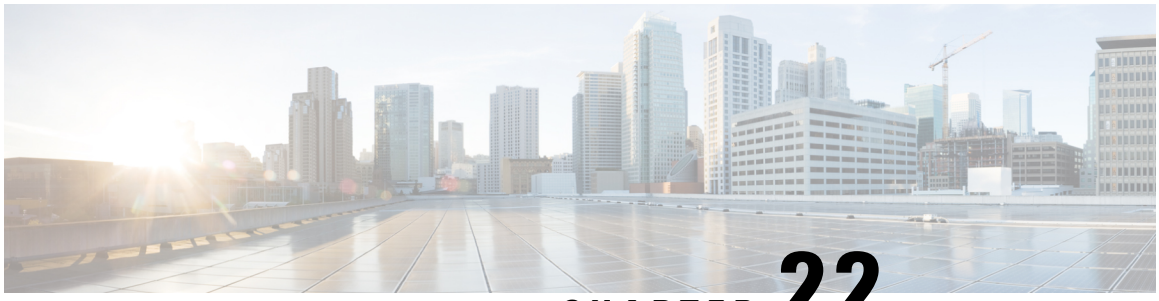
- **Total Devices Tagged**—The total number of devices tagged for the Location Personas rule from the day on which the Location Personas rule is created.

- **Total Users Tagged**—The total number of visitors tagged for the particular Location Personas rule from the day on which the Location Personas rule is created.
- **Total Tags Removed**—The total number of visitors removed from the tags mentioned in the Location Personas rule from the day on which Location Personas rule is created.

Rule Activity

This section displays the number of customers and devices tagged based on the particular Location Personas rule during the specified period.

- **Tagging Trends**—Displays the total number of devices and customers tagged for the particular rule during the specified period. Also displays the number the customers removed from the tags based on the particular Location Personas rule. The line graph represents the total number of tags added or removed on each day of the specified period. If the duration specified is less than a week, the data will be shown in a bar graph. If the duration specified is not more that 2 days, the graph displays the number of customers tagged at various timings of each day.
- **Tags Added**—Displays the total number of tags created for the rule.
- **Device Tags added by Location**—Displays the number of devices tagged from each location during the specified period.
- **Tags Removed by Location**—This section will be displayed only if it is specified in the Location Personas rule to remove the filtered devices from a particular tag. The total number of devices untagged from each location based on the particular Location Personas rule during the particular period is shown.
- **Tagging by Time of Day**—This bar graph displays the number of customers added to various tags based on the Location Personas rule, at various timings of a day, during the specified period. This helps in identifying the time at which the customers targeted by this rule visits the targeted locations the most.



CHAPTER 22

Cisco Spaces: Asset Tracker App

- Working with the Cisco Spaces: Asset Tracker App, on page 235

Working with the Cisco Spaces: Asset Tracker App

The Cisco Spaces: Asset Tracker app enables you to:

- Search, monitor, categorize, and manage tracked assets across configured locations using list and map views.
- Associate tags with assets, assign labels, configure rules and notifications, manage user access, and review tag reports.

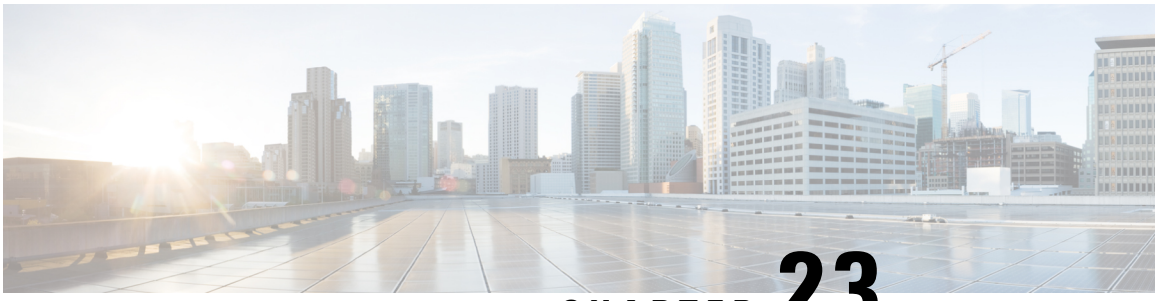
For more information, refer to the Cisco Spaces: Asset Tracker App Configuration Guide.



PART V

Location Hierarchy

- Location Hierarchy, on page 239



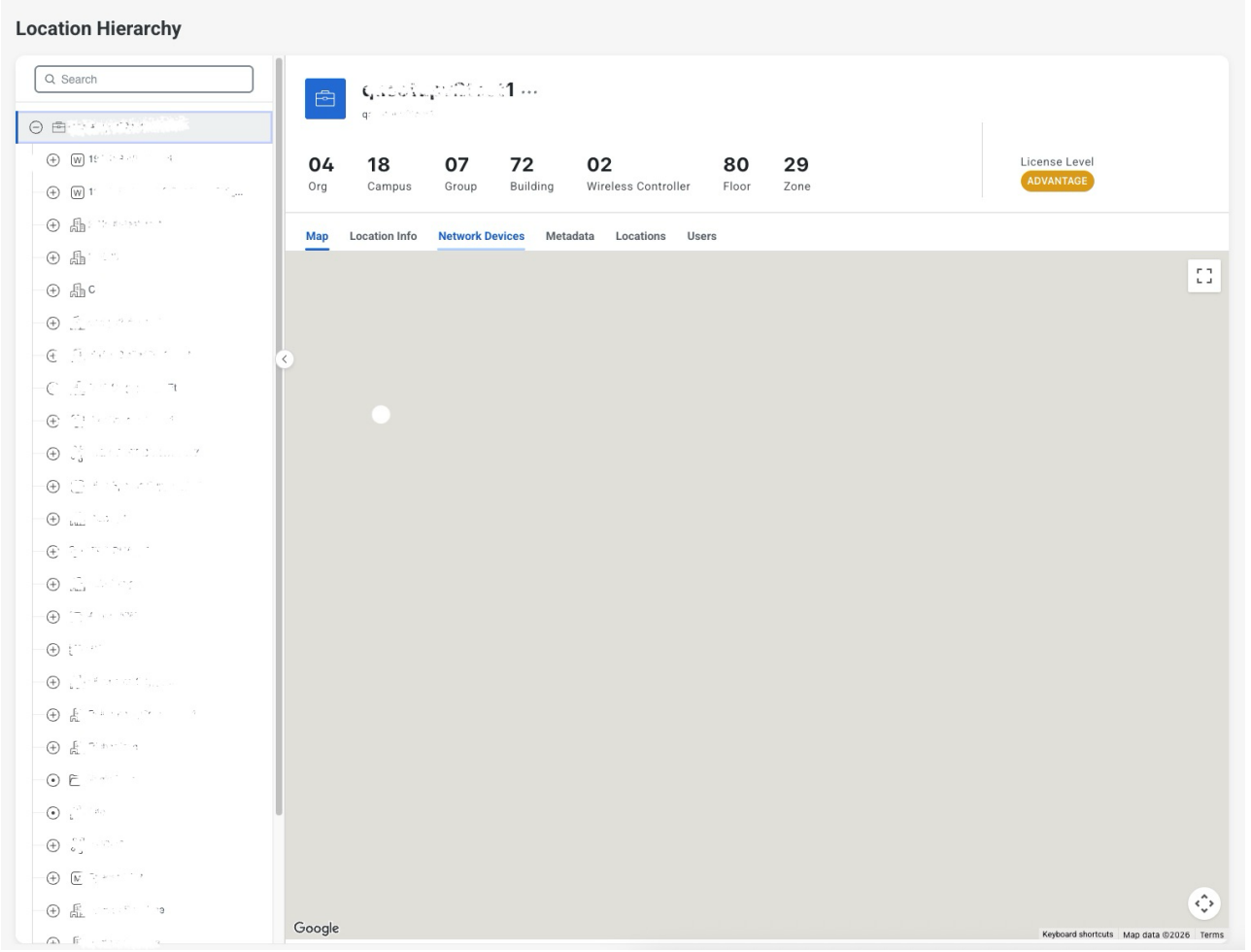
CHAPTER 23

Location Hierarchy

Location Hierarchy's enhanced user interface simplifies the import of locations in the same structure that you have defined using Cisco AireOS Wireless Controller, Cisco Catalyst 9800 Series Wireless Controller, or Cisco Meraki, in your wireless network.

The hierarchical structure in maps imported from Cisco Prime Infrastructure or Catalyst Center is automatically reflected in Location Hierarchy.

In **Location Hierarchy** window, the default customer name (root location) is automatically selected, and the **Map** tab displays the location on the map.



The left pane of the **Location Hierarchy** window displays the imported root locations with the default customer name (root name). You can click the plus sign to expand and view the hierarchy. You can view the buildings and the associated floors in the root location.

If you select a root location from the left pane, you can also view additional information related to the number of organizations, campuses, wireless controller, buildings, groups, floors and zones.

The screen opens with the Location Hierarchy title, a searchable hierarchy tree, a collapsible left pane, and the selected root location when no other location is already selected.

The selected-location summary can also display a license-level badge when the account is enabled for Smart Licensing and license information is available for the selected location.

When Smart Licensing is enabled, Cisco Spaces can display license-level badges next to locations in the hierarchy tree. The badge indicates the license level that is applicable to the corresponding hierarchy node.

For a selected location, building or floor, additional information is displayed in the following tabs:

- **Map**: Displays the selected location on the map
- **Location Info**: Displays the location data information
- **Network Devices**: Displays all the connected network devices and running devices and view the count of these devices

- **Metadata**: Displays the configured metadata information
- **Rules**: Displays the rules for **Captive Portal**, **Engagement**, **Location Personas** and **Density**
- **Locations**: Displays the location nodes
- **Users**: Displays the users
- **License Usage**: Displays the license type, access points, webex devices, meraki camera, locations and building units information

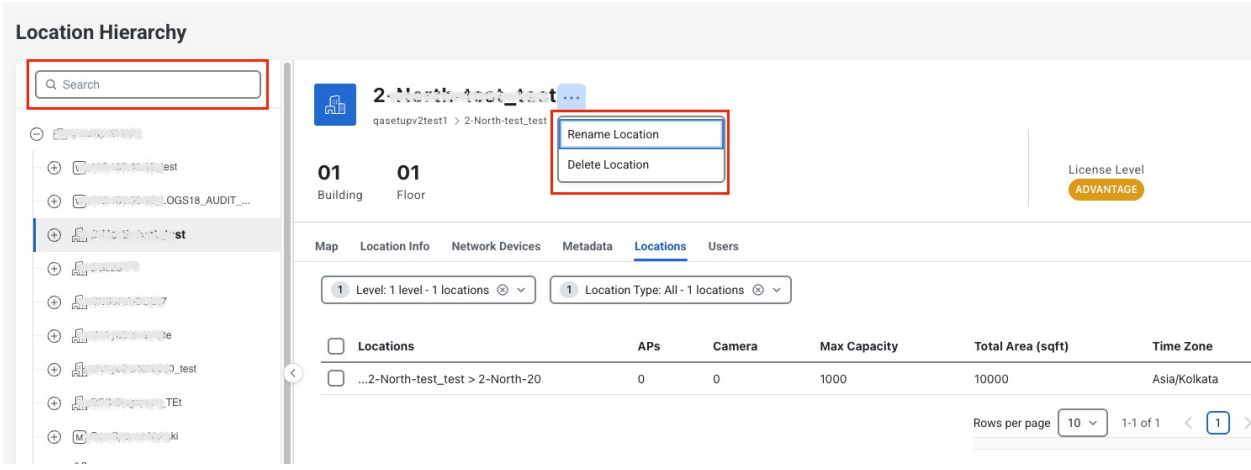
Note

- The **Rules** tab is displayed only for license levels of Advantage or higher.
- The **License Usage** tab is displayed only when Smart Licensing is enabled for the account.

You can perform the following additional tasks in the **Location Hierarchy** window:

- **Search**: Use the **Search** field to search for available locations. The search functionality works if you enter just a single character. The **Recent Searches** area displays the search results.
- **Rename**: Click the three dots next to the location and click **Rename Location** to edit the location name.
  - For the root location, only the option to rename the location is displayed.
  - For all other locations except the root, both the options to rename and delete the location is displayed.
- **Delete**: Click the three dots next to the location and click **Delete Location** to delete the location from **Location Hierarchy**.
- **Rename** and **Delete** actions are available only for locations where the signed-in user has Full access. Polygon zones are not renamed from this menu; they are updated from the floor map. Wireless Controller locations can also show Add/Edit Controller, and AP Zone locations can show Modify Access Points.

Figure 37: Location Hierarchy - Rename and Delete options



Location Hierarchy shows rich maps, if they are available for a particular floor. The option to upload rich maps is currently available under **Setup** > **Locations & Maps**. Click the **3D** toggle button to switch between 2D and 3D floor maps.

The 2D/3D toggle is shown only for floor locations. The 3D view is enabled when the selected floor has supported rich-map data and the parent building or network has a valid rich-map status. If rich maps are not enabled, the 2D/3D control is displayed in a disabled state.

In **Location Hierarchy**, only those locations that a Cisco Spaces user can access are displayed. The accessibility to these locations are defined when you create or edit roles or invite or edit the Cisco Spaces user in **Admin Management**.

- Manage Locations in Map view, on page 242
- Update Location Information, on page 245
- View the Network Devices, on page 247
- Configure Metadata, on page 248
- View Locations, on page 250
- View Users, on page 255
- View License Usage, on page 255

Manage Locations in Map view

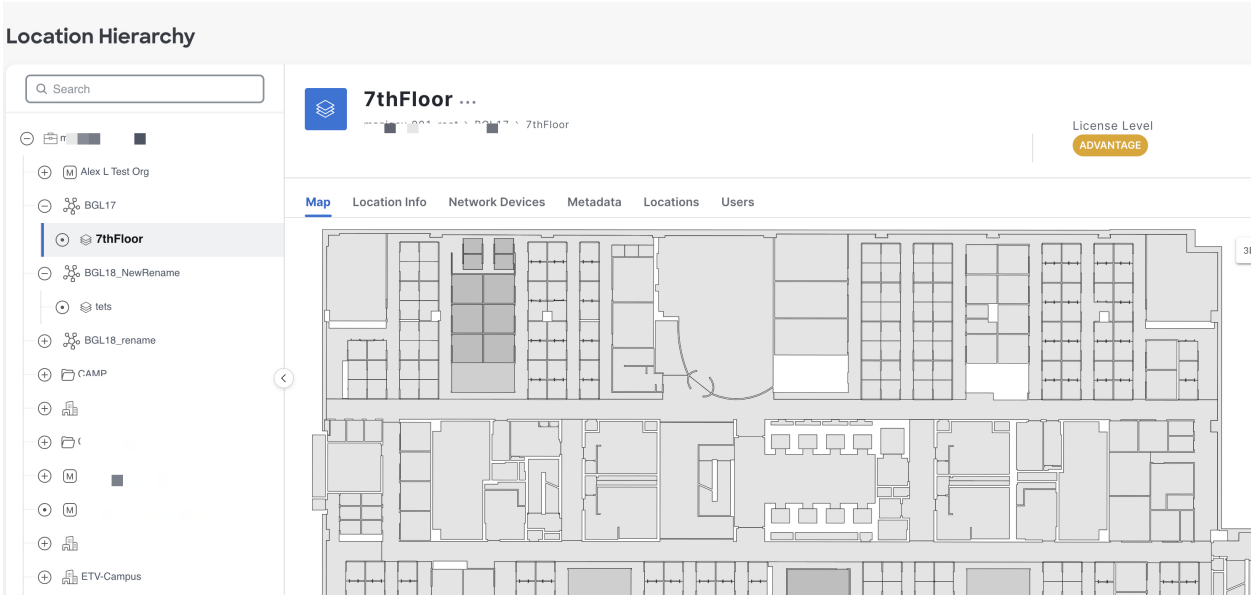
Use the **Map** tab (**Cisco Spaces dashboard** > **Menu icon (** **)** > **Location Hierarchy** > **Root Location**) to view the selected location, campus, building and floor information on the map.

The **Map** tab displays diff ernet map types such as default world map, latitude and longitude based maps, and 2D or 3D floor maps.

If you select the root location, the default world map is displayed.

However, in some instances, the map automatically zooms into the precise location on the map and is displayed with a map pin. You can click on the map pin to view the additional information such as location address, total area, maximum capacity, time zone details and so on. The precise location is plotted based on the latitude and longitude information.

Figure 38: Map Tab



If you select a building, the default world map is displayed.

If you select a floor, the exact floor map image is displayed. Use the Polygon tool ( ) to create zones. For more information, refer to Create a Zone for a Floor Location, on page 243.

Depending on the location you select, view these information:

- Organization
- Campus
- Building
- Floor
- Zone

Create a Zone for a Floor Location

Use the **Map** tab to create Cisco CMX zones in **Location Hierarchy**.

The current implementation creates and updates polygon zones from the floor map for supported floor maps. Zone creation is available only when the selected floor has Full access and a 2D floor map is available.

Note Currently, Cisco Meraki zone-based reports are only supported in the **Live Occupancy** application and **Firehose** device location update events.

In Location Hierarchy 2.0, you can create polygon zones for the floor locations under the Cisco Meraki network. To create polygon zones on the floor map, use the **Polygon tool** ( ) that is available in the floor

map view under the **Map** tab. The new polygon zones created are displayed under both Location Hierarchy and Location Hierarchy 2.0.

Procedure

Step 1 Log in to Cisco Spaces.

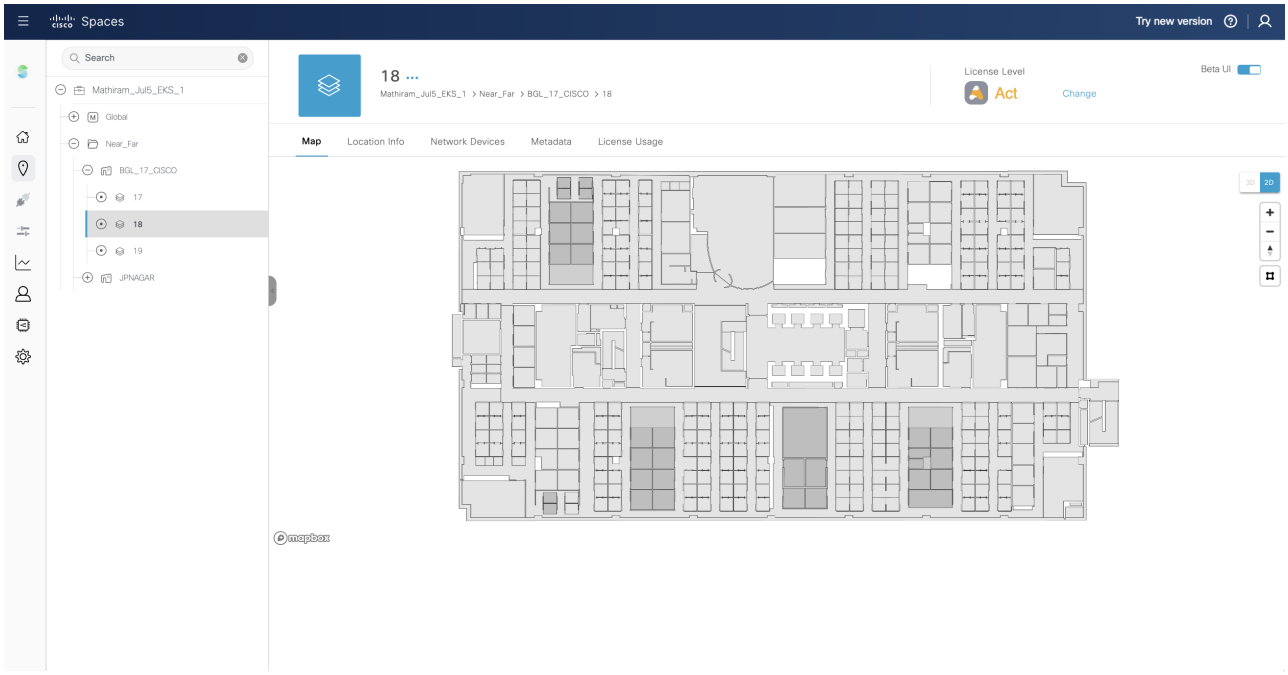
Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Location Hierarchy**.

The **Location Hierarchy** window is displayed.

Step 3 In the left pane, navigate to the required floor location.

The floor map is displayed.

Figure 39: Map Tab



Step 4 Click the Polygon tool ( ) on the map.

The cursor changes to a plus icon.

Step 5 Click the required map area and move the cursor to draw a polygonal zone of your choice.

Step 6 Double-click to complete the zone creation.

A pop-up window is displayed on the right pane.

Step 7 In the **Zone Name** field, enter the new zone name.

Step 8 Select the overlay color to distinguish the zone.

Step 9 Click **Save**.

- The new zone is created, and the **Location Hierarchy** window is refreshed to display the root location.

- In the left pane, navigate to the floor where you created the new zone and the zone is now listed as a new item under the floor hierarchy.

Step 10 (Optional) Click the Polygon tool ( ) on the map to update the zone details.

Update Location Information

Use the **Location Info** tab (**Cisco Spaces dashboard** > **Menu icon ( )** > **Location Hierarchy** > **Root Location**) to view and edit the location information.

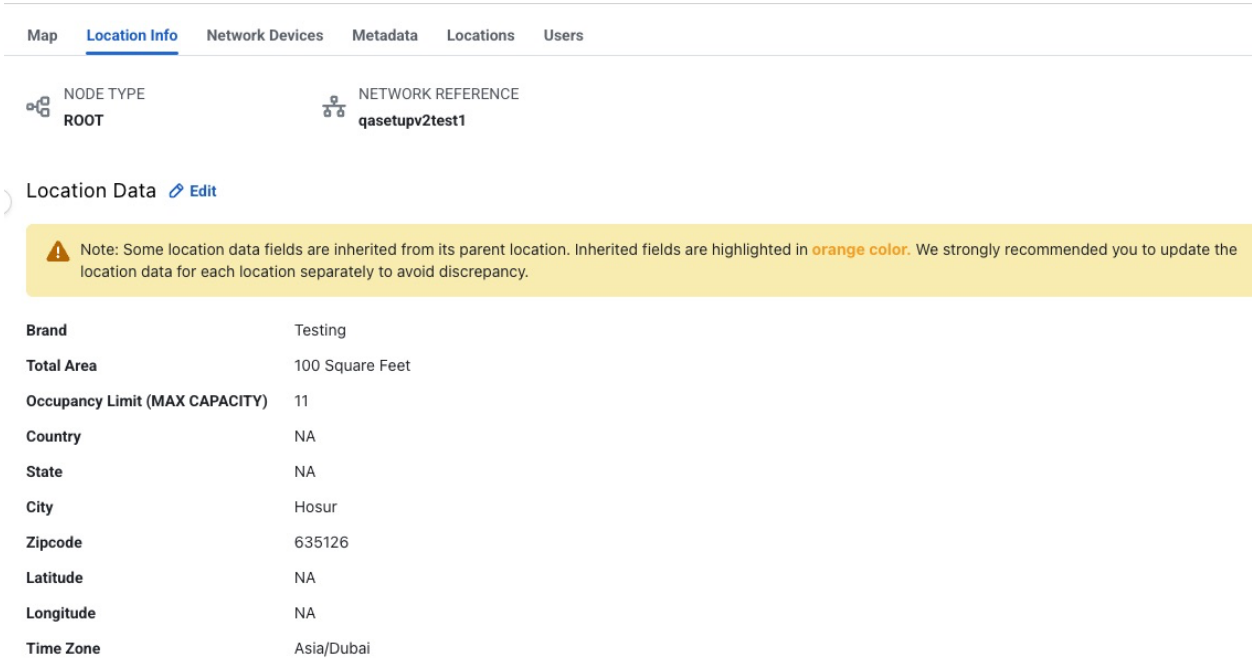
For the selected location, the **Node Type** and **Network Reference** details are displayed.

The Location Info tab displays read-only details for the selected location. The displayed details can include **Node Type, Network Reference, Brand, Total Area, Occupancy Limit, Address, Country, State, City, Zipcode, Latitude, Longitude,** and **Time Zone**.

The Node Type value identifies the hierarchy level of the selected location, such as **ROOT, NETWORK, or FLOOR.** The Network Reference value identifies the reference name associated with the selected location in the hierarchy.

If a value is not configured for the selected location, Cisco Spaces displays **NA**.

Figure 40: Location Info Tab



Click **Edit** to update location information. For more information, refer to Edit Location Info, on page 246.

Note Location data fields inherited from the parent location are highlighted in orange. For example, a floor can inherit **Address** and **Time Zone** values from the parent network or building. Update each location separately if you want to override inherited values.

Edit Location Info

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Location Hierarchy**.

The **Location Hierarchy** window is displayed.

Step 3 In the left pane, navigate to the required location.

Step 4 Click the **Location Info** tab.

Step 5 Click **Edit** next to **Location Data**.

The slide-in window is displayed.

Step 6

Note The fields displayed in the **Edit Details** drawer vary based on the selected node type. For the root location, the drawer displays fields such as **Location Name, Brand, Total Area, Unit, Occupancy Limit,** and **Time Zone**. For network or building locations, the drawer can also display **Address, Latitude, Longitude,** and the map panel.

Update the following location information as required:

a) **Location Name**: Edit the name of the location.
b) **Brand**: Edit the name of the brand.
c) **Total Area**: Edit the total area details. The value must be numeric and cannot include commas.
d) **Unit**: Select the unit for the total area entered. The options are **Square Feet** and **Square Meter**.
e) **Occupancy Limit (Max Capacity)**: Enter a positive integer.
f) **Address**: Enter the address details and select from the displayed options. The selected address is plotted on the map displayed on the right side. The map panel provides Map and Satellite views and supports marker-based location selection.
g) **Latitude and Longitude**: Edit decimal coordinates directly or drag the marker on the map. Values can be positive or negative decimal numbers and cannot include commas.
h) **Time Zone**: Select a valid time zone from the searchable **Time Zone** list.

Step 7 Click **Save**.

Edit Access Point Prefix

You can add APs of multiple prefixes to a network. For example, if you have APs with prefixes, AB, BC, and CA, and if you want to group the APs with AB and BC under one wireless network, you can do so.

The **Access Points Prefix Used** option will be available in the **Location Info** tab only for the network locations. However, the Access Points Prefix Used option will not be available for the **Unconfigured** network.

To add APs of multiple prefixes to a network of a Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller, follow these steps:

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Location Hierarchy**.

The **Location Hierarchy** window is displayed.

Step 3 In the left pane, navigate to the required network.

Step 4 Click the **Location Info** tab.

Step 5 Click **Add/Edit** next to **Access Point Prefix Used**.

Step 6 In the **Add/Edit Prefix** window, in the **Prefix** field, enter the prefix.

The access points with the prefix entered get listed.

Step 7 Click **Add Prefix**.

The newly added prefix gets listed under **Added Prefixes** in the right pane of the window. **Add Prefix** is enabled only if the APs with prefix entered are available.

Step 8 Click **Save**.

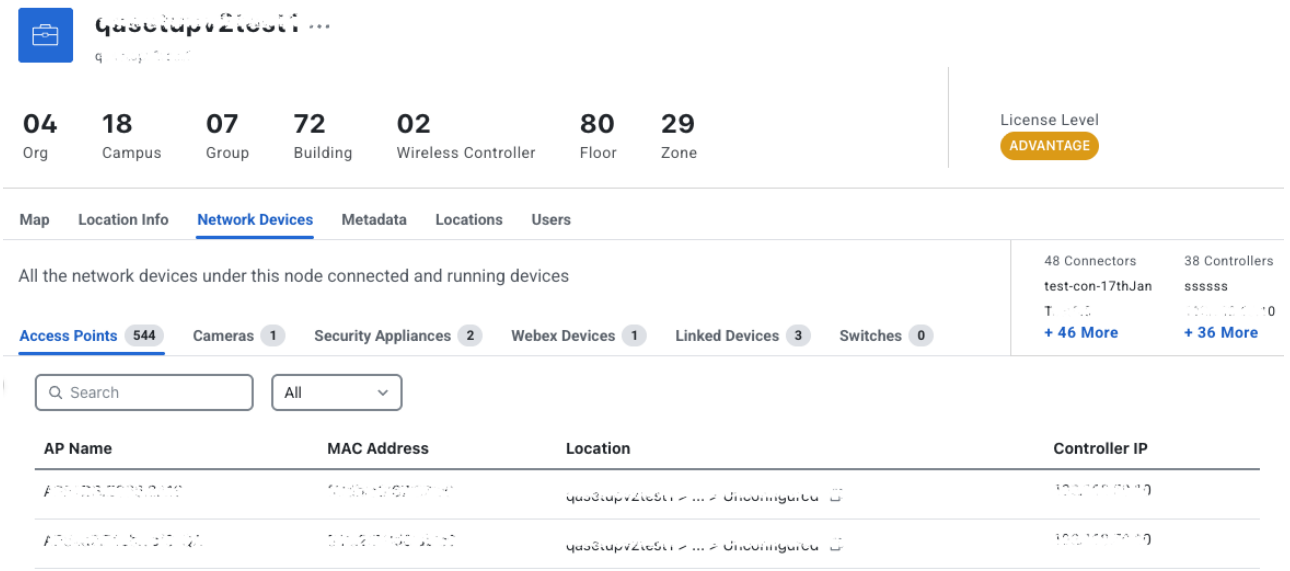
After adding the prefix, the APs under the **unconfigured** network with this prefix is moved to this network.

Use the trash icon in the Existing Prefixes panel to remove a prefix before clicking **Save**.

View the Network Devices

Use the **Network Devices** tab (**Cisco Spaces dashboard** > **Menu icon ( )** > **Location Hierarchy** > **Root Location**) to view all the network devices under the selected node. The root location displays all the connected devices available within the location hierarchy.

Figure 41: Network Devices tab



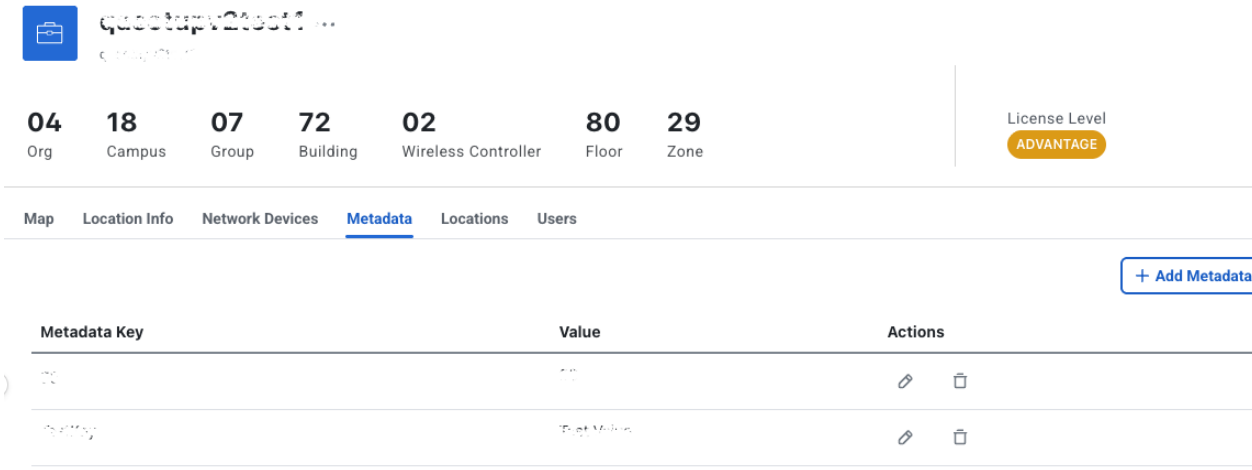
Depending on the selected location, you can view the following information:

- **Access Points**: Displays the name of the AP, MAC address and the location hierarchy path. Use the **Search Table** field to search for a specific AP. Click the copy icon next to the **Location** field to copy the hierarchy path. Navigate to the **Setup** window to configure the AP.
- **Cameras**: Displays the connected camera details such as camera name, serial number, MAC address and status of the trip-wire as a set or not. Use the **Search Table** field to search for a specific camera. Navigate to the **Connect your Meraki Camera** window to connect additional devices.
- **Security Appliances**: Displays the detailed list of security appliance devices for the respective locations.
- **Webex Devices**: Displays the connected Cisco Webex devices.
- **Linked Devices**: Displays the linked devices configured for this location. You can link IoT Devices, Non-Webex Signages and Smart PUDs.
- **Switches**: Displays the switches configured for this location. Navigate to **Setup** > **Wired Network** to onboard your switches.

Configure Metadata

Use the **Metadata** tab (**Cisco Spaces dashboard** > **Menu icon ( )** > **Location Hierarchy** > **Root Location**) to view the metadata information. If metadata is not configured yet, click **Add Metadata** to add metadata. For more information, refer to Add Metadata, on page 249.

Figure 42: Metadata Tab



Depending on the selected location, you can view the following information:

- **Metadata Key**: Displays the metadata key.
- **Value**: Displays the value for the metadata key. The value can be alphanumeric and accepts special characters also, for example, xyz123@.

Add Metadata

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Location Hierarchy**.

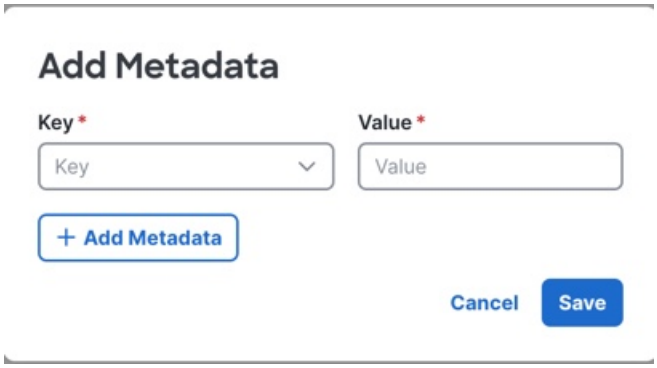
The **Location Hierarchy** window is displayed.

Step 3 In the left pane, navigate to the required location.

Step 4 Click the **Metadata** tab.

Step 5 Click **Add Metadata**.

Figure 43: Add Metadata



Step 6 In the **Key** field, enter or select a metadata key.

Step 7 In the **Value** field, enter a value for the key.

Step 8 (Optional) Click **Add Metadata** to add multiple metadata keys and the corresponding values.

Click the **Delete** icon next to the metadata key to delete the keys.

Step 9 Click **Save**.

After **Save**, the Metadata tab refreshes and displays the saved keys and values. Existing metadata can be edited or deleted from the Actions column.

View Locations

Use the **Locations** tab (**Cisco Spaces Dashboard** > **Menu icon ( )** > **Location Hierarchy** > **Root Location**) to view the location information such as **Location Type** and **Level**.

Use the **Location Type** and **Level** drop-down options to select the location preferences. The location types are:

- Network/Building
- Campus
- Group
- Organization
- Wireless Controller
- CMX

View these details for the selected location:

- Locations
- APs
- Camera

- Max Capacity
- Total Area (sqft)
- Time Zone

Select the required check box next to the location and click **Create Group** to add location to create your own group.

If a single selected row is a group that has child locations, the Locations tab also displays **Ungroup**.

Create a Group

Use this procedure to organize multiple child locations by creating a group.

Before you begin

- Verify that the parent building and the child location that you want to group already exist.
- Verify that your account has permission to update the location hierarchy.
- All selected locations must have the same parent node. If the selected locations belong to different parents, Cisco Spaces displays an error and does not create the group.

Procedure

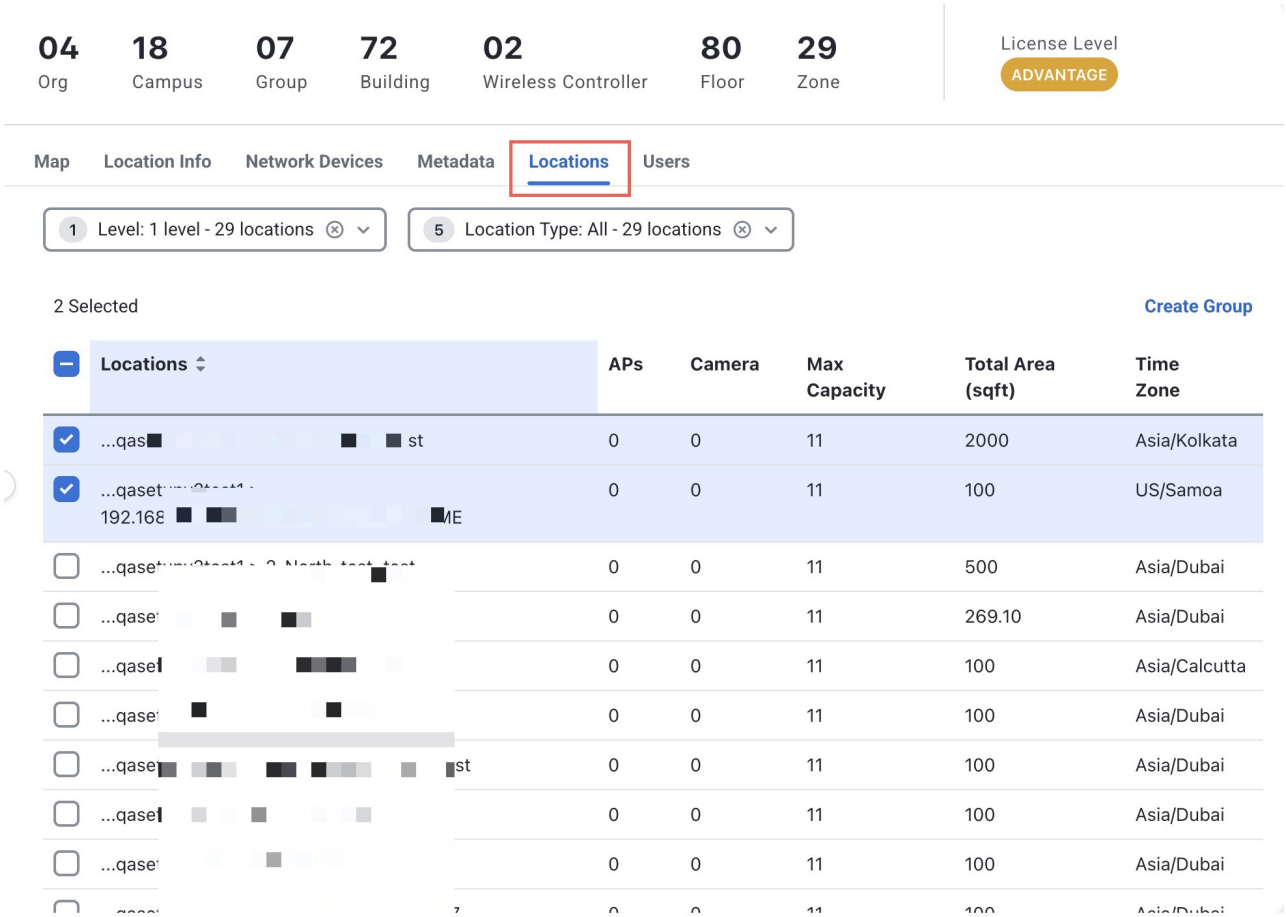
Step 1 In the left navigation pane, click **Location Hierarchy**.

Step 2 In the left pane, navigate to the location where you want to create a group.

Step 3 Click the **Locations** tab.

Step 4 Check the check box for each location that you want to add to the group.

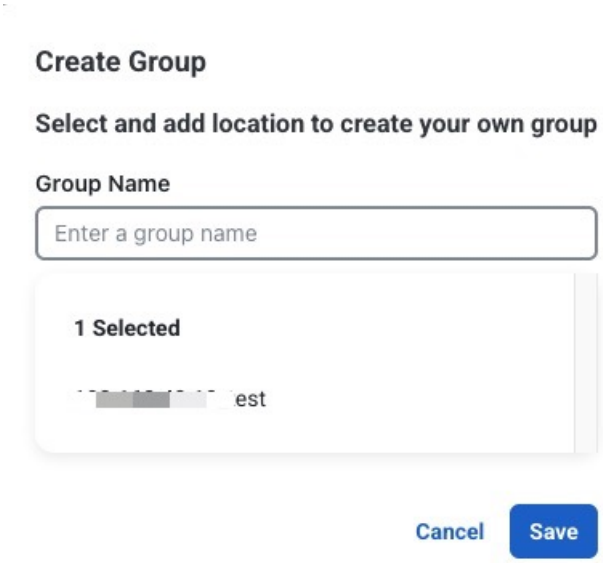
Figure 44: Locations Tab



Step 5 Click **Create Group**.
The **Create Group** pop-up window is displayed.

Step 6 In the **Create Group** pop-up window, enter a name in the **Group Name** field.

Figure 45: Create Group



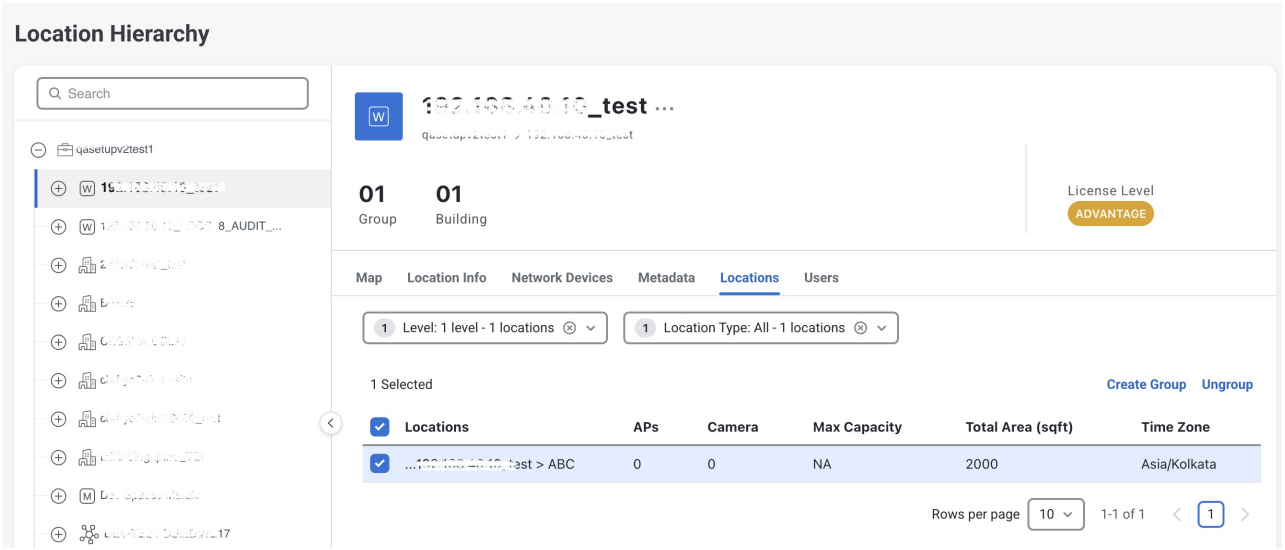
Step 7 Review the selected locations, and then click **Save**.

Step 8 Verify that the new group appears in the hierarchy under the selected building.
The new group is created under the selected building and moves the selected locations under that group. The building summary also updates to show the new group count.

Step 9 (Optional) Perform these steps if required.

a) To ungroup the location, select a group row that has child locations and click **Ungroup**.

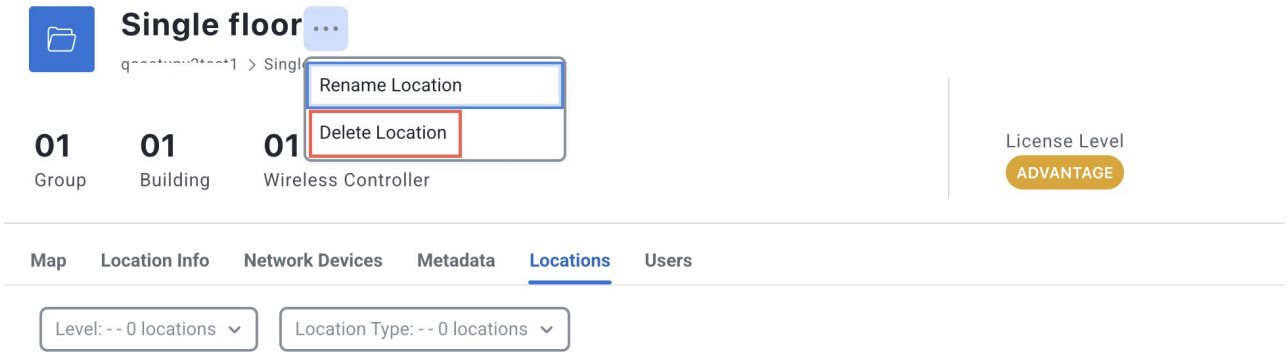
Figure 46: Ungroup



b) In the warning dialog, click **Yes** to confirm the ungroup action.

c) To delete a group or another non-root location, open the location action menu and click **Delete Location**.

Figure 47: Delete Location



Split License

Split License feature allows you to upgrade licenses at the location level.

You can upgrade location-level license to higher tiers (ADVANTAGE or Unlimited), regardless of the account-level license being at a lower tier, for example: ESSENTIAL, EXTEND, SMART OPS, and SMART VENUES. This flexibility extends to the floor level within the **Location Hierarchy**. Use the **License Level Change** option available in the **Location Hierarchy** (Beta UI) to upgrade the license type.

IoT Services licenses can be assigned at the campus or building level. The effective license level is displayed for supported locations in the hierarchy.

A valid IoT Services license is required to configure IoT Services for a campus or building. If the selected location does not have the required license, users can view the location and its existing information but cannot modify the IoT Services configuration.

To enable additional IoT Services capabilities for a location, assign a supported higher-tier license to the campus or building by using the location-level license change workflow.

The apps that include Split License support are:

- **Location Analytics**
- **Live Occupancy**
- **Captive Portal**
- **Detect and Locate**
- **IoT Explorer**
- **Environmental Analytics**
- **Engagements**
- **Location Personas**
- **Space Manager**

- **Space Experience**

To activate **Split License** feature for a location, click **Change** and select the license upgrade options.

The Change link is displayed next to **License Level** in the selected-location header. Use this link to modify the license level for the selected location.

Note This upgrade allows you to experience higher-tier license features in **Location Analytics** app and also in the Density Rule feature in **Live Occupancy** application.

The **Split License** feature is only available for accounts registered with the **Cisco Smart Software Manager** (CSSM) system and integrated with Cisco Spaces account by registering the Smart Licensing token with the Cisco Spaces dashboard. If your account is not registered with CSSM, we recommend reaching out to your account administrator.

View Users

Use the **Users** tab (**Cisco Spaces Dashboard** > **Menu icon ( )** > **Location Hierarchy** > **Root Location**) to view the users and their role permissions.

View these details:

- User
- Role
- Permissions: Read & Write
- Permissions: Read only
- Locations

Use the **Search** option to search for users. You can click a user to edit the permission setting in the **Admin Management** > **Edit User** window.

View License Usage

Use the **License Usage** tab (**Cisco Spaces Dashboard** > **Menu icon ( )** > **Location Hierarchy** > **Root Location**) to view the license type applicable for the logged in account.

The **License Usage** tab is visible only when Smart Licensing is enabled. For a selected location, usage is loaded from the location-specific license service.

View these details:

- License
- Access Points
- Webex Devices

- Meraki Camera
- Locations
- Building Units

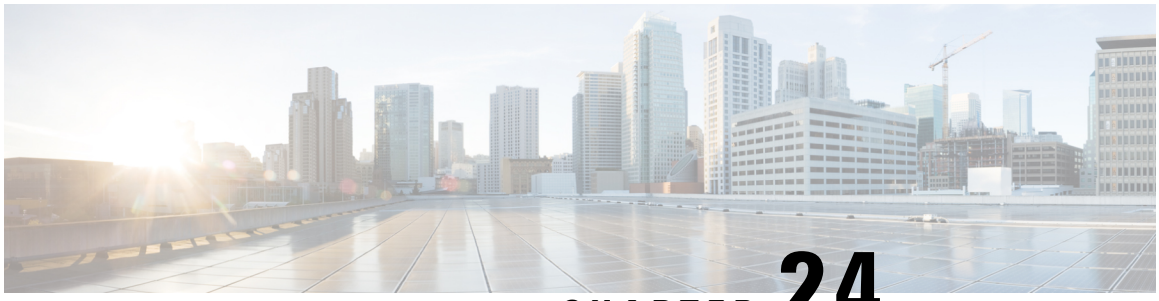
Locations indicates the number of location nodes counted for license usage under the selected hierarchy context. Building Units indicates the number of building-level units counted for license usage under the selected hierarchy context.



PART VI

Integrations

- Cisco, on page 259
- Third party, on page 263



CHAPTER 24

Cisco

This chapter provides information on the integration of Cisco Spaces with Catalyst Center.

- Overview, on page 259
- Integrate Cisco Spaces with Catalyst Center, on page 260

Overview

Cisco Spaces enables you to integrate with Cisco Catalyst Center (formerly known as Cisco DNA Center) so that you can monitor the Catalyst Center sites using Cisco Spaces.

Note The Catalyst Center and Cisco Spaces integration is currently limited to only automatic map exports and synchronization for the location hierarchy. The integration does not support captive portal-based authentication features.

For more information, refer to "About Cisco Spaces Integration" in the *Catalyst Center User Guide* at:

https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html

Prerequisites

- Catalyst Center, Release **2.1.2.3 or higher**.
- Catalyst Center must be able to connect to https://dnaspaces.io:443 for the initial activation. It may also require access to European Union (EU) (https://dnaspaces.eu:443) or Singapore (https://ciscospaces.sg:443) depending on your Cisco Spaces account region.
- You must connect your wireless network to Cisco Spaces using Cisco Spaces: Connector. To connect, log in to the Cisco Spaces dashboard and choose **Setup** > **Wireless Networks**.
- Catalyst Center checks SSL/TLS certificate revocation status using OCSP/CRL. TCP 80 is port used by Catalyst Center for outbound communication to device and other systems. To successfully verify the certificate revocation status, these URLs must be reachable both directly and through the proxy server that's configured for Catalyst Center. Otherwise, certificate revocation check will be skipped when Catalyst Center connects to cisco.com.

  http://validation.identrust.com

  http://commercial.ocsp.identrust.com

For more information, refer to "Communication ports" in the Cisco Catalyst Center Security Best Practices Guide.

Integrate Cisco Spaces with Catalyst Center

To integrate Cisco Spaces with Catalyst Center, perform the following steps:

Procedure

Step 1 Log in to Cisco Spaces.

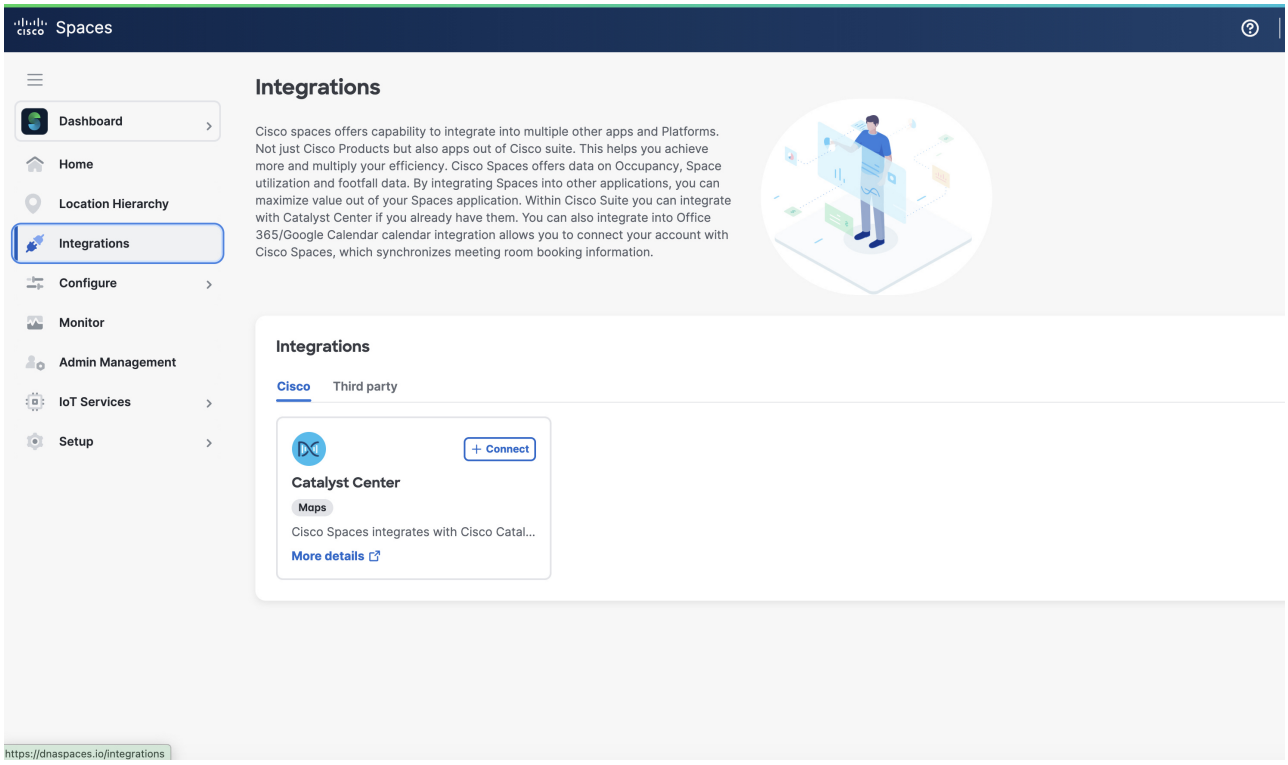
Step 2 In the left navigation panel, choose **Integrations**.
The **Integrations** window is displayed

Step 3 Under **Integrations**.

In the **Cisco** tab, **Catalyst Center** is displayed.

In the **Third party** tab, **Google Calendar**, **Office 365**, and **Hamina** are displayed.

Figure 48: Integrations



Step 4 In the **Catalyst Center**, click **Connect**.
The **Cisco Catalyst Center Integration** window is displayed.

Step 5 If the account is already connected, click **Manage**.

Step 6 Click **Add Instance**.

Step 7 In the **Create new token** pop-up window, enter the Catalyst Center instance name and click **Generate**.

A success message confirms that the new token is created and displays the token in the window. Copy the token.

Note The new token remains valid for five minutes (5 min).

Step 8 Click **Done**.

Step 9 (Optional) In the **Token** column, click **View token** and use this tenant token in Catalyst Center.

In the **Status** column, if it is showing active you can view token.

Step 10 (Optional) In the **Token** column, click **Re-generate**.

In the **Status** column, if it is showing expired you can regenerate another token.

Step 11 (Optional) Click **Done**.

Step 12 To delete an instance, click the delete icon.

A warning message appears.

Step 13 Click **Delete.**

Step 14 Log in to Catalyst Center.

Step 15 Click the **Menu** icon ( ) and choose **System** > **Settings**.

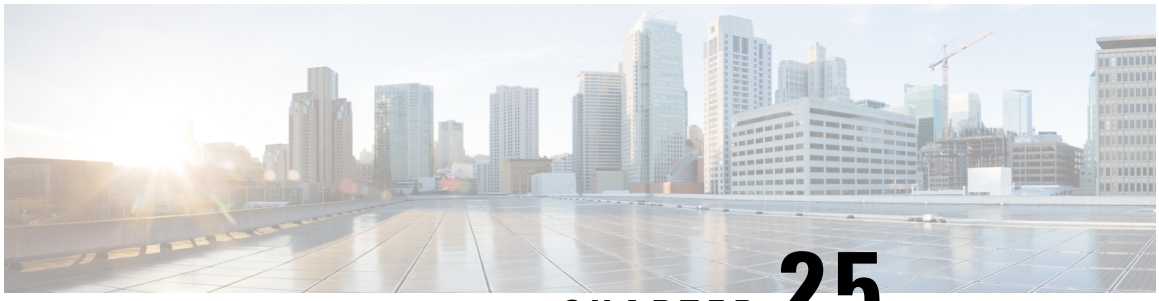
Step 16 Click **CMX Servers/Cisco Spaces**.

Step 17 In the **CMX Servers/Cisco Spaces** window, under the Cisco Spaces section, click **Activate**.

Step 18 In the **Integrate Cisco Spaces** pop-up window, paste the tenant token and click **Connect**.

After the integration is complete with Cisco Spaces, the following success message is displayed: *This cluster is integrated with Cisco Spaces successfully*. The status is displayed as **Activated**.

After activating the Cisco Spaces token, you can assign Cisco Spaces to Catalyst Center sites and begin to monitor those sites. For more information, refer to the Catalyst Center User Guide.



CHAPTER 25

Third party

This chapter provides information on third-party integrations.

Google Calendar Integration

The Google Calendar integration enables you to connect your Google account with Cisco Spaces. This synchronizes meeting room booking information. The Cisco Spaces digital signage, with Google Calendar booking information, allows you to view available rooms in an intuitive, map-based approach instead of traditional lists of rooms that provide little context.

Office 365 Calendar Integration

The Office 365 calendar integration enables you to connect your Microsoft account with Cisco Spaces, which synchronizes meeting room booking information. The Cisco Spaces digital signage, equipped with Office 365 calendar booking information, enables you to easily access and visualize available rooms using an intuitive, map-based interface. This approach offers a more contextual and user-friendly experience compared to the traditional room lists.

- Calendar GUI Integrations, on page 263
- Integrate Google Calendar, on page 263
- Integrate Office 365 Calendar, on page 265
- Hamina integration, on page 267

Calendar GUI Integrations

The Microsoft 365 calendar integration feature is introduced in Cisco Spaces. Use this feature to connect your Microsoft 365 calendar account with the Cisco Spaces application and view the integrated calendar details in the Cisco Spaces dashboard **Menu** > **Integrations**.

The imported calendars are displayed in the Cisco Spaces: Space Manager application.

Integrate Google Calendar

The Google Calendar integration enables you to connect your Google account with Cisco Spaces, which synchronizes meeting room booking information. With the Cisco Spaces digital signage, you can easily view available rooms in an intuitive, map-based approach instead of traditional lists that lack context. This integration brings your meeting rooms to life by displaying dynamic calendar data on a user-friendly digital signage application.

Procedure

Step 1 Log in to Cisco Spaces.

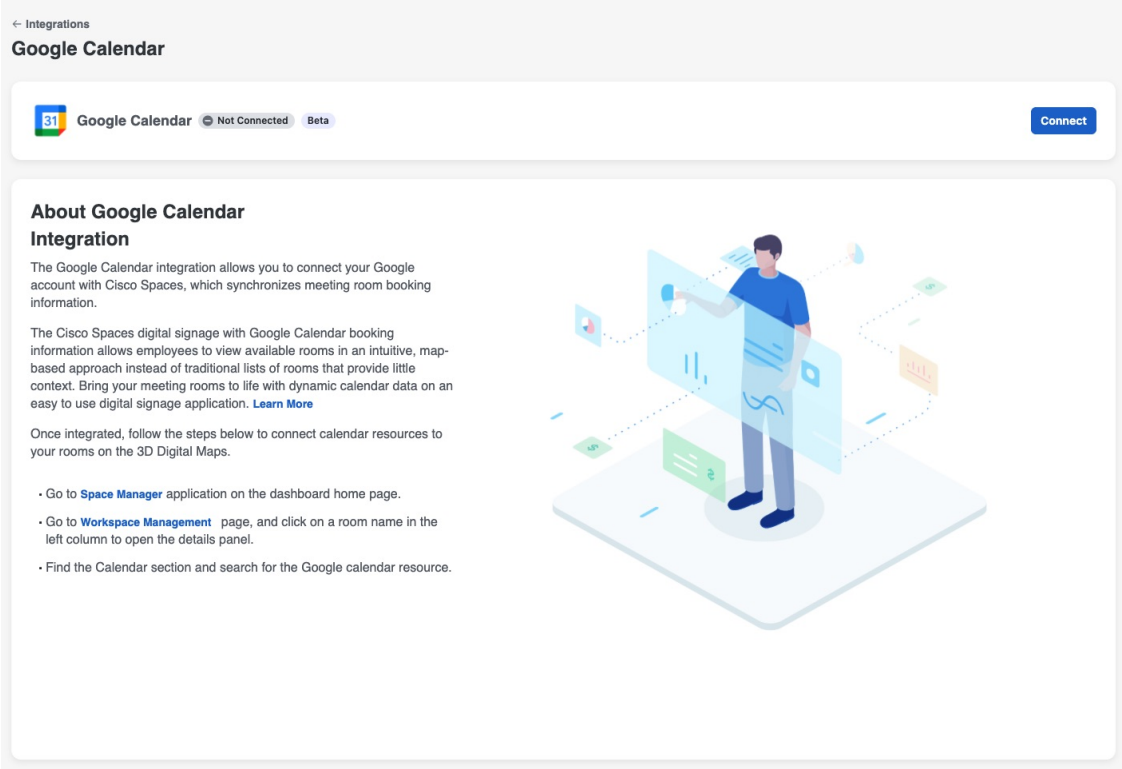
The Cisco Spaces **Home** window is displayed.

Step 2 From the top-left corner, click the **Menu** icon ( ) and choose **Integrations** > **Third party** > **Google Calendar Integrations**.

Step 3 Click **Connect**.

The **Google Calendar Integrations** window is displayed.

Figure 49: Google Calendar Integrations



Step 4 Click **Connect**.

Step 5 If the account is already connected, click **Manage**.

To disconnect, click **Disconnect**.

Step 6 In the **Sign in - Google Accounts** pop-up window, enter your Google account credentials.

Verfiy that you select a valid google account where the calendar bookings are available from the listed **Sign in - Google Accounts** pop-up window.

Step 7 After the account is verified, click **Proceed**.

Step 8 Click **Go to dnaspaces.io** > **Continue** to integrate the Google account with Cisco Spaces.

A success message `Calendar integration is successfull` is displayed.

Step 9 View the integrated Google calendar details in the **My Integrations** area along with the number of connected resources. The integration details page can display calendar resource counters such as **Imported**, **Mapped**, and **Not Mapped**. **Imported** indicates the calendar resources imported into Cisco Spaces. **Mapped** indicates the resources that are associated with rooms or workspaces. **Not Mapped** indicates imported resources that are not yet associated with a room or workspace. A green tick mark indicates that the integration is successful.

The integrated calendars are available in the Cisco Spaces: Smart Workspaces app for use.

- To remove the Google Calendar Integrations, click **Remove** in the tile view.
- To disconnect the current account integration, click **Disconnect** and follow the instructions.

Note During integration, Cisco Spaces may display intermediate status values while the calendar account is being connected and resources are being imported. Wait until the integration status is complete before mapping calendar resources to rooms or workspaces.

What to do next

To successfully connect calendar resources to your rooms on the 3D Digital Maps:

1. Navigate to **Cisco Smart Workspaces** application.
2. Proceed to the **Workspace Management** window and select a room name from the left column to access the **Details** panel.
3. From the **Details** panel, locate the **Calendar** area and search for the Google calendar resource.

Integrate Office 365 Calendar

The Office 365 calendar integration enables you to seamlessly connect your Microsoft account with Cisco Spaces, resulting in the synchronization of meeting room booking information. The Cisco Spaces digital signage, combined with Office 365 calendar booking information, provides you with a user-friendly and intuitive map-based approach to view available rooms. This approach is far more effective than traditional lists of rooms, which often lack context. By utilizing this easy-to-use digital signage application, you can bring your meeting rooms to life with dynamic calendar data.

Procedure

Step 1 Log in to Cisco Spaces.

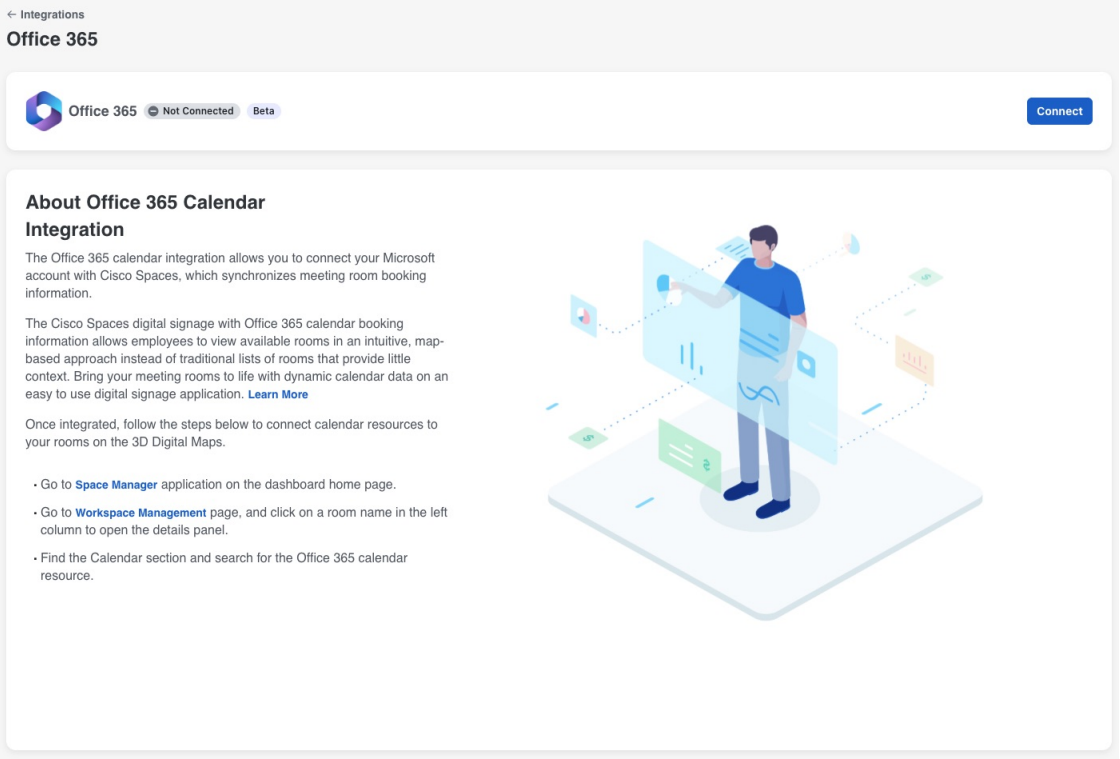
The Cisco Spaces **Home** window is displayed.

Step 2 From the top-left corner, click the **Menu** icon ( ) and choose **Integrations** > **Third party > Office 365**.

Step 3 Click **Connect**.

The **Integrations Office 365** window is displayed.

Figure 50: Office 365 Integrations



Step 4 Click **Connect**.

Step 5 If the account is already connected, click **Manage**.

To disconnect, click **Disconnect**.

Step 6 Follow the on-screen instructions and enter your Office 365 account credentials to integrate Office 365 calendar.

Step 7 After the account is validated, click **Proceed**.

Step 8 Click **Go to dnaspaces.io** > **Continue** to integrate the Office 365 account with Cisco Spaces.

A success message `Calendar integration is successfull` is displayed.

Step 9 View the integrated Office 365 calendar details in the **My Integrations** area along with the number of connected resources. The integration details page can display calendar resource counters such as **Imported**, **Mapped**, and **Not Mapped**. **Imported** indicates the calendar resources imported into Cisco Spaces. **Mapped** indicates the resources that are associated with rooms or workspaces. **Not Mapped** indicates imported resources that are not yet associated with a room or workspace. A green tick mark indicates that the integration is successful.

The integrated calendars are available in the Cisco Spaces: Smart Workspaces app for use.

- To remove the Office 365 calendar, click **Remove** in the tile view.
- To disconnect the current account integration, click **Disconnect** and follow the instructions.

Note During integration, Cisco Spaces may display intermediate status values while the calendar account is being connected and resources are being imported. Wait until the integration status is complete before mapping calendar resources to rooms or workspaces.

What to do next

To successfully connect calendar resources to your rooms on the 3D Digital Maps:

1. Navigate to **Cisco Smart Workspaces** application.
2. Proceed to the **Workspace Management** window and select a room name from the left column to access the **Details** panel.
3. From the **Details** panel, locate the **Calendar** area and search for the Google calendar resource.

Hamina integration

Cisco Spaces enables you to integrate with Hamina so that Hamina-origin mapping data can be reviewed in the Cisco Spaces Location Maps workflow.

The Hamina integration adds a dedicated third-party integration entry in Cisco Spaces, a token-based onboarding flow, and token lifecycle management from the Cisco Spaces dashboard. After the token is used in Hamina, Hamina-sourced location and floor data can be reviewed in Location Maps so that teams can validate imported mapping content before continuing the digital mapping workflow.

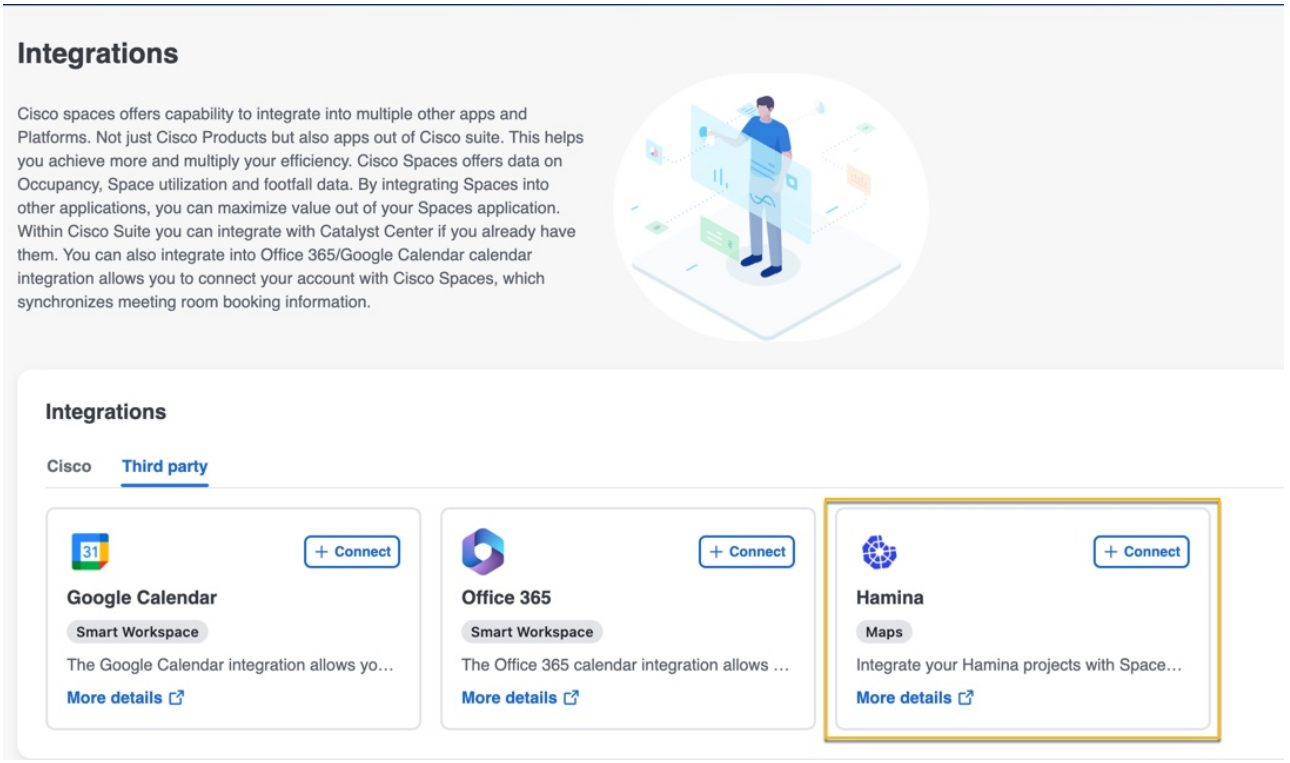
The setup starts in Cisco Spaces and is completed in Hamina by using the token generated from the Cisco Spaces dashboard.

The Hamina integration is available from the Cisco Spaces dashboard under **Integrations** > **Third Party** > **Hamina**. In the **Hamina** tile, click **+ Connect** open the **Accouts** page.

The Hamina integration setup starts in Cisco Spaces and is completed in Hamina by using the token generated from the Cisco Spaces dashboard.

From the Hamina integration page, you can generate a one-time activation token, copy the token into Hamina, and manage the token lifecycle from Cisco Spaces.

Figure 51: Hamina tile in the Third Party integrations area



Prerequisites for Hamina integration

Use these requirements before you integrate Cisco Spaces with Hamina or review imported Hamina mapping data in Location Maps.

- You must be able to log in to the Cisco Spaces dashboard.
- You must have access to the Hamina account or interface where the Cisco Spaces token is entered.
- You must have permission to manage third-party integrations in Cisco Spaces.
- To review imported mapping data, Location Maps must be available for the Cisco Spaces account.

Integrate Cisco Spaces with Hamina

To integrate Cisco Spaces with Hamina, generate a one-time activation token in Cisco Spaces and enter the token in the Hamina integration setup flow.

Procedure

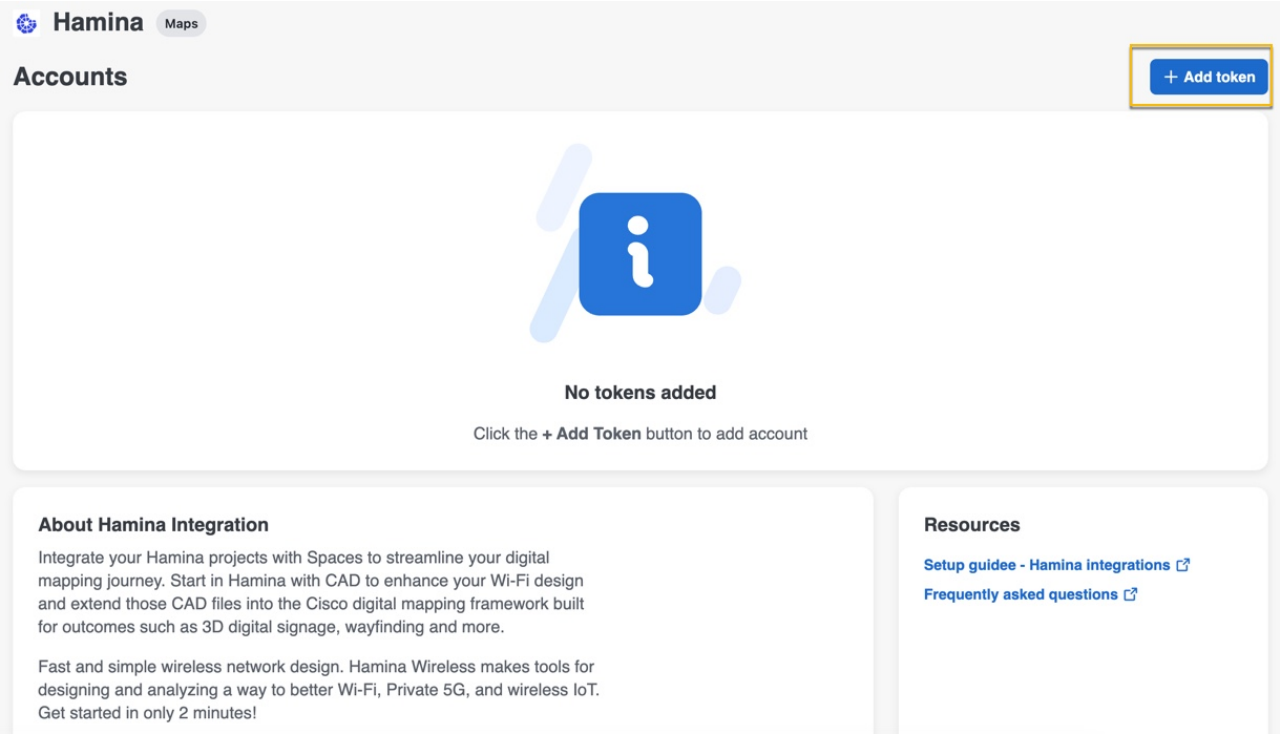
Step 1 Log in to Cisco Spaces.

Step 2 In the left navigation panel, choose **Integrations** > **Third Party** > **Hamina**.

The **Accounts** window is displayed.

Step 3 Click **+ Add token**.

Figure 52: Hamina



Step 4 In the **Add Token** pop-up window, enter a token instance name.

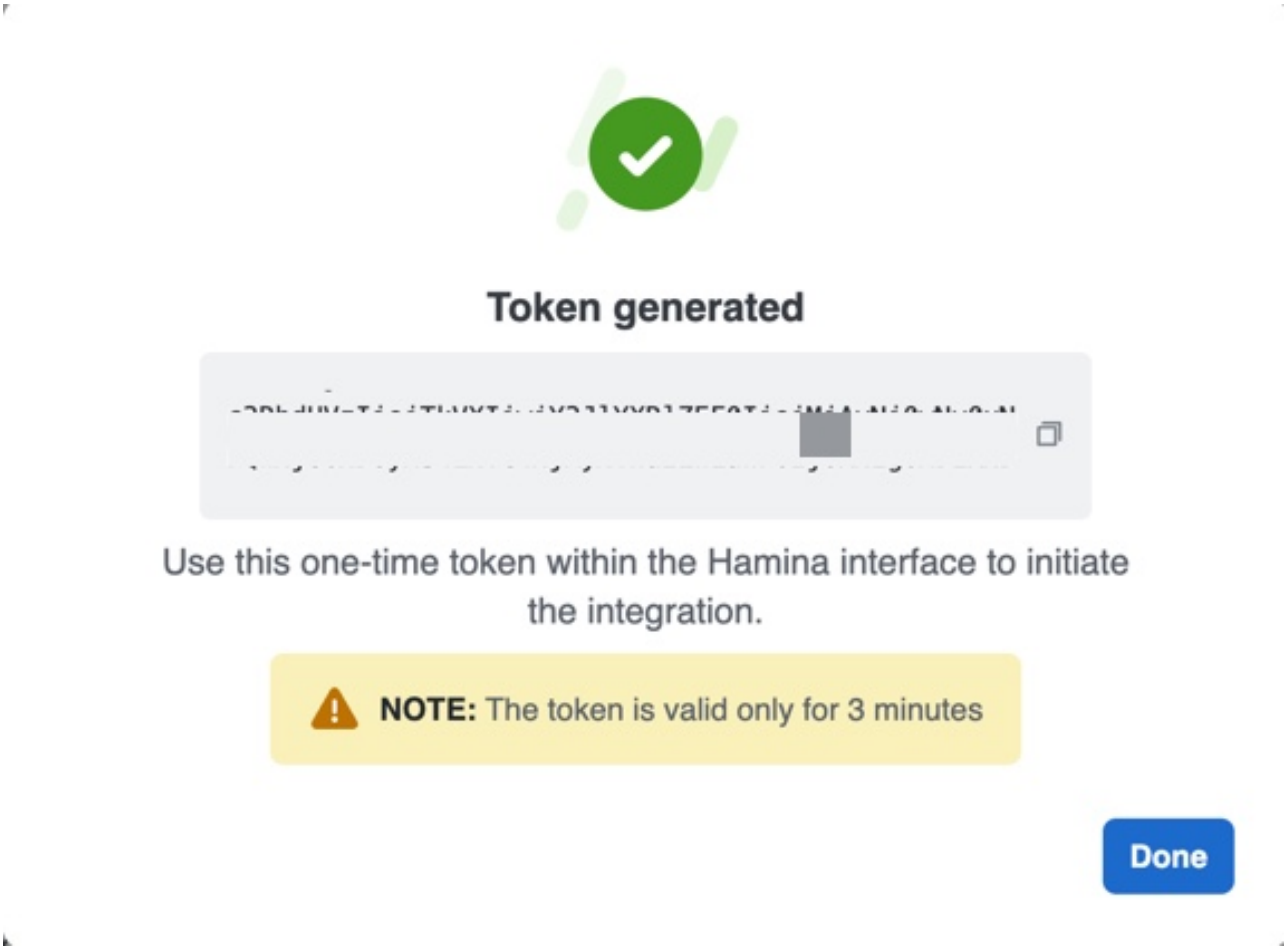
Use a name that helps identify the Hamina connection, location, or account where the token will be used.

Step 5 Click **Generate**.

A one-time token is generated.

Step 6 Copy the generated token. Use this one-time token within the Hamina interface to initiate the integration. The token is valid only for four minutes.

Figure 53: Token



Step 7 Log in to Hamina.

Step 8 Paste the Cisco Spaces token into the Hamina integration setup flow, and complete the setup in Hamina.

After the token is accepted in Hamina, the integration can begin sending Hamina-origin mapping data into the Cisco Spaces Location Maps workflow.

Manage Hamina tokens

After a Hamina token is created, you can use the Hamina integration page in Cisco Spaces to review token status and manage tokens.

Procedure

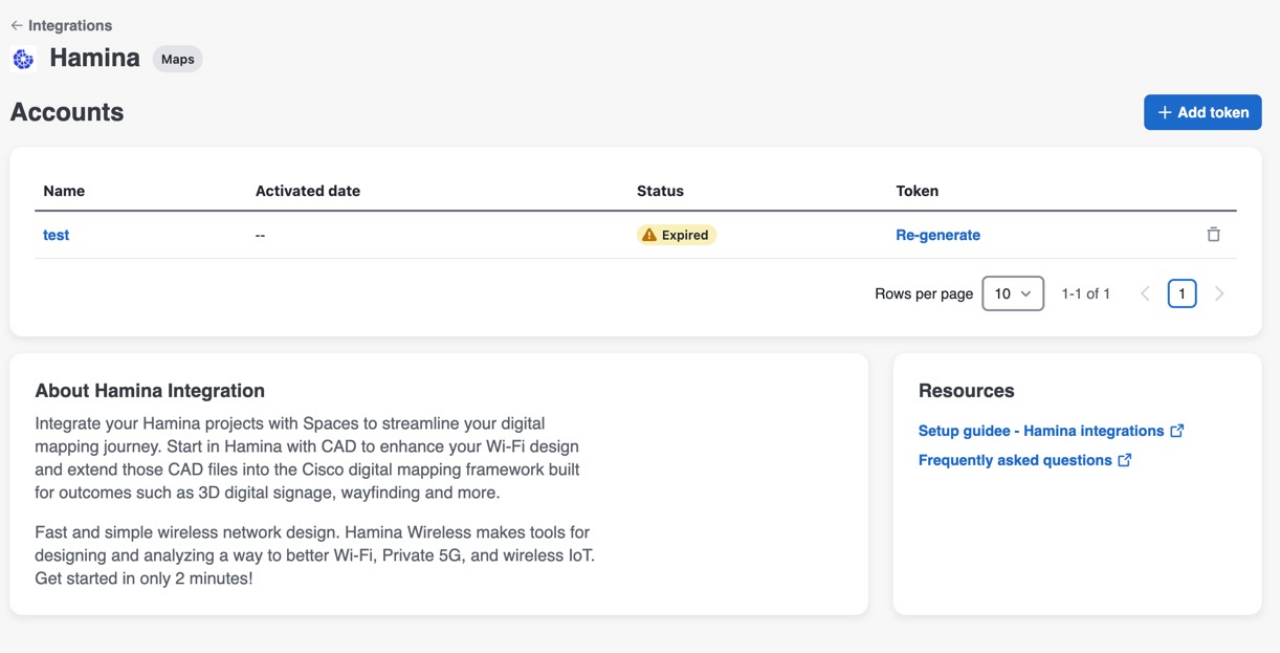
Step 1 Log in to Cisco Spaces.

Step 2 Choose **Integrations** > **Third Party** > **Hamina** > **Manage**.

Step 3 In the **Accounts** area, review the listed Hamina tokens and their status.

Step 4 To create another token, click **Add token** and generate a new one-time token.

Figure 54: Add token



Step 5 To replace an expired token, use the regenerate option for the expired token.

Step 6 To remove a token that is no longer required, delete the inactive token from the Hamina integration page.

Review Hamina locations in Location Maps

After Hamina data reaches Cisco Spaces, dashboard users can review Hamina-origin locations in Location Maps when validation is required. The review queue identifies the location, source, status, and available action for each item.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 Open **Location Maps**.

Step 3 Open the **Review** area.

The review queue is displayed.

Step 4 Locate review items where the source is **Hamina**.

Step 5 Review the location name, source, status, and available action.

Step 6 Select the recommended action for the Hamina-sourced review item.

Step 7 Validate the building or floor details shown in the review flow.

After the review is completed, continue with the next Location Maps action for the item.

Review floor order for Hamina-imported buildings

When a Hamina-imported building requires floor review, Location Maps displays a floor order review step before the workflow continues.

Procedure

Step 1 In **Location Maps** > **Review**, open the Hamina-sourced item that requires floor review.

The Review Floor Order window is displayed.

Step 2 Review the imported floors for the building.

Step 3 Verify that the floor names and order are correct.

Step 4 If required, adjust the floor order.

Step 5 Confirm the imported order and proceed.

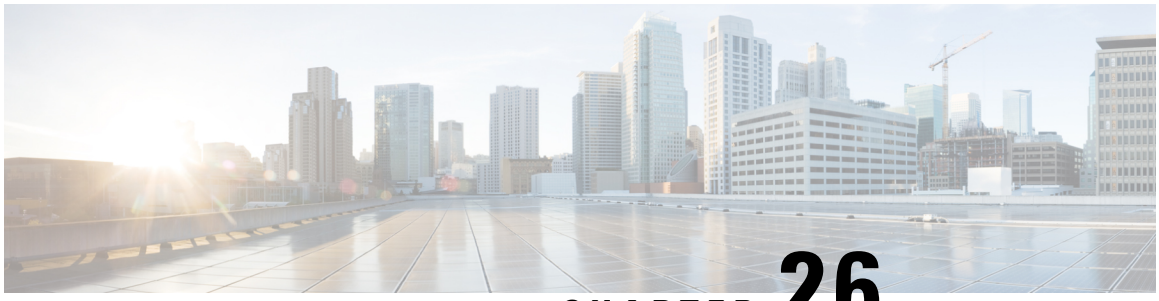
After the floor order is confirmed, Location Maps continues the digital mapping workflow for the Hamina-imported building.



PART VII

Configure

- Cisco Spaces SDK Integration, on page 275
- Notifications, on page 281
- Location Compute, on page 287



CHAPTER 26

Cisco Spaces SDK Integration

This chapter provides information on the integration of **Cisco Spaces Software Development Kit** (SDK).

- Cisco Spaces SDK Integration, on page 275
- Integrating Cisco Spaces, on page 275

Cisco Spaces SDK Integration

The **Cisco Spaces Software Development Kit** (SDK) leverages OpenRoaming technology to attach users, seamlessly and securely, to Wi-Fi networks, without the need for user interaction. The Cisco Spaces SDK allows an iOS or Android application developer to configure iOS and Android devices with an identity of choice that can be verified with the back-end system. The Cisco Spaces SDK also allows the developer to add more information about the users, and engage with them, directly on their device, through the iOS and Android notification framework.

The SDK configuration section is accessible through **Menu** icon ( ) > **Configure** > **Cisco Spaces SDK**. This allows the customers to register their native app (iOS and/or Android) with Cisco Spaces.

Integrating Cisco Spaces

The Cisco Spaces Software Development Kit (SDK) is a platform-independent SDK (Software Development Kit), across iOS and Android platforms, that Cisco Spaces customers can use to enable Apps to provision and manage OpenRoaming user profiles in a mobile device. For more information, see Cisco Spaces SDK Developer Documentation.

Before you begin

Following Google's deprecation of API key-based functionality, a new method using Firebase JSON through Google Cloud Messaging (GCM) is introduced in the Cisco Spaces Software Development Kit (SDK) (**Cisco Spaces Dashboard** > **Configure** > **Cisco Spaces SDK**).

Before this, in Cisco Spaces Dashboard, you had to configure the API Key, but now it has changed to Firebase JSON.

Cisco Spaces utilizes this to trigger push notifications on Android devices using the SDK.

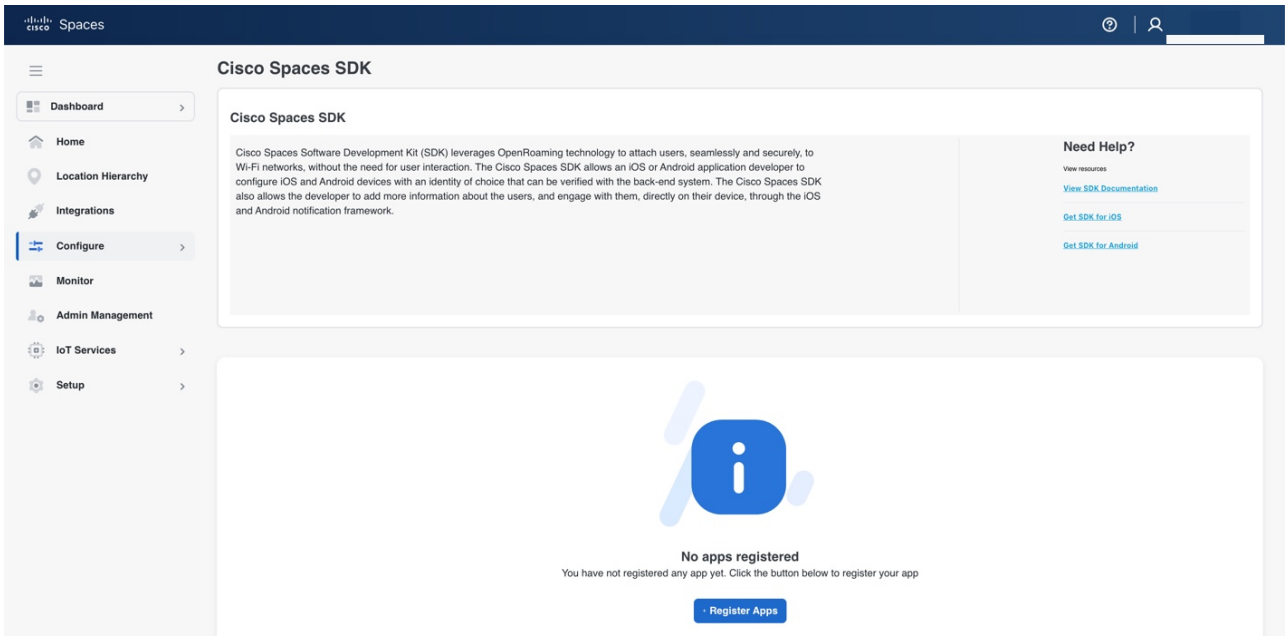
Procedure

Step 1 Log in to Cisco Spaces.

The Cisco Spaces **Home** window is displayed.

Step 2 From the top-left corner, click the **Menu** icon ( ) and choose **Configure** > **Cisco Spaces SDK**.

Figure 55: Cisco Spaces SDK



The **Cisco Spaces SDK** window is displayed.

Step 3 Click **Register App**.

Step 4 To choose the platform for the new app, check either the **iOS** or **Android** check box or both.

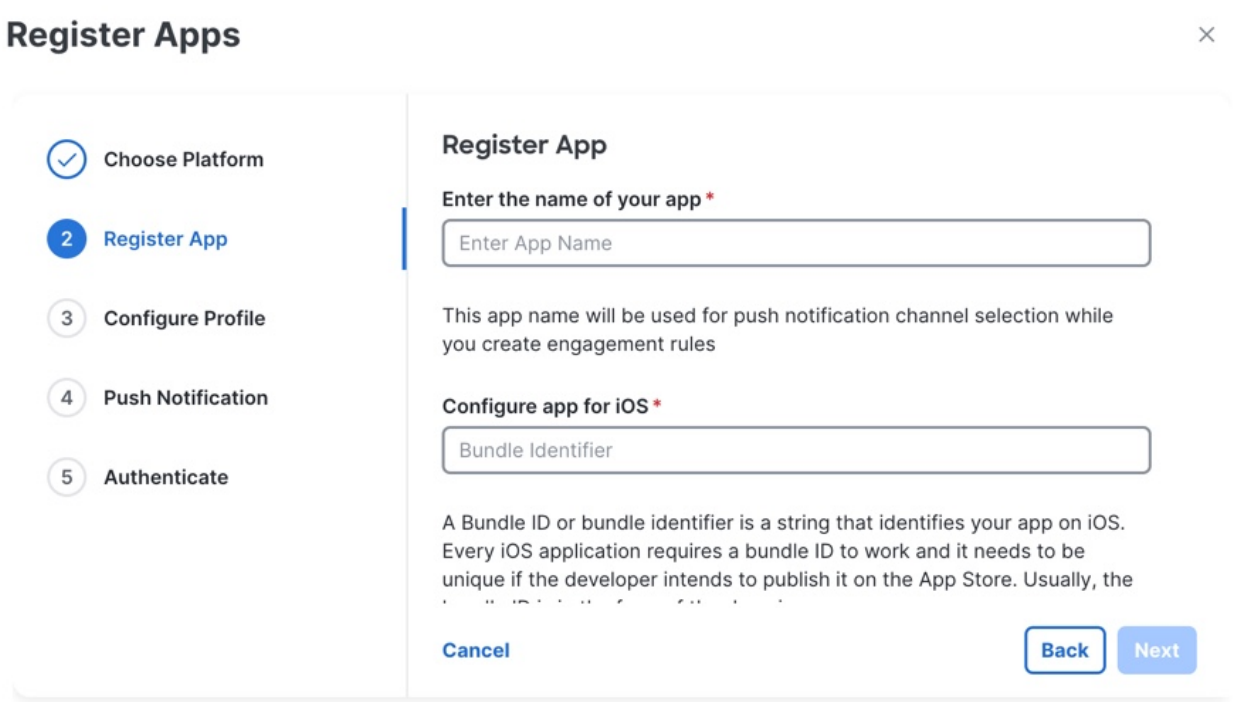
If you select both platforms, the subsequent windows display parameters for both platforms.

Step 5 Click **Next**.

To successfully register a new app, enter information in the following sections:

- Register App
- Configure Profile
- Push Notification
- Authenticate

Figure 56: Register App Sections



Step 6 In the **Register App** section, enter the following:

- **App Name**: Enter the name of the application.
- **Bundle Identifier**: Enter the Bundle ID or bundle identifier string that identifies your app on the iOS platform.

Note Every iOS application requires a bundle ID to work and must be unique if the developer intends to publish it on the App Store. The bundle ID is in the format `domain.your-company.app-name`.

- **Package Name**: Enter the unique package name to identify an Android app.

Note The package name of an app is in the format `domain.your-company.app-name`. However, you can choose to enter any name.

Step 7 Click **Next**.

Step 8 In the **Configure Profile** section, enter the following:

- **Displayed Operator Name**: Enter a valid identifier. This name is displayed as the Wi-Fi SSID name on the user's android or iOS device.
- **Domain**: Enter a unique domain name for the profile.
  - The domain name is available in the OpenRoaming app. For more information see, Configure Network Controller.
  - You should add this domain name in the controller configuration.
  - If you have more than one app, then each app must have a unique domain name.
- **Roaming Consortium OIs**: From the **Roaming Consortium OIs** drop-down list, check the check box next to the array of Roaming Consortium Organization (RCO) identifiers. This is optional.

Step 9 To enable push notifications for iOS, check the **Enable Push Notification for iOS** check box.

a) Enter the iOS App ID.
b) Click **Upload** to browse and upload the APNS P12 and Certificate.
c) Enter the APNS certificate password.

Step 10 To enable push notifications for Android, check the **Enable Push Notification for Android** check box.

a) Enter the Android App ID.
b) Enter the API key.

Step 11 Click **Next**.

Step 12 To support Apple sign-in as the user identity for the new mobile app, check **Enable Apple Sign In** in the **Authenticate** section.

a) In the **Enter Client ID** field, enter the apple account sign-in client ID.
b) In the **Enter Secret Key** field, enter the secret key for Apple account.

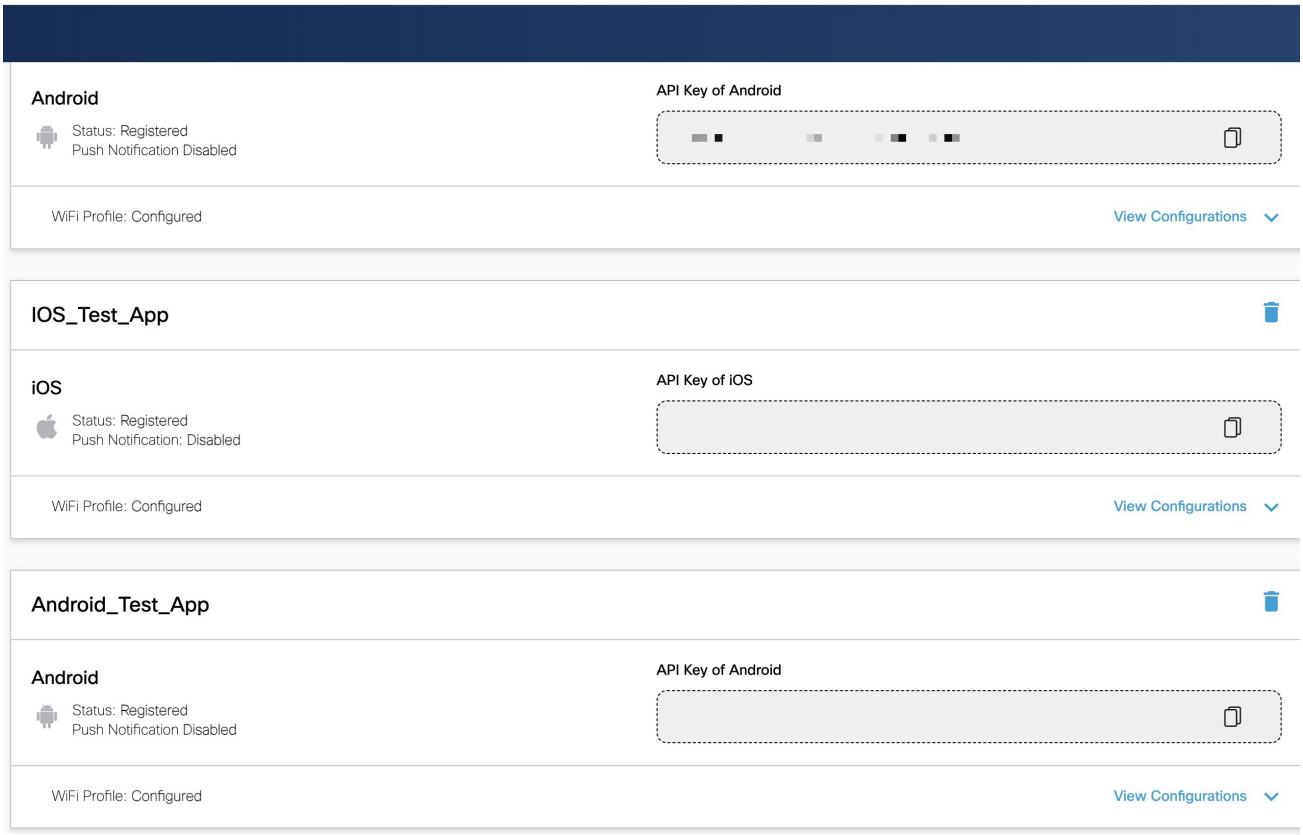
Step 13 To support Google sign-in as the user identity for the new mobile app, check **Enable Google Sign In** in the **Authenticate** section.

a) In the **Enter Client ID** field, enter the google account sign-in client ID.
b) In the **Enter Secret Key** field, enter the secret key for Google account.

Step 14 Click **Register App** to complete the app registration.

The registered apps are displayed.

Figure 57: Registered Android and iOS Apps

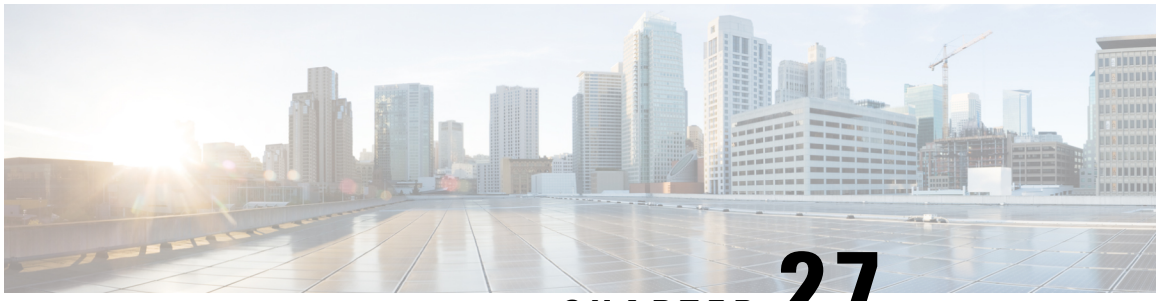


You can click:

- **View Configurations**: To view the application configuration details.
- **Delete** icon: To delete the registered application.

Step 15 (Optional) Click **Edit** to update push notifications for iOS and Android platforms.

Step 16 (Optional) Click **Update**.



CHAPTER 27

Notifications

- Configure notifications overview, on page 281
- Manage categories, on page 282
- Manage subscribers, on page 283

Configure notifications overview

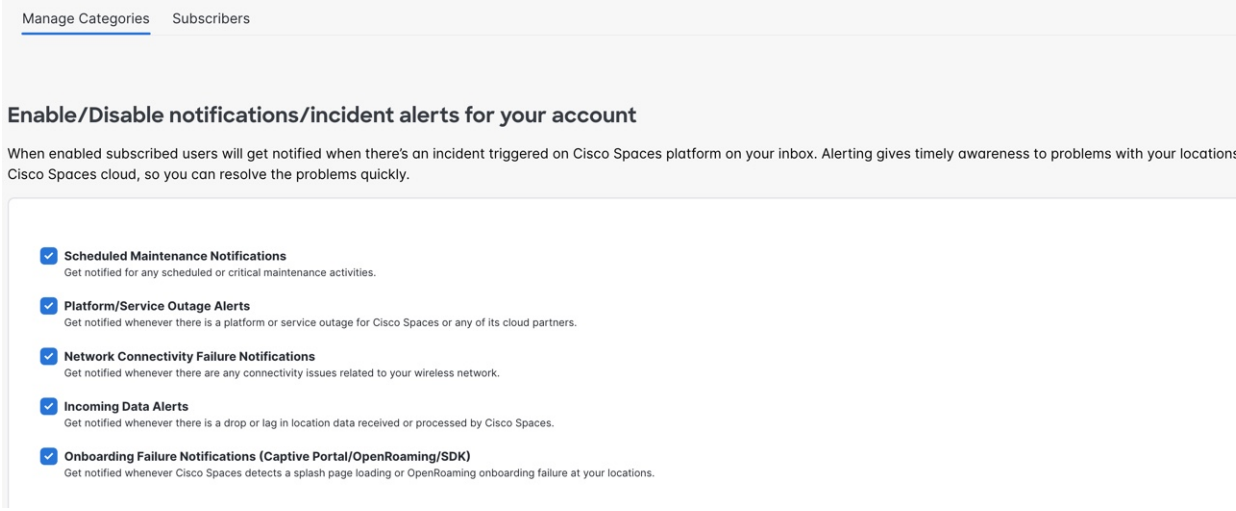
The **Notifications** feature in Cisco Spaces allows you to configure subscriber notifications (**Configure** > **Notifications**) and receive notifications on critical incidents. Enable this feature to receive email notifications when an incident occurs on the Cisco Spaces platform.

Subscriber notification provides updates about issues with Cisco Spaces cloud or locations and help you address them on a timely manner.

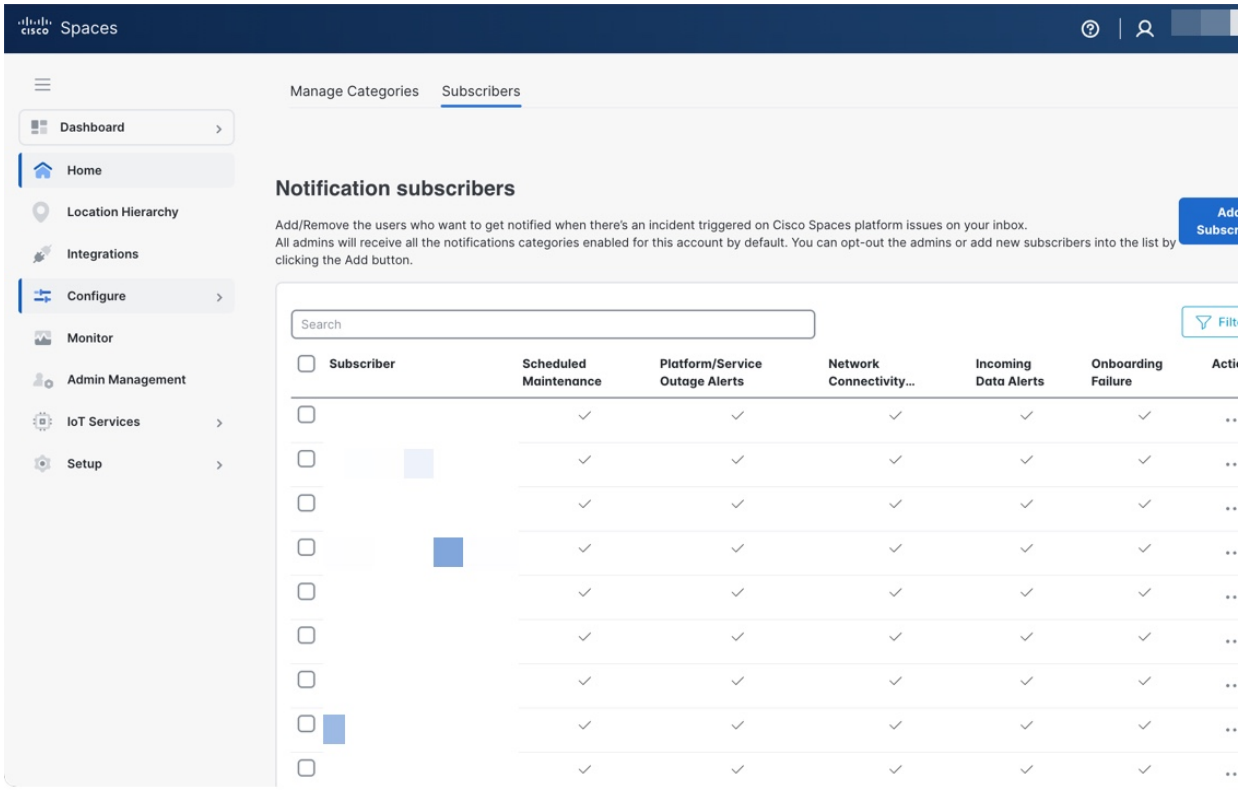
Note This feature is available for all users with administrator access (Read-only and Read-Write).

Use these tabs:

- **Manage Categories**: If you are an administrator with Read-Write access, configure subscriber notifications for your account by navigating to **Configure** > **Notifications** > **Manage Categories**.



- **Subscribers**: To manage subscribers, navigate to the **Subscribers** tab (**Configure** > **Notifications** > **Subscribers**).



All administrators and subscribers receive the notifications based on the categories enabled for the account.

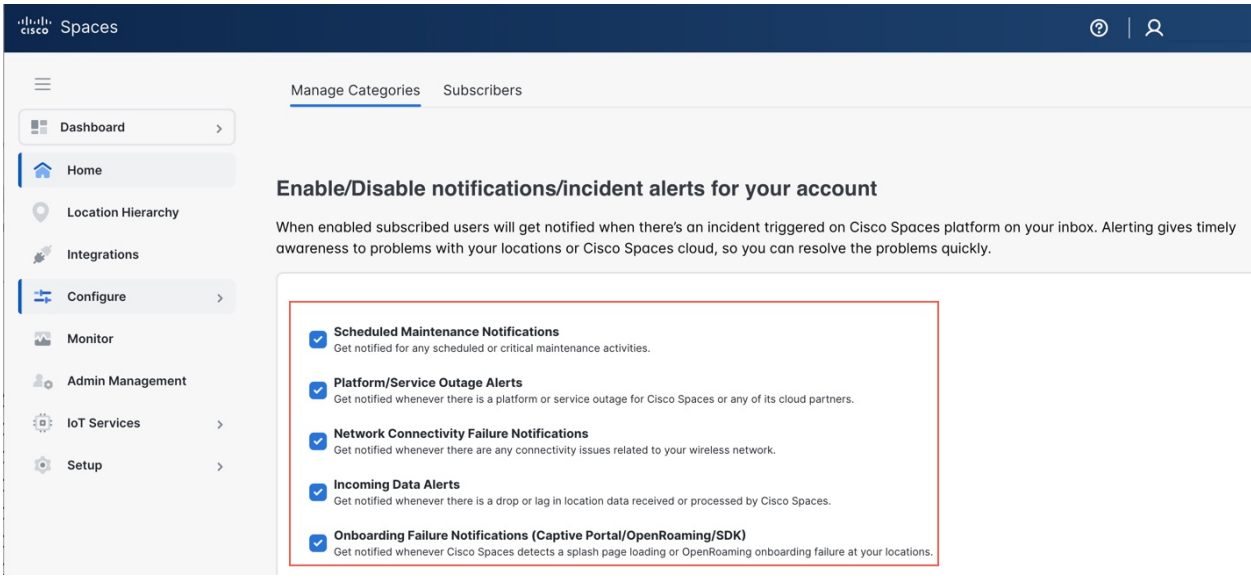
Manage categories

The **Manage Categories** tab allows you to select the categories available for enabling the notifications. Use the categories available to enable or disable notifications and incident alerts for your account.

These are the categories in the **Manage Categories** tab.

- **Scheduled Maintenance Notifications**: Select **Scheduled Maintenance Notifications** check box to get notified in case of any scheduled or critical maintenance activities.
- **Platform/Service Outage Alerts**: Select **Platform/Service Outage Alerts** check box to get notified whenever there is a Cisco Spaces platform or service outage or any of its cloud partners.
- **Network Connectivity Failure Notifications**: Select **Network Connectivity Failure Notifications** check box to get notified whenever there are any connectivity issues related to your wireless network.
- **Incoming Data Alerts**: Select **Incoming Data Alerts** check box to get notified whenever there is a drop or lag in location data received or processed by Cisco Spaces.
- **Onboarding Failure Notifications (Captive Portal/OpenRoaming/SDK)**: Select **Incoming Data Alerts** check box to get notified whenever Cisco Spaces detects a splash page loading or OpenRoaming onboarding failure at your locations.

Figure 58: Notification Categories



When you enable the notifications, subscribers receive notifications in their mailbox whenever an incident is triggered on the Cisco Spaces platform. Alerts provide timely awareness of issues with your locations or the Cisco Spaces cloud, allowing you to resolve problems quickly.

Manage subscribers

The **Subscribers** tab allows you to add or edit subscribers. You can add or remove subscribers who want to receive notifications in their mailbox whenever an incident is triggered on the Cisco Spaces platform.

By default, all Cisco Spaces administrators receive notifications for all enabled categories under the account. You can opt-out specific administrators or add new subscribers to the list by clicking the **Add Subscriber** button.

Use the **Search** field in the **Notification subscribers** window to search for subscribers.

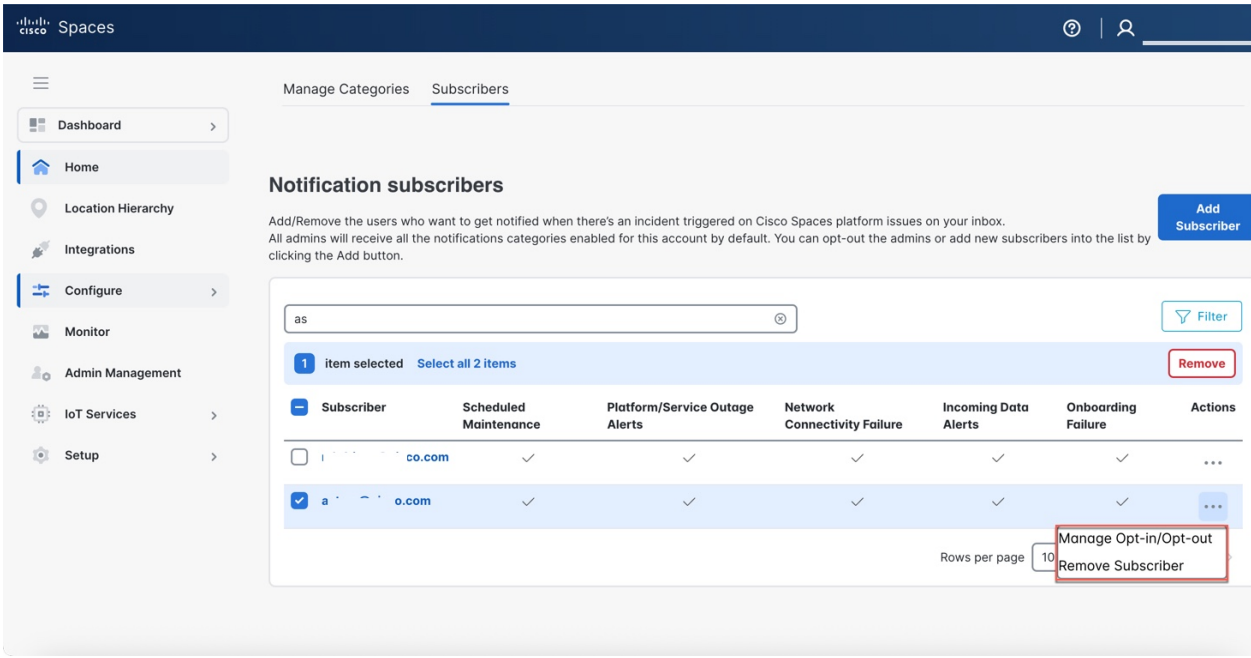
Subscriber details

The table provides detailed information about the subscribers.

Table 16: Subscriber details

Field	Description
Subscriber	Email address of the subscriber.
Scheduled Maintenance	A tick mark indicates that this notification category is enabled for the subscriber.
Platform/Service Outage Alerts	A tick mark indicates that this notification category is enabled for the subscriber.
Network Connectivity Failure	A tick mark indicates that this notification category is enabled for the subscriber.
Incoming Data Alerts	A tick mark indicates that this notification category is enabled for the subscriber.
Onboarding Failure	A tick mark indicates that this notification category is enabled for the subscriber.
Actions	Click the three dots under the **Action** column either to • manage **Opt-in** or **Opt-out** the notifications categories, and • remove the subscribers. **Note** An administrator with Read-Write access only can **Opt-in** or **Opt-out** the notifications categories and remove the subscribers.

Figure 59: Notification Subscribers



Add subscribers

You need to add subscribers to the alert list. Only the subscribed users get notified when there's an incident triggered on Cisco Spaces platform.

Complete these steps to add new subscribers.

Procedure

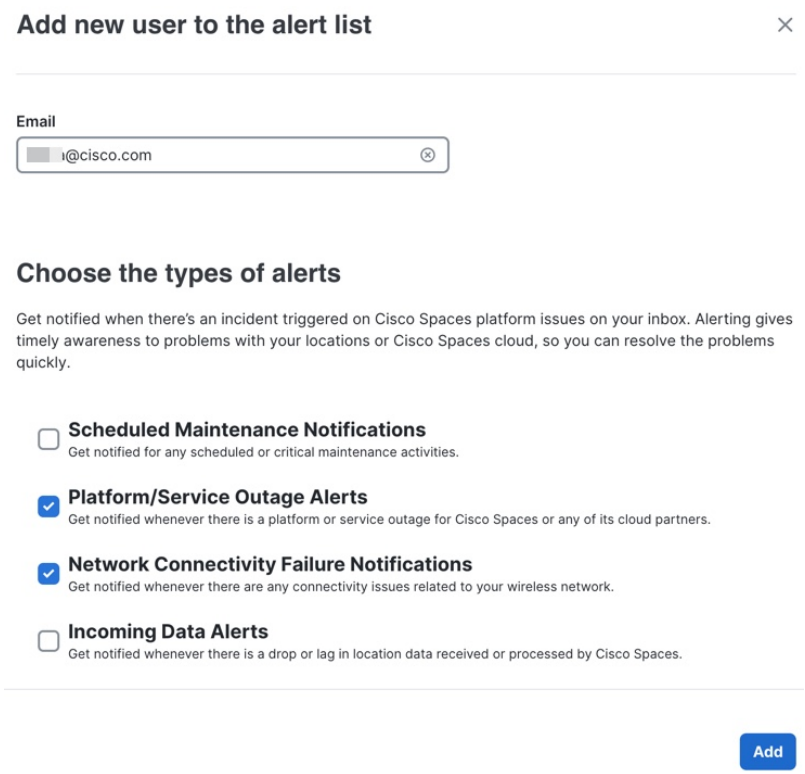
Step 1 Log in to Cisco Spaces.

The Cisco Spaces **Home** window is displayed.

Step 2 From the top-left corner, click the **Menu** icon ( ) and choose **Configure** > **Notifications** > **Subscribers**.

Step 3 Click **Add Subscriber**.

Figure 60: Add Subscriber



The **Add new user to the alert list** slide-in window is displayed.

Step 4 In the **Email** field, enter the email address of the new subscriber.

Step 5 Check the required **Notification Categories** check box.

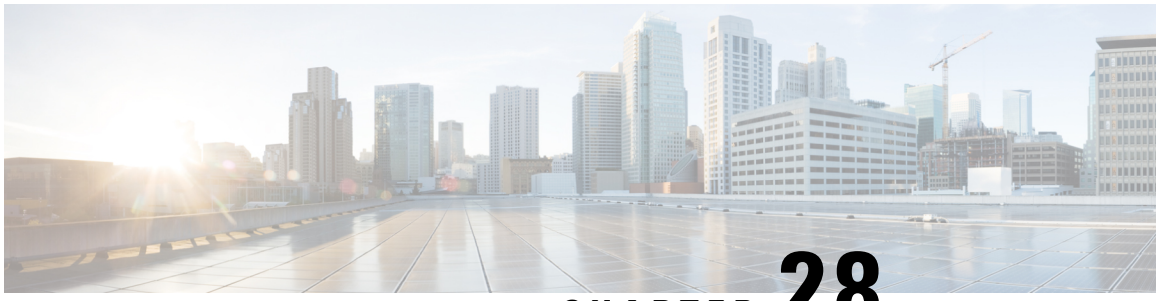
You can opt in for receiving notifications and incident alerts for five notification categories. You can select more than one category.

Step 6 Click **Add**.

The new user is added to the notification subscriber list.

What to do next

The **Notification subscribers** window displays the new subscriber details. Use the **Actions** column to manage subscription.



CHAPTER 28

Location Compute

- Location Compute, on page 287
- Activate UWB Location, on page 288
- View the UWB Activation Log, on page 291
- View UWB-Enabled Access Points, on page 292
- Deactivate UWB Location, on page 293

Location Compute

Location Compute enables Ultra-Wideband (UWB) location services on supported access points and provides a centralized view of UWB readiness and activation status across configured locations.

It collects UWB ranging data between access points, organizes the access points into clusters, assigns a role to each access point, and pushes the cluster configuration to the access points.

The **Locations Compute** window shows the number of UWB-capable access points that are activated or not activated. The **Locations** table shows each eligible location, its hierarchy path, activation status, and the number of eligible access points.

You can expand a building to review floor-level status, view the UWB-enabled access points and their cluster roles, review activation history, or deactivate UWB Location.

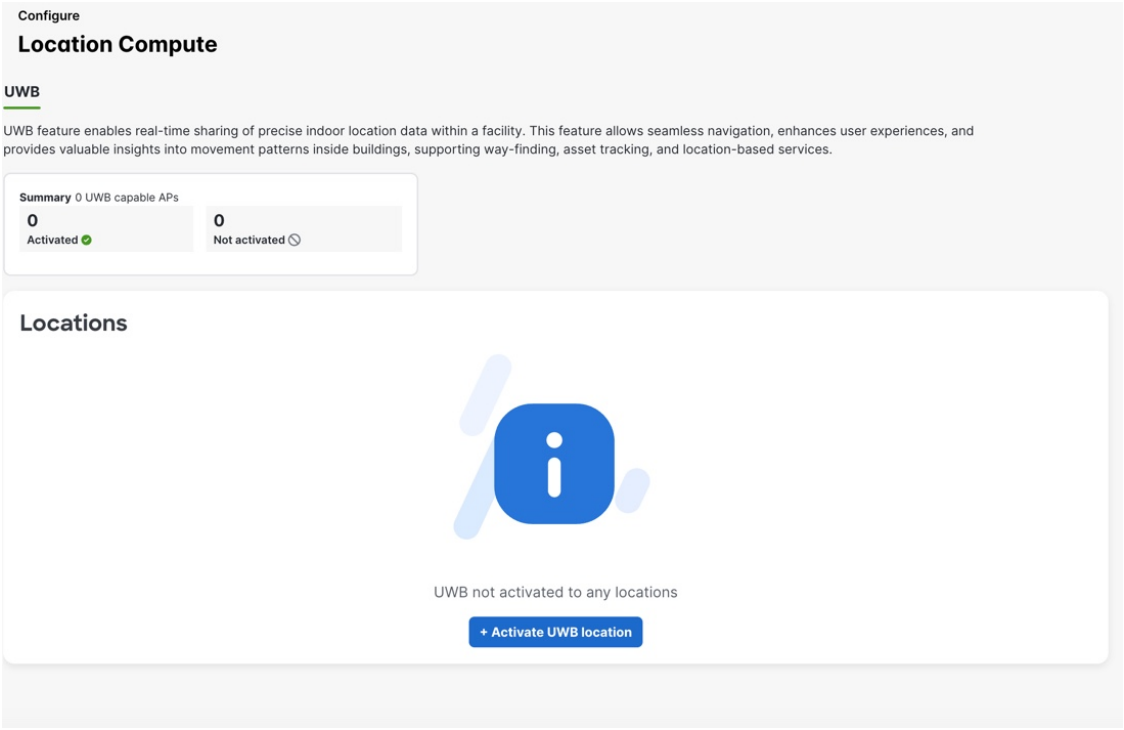
UWB Location supports high-precision location use cases such as asset tracking, indoor navigation, wayfinding, and location-based analytics.

Activate UWB Location before using the UWB capability of supported tags or applications at a location.

The primary functions and benefits include:

- **Real-time Data**: Enables the sharing of precise indoor location data in real-time.
- **Navigation & Way-finding:** Supports seamless navigation and way-finding for users inside buildings.
- **Asset Tracking:** Allows for the monitoring and tracking of physical assets within the facility.
- **Operational Insights:** Provides valuable data on movement patterns to enhance user experiences and location-based services.

Figure 61: Location compute



UWB Activation

UWB activation is initiated for a building and processed separately for each floor. Only supported UWB-capable access points that are placed on a floor map are eligible to appear in **Location Compute**.

During activation, Cisco Spaces performs these actions:

- Collects UWB ranging data between access points.
- Creates access point clusters.
- Assigns **Primary TX**, **Secondary TX**, or **RX** roles.
- Pushes the cluster configuration to the access points.

UWB Location is a prerequisite for UWB-based asset location. If UWB Location is not activated, a tag that supports BLE and UWB continues to provide BLE data, but its UWB location capability is unavailable through Cisco Spaces.

Activate UWB Location

Enable UWB on supported access points in a building to provide UWB-based location and ranging services.

Use this task when you want to activate Ultra-Wideband technology in a building. Activation will start several non-disruptive processes on your controller and access points.

Before you begin

- Ensure you have administrator access to the controller's management interface.
- Verify that the building contains UWB-capable access points.
- You have permission to configure Location Compute.
- The building and floors are available in the Cisco Spaces location hierarchy.
- Supported UWB-capable access points are assigned to the appropriate floors.
- The access points are placed on the floor maps.

Follow these steps to activate UWB location:

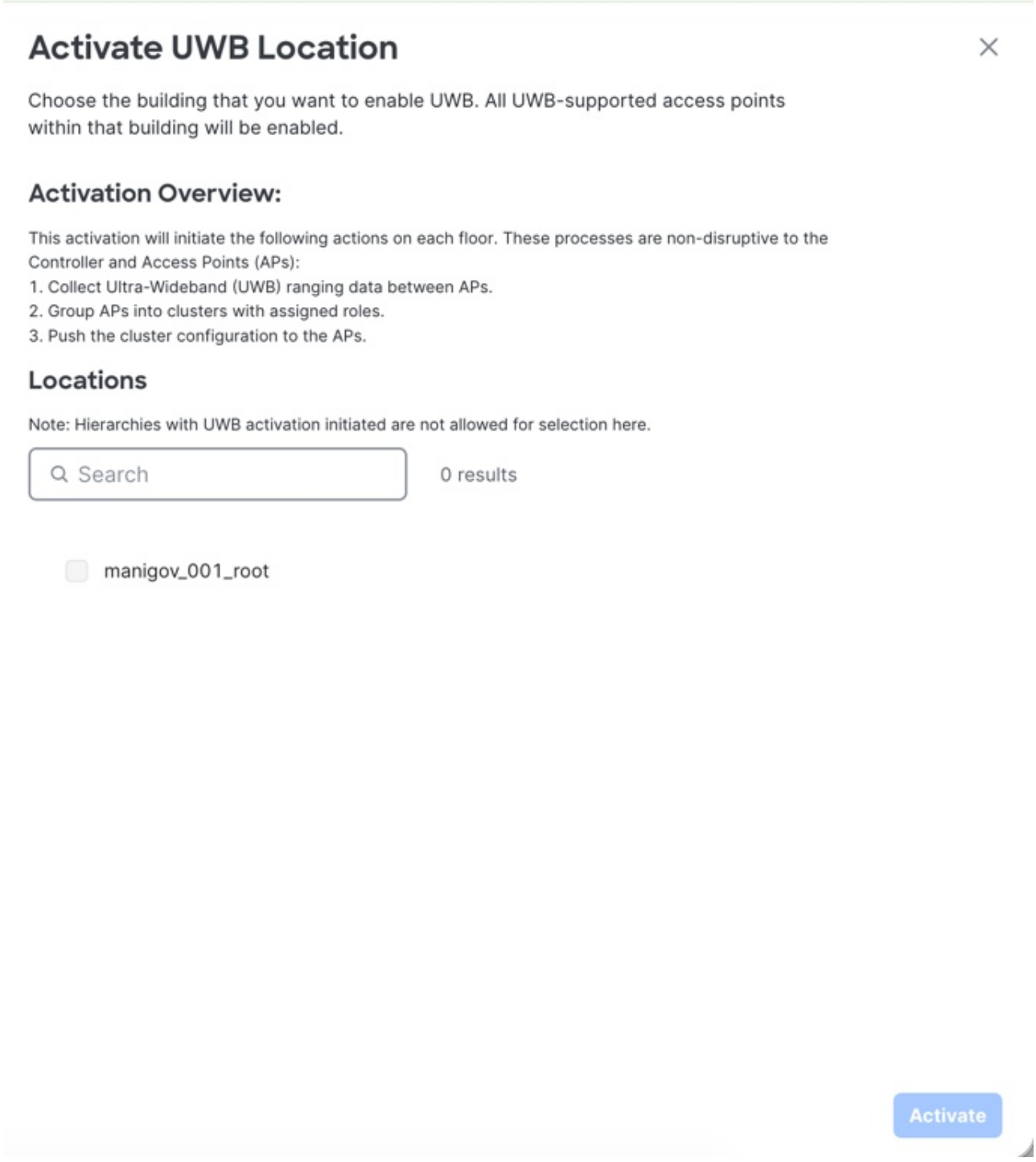
Procedure

Step 1 On the Cisco Spaces left navigation pane, choose **Configure** > **Location Compute**.

Step 2 In the **Location Compute** window, click **+ Activate UWB Location**.

The **Activate UWB Location** slide-in window is displayed.

Figure 62: Activate UWB Location



Step 3 In the **Search** field, enter the building name.

Step 4 Check the check box for the building where you want to enable UWB.

You cannot select hierarchies that already have UWB activation in progress.

Step 5 Click **Activate**.

The UWB activation process is initiated.

- The following actions occur automatically for each floor:
  - The system collects Ultra-Wideband (UWB) ranging data between access points.
  - Access points are grouped into clusters with assigned roles.
  - Cluster configurations are pushed to all APs in the building.
- Monitor the activation status to ensure all access points are successfully enabled.

All UWB-capable access points within the selected building are enabled for Ultra-Wideband services, allowing advanced location and ranging functionality.

Initiate the UWB activation process.

What to do next

Optionally, verify UWB functionality by checking device location accuracy or reviewing status reports in the platform's dashboard.

View the UWB Activation Log

Review the processing stages and request history for UWB activation or deactivation at a building or floor.

Procedure

Step 1 On the Cisco Spaces left navigation pane, choose **Configure** > **Location Compute**.

Step 2 In the **Locations** table, locate the required building or floor.

Step 3 The **Activation** status slide-in pane appears.

A completed activation can include these stages:

- **Activation Started**
- **Ranging Completed**
- **Initiate Clustering**
- **Clustering Completed**
- **Clusters Pushed**
- **Clusters push successful**
- **Completed**

Review **Request History**.

Step 4 Click the **Close** icon.

View UWB-Enabled Access Points

View the UWB-capable access points that are enabled on a floor and verify their assigned cluster roles.

Before you begin

UWB Location is activated for the building.

Procedure

Step 1 On the Cisco Spaces left navigation pane, choose **Configure** > **Location Compute**.

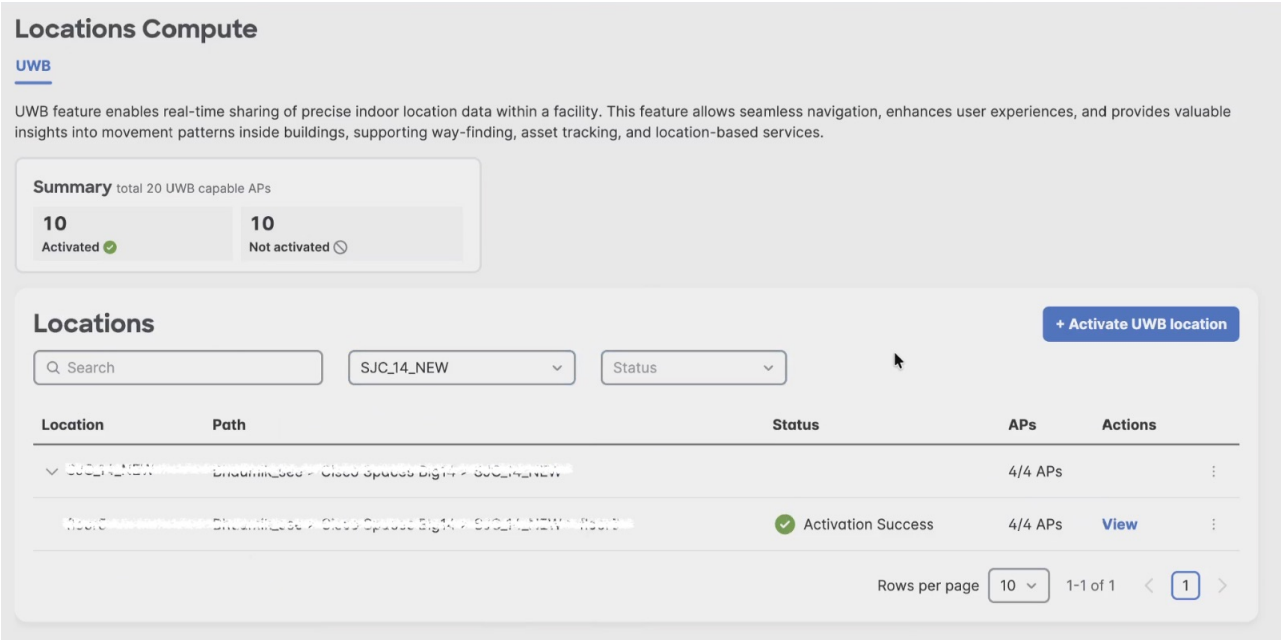
Step 2 Find the required building by using one of these options:

a) In the **Search** field, enter the value.
b) Choose a location from the **All UWB-Capable Locations** drop-down list.
c) Choose an activation state from the **Status** drop-down list.

Step 3 In the **Location** column, click the expand icon next to the building.
The floor rows show the hierarchy **Path**, activation **Status**, and number of eligible **APs**.

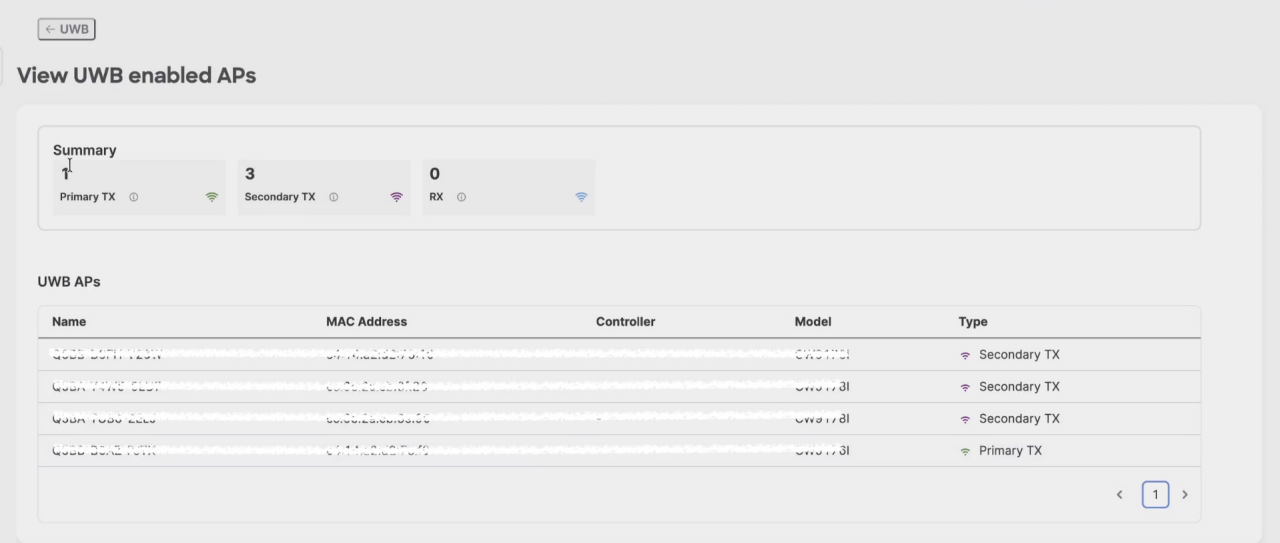
Step 4 In the **Actions** column, click **View** for a floor with the **Activation Success** status.

Figure 63:



Step 5 The **View UWB enabled APs** window appears.
Fig

Figure 64:



The **UWB APs** table displays these information:

a. **Name**

b. **MAC Address**

c. **Controller**

d. **Model**

e. **Type**

Review the access point details and assigned roles.

What to do next

Click the **UWB back arrow** to return to the **Locations Compute** window.

Deactivate UWB Location

Deactivate UWB Location for a building or an individual floor when UWB location services are no longer required.

Before you begin

Deactivation disables UWB location services for the selected building or floor. Applications that depend on UWB location, including UWB-based asset location, are affected. BLE data from tags that support BLE and UWB can continue to be received.

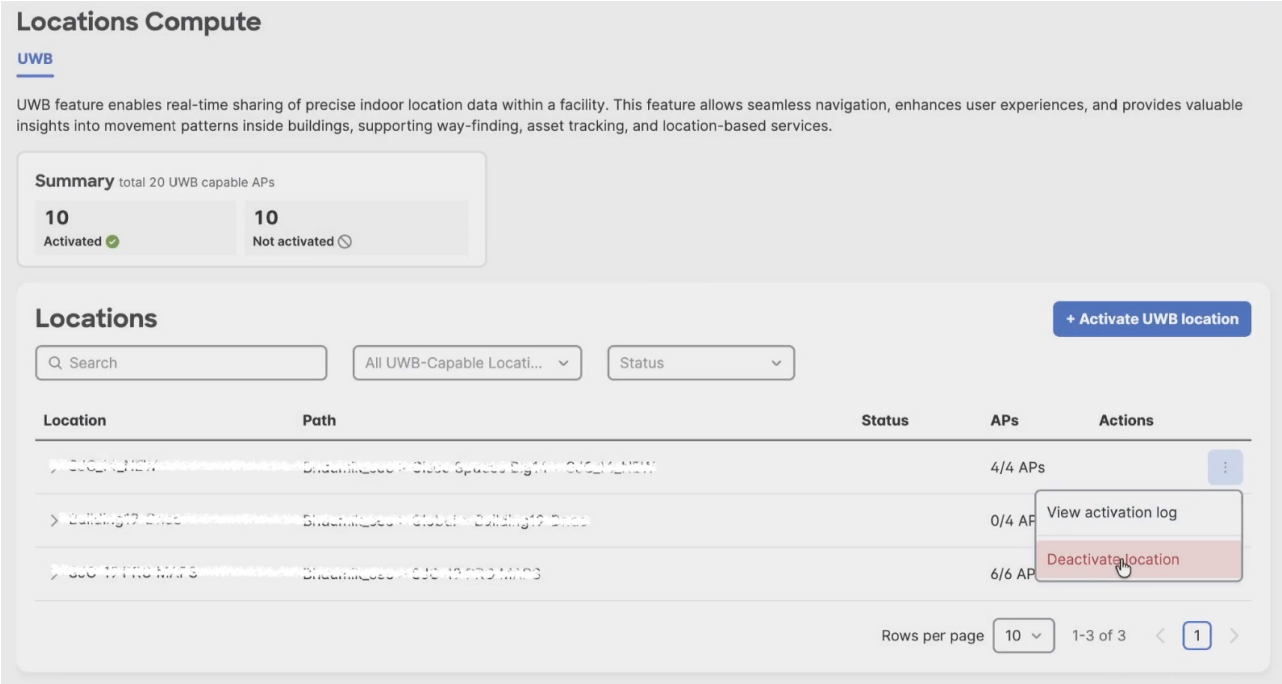
Procedure

Step 1 On the Cisco Spaces left navigation pane, choose **Configure** > **Location Compute**.

Step 2 In the **Locations** column, click the building expand icon and locate the required floor.

Step 3 In the **Actions** column, click the three-dot icon for the required building or floor.

Figure 65:



Step 4 Click **Deactivate location**.
The deactivation request starts for the selected scope. Cisco Spaces disables the applicable UWB clusters.

What to do next

In the **Actions** column, click the three-dot icon.

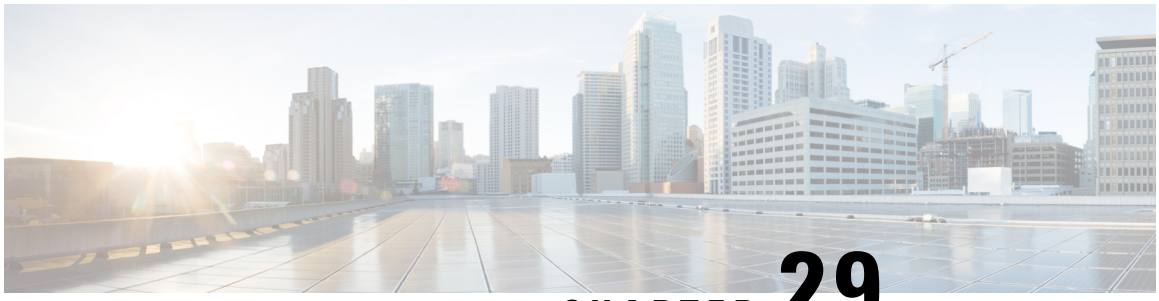
Click **View activation log** to verify the deactivation result under **Request History**.



PART VIII

Monitor

- Monitoring and Support, on page 297



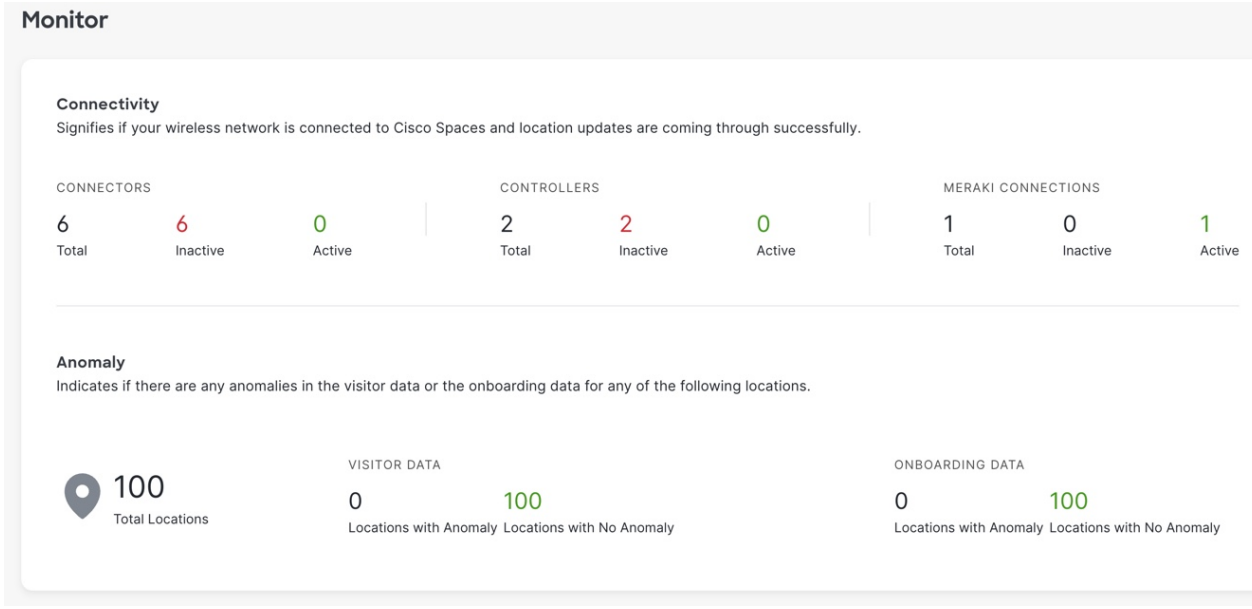
CHAPTER 29

Monitoring and Support

This chapter describes the monitoring details that are displayed in Cisco Spaces.

To access the **Monitor** window, in the **Cisco Spaces** dashboard, click the three-line menu icon at the top-left, and choose **Monitor**.

Figure 66: Monitor



- Monitor, on page 297

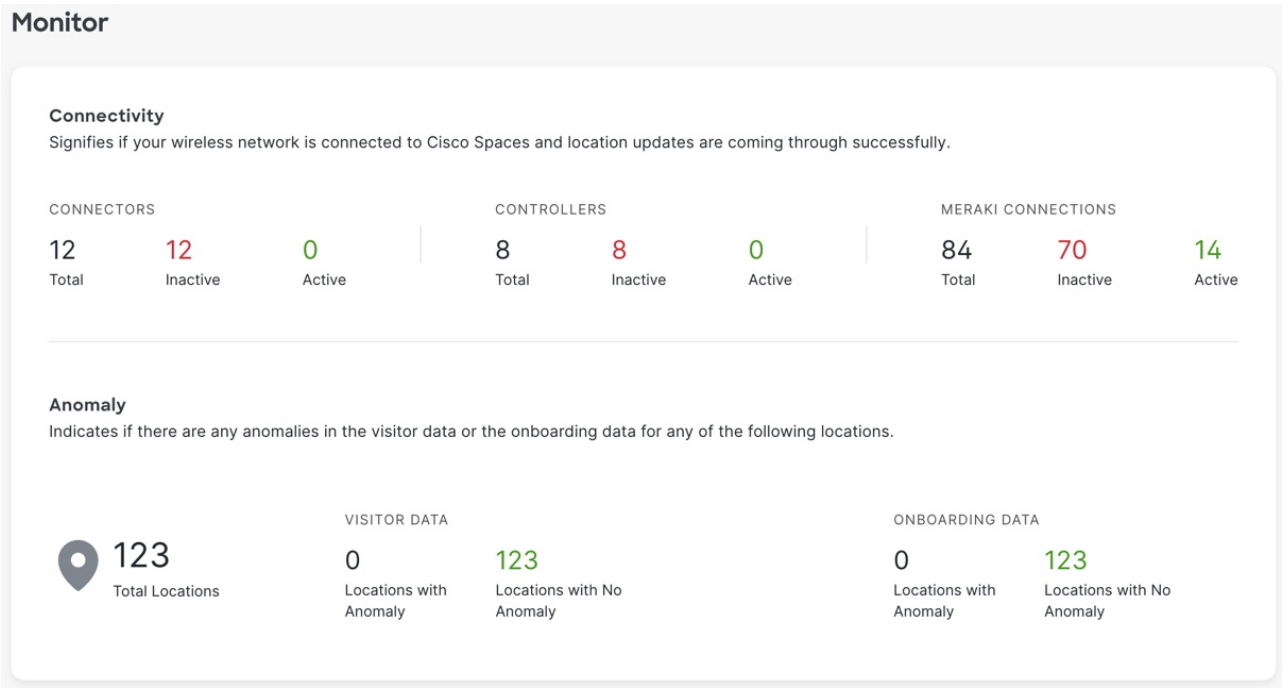
Monitor

The **Monitor** window serves as the centralized health and diagnostic hub for your Cisco Spaces environment. Use the **Monitor** feature to monitor the health details and performance metrics of Cisco Spaces.

It provides real-time visibility into the connectivity status of your wireless infrastructure, the integrity of your location data, and the operational uptime of your installed Cisco Spaces applications.

By using this feature, administrators can quickly identify connectivity gaps, address data anomalies, and ensure that location services are functioning optimally.

Figure 67: Monitor



View these details:

- **Connectivity**: Signifies if your wireless network is connected to Cisco Spaces and location updates are coming through successfully. View the details for connectors, controllers and Meraki connections.
- **Anomaly**: Displays the current status of location updates and internet provisioning (this is applicable only of you have configured customer acquisition through captive portals) in the locations. This section is marked as up if location updates and internet provisioning are happening for all the locations without any issues. If any of them is not happening for any location, the status will be down. If both location update and internet provisioning are not happening for a location, such locations will be listed out.
- **Connectors**: Displays the active connectors. Click a controller to view the descriptions, OVA version, control channel status, control channel last heard (UTC) and data channel status for active connectors.
- **Controllers**: Displays the active controllers. View the description, type, last geard (UTC) and status for active controllers. You can monitor the status of your wireless controllers. This provides insight into whether your hardware is successfully transmitting data to the platform.
- **Meraki Networs**: Displays the Cisco Meraki networks that are synchronized and the status. You can track the status of your Cisco Meraki network integrations. It shows the total number of networks, how many are active, and how many are currently inactive.
- **Location Updates**: Displays the current location update status for the locations to which you have access. This section will be marked as up if location updates are received from all the locations, and the status will be **All Locations Connected**. If there is any location update issue, this section will be marked as down, and the total number of locations that have location update issue will be displayed.
- **Cisco Spaces apps**: Displays the apps and their status.

  For each application, you can view:

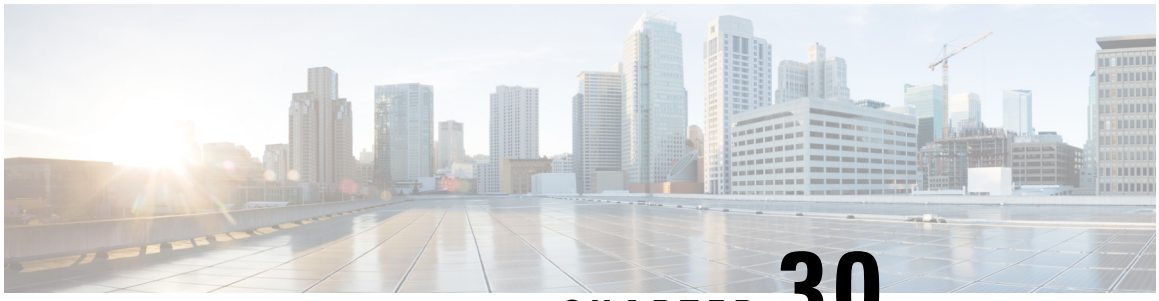
- **Uptime %**: The percentage of time the application has been operational.
- **Status**: A clear indicator (Up/Down) of the current operational state of the application.



PART IX

Admin Management

- Managing Cisco Spaces Users and Accounts, on page 303



CHAPTER 30

Managing Cisco Spaces Users and Accounts

This chapter explains how to invite and manage Cisco Spaces users and accounts.

- Manage Cisco Spaces Users, on page 303
- Manage the Cisco Spaces Accounts, on page 309
- Location-Based RBAC (Role-Based Access Control) in Cisco Spaces, on page 310

Manage Cisco Spaces Users

Cisco Spaces provides users with different rights and privileges based on the role they perform.

After you log in to the Cisco Spaces **Home** page, click **Admin Management** from the left navigation.

These tabs are available:

- **Admins**: Use the **Admins** tab to view Cisco Spaces users, invite new administrators, edit user roles, remove users, and resend pending invitations.

  The **Admins** table displays details such as **Name, Email, Role, Read & Write, Read only,** and **Locations**. Use the **Search** field to search for existing users. The table can also display the result count, pagination controls, row check boxes, and the row action menu.

- **Roles**: Use the **Roles** tab to search for roles, create roles, edit roles, remove roles, and manage permission templates.

  The **Roles** table displays role details such as **Role, Read & Write, Read only,** and **Locations**. The values in **Read & Write** and **Read only** summarize the apps assigned to the role.

Invite a Cisco Spaces User

When a Cisco Spaces account is created, a **Dashboard Admin Role** user is created for the account with the email ID provided. This **Dashboard Admin** can invite other users to Cisco Spaces.

Cisco Spaces provides only one default user role, **Dashboard Admin Role**.

By default, **Dashboard Admin Role** has read and write access rights only to the role types, **DNASpaces** (including menu items in the left pane, of the dashboard, and the apps Behavior Metrics, OpenRoaming, Location Analytics, Engagements, and Location Personas), **Captive Portals**, and **Asset Locator**.

Note

- If the **Dashboard Admin Role** requires access to any other role types (apps) such as **BLEManager**, contact the Cisco Spaces support team.
- By default, a **Dashboard Admin Role** for the **ESSENTIAL** license has access only to **Cisco Spaces**.

Cisco Spaces allows you to define user roles with different access rights to different apps.

For example, you can create a user role with read-and-write permission in the **Captive Portals** app, and read-only permission in the **Asset Locator** app.

You can include the following role types (apps) in a user role if that particular service is enabled for your account.

- **Cisco Spaces**: This role type provides access to all the menu items in the left pane of the Cisco Spaces dashboard such as Location Hierarchy, Admin Management, Monitoring and Support, Setup, and so on. In addition, this role type provides access to the apps such as Behavior Metrics, OpenRoaming, Location Analytics, Engagements, and Location Personas.
- **Captive Portals**: This role type provides access rights to the **Captive Portals** app.
- **IoT Services**: This role type provides access rights to the **IoT Services** app.
- **MapService**: This role type provides access rights to **Map Service**.
- **Location Analytics**: This role type provides access rights to the **Location Analytics** app.
- **Live Occupancy**: This role type provides access rights to the **Live Occupancy** app.
- **Behavior Metrics**: This role type provides access rights to the **Behavior Metrics** app.
- **Impact Analysis**: This role type provides access rights to the **Impact Analysis** app.
- **Camera Metrics**: This role type provides access rights to the **Camera Metrics** app.
- **Engagements**: This role type provides access rights to the **Engagements** app.
- **Location Personas**: This role type provides access rights to the **Location Personas** app.
- **OpenRoaming**: This role type provides access rights to the **OpenRoaming** app.
- **Detect and Locate**: This role type provides access rights to the **Detect and Locate** app.
- **IoT Explorer**: This role type provides access rights to the **IoT Explorer** app.
- **Space Manager**: This role type provides access rights to the **Space Manager** app.
- **Space Experience**: This role type provides access rights to the **Space Experience** app.
- **Environmental Analytics**: This role type provides access rights to the **Environmental Analytics** app.
- **Space Utilization**: This role type provides access rights to the **Space Utilization** app.
- **Energy Utilization**: This role type provides access rights to the **Energy Utilization** app.
- **Asset Locator**: This role type provides access rights to the **Asset Locator** app.
- **Proximity Reporting**: This role type provides access rights to the **Proximity Reporting** app.

- **Partner Dashboard**: This role type provides access rights to the **Partner Dashboard** app.

Note

- Import of duplicate payload from Catalyst Center to **Mapservice** is restricted. In the **Import History** section, the following error message is displayed: `Warning: Import ignored due to no changes in request payload`.
- Access to Map Services is no more provided as part of the DNASpaces. However, you can assign **MapServices** to a role only with **Cisco Spaces**. For example, you can create a role with read and write access to **MapServices** and Read Only access to **Cisco Spaces**.
- For the Dashboard Admin role, access to **Location Analytics** is provided by default. For other roles, you must assign access separately. However, you can assign **Location Analytics** to a role only along with the **Cisco Spaces** service. For example, you can create a role with read and write access to **Location Analytics** and Read Only access to **Cisco Spaces**. The Location Analytics tile is disabled for Cisco Spaces user accounts that do not have access to **Location Analytics**.

Follow these steps to invite a Cisco Spaces user.

Procedure

Step 1 From the left navigation menu, choose **Admin Management** > **Admins**.

Step 2 Click **Invite Admin**.

Step 3 In the **Invite Admin** window, enter the following details:

a) In the **Email** field, enter the email address of the user to add.

b) From the **Role Name** drop-down list, select the user role that you want to provide to this user.

- The default user role and the user roles defined earlier are displayed in the drop-down list. If the required user role is not there, you can define a new user role using **Create New Role**.
- Click **Create New Role** to create a new user role. For more information on creating a new user role, refer to Create a User Role, on page 306. The user roles defined are listed on the **Roles** tab.
- After you select a role name, Cisco Spaces displays a privilege preview table with the **Apps** and **Permission Type** details for the selected role. Review the privileges before inviting the user.

Step 4 Check the **Restrict this role to specific locations** check box if you want to restrict the selected role to any particular location.

a) Click **+ Add Locations**.

b) In the **Choose Locations** window, use **Search** to find a location, or expand and collapse the location hierarchy to browse locations.

c) Check the check box for each required location. The selected locations are displayed in the **Selected Locations** pane.

d) Review the selected-location count and selected-location chips.

e) Click **Done**.

Note If a parent location is selected, access applies to the selected parent location and the child locations under it, based on the location hierarchy. License badges such as **ADVANTAGE** can appear next to locations to indicate the license level for that location.

Step 5 Click **Invite**.

Note
- The **Invite Admin** option is only available for Cisco Spaces administrators with read and write permissions.
- Certain apps such as Captive Portals have provisions to manage the users for that particular app. For example, a Captive Portals app user with read and write permission can invite users with user roles **Creative User** or **Access Code Manger** from the **User Management** option in the Captive Portals app. Admin Management users are displayed in the **User Management** window. However, from the **User Management** option in the Captive Portals app, you cannot modify a user account created through **Admin Management**.
- If an invited user has not accepted the invitation, the user status is displayed as **Invited - Not yet responded**. To send the invitation again, click **RESEND** for the pending user.

Create a User Role

To create a Cisco Spaces user role, follow these steps:

Procedure

Step 1 From the left navigation menu, choose **Admin Management** > **Roles** tab.

Note You can also click **Create New Role** in the **Role Name** drop-down list in the **Invite Admin** window.

Step 2 Click **Create New Role**.

Step 3 In the **Create New Role** slide-in window, enter the following details:

a) In the **ROLE NAME** field, enter a name for the user role.

b) In the **APPS** area, check the check boxes for the role types that you want to provide to this user role.

For more information on role types (apps), refer to the role types described in Invite a Cisco Spaces User, on page 303.

c) From the drop-down list that displays for each role type, choose the access right to be provided for this particular user role.

You can set the access right as **Read Only** or **Read/Write**.

For example, if you want to create a user role that has complete access to Dashboard menu items, and read-only access to the captive portal app, check the **Cisco Spaces** check box, and from the corresponding drop-down list choose **Read/Write**. Then check the **Captive Portal** check box, and from the corresponding drop-down list choose **Read only**.

Step 4 Check the **Restrict this role to specific locations** check box to restrict role access to specific locations.

The **+ Add Locations** option is displayed.

Step 5 Click **+ Add Locations** to select locations.

a) In the **Choose Locations** slide-in window, use **Search** to find a location, or expand and collapse the location hierarchy to browse locations.
b) Select the check box for each required location. The selected locations are displayed in the **Selected Locations** pane.
c) Review the selected-location count and selected-location chips.
d) Click **Done**.

Step 6 Click **Create Role**.

The user role is available in the **Role Name** drop-down list of the **Invite Admin** window.

Edit a User Role

As a Dashboard Admin user with read and write permissions, you can change the role of a Cisco Spaces user.

Note Users from external partner organizations are automatically listed in the **Admin Management** tab after they sign in through Cisco Federation. The identity provider (IdP) of the partner organization assigns their roles. Only the **Delete** option is available for these users; the **Edit** option is not available. To change a user's role, update the role assignment in the partner organization's identity provider (IdP).

Procedure

Step 1 From the left navigation menu, choose **Admin Management** > **Roles**.

Step 2 Click the row action menu for the role that you want to edit, and choose **Edit Role**.

The **Edit Role** slide-in window is displayed.

Step 3 Update the role name, app permissions, or location restrictions as required.

Step 4 Click **Update**.

Remove a User Role

Use this task to remove a user role that is no longer required.

Procedure

Step 1 From the left navigation menu, choose **Admin Management** > **Roles**.

Step 2 Click the row action menu for the role that you want to remove, and choose **Remove Role**.

Step 3 Review the confirmation message and click **Remove**.

Note A role cannot be removed if it is assigned to one or more users. Before removing the role, assign those users to another role.

Edit Cisco Spaces User

As a Dashboard Admin user with read and write permission, you can change the user role of a user. For example, a Dashboard Admin Read can be promoted to a Dashboard Admin Read and Write user.

Follow these steps to edit the user privileges of a Cisco Spaces user.

Procedure

Step 1 From the left navigation menu, click **Admin Management**.

The **Admin** page is displayed with the list of e-mail IDs of the Cisco Spaces users.

Step 2 Click the three dots next to the user (at the far right) you want to edit.

Step 3 Click the **Edit User**.

The **Edit User** page displays the user email address as a read-only field.

Step 4 From the **Role Name** drop-down list, choose the type of access that you want to provide to the user.

The default user roles and the user roles defined earlier are available in the drop-down list for selection. If the required user role is not there, you can define a user role using **Create New Role**. For more information on creating a new user role, refer to Create a User Role, on page 306.

After you select a role, Cisco Spaces displays a privilege preview table with the **Apps** and **Permission Type** details for the selected role.

Step 5 Click **Update**.

Delete a Cisco Spaces User

If a user no more needs access to Cisco Spaces, we recommend that you delete such users from the Cisco Spaces user list.

Any user with admin privileges can delete other users.

Follow these steps to delete an existing Cisco Spaces user.

Procedure

Step 1 From the left navigation menu, click **Admin Management**.

The **Admins** page is displayed with the list of the Cisco Spaces users.

Step 2 Click the three dots next to the user (at the far right) you want to edit.

Step 3 Click **Remove**.

To delete multiple users, select the check box for the corresponding e-mail IDs, and click **Remove** option which displays on the top right of the window.

A confirmation message is displayed before the user is removed. Removing a user revokes the user's access to Cisco Spaces. Pending invited users can also be removed from the **Admins** table. Some protected users, such as the account owner or the currently signed-in administrator, may not be available for removal.

Manage the Cisco Spaces Accounts

This section describes how to manage the Cisco Spaces accounts.

Change the Cisco Spaces Password

We recommend that you change the Cisco Spaces password at frequent intervals to ensure more security for your application.

Follow these steps to change the password of your Cisco Spaces account.

Procedure

Step 1 In the **Cisco Spaces Home** page, click the **User Account** icon that is displayed at the far right of the dashboard.

Step 2 Click **Change Password**.

Step 3 In the window that displays, do the following:

a) In the **Current Password** field, enter the current password for your Cisco Spaces account.
b) In the **New Password** field, enter the new password that you want for your Cisco Spaces account.
c) In the **Confirm Password** field, reenter the new password for confirmation.
d) Click **Change Password**.

Password Strength

The Cisco Spaces password requires the following parameters:

- At least 8 characters
- At least 1 upper case letter (A-Z)
- At least 1 lower case letter (a-z)
- At least 1 special character
- At least 1 numeric character(0-9)

Signing Out of Cisco Spaces

To sign out of Cisco Spaces, follow these steps:

Procedure

Step 1 In the **Cisco Spaces** dashboard, click the **User Account** icon () that displays in the far right of the dashboard.

Step 2 Click **Logout**.

Location-Based RBAC (Role-Based Access Control) in Cisco Spaces

Location-Based RBAC (Role-Based Access Control) in Cisco Spaces is an enhanced security feature that allows administrators to restrict user roles and permissions to specific physical locations within Cisco Spaces. This means when creating or assigning a user role, you can limit that role's access rights to particular locations such as campuses, buildings, floors, or zones.

Use the **Restrict this role to specific locations** option to enable this feature. This option is available during role creation (**Admin Management** > **Roles** > **Create Role**) and when inviting users (**Admin Management** > **Invite Admin**).

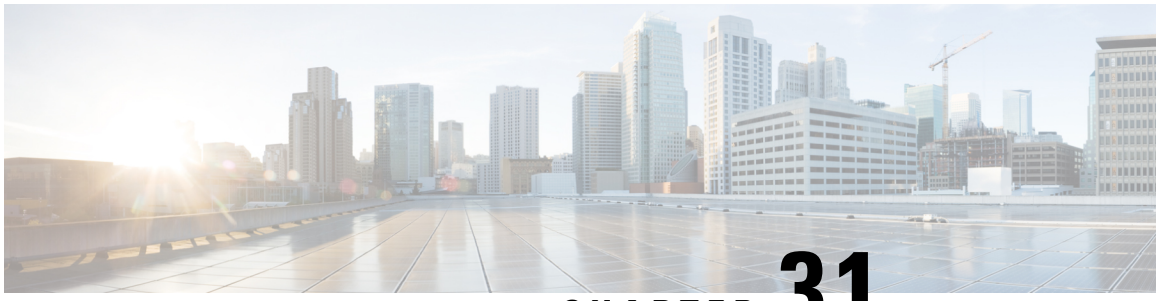
When location restriction is enabled, Cisco Spaces displays the **Choose Locations** window. Use this window to search the location hierarchy, expand or collapse location levels, select locations, review selected-location chips, and confirm the selection. The selected locations are displayed in the user or role details and in the **Locations** column of the **Admins** or **Roles table**.



PART X

Setup

- Set Up Wireless Network, on page 313
- Set Up Wired Network, on page 323
- Set Up Locations and Maps, on page 325
- Set Up Meraki Camera, on page 353
- Set Up Data Export, on page 361
- Set Up Cisco Webex, on page 371
- Set Up pxGrid Cloud, on page 375
- **Set Up Access Point Auto Location**, on page 379
- Plugins, on page 391



CHAPTER 31

Set Up Wireless Network

This chapter provides instructions on how to set up Cisco Spaces to work with various wireless networks and how to configure these networks using different methods.

- Setting Up Cisco Spaces to Work with Various Wireless Networks, on page 313
- Wireless Network Bars, on page 315
- Set Up Meraki API Key Method, on page 319
- Wireless Network Status, on page 321

Setting Up Cisco Spaces to Work with Various Wireless Networks

You can set up Cisco Spaces with wireless networks that are based on the following options:

- Cisco AireOS wireless controllers
- Cisco Catalyst 9800 wireless controllers
- Cisco Meraki

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the **Home** page, from the left navigation pane, choose **Setup** > **Wireless Networks**.

Step 3 In the **Connect your wireless network** window, click **Add New**.

The **Connect your wireless network** window is displayed with the options **AireOS Controller/Catalyst 9800 Wireless Controller** and **Cisco Meraki**.

- For **AireOS Controller/Catalyst 9800 Wireless Controller**, these configurations are available:
  - **Via Spaces Connector**: To connect Cisco Spaces to Cisco Wireless Controller using Cisco Spaces: Connector.
  - **Connect Cisco Wireless Controllers directly**: To connect Cisco Spaces to Cisco Wireless Controller using a Cisco Wireless Controller Direct Connect.

- **Connect WLC directly**: To connect Cisco Spaces to Cisco Wireless Controller using a Cisco Wireless Controller Direct Connect.
- **Connect via CMX Tethering**: To connect Cisco Spaces Cisco Wireless Controller using Cisco CMX.



Note This option is available only for supported legacy customers who already use **CMX Tethering**. It is deprecated for new deployments.

- For **Cisco Meraki**, these configurations are available:
  - **Connect via Meraki Login**: To connect Cisco Spaces to Cisco Meraki using a Cisco Meraki account.
  - **Connect via API Key**: To connect Cisco Spaces to Cisco Meraki using a Cisco Meraki API Key.

    You can login to the **Meraki** dashboard, choose **Account Name** > **My Profile** > **API Access**, and click **Generate** to generate an API Key. Enter this key in the **Connect via API key** field in the Cisco Spaces dashboard to add your network to Cisco Spaces. For more information, see Set Up Meraki API Key Method, on page 319.



Note For new Cisco Spaces accounts, click **Get Started**.

Step 4 Click **Select** to choose your preferred method through which you want to connect to Cisco Spaces.

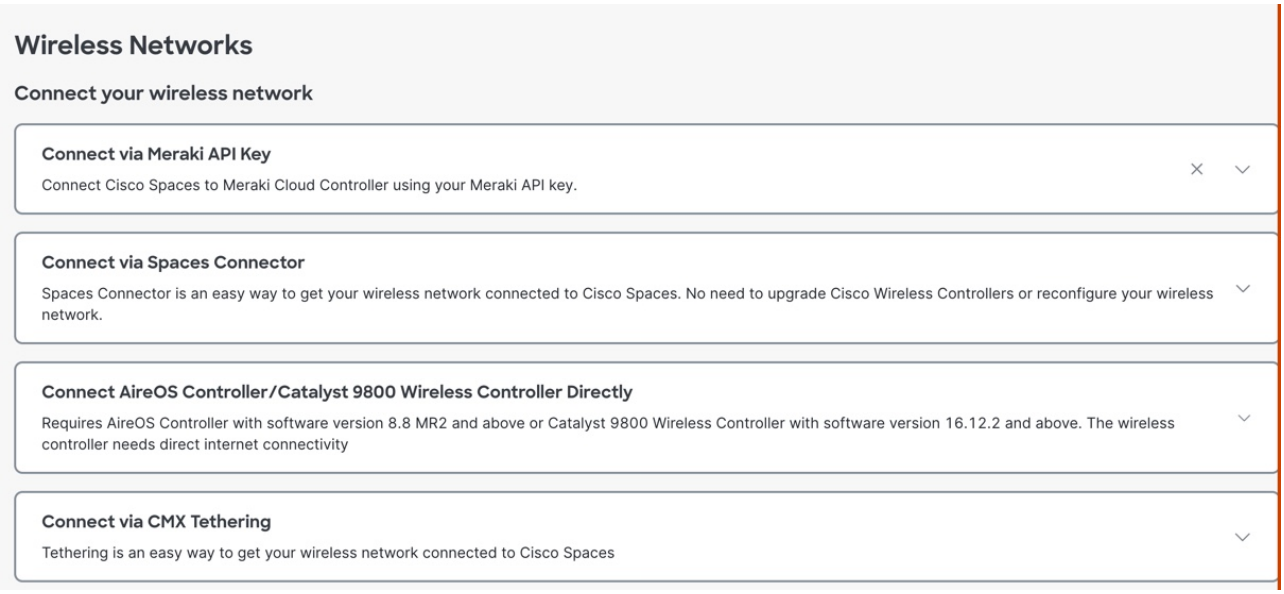
The prerequisites for connecting to the wireless network using the selected method are displayed.

Step 5 Click **Continue Setup**.

The following message is displayed: `Successfully saved the configuration`.

Step 6 A bar corresponding to the wireless network configuration method selected is displayed in the **Connect your wireless network** window. For example, if **Via Spaces Connector** is selected, a bar with the label **Connect via Spaces Connector** displays.

Figure 68: Connected wireless networks



Step 7 To view the instructions and configure the wireless network, click the drop-down button at the far right of the bar.

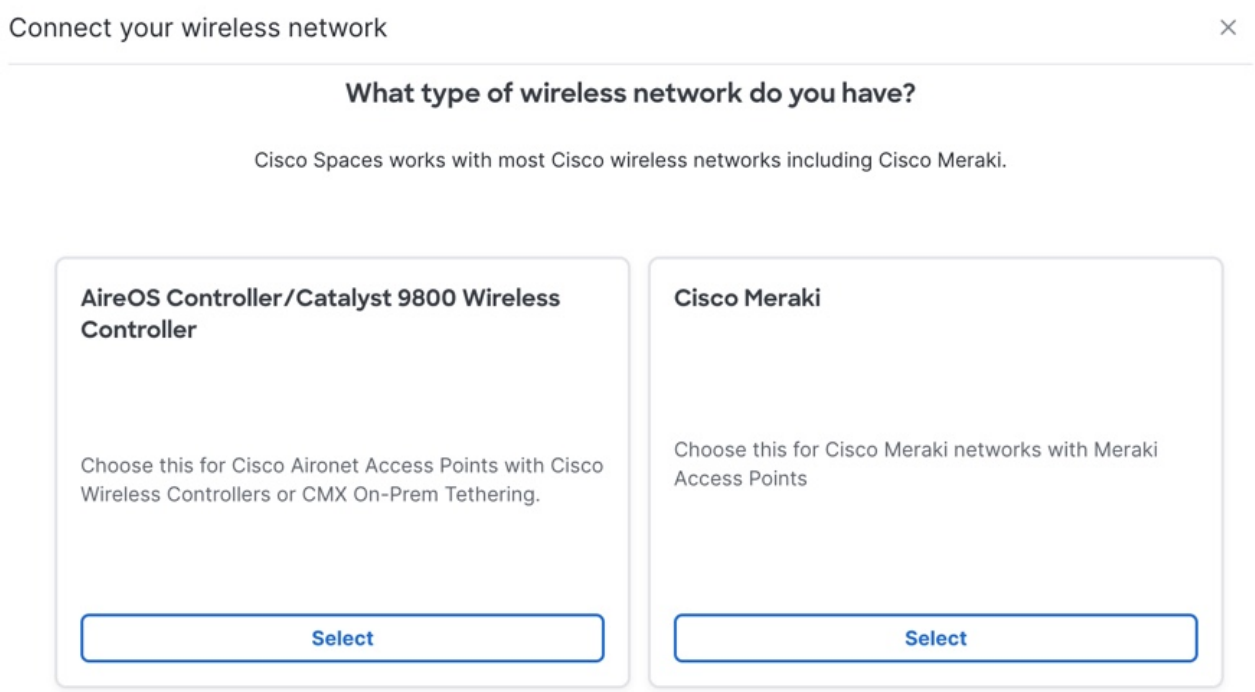
The instructions and the features to connect to preferred wireless network are displayed.

Step 8 Follow the on-screen instructions to add the wireless network.

Wireless Network Bars

To connect your wireless network with Cisco Spaces, use any available options in the **Setup** > **Wireless Networks** > **Connect your wireless network** window.

Figure 69: Wireless Network



The following tabs are displayed for Cisco Meraki based on your selection:

- **Connect via Meraki API Key**: Use this option to connect Cisco Spaces to Cisco Meraki Cloud Controller using your Cisco Meraki API key. Follow the on-screen instructions to import a Cisco Meraki organization and the related child locations to the location hierarchy using the **Import Networks** option.

Note We recommend using **Connect via API Key** to connect Cisco Meraki with Cisco Spaces.

Perform the following:

1. **Connect your Meraki**: Connect Cisco Meraki with Cisco Spaces using the API key.
2. **Configure Meraki scanning API**: Cisco Meraki scanning APIs are automatically configured after importing the networks into the location hierarchy.

Note To configure manually, use the **Post URL** with URL validator and **Secret Key** and validate manually in the Cisco Meraki dashboard to establish a connection with Cisco Spaces.

3. **Import Meraki Networks into Location Hierarchy**: Click **Import Networks** to import the Cisco Meraki networks.

For more information, refer to Location Hierarchy.

Note The synchronized user count is displayed under the **Connect your Meraki** options. (**Connect via Meraki Login** and **Connect via Meraki API Key**).

The following bars are displayed for Cisco AireOS based on the connection method selected:

- **Connect via Spaces Connector**: Use 'to connect Cisco Spaces to Cisco Wireless Controller'

Note You need not upgrade your Cisco Wireless Controllers or reconfigure your wireless network when you use **Connect via Spaces Connector** option.

Perform the following:

1. **Install Spaces Connector OVA**: Download and install Cisco Spaces: Connector OVA as a virtual machine.

   Click the **Download Spaces Connector** link to download the Spaces Connector.

2. **Configure Spaces Connector**: Click **Create Connector** to create a new connector. You need a token to configure Cisco Spaces: Connector. Connect to `https://<your connector IP>/` from a browser to configure the token. You can optionally configure Cisco Spaces: Connector to connect via HTTPS proxy.

   Click **View Connectors** to view the available connectors.

3. **Add Controllers**: Click **Add Controllers** to add Cisco Wireless Controllers. Click **View Controllers** to view the available controllers.

4. **Import Maps**: Click **Import/Sync Maps** to import or synchronize the maps. You must upload a Cisco Prime Infrastructure or Catalyst Center (version 1.3.1 and above) map to work with Cisco Spaces: Detect and Locate, Asset Tracker, and IoT Services.

5. **Setup location hierarchy**: Click **Add Locations** to add the imported maps to Location Hierarchy.

Note

- You can view the location hierarchy using the **View Location Hierarchy** option.
- For the OpenRoaming app, you can configure the hotspots through the **Add OpenRoaming Hotspot** option. You can also view the configurations for the OpenRoaming app for various controllers separately using the **OpenRoaming Controller Configuration** option.
- The Network Configuration Protocol (NETCONF) support is available from Hotspot client version v2.2.95 and on Cisco Catalyst 9800 Series Wireless Controllers version 17.12.

For more information, refer to Cisco Spaces: Connector Configuration Guide.

- **Connect AireOS Controller/Catalyst 9800 Wireless Controller Directly**: Use 'to connect Cisco Spaces to Cisco Wireless Controller (**Connect AireOS Controller/Catalyst 9800 Wireless Controller**)'.

Note To connect to this wireless network, you need either an AireOS Controller with software version 8.8 MR2 or later, or a Catalyst 9800 Wireless Controller with software version 16.12.2 or later. The wireless controller needs direct internet connectivity.

Perform the following:

1. **Install Root Certificate**: You can install the certificate from AireOS Controller CLI with View root certificate.
2. **Configure Token in AireOS Controller**: You can view token and contollers using the View Token and View Controllers options
3. **Import Maps**: You can now manage maps from the **Setup** window under Connect WLC/Catalyst 9800 Directly and Connect Via Spaces Connector
   - **Import/Sync Maps**: Upload a Cisco Prime Infrastructure or the Catalyst Center map in order to work with Detect & Locate, Asset Tracker, and IoT Services seamlessly.
   - **Map Upload History**: View the list of uploaded maps. You can view the filename, source type, status and other related information.
   - **Manage Maps**: Navigate to the **Map Service** application to manage maps.
4. **Setup location hierarchy**

- **Connect via CMX Tethering**: Use 'to connect Cisco Spaces to Cisco Wireless Controller'. Displays step-by-step instructions to configure location updates for a Cisco CMX node using CMX tethering with token. You can create the token using the **Create New Token** option in Step 2, and configure it in Cisco CMX.

Note **CMX Tethering** is supported only for legacy customers who already use this connection method. New customers must use the currently supported wireless network onboarding methods. **CMX Tethering** is deprecated for new deployments.

For legacy customers, use **CMX Tethering** only to manage an existing CMX-based deployment. The **CMX Tethering** option may not be displayed for new customers or accounts that are not enabled for this legacy workflow.

The other options available on the **Connect your wireless network** window are:

Table 17: Connect your wireless network Options

View Configuration Steps	Redirects to the documentation for the particular wireless network.

System Requirements	Provides the system requirements for Cisco Spaces.
Frequently asked questions	Provides the link to the frequently asked questions for Cisco Spaces.
Cisco AireOS Controller/Catalyst 9800 Wireless Controller	Displays instructions to import a Cisco CMX Node (CMX On-Prem) to the **Location Hierarchy** window.
Cisco Meraki	Displays instructions to import a Meraki Organization to the **Location Hierarchy** window.

Set Up Meraki API Key Method

Use the **Cisco Meraki** option to integrate Cisco Spaces with Meraki. Use the Meraki account credentials to connect to Cisco Meraki cloud, import locations into Cisco Spaces and activate or synchronize the Meraki networks.

Procedure

Step 1 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Wireless Networks** > **Add New** > **Cisco Meraki** > **Connect via API key**.

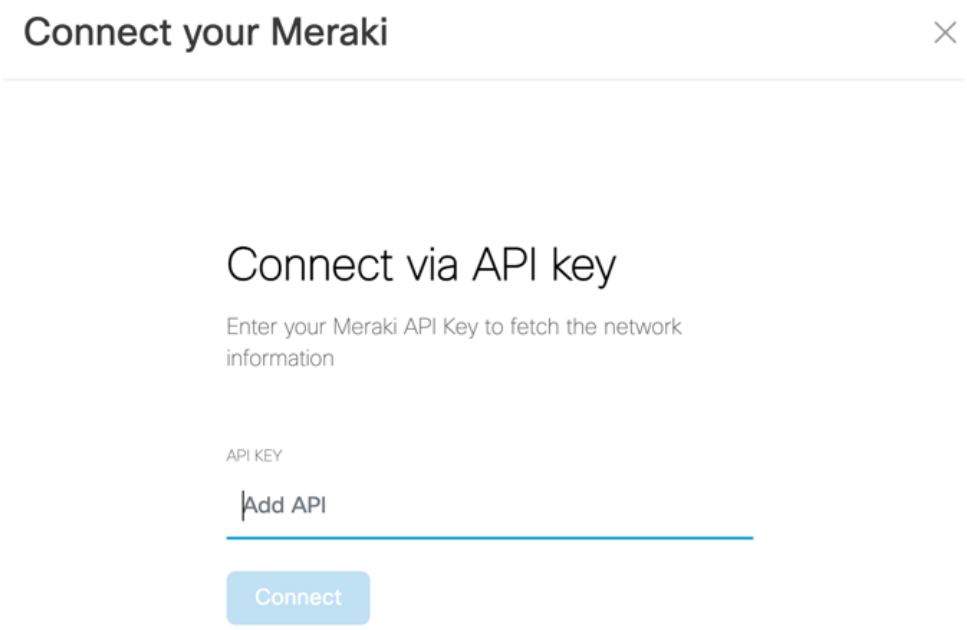
Step 2 In the Meraki dashboard, navigate to **Organization** > **Configure** > **Settings** and enable **Dashboard API Access**.

Step 3 In the Meraki dashboard, navigate to **Username** > **My Profile** > **API Access** and generate the API token. The generated API token is an alphanumeric value.

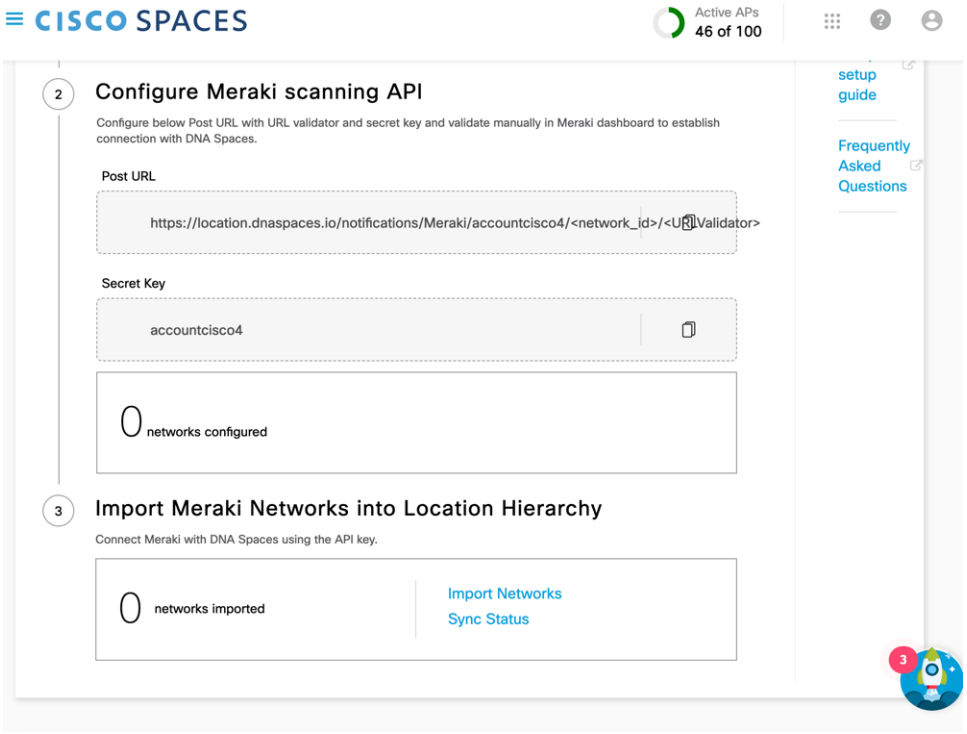
Step 4 Copy the generated API token to enter it in the Cisco Spaces dashboard.

Step 5 In the Cisco Spaces dashboard, perform the following:

a) In the **Connect your Meraki** pop-up window, paste the copied API token in the **API KEY** field.



b) Click **Connect**. After a successful synchronization with Meraki, the connection status displays as active.
c) From the **Configure Meraki scanning API** area, copy the values for **Post URL** and **Secret Key**.



Step 6 In the Meraki dashboard, navigate to your specific network and choose **Network-wide** > **Configure** > **General**.

Step 7 Scroll down to **Location and Scanning** and enable **Analytics and Scanning API**.

Step 8 In the **Post URLs** field, paste the post URL and secret key.

Step 9 From the **Location and Scanning** field, copy the **`validator ID`**.

Step 10 Edit the post URL **`<URLValidator>`** with the validator.

Step 11 Click **Validate** to validate the post URL functions.

Step 12 The dashboard opens an Import Networks wizard, select **Meraki Organization > Next > Choose Networks > Import Locations**.

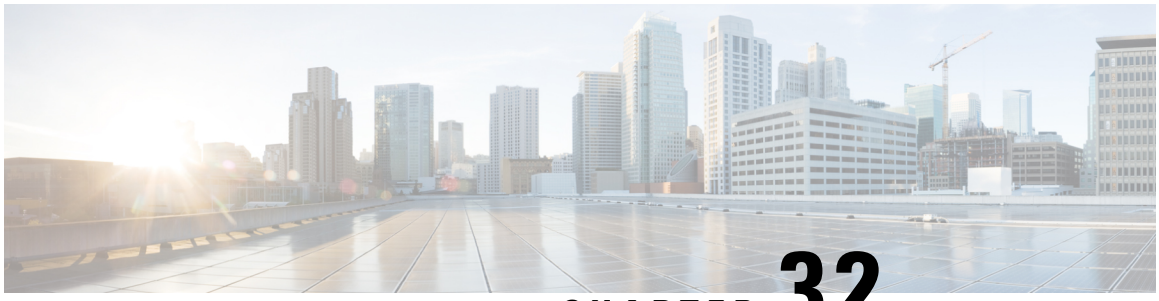
After successful synchronization, verify if the networks are displayed in the **Location Hierarchy**.



Note If IP address restriction is enabled on the Cisco Meraki dashboard, reach out to Cisco Spaces support to add Cisco Spaces IP addresses to the allowed list.

Wireless Network Status

The **Wireless Network Status** option enables you to view the synchronization status of your wireless network. You can view the time at which the last synchronization happened.



CHAPTER 32

Set Up Wired Network

• Set Up Wired Network, on page 323

Set Up Wired Network

The Cisco Spaces**: Connector** enables you to connect your wired and wireless networks with Cisco Spaces.

To set up a wired network, you must have Cisco Catalyst 9300 Series switches and also Cisco Spaces**: Connector** installed on a virtual machine.

Cisco Spaces: Connector 3.0 is now available under the **Menu (** **)** > **Setup** > **Wired Network** section. You can create 3.0 connectors under the **Wired Network**.

Connector 3.0 capabilities such as service association, instance tracking, and metrics visualizations, are available in the **Wired Network** section.

The Wired Network page includes connector and switch management actions, such as **Create Connector**, **View Connectors**, **Add Switches**, and **View Switches**. In the Configure Spaces Connector section, you can create connectors.

- In the **Configure Spaces Connector** section.
- Click **Create Connectors**.
- Click **Create New Connector**.
- In the **Spaces Connector Name** field, enter the spaces connector name.
- Click **Save**.
- Click **View Connectors**.
- In the **Actions** column, click the Test Connectivity, Edit, or Delete icon if needed.
- In the **Add Switch** section.
- Click **Add Switches**.
- Select **Add new switch**.

  Select **Connectors** from the drop-down list.

In the **Switch Name** field, enter the Switch name.

In the **Switch IP** field, enter Switch IP.

In the **Netconfig Username** field, enter the Netconfig Username.

Click **Add Location**, then select the location from the loation hierarchy.

- Select **Choose switches from another connector**.

  Click **Add Location**, then select the location from the loation hierarchy.

  Choose connector from the drop-down list.

- Select **Import switches from spreadsheet**.

  Select **Connector** from the drop-down list.

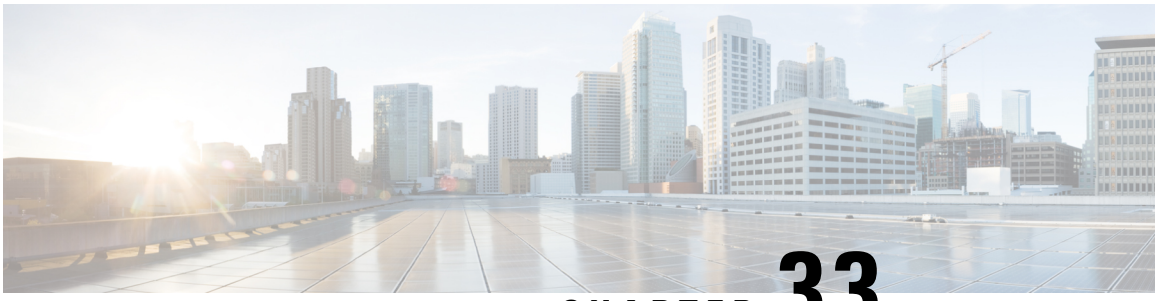
  Follow the on-screen instructions.

  Click **Next**.

- Click **Save**.
- Click **View Switches**.
- In the **Actions** column, click the Test Connectivity, Edit, or Delete icon if required.

For more information about setting up Cisco Spaces**: Connector**, refer to the *Cisco Spaces**: Connector** Configuration Guide* at:

https://www.cisco.com/c/en/us/td/docs/wireless/spaces/connector/config/b_connector_30.html.



CHAPTER 33

Set Up Locations and Maps

- Locations and Maps, on page 325
- Import Locations, on page 331
- Add Network Map, on page 344
- Add Digital Map, on page 346
- Set Default Map View, on page 349
- Catalyst Center Map Export, on page 350

Locations and Maps

The Locations and Maps feature in Cisco Spaces helps to import, normalize and unify network hierarchies from various sources such as Cisco Meraki, Catalyst Center, and Cisco Prime Infrastructure into a single business-orientated hierarchy. Use this feature as a platform to standardize the network hierarchy structure and provide a standardized location hierarchy view.

Apart from the traditional way of creating location hierarchy by importing/syncing from network sources, this new feature includes a new option to create a business centric hierarchy from a Microsoft Excel (.xlsx) file. The Microsoft Excel (.xlsx) file import allows to perform bulk add/update of the metadata information for multiple locations.

While Cisco Spaces creates a logical location hierarchy matching the network hierarchy, most Cisco Spaces users have one more source where the hierarchy/names differ because of the taxonomy, or because they are managed by different teams/people. With the Locations and Maps feature, you can create a business orientated hierarchy, merge/unify hierarchies from different network sources into the business hierarchy making it a clean unified hierarchy thereby helping in managing various outcomes.

You can import your business locations and organize them within Cisco Spaces based on the physical business locations and network deployments. You can also organize the hierarchy based on specific brands, regions, campuses, and other taxonomies relevant for the business.

The Locations and Maps feature in Cisco Spaces helps to translate your IT network view into a business view and present a cleaner business relevant insights report. Any changes to your network topology are automatically reflected in Cisco Spaces making it easy to manage.

The **Locations and Maps** window has these tabs:

- **Locations**: Use this tab to add or manage locations.
- **Network Maps**: Use this tab to add Network Maps.

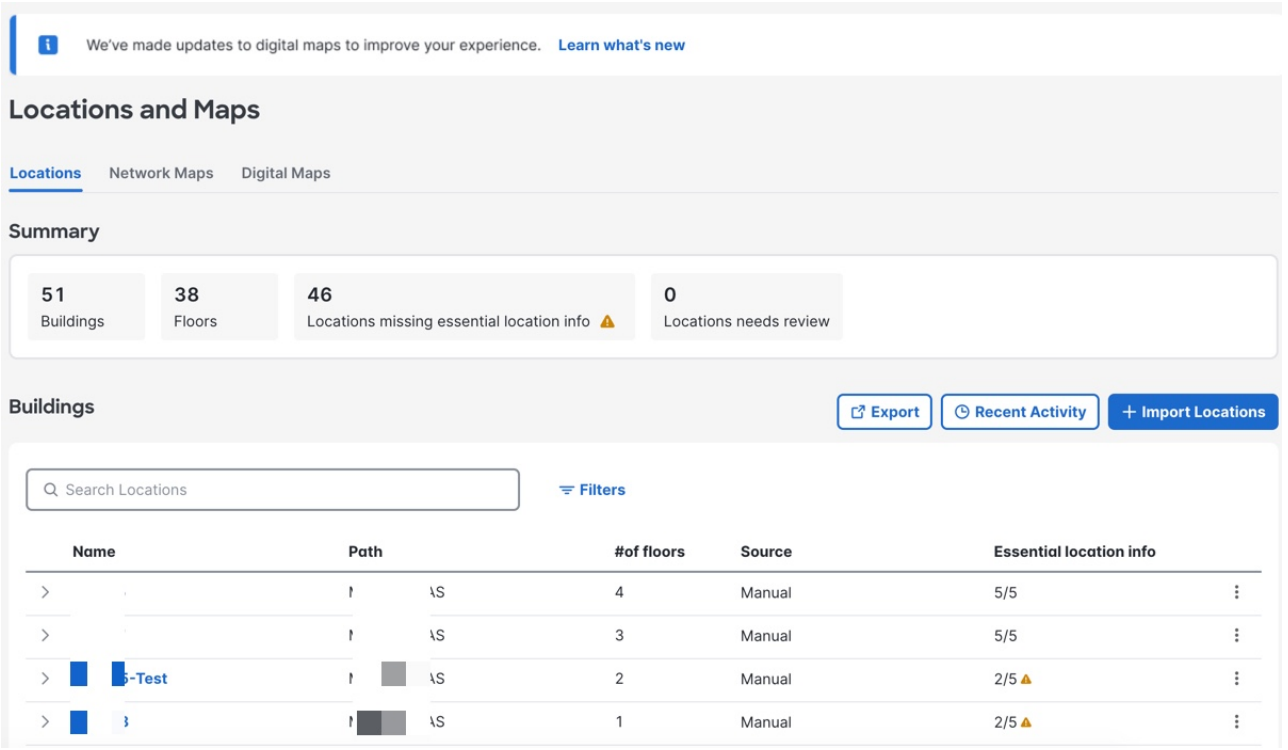
- **Digital Maps**: Use this tab to add or manage Digital Maps.

Use the **Filter** option in these tabs to open the **Filter** drawer, select your filter values, and then apply them to the list.

Each tab under **Setup** > **Locations and Maps** includes a list-level search field and a Filter drawer. You can open the Filter drawer, select one or more filter values, click **Apply**, and remove individual filters by clicking the active filter chips above the table or reset the list by clicking **Clear all**.

You can also narrow the list by selecting a location from the location hierarchy picker within the Filter drawer. This allows you to filter by campus, building, floor, network, or other supported hierarchy levels before applying filters specific to each tab.

Figure 70: Locations and Maps



Map Service

The **Map Service** feature has been merged with **Locations and Maps** and is no longer available as a standalone feature. The **Map Service** option remains under **Legacy items** to help users navigate from the previous workflow.

To access the migrated Map Service functionality:

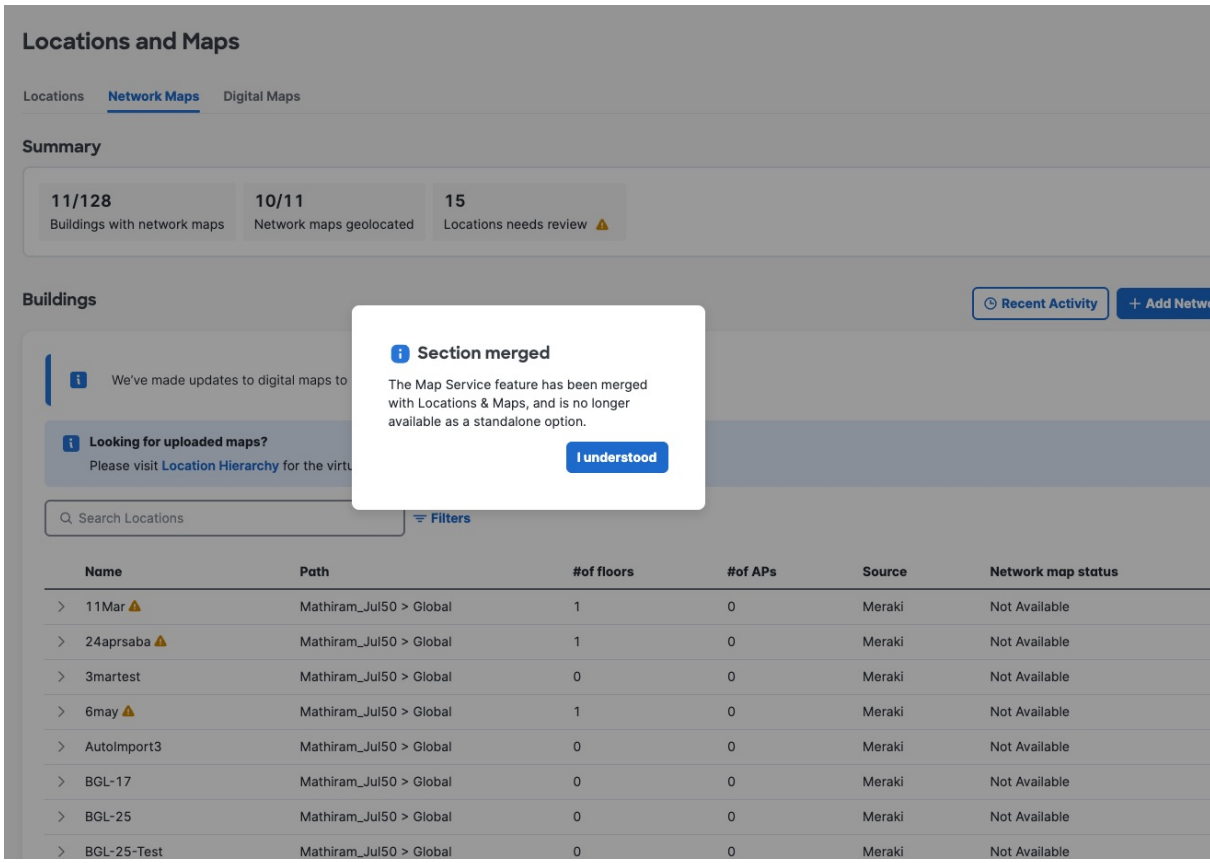
1. In the Cisco Spaces left navigation panel, choose **Setup** > **Legacy items** > **Map Service**.

   A notification indicates that Map Service has moved to **Locations and Maps**

Note The **Network Maps** tab is selected by default.

2. Click **I understood**.

Figure 71:



Note The **Map Service** option under **Legacy items** is a navigation shortcut. All map-management operations are performed in **Locations and Maps**.

Locations Tab

The **Summary** section in the **Locations** tab displays the number of buildings and floors. The **Buildings** section in the **Locations** tab displays the following information related to the imported location:

- Name
- Path
- #of Floors
- Source
- Essential Location Info

Perform these tasks:

- Enter the building name in the **Search Locations** field and filter the specified building information.
- Click **Export** to export the location data. You can click **Download** to download the same.
- Click **Recent Activity** to open the **Recent Activity** window and view the recent activity details.
- Click **Import Locations** to import locations. For detailed information, refer to Import Locations, on page 331.

When no locations are available, the **Locations** tab shows a Day 0 onboarding view with a **Click to Get Started** call to action (CTA). To start importing locations, navigate to **Setup** > **Locations and Maps** > **Locations**, then click either **Click to Get Started** or **Add Locations**.

To filter the Locations list, go to **Setup** > **Locations and Maps** > **Locations** and select **Filter**. In the Filter drawer, you can choose a hierarchy node, one or more Sources, a Number of Floors value or a custom floor range, and Location Metadata status. Click **Apply** to refresh the list.

After applying filters, the active filter options appear above the table. You can remove filters one at a time by clicking the individual filter options or reset the list to show all locations by clicking **Clear all**.

If imported locations require review, a review banner displays the number of pending items. Click **Review** on the banner to open the review workflow, where you can complete actions such as merge, retain, create, skip, or delete as needed.

If essential location information is incomplete, you can update it from the warning message or the row action menu. Navigate to the relevant building in the **Locations** table, click the warning icon or the action menu, and select the metadata update option to complete the missing details.

Network Maps Tab

The **Network Maps** tab also displays the imported location information. The **Buildings** section in the **Network Maps** tab displays the following information related to the imported location:

- Name
- Path
- #of Floors
- #of APs
- Source
- Network Map Status

Perform these tasks:

- Enter the building name in the **Search Locations** field and filter the specified building information.
- Click **Recent Activity** to open the **Recent Activity** window and view the recent activity details.
- Click **Add Network Map** to add network maps. For detailed information, refer to, Add Network Map, on page 344.

In the **Network Maps** tab, you can review two summary indicators before uploading or validating maps: the number of buildings with network maps and the number of network maps that are geolocated. These indicators help you confirm how many locations already have map coverage and how many are positioned geographically.

To filter network map results, navigate to **Setup** > **Locations and Maps** > **Network Maps**, then select **Filter**. In the Filter drawer, choose a hierarchy node, one or more Sources, a Number of APs value or custom AP range, and a Number of Floors value or custom floor range. Click **Apply** to refresh the list.

If a building does not yet have a network map, a warning tooltip appears in the building row. Open the tooltip and use the provided action to start the upload or import flow for that building.

Digital Maps Tab

Digital Maps is an upgraded version of Rich Maps. Two variations of Digital Maps available are:

- **STANDARD** Maps: Shows 2D flat maps without support for meeting rooms or integration with **Cisco Smart Workspaces**.
- **PRO** Maps: Shows 3D visualizations and include all the available features of **Cisco Smart Workspaces**, similar to Rich Maps.

The **Digital Maps** tab also displays the imported location information.

The **Buildings** section in the **Digital Maps** tab displays the following information related to the imported location:

- Name
- Path
- #of Floors
- Digital map status
- Actions



Note In the **Digital Maps** tab, the **Actions** menu adapts to the building's status. These options are available based on the building state.

- **Add digital maps**
- **Add/update floors**
- **Set default map view**
- **Set address**
- **Confirm address**
- **Review**
- **Cancel**
- **View/Edit**
- **Preview**
- **Delete Digital Map**
- **View History**
- **Export to Catalyst Center**

Perform these tasks:

- Enter the building name in the **Search Locations** field and filter the specified building information.
- Click **Recent Activity** to open the **Recent Activity** window and view the recent activity details.
- Click **Add Digital Map** in the **Actions** column to add digital maps. For detailed information, refer to Add Digital Map, on page 346.
- You can also click **Upload CAD File** under **Actions** column to add digital maps to the selected location.

To filter digital map results, navigate to **Setup** > **Locations and Maps** > **Digital Maps**, then select **Filter**. In the Filter drawer, choose a hierarchy node, one or more Processing Status values, and a Number of Floors value or custom floor range. Click **Apply** to refresh the list.

After you apply filters, the selected values appear as filter chips above the table. You can remove a single filter from the chip row or click **Clear all** to reset the filtered list.



Note Locations with ADVANTAGE licenses have exclusive access to the PRO variant, while the STANDARD variant remains accessible to other license types, including ESSENTIAL, EXTEND, and SMART_OPERATIONS.



Note Digital map actions are displayed based on the selected building or floor and the license entitlement assigned to that location. If a digital map action is unavailable, verify that the required license is assigned to the correct building or floor.

Digital Maps: User Experience Enhancements

The following enhancements are made in the Cisco Spaces dashboard:

- The **Select Floor** window is redesigned to minimize user effort. The new design reduces the number of entries required from users, enabling a quicker and more efficient process by automatically generating the floor level number and short name for each floor.
- The file upload process is enhanced to improve efficiency. You can now upload files for multiple floors simultaneously, with each being processed in parallel. The full-page loader that previously displayed during single floor uploads is replaced by individual loader indicators for each floor, allowing clear visibility into the status of each upload.

  If any floor file requires additional time, you have the option to cancel that specific upload without affecting the progress of others. This enables better management of successful uploads and more effective time allocation.
- **Map Processing Status Reporting with Estimated Time and Email Notifications**: Map Processing feature is enhanced to address the issues reported with time-intensive map generation. With this enhancement, after you successfully submit the map, the window is displayed with an estimated processing time. You can also view the processing status, including a tentative ETA or error details, by hovering over the status message for each building in the Digital Maps list view. Additionally, the submitter receives email notifications regarding any changes in the map status.

- **Re-Processing Maps/Re-submission of CAD Files**: The map re-processing experience is enhanced to include a feature that allows you to specify the exact changes needed. This helps to reduce the turnaround time. You can select from a list of common reasons and provide additional comments, along with any supporting documents or images as evidence for the re-processing request.

The current processing status experience enhances user interaction by providing richer hover details. When you hover over the processing status, the interface shows floor-level grouping, the submitted date, the expected review timeline, the draft state, and detailed error information for the affected floors.

If a preview session is interrupted, you can resume your previous work or discard unpublished changes. This feature helps you return to unfinished map preparation without restarting the entire workflow.

When you try to save or publish with unsaved editor changes, the interface displays confirmation dialogs. These dialogs let you choose to save and continue or discard the pending edits based on your selected action.

Network Map Calibration

The **Network Map Calibration** tool enables precise alignment of 2D network map images with 3D **Digital Maps**. You can access the tool from the **Digital Map Editor**, allowing you to precisely place GPS markers ensuring client and access point positions are accurately represented.

The Network Map Calibration link is enabled in the user interface only for maps that have associated network maps.

Use **Network Map Calibration** after you have a digital map preview and a related network map for the same building. Open the Digital Maps editor for that building, launch the calibration tool, and align the network map markers so that device and AP positions match the final map view more accurately. This process helps ensure better accuracy between the network map and the digital map.

STANDARD Maps (BETA)

STANDARD Maps (BETA): The beta version of STANDARD Digital Maps (with a beta watermark) has been introduced in Cisco Spaces. The STANDARD maps are generated more quickly compared to the PRO version but with fewer features, thus supporting a limited range of use cases.

You might notice that the orientation and positioning of STANDARD maps may not always align perfectly with the actual building position on the earth map. We recommend that you adjust the position and orientation of STANDARD maps using the tools available in the **Standard Map** preview.



Note

- The PRO maps are exclusively available to locations with ADVANTAGE or UNLIMITED licenses, while STANDARD maps are accessible for locations with ESSENTIAL or Extend licenses.
- You can use the STANDARD version of the map for device placement. For locations with ADVANTAGE or UNLIMITED licenses, use the STANDARD map until the PRO version is fully generated.

Import Locations

Use the **Locations** tab to import the business hierarchy.

After you successfully import locations, you can immediately review the imported hierarchy and update any incomplete metadata. Then, use the **Filters** option in the **Locations** tab to validate the imported data by source,

floor count, or metadata completeness before proceeding to Digital Maps. This process helps ensure your data is accurate and complete before moving forward.

Procedure

Step 1 Log in to Cisco Spaces.

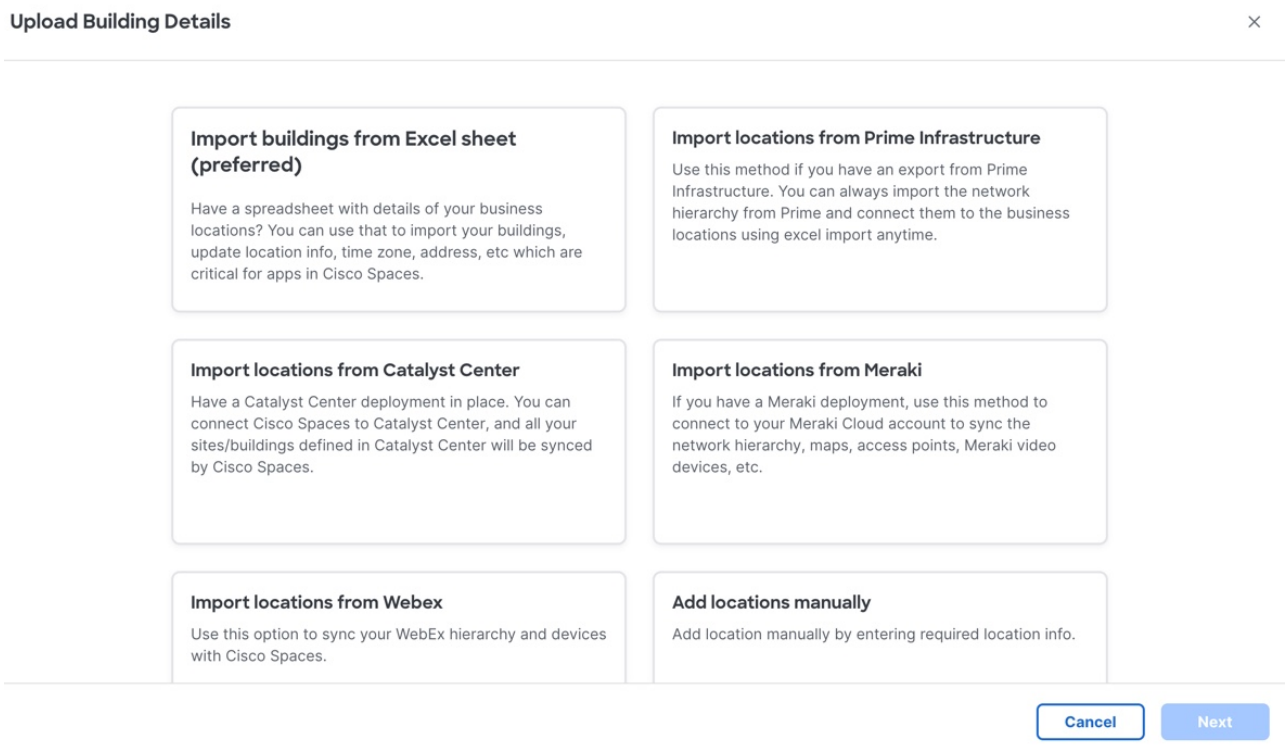
Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed with the **Locations** tab selected. The other tabs available are **Network Maps** and **Digital Maps**.

Step 3 In the **Locations** tab, click **Add Locations**. If locations are already imported and available, then **Import Locations** option is displayed.

The **Upload Building Details** window is displayed with the various methods to upload the locations.

Figure 72: Upload Building Details



Step 4 Import the locations using the following methods:

- Import buildings from Excel sheet (preferred)
- Import locations from Cisco Prime Infrastructure
- Import locations from Catalyst Center
- Import locations from Cisco Meraki

- Import locations from Cisco Webex
- Add locations manually

The imported location details are displayed in the **Locations** tab.

- The **Summary** section displays the details of the buildings, floors, missing location metadata information and locations that need review.
- The **Building** section in the **Locations** tab displays the location details such as name, path, number of floors, source and so on.
- In the **Building** section, the **Essential Location Info** field displays an alert if the required location metadata is not updated.

Step 5 In the **Essential Location Info** field, click **Alert** icon ( ) to add the missing metadata if required.

A pop-up window is displayed with the information related to missing location metadata. Click **Click Here** to update the location info.

Step 6 Click **Review** to view and proceed with location reviews. For more information, see Review Locations.

The **Review** option is displayed when you import locations using methods other than **Import buildings from Excel sheet** method.

Step 7 (Optional) In the **Locations** tab, use the following options as required:

- **Export**: Click to export the imported business location details into a Microsoft Excel file (.xls). You can click **Download** to download the same.
- **Recent Activity**: Click to view the recent activity details. The **Recent Activity** slide in window displays the history of activities happened in the recent past.
  - File Name
  - User
  - Type
  - Time
  - Status
- **Filter**: Click to view the filter options. In the **Filter** slide-in window that is displayed, choose the location from the **Locations** drop-down list and the required filter options and click **Apply**. The filter options are: **Source**, **# of Floors** and **Location Metadata**.

Import Buildings from Microsoft Excel Sheet

Use the **Import buildings from Excel sheet** option to add locations by importing a Microsoft Excel (.xlsx) file. We recommend that you choose this method to import the locations with buildings, location metadata, time zone, address, and so on that are important for Cisco Spaces application.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed with the **Locations** tab selected.

Step 3 In the **Locations** tab, click **Add Locations**. If locations are already imported and available, then **Import Locations** option is displayed.

The **Upload Building Details** window is displayed with various methods to upload the locations.

Step 4 Click **Import buildings from Excel sheet** and click **Next**.

Step 5 In the **Import Location Details** window, drag and drop the Microsoft Excel (.xlsx) file or click **Click here to upload** to upload the Microsoft Excel (.xlsx) file with details of the business locations to be imported.

Note If you do not have the template, you can download the template from the link available in the **Import Location Details** window and upload the same with the building details in the correct format.

Step 6 Click **Next**.

The **Import Location Details** window is displayed with location information from the Microsoft Excel (.xlsx) file in the left column and existing location level and group level information in the right column.

Step 7 In the **Import Location Details** window, map the imported location metadata in the **Column from CSV** column with the corresponding hierarchy and group levels under the **Link to** drop-down and assign respective location metadata values accordingly.

The options available in the **Link to** drop-down are:

- **Location Info**: Use this for location metadata information such as Country, City, Occupancy, Band, Address, Time Zone and so on. You must assign a corresponding metadata value also.
- **Hierarchy Level**: Use this to map the **Level** column value from the Microsoft Excel (.xlsx) file. The Microsoft Excel (.xlsx) file can have multiple **Level** values. Level values from the Microsoft Excel (.xlsx) file are mapped as **Hierarchy Level** in the Location Hierarchy.

  For each **Hierarchy Level**, you can assign a grouping level value. The options are: **Grouping Level1**, **Grouping Level2** and **Grouping Level3**.

  In the Microsoft Excel (.xlsx) file, you can have `NYC1 Campus` as **Level1** and `NYC2 Campus` as **Level2**. In the **Import Location Details** window, you can map **Level1** and **Level2** with **Hierarchy Level** in the **Link to** drop-down list. For **Level1**, you can assign the grouping value as **Grouping Level1** and **Grouping Level2** for **Level2**.
- **Location Name**: Use this to map with the **Location** column value from the Microsoft Excel (.xlsx) file.

Note You need not assign any value for **Location Name**. The location name is directly fetched from the Excel file and cannot be modified or mapped with any header columns.

- **Location ID**: The Location ID is auto-generated after the location import is successfully complete.

Step 8 Click **Next**.

The **Merge Locations** window is displayed.

- A message indicating that the Location Hierarchy in Cisco Spaces is updated to include new locations discovered by importing the Microsoft Excel (.xlsx) file.
- The **Merge Locations** window displays the number of new locations and their levels imported using **Import buildings from Excel sheet** method.
- The **Merge Locations** window displays three columns: **Locations found in CSV**, **Actions** and **Existing Locations**.
- You must review the hierarchy and take necessary action using the **Action** drop-down list.
- You can use the **Search Location** field to enter search criteria and search for location name.

Step 9 In the **Locations found in CSV**, click the plus symbol to expand the location.

Step 10 From the **Actions** drop-down list, select the required action to merge the imported location with the existing Location Hierarchy displayed on the right side.

The options are:

- **Create New**: Select this option if you want to create the imported location as a new location into the existing Location Hierarchy.
- **Merge With**: Select this option if the imported locations from the Microsoft Excel (.xlsx) file are repeating and the location already exists in the Location Hierarchy. We recommend that you perform this action with attention as you cannot revert once you merge the locations.
- **Skip**: Select this option if you want to skip importing the locations into the Location Hierarchy. We recommend that you perform this action with attention as you cannot revert once you skip the locations.

Note In the existing Location Hierarchy:

- If there are no existing campuses or buildings, the new imported locations are added as new entries.
- If there are locations with similar name, you can merge the new locations with the existing ones.

Step 11 Click **Next**.

You need to review the merge location updates displayed in the **Merge Locations** section. You can view the number of locations that are processed.

Step 12 Click **Submit**.

A success message is displayed indicating that the location details are uploaded.

You can click **Add Digital Maps** if you want to add digital maps or **View Locations** to view the locations.

Step 13 Click **Close this window** to return back to **Locations** tab.
The **Building** section in the **Locations** tab displays the location details such as name, path, number of floors, source and so on. The **Summary** section displays the details of the buildings, floors, missing location metadata information and locations that need review.

Import Locations from Cisco Prime Infrastructure

Use the **Import locations from Prime Infrastructure** option to add locations using an export file from Cisco Prime Infrastructure into Cisco Spaces. You can import the network hierarchy from Cisco Prime Infrastructure and connect them to the business locations.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed with the **Locations** tab selected.

Step 3 In the **Locations** tab, click **Add Locations**. If imported locations are already available, then **Import Locations** option is displayed.

The **Upload Building Details** window is displayed with the various methods to upload the locations.

Step 4 Click **Import locations from Prime Infrastructure** and click **Next**.

The **Import Location Details** window is displayed.

Step 5 In the **Import Location Details** window, drag and drop the Cisco Prime Infrastructure map file as a .GZ file (compressed archive file) or click **Click here to upload** to upload the .GZ file with the Cisco Prime Infrastructure map information.

Step 6 Click **Next**.

The **Import Location Details** displays a message indicating that the map data is processing. The Map Service takes some time to process the same. You can verify the map data processing status in the **Recent Activity** section.

After the map data is processed successfully, you must merge the map data with the locations.

Step 7 Click **Close this window** to close the window.

The **Building** section in the **Locations** tab displays the newly imported location details. The same location information is also displayed in the Cisco Spaces Location Hierarchy.

An alert message indicating that the import of maps from Cisco Prime Infrastructure added new locations to the Location Hierarchy is displayed in the **Location** tab.

Step 8 Click **Review** to review and take appropriate action.

The **Merge Locations** window is displayed.

- A message indicating that the Location Hierarchy in Cisco Spaces is updated to include new locations discovered by importing Cisco Prime Infrastructure maps.

- The **Merge Locations** window displays the number of new sites and building imported using **Import locations from Prime Infrastructure** method.
- The **Merge Locations** window displays three columns: **Locations from Prime Map**, **Actions** and **Existing Locations**.
- You must review the hierarchy and take necessary action using the **Action** drop-down list.
- You can use the **Search Location** field to enter search criteria and search for location name.

Step 9 In the **Locations from Prime Map**, click the plus symbol to expand the location.

The location hierarchy includes campus, buildings, and floors.

Step 10 From the **Actions** drop-down list, select the required action to merge the imported location with the existing Location Hierarchy displayed on the right side.

The options are:

- **Merge With**: Select this option if the imported locations from Cisco Prime Infrastructure are repeating and the location already exists in the Location Hierarchy. We recommend that you perform this action with attention as you cannot revert once you merge the locations.
- **Delete**: Select this option if you want to remove the imported locations from the existing Location Hierarchy. We recommend that you perform this action with attention as you cannot revert once you delete the locations.
- **Create New**: Select this option if you want to create or add a new location into the existing Location Hierarchy.
- **Accept**: Select this option if the locations imported from Cisco Prime Infrastructure are accepted as it is with the existing Location Hierarchy.

Note In the existing Location Hierarchy:

- If there are no existing campuses or buildings, the new imported locations are added as new entries.
- If there are locations with similar name, you can merge the new locations with the existing ones.

Step 11 Click **Next**.

You need to review the merge location updates displayed in the **Locations** section. You can view the number of locations that are processed.

Step 12 Click **Submit**.

A success message is displayed indicating that the location details are uploaded.

You can click **Add Digital Maps** if you want to add digital maps or **View Locations** to view the locations.

Step 13 Click **Close this window**.

The **Building** section in the **Locations** tab displays the location details such as name, path, number of floors, source and so on.

The **Summary** section displays the details of the buildings, floors, missing location metadata information and locations that need review.

Import locations from Cisco Catalyst Center

Use the **Import locations from DNA Center** option to add locations from Catalyst Center. You can connect Cisco Spaces to Catalyst Center and all the sites or buildings defined in Catalyst Centeris synchronized with Cisco Spaces.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed with the **Locations** tab selected.

Step 3 In the **Locations** tab, click **Add Locations**. If locations are already imported and available, then **Import Locations** option is displayed.

The **Upload Building Details** window is displayed with various methods to upload the locations.

Step 4 Click **Import locations from DNA Center** and click **Next**.

To import locations from Catalyst Center, you must integrate Catalyst Center maps with Cisco Spaces.

Step 5 (Optional) Click **View How to Integrate DNA Center Maps**.

The **Cisco DNA Center Integration** window is displayed.

Cisco Spaces integrates with Catalyst Center for map synchronization and to provide device location updates to Catalyst Center. To integrate Cisco Spaces with Catalyst Center, click **Create Token** to create a token and configure the token in Catalyst Center.

Note Cisco Spaces integration feature in Catalyst Center is available for limited users. For additional support, contact Cisco Spaces support team.

Step 6 Click **Next**.

The **Import Location Details** window is displayed.

Step 7 Follow the instructions to connect the Catalyst Center.

Step 8 Click **Finish**.

The **Building** section in the **Locations** tab displays the location details. The **Summary** section displays the details of the buildings, floors, missing location metadata information, and locations that need review.

Import locations from Cisco Meraki

Use the **Import locations from Meraki** option to add locations from Cisco Meraki. If you have a Cisco Meraki deployment, use this method to connect to your Cisco Meraki Cloud account to synchronize the network hierarchy, maps, Access Points, and Meraki video devices.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed with the **Locations** tab selected.

Step 3 In the **Locations** tab, click **Add Locations**. If locations are already imported and available, then **Import Locations** option is displayed.

The **Upload Building Details** window is displayed with various methods to upload the locations.

Step 4 Click **Import locations from Meraki** and click **Next**.

The **Import Location Details** window is displayed.

To import locations from Cisco Meraki, you must connect your Cisco Meraki with Cisco Spaces.

Step 5 (Optional) Click **View How to Integrate Meraki** to view the instructions.

Step 6 In the **Import Location Details** window, click **Next**.

Step 7 Read the instructions to connect Cisco Meraki and click **Next**.

The **Connect your wireless network** window is displayed. You can connect use this option to connect to Cisco Meraki.

Step 8 If you are already connected, proceed with adding locations using the Location Hierarchy.

Import Locations from Cisco Webex

Use the **Import locations from Webex** option to synchronize the Cisco Webex hierarchy and devices with Cisco Spaces.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed with the **Locations** tab selected.

Step 3 In the **Locations** tab, click **Add Locations**. If imported locations are already available, then **Import Locations** option is displayed.

The **Upload Building Details** window is displayed with various methods to upload the locations.

Step 4 Click **Import locations from Webex** and click **Next**.

The **Import Location Details** window is displayed.

To import locations from Cisco Webex, you must onboard Cisco Webex. After a successful onboard, your locations are automatically displayed in **Setup** > **Locations and Maps**.

Step 5 Follow the instructions to activate **Cisco Smart Workspaces**.

Step 6 In the **Activation token** field, enter the token generated from **Cisco Smart Workspaces**.

Step 7 Click **Activate**.

Add Locations Manually

Use the **Add locations manually** option to add a standalone building directly under the root location without importing a Microsoft Excel (.xlsx) file or a network map.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

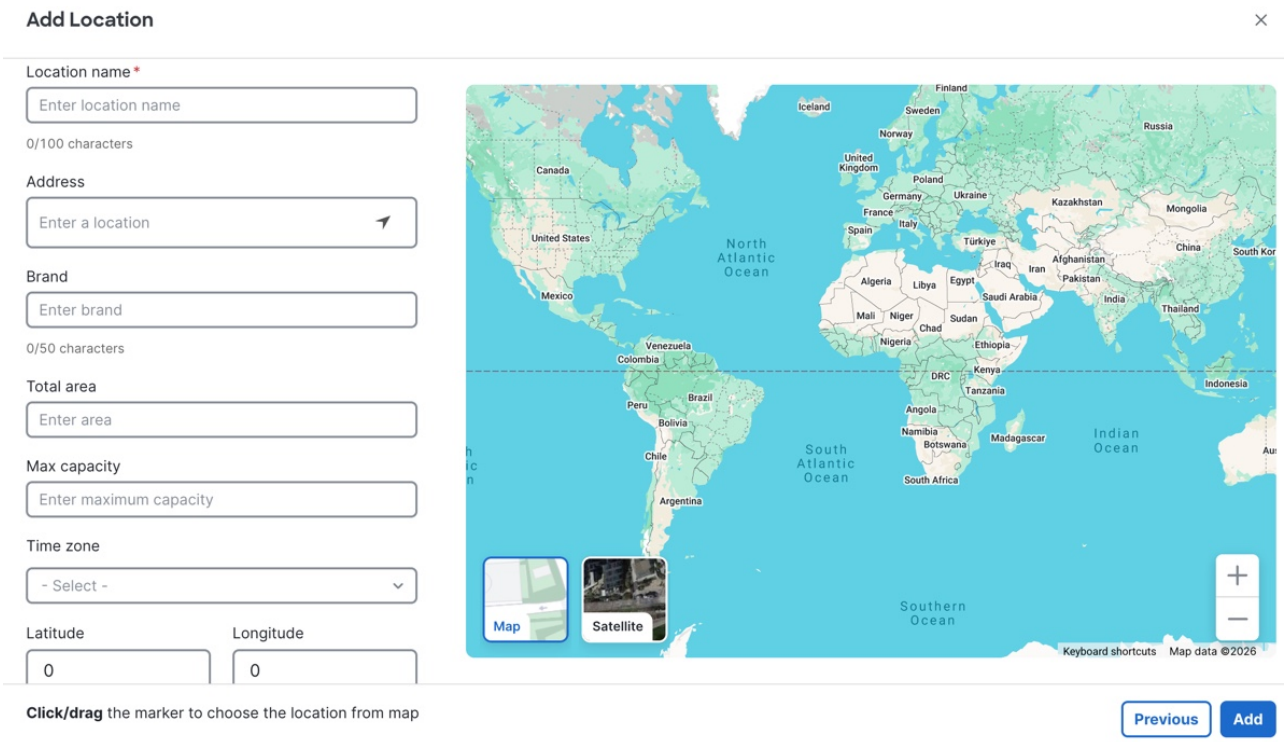
The **Locations and Maps** window is displayed with the **Locations** tab selected.

Step 3 In the **Locations** tab, click **Add Locations**. If locations are already imported and available, then **Import Locations** option is displayed.

The **Upload Building Details** window is displayed with the various methods to upload the locations.

Step 4 Click **Add locations manually** and click **Next**.

Figure 73: Add Location



Step 5 In the **Add Location** window, enter the following location details to add a new location:

- **Location Name**: Name for the new location.
- **Brand**: Brand for the new location.
- **Total Area**: Total area details for the new location.
- **Max Capacity**: Maximum capacity information for the new location.
- **Address**: The address of the new location. You can manually enter the address or drag the marker to choose the address from map displayed on the right side.
- **Time Zone**: Select the time zone from the drop-down list.
- **Latitude**: Latitude of the new location.
- **Longitude**: Longitude of the new location.

Step 6 Click **Add**.

A success message is displayed indicating that a new location is added. You can click **Add Another Location** if you want to add more locations manually.

Step 7 Click **Done**.

The **Building** section in the **Locations** tab displays the location details. The Summary section displays the details of the buildings, floors, missing location metadata information and locations that need review.

Update Location Information

The **Locations** tab displays an alert message if location metadata is missing for the imported location.

You can update location information as part of map preparation. You refine the building address, verify geo-coordinates, and save corrected metadata before proceeding to floor selection or map upload workflows.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed with the **Locations** tab selected.

Step 3 In the **Buildings** section, next to Essential Location Info field, click the Alert icon to update the missing location metadata.

The **Update Location Info** window is displayed.

Step 4 In the **Update Location Info** window, update the following location details as required:

- **Location Name**: Name for the new location.
- **Brand**: Brand for the new location.
- **Total Area**: Total area details for the new location.
- **Max Capacity**: Maximum capacity information for the new location.
- **Address**: The address of the new location. You can manually enter the address or drag the marker to choose the address from map displayed on the right side.
- **Time Zone**: Select the time zone from the drop-down list.
- **Latitude**: Latitude of the new location.
- **Longitude**: Longitude of the new location.

Step 5 Click **Update**.

Review Locations

In the **Locations and Maps** window, an alert message is displayed if the imported location hierarchies need review. You need to review the locations and need necessary actions.

During review, the system validates unsupported merge combinations and displays actionable error messages. The interface prevents unsupported merges such as Webex-to-Webex, Meraki-to-Meraki, certain same-source hierarchy merges, and floor merges that do not correspond to the correct building context.

If you must merge a floor, first complete the review and merge steps for the parent building. Then return to the floor-level review items. This process keeps the final hierarchy consistent and prevents invalid merges between floors or between floors and different buildings.

Procedure

Step 1 In the **Locations and Maps** window, click **Preview** to view and proceed with location reviews.

The **Review Locations** window displays all sources from which locations are imported, for example, Cisco Meraki or Catalyst Center. You can also view the number of sites, buildings and campuses imported for each location.

Step 2 Select the source location to review and click **Next**.

The **Review Locations** window displays the imported location hierarchy levels for the selected source in the left column and existing destination location hierarchy levels in the right column. Use the **Search Locations** field to search for specific locations.

Step 3 Use the options available in the **Action** drop-down list and select a recommended action to merge each level in the source location hierarchy with a relevant destination business hierarchy level in the right column.

By default, Cisco Spaces recommends some actions for reviewing the imported location hierarchy. The available actions are: Merge with, Accept, Create New and Delete.

- The action that you opt for the highest node in the source location hierarchy is automatically cascaded over to the subsequent nodes.
- You cannot delete a campus node from the source location hierarchy if the levels under the campus node are already merged with any relevant destination business hierarchy level.
- You cannot merge a building from the source location hierarchy to a campus in the destination business hierarchy.
- You can merge a site from the source location hierarchy to a campus in the destination business hierarchy.
- If the name of the source location hierarchy matches with any business hierarchy available in Cisco Spaces Location Hierarchy, then Cisco Spaces automatically displays the matching destination levels, and you proceed with the merge action.
- If the source location hierarchy is new, then select **Create** action to automatically create a new business hierarchy in Cisco Spaces Location Hierarchy.

Step 4 From the **Existing Locations** drop-down list, select the relevant destination level to merge and unify the imported location hierarchies from any source location with the business hierarchy available in Cisco Spaces Location Hierarchy.

The **Existing Locations** drop-down list displays all the destination nodes available in the Cisco Spaces Location Hierarchy. You can view the source from where the business hierarchy is imported in the drop-down list.

Step 5 Click **Next**.

The **Merge Locations** window displays the summary of the actions and its implications with respect to the associated analytics data. We recommend that you review this alert information before proceeding.

Note If a location that you selected to be deleted includes rules associated with it, you cannot proceed with the delete action. You need to review the action and update your merge preferences accordingly.

If a location that you selected to be deleted includes reports associated with it, you can proceed with the delete action. The reports are generated again after the locations are merged.

Step 6 Click **Agree and Continue**.

The selected review actions are processed, and the location is marked as reviewed. If you select to merge the source location level with a relevant destination node, all the properties of the source location levels are applied to the destination node in the business hierarchy.

Add Network Map

Use the **Network Maps** tab to add a network map and view the locations with the network maps associated with it. You can import locations only if the source has network maps associated with it. Currently, Cisco Prime Infrastructure, Catalyst Center, Cisco Meraki and Cisco Connected Mobile Experiences includes network maps.

In addition to the basic add-network-map workflow, the current page supports filter-based validation of imported network map coverage. Use the Filter drawer to narrow the list by hierarchy, source, number of APs, and number of floors before taking action on a building.

If a location does not yet have a network map, use the row-level warning tooltip to open the upload or import path for that building.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed.

Step 3 Click **Network Maps** tab.

Step 4 Click **Add Network Map**.

The **Upload Building Details** window is displayed.

Step 5 Import the locations using the following methods that include network maps:

- Import locations from Cisco Prime Infrastructure
- Import locations from Catalyst Center
- Import locations from Cisco Meraki
- Import locations from Cisco CMX

- Add locations manually

The imported location details are displayed in the **Locations and Maps** window under the **Network Maps** tab.

Step 6 Click **Preview** to view and proceed with location reviews. For more information, see Review Locations.

Step 7 (Optional) In the **Network Maps** tab, use the following options as required:

- **Export**: Click to export the imported business location details into a Microsoft Excel file (.xls). You can click **Download** to download the same.
- **Recent Activity**: Click to view the recent activity details. The **Recent Activity** slide-in window displays the following information:
  - File Name
  - User
  - Type
  - Time
  - Status
- **Filter**: Click to view the filter options. In the **Filter** slide-in window that is displayed, choose the location from the **Locations** drop-down list and the required filter options and click **Select** to apply.

Import locations from Cisco CMX

Use the **Import locations from CMX** option to import locations from Cisco CMX. You must tether Cisco CMX with Cisco Spaces to import locations.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed.

Step 3 Click **Network Maps** tab.

Step 4 Click **Add Network Map**.

The **Upload Building Details** window is displayed with various methods to upload the locations.

Step 5 Click **Import locations from CMX** and click **Next**.

The **Import Location Details** window is displayed.

Step 6 (Optional) Click **Learn how to tether CMX** to view the instructions to tether Cisco CMX with Cisco Spaces. For more information, see Cisco CMX Tethering.

Step 7 In the **Import Location Details** window, click **Next**.

Step 8 Read the instructions to connect Cisco CMX and click **Next**.

The **Connect your wireless network** window is displayed. Use this option to connect to Cisco CMX.

Step 9 If you are already connected, proceed with adding locations using the Location Hierarchy.

Add Digital Map

Use the **Digital Maps** tab to add digital maps for buildings in your location hierarchy. You need to upload the Computer-aided design (CAD) file(s) for the floor to convert them into a three-dimensional floor plan.

The **Summary** area displays the number of buildings for which digital maps are imported, number of buildings for which map review is pending and number of buildings with errors.

The **Buildings** area displays the locations available.

Working with your building floor plans is more efficient than ever with the redesigned Digital Maps management. The new listing screen provides a floor-level view with contextual actions based on each floor's status—from setting the building address to adding floors, uploading CAD files, and reviewing, editing, or publishing maps.

Granular per-floor statuses replace the earlier building-level view, and each floor can be reviewed and published independently on its own schedule.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed.

Step 3 Click **Digital Maps** tab.

Step 4 Select the building or floor you want to add digital maps.

Step 5 In the **Actions** column, click **Add digital maps**.

The **Add Digital Map: Support DNA** window is displayed.

a) Read through the CAD file (.dwg) or Vector PDF related information displayed.
b) Click **Proceed**.

Step 6 To confirm the address, complete these steps and click **Confirm Address**.

a) To select the location, either enter the building name in the **Search** field or click directly on the map to place a marker.
b) Alternatively, click and drag the marker to adjust the location on the map as needed.

Verify that the building location on the map is correct.



Note If you want to choose the location from the map displayed on the right panel, you need to provide permission to Cisco Spaces to use the current location to populate the geo-coordinates.



Note If you have not added address details when adding digital maps, click **Set address** in the **Actions** section.

Step 7 (Optional) To add a new floor, click **Add/update floors**.

Step 8 Click **Add new floor** and enter these details:

a) In the**Floor Name**: Enter the name of the new floor.
b) In the **Level Number**: Select the level number of the new floor.
c) In the **Short Name**: Enter the short name of the new floor.

Step 9 Click **Save**.

Step 10 Click the building drop-down list to view the floors.

Step 11 To add **Add digital maps** for the floors:

a) Click **Add digital maps**.
b) Click **Proceed**.

Step 12 Upload source files to use for Digital Maps generation. You can drag and drop files to the designated upload section or click **Choose file** to browse locally and upload them.

- The upload wizard is simplified to a single step — update floor metadata and upload CAD files for multiple floors in one shot. Level numbers can now be edited during upload. AI-generated previews are typically available within 15 minutes, so you can catch issues early — and cancel processing if needed.
- A warning message is displayed if the file is already exists.
- (Optional) Choose the reason from **Reason for force submission** drop-down list.
- Use the **Supplementary information for processing the CAD file** section to enter upload information.

We recommend that CAD file must contains all layers, such as architecture, furniture, names, and IDs for all the elements to convert. Only the elements with names or IDs can support sensor assignments.

Note

- Upload only one CAD file per floor. Cross references (XREFs) are not supported.
- The supported file types are ZIP, AutoCAD Drawing file (DWG), AutoCAD Drawing Interchange File (DXF), Portable Document Format (PDF).
- You can upload one file per floor or use **Bulk Upload** to upload multiple source files together. The page displays per-floor upload progress and lets you cancel or replace an upload if needed.

  If you perform a bulk upload after individual floor files are already staged, a confirmation pop-up appears. Confirm the bulk action to replace the existing staged files for that workflow.

  When you upload a file identical to a previously processed one, the interface requires you to provide a re-processing reason and additional comments. Select a reason, enter comments explaining the correction, and optionally upload supporting evidence such as reference files or explanatory documents. You can upload supporting files from the floor card when more context is needed for re-processing.

  For buildings in review or draft state, you can use **View/Edit** or **Review** from the window to reopen the editor. When a building has an in-progress PRO map workflow, the contextual menu also shows **Preview** option, allowing you to inspect the current generated state.

Note

- After uploading and confirming files, the workflow presents contextual actions based on the building state and license type. These actions include **Save**, **Submit**, **Publish this Building**, **Skip this Building**, **Back to Preview**, **Resume**, **Discard changes**, **Cancel processing**, and others.
- Users can add, edit, or remove floor details at the building level.

Step 13 Click **Submit**.

A success message appears, along with a **Note**.

Step 14 Click **Done**.

The CAD file(s) and the location metadata are processed, Then, the map is digitized. The **processing** status appears in the **Digital Map processing status** section.

(Optional) After some time, the message **AI preview available** appears in the **Digital Map processing status** section.

(Optional) Click **View**.

Step 15 Click **Review** if the map is processed and ready to review.

Step 16 In the **Review Digital Maps** window, select the building you want to review and click **Next**.

The digitized map is displayed.

Step 17 (Optional) Select a floor or space and click to update them if required.

A pop-up window is displayed, and you can edit the name or update the type category.

Step 18 Click **Publish this Building**.

The digitized map is published and available for other applications to use them, for example, Cisco Smart Workspaces, Environmental Metrics app and so on.

In Cisco Spaces Location Hierarchy, for a selected location, digital maps are displayed by default if the location has digital maps.

Click **Skip this building** if you want to discard the changes.

Additionally, use the **View History** option to inspect building-level map workflow events and **Delete Digital Map** option to remove an existing digital map when you have the appropriate permissions and state conditions are met.

Set Default Map View

Use the Set default map view option to configure the initial map orientation and perspective for a digital map. The default map view determines how the map is displayed when users open the digital map for the selected floor.

Before you begin

Ensure that the digital map is created and available for the building.

Procedure

Step 1 Log in to **Cisco Spaces**.

Step 2 In the **Cisco Spaces** dashboard, click the Menu icon and choose **Setup > Locations and Maps**.
The **Locations and Maps** window is displayed.

Step 3 Click the **Digital Maps** tab.

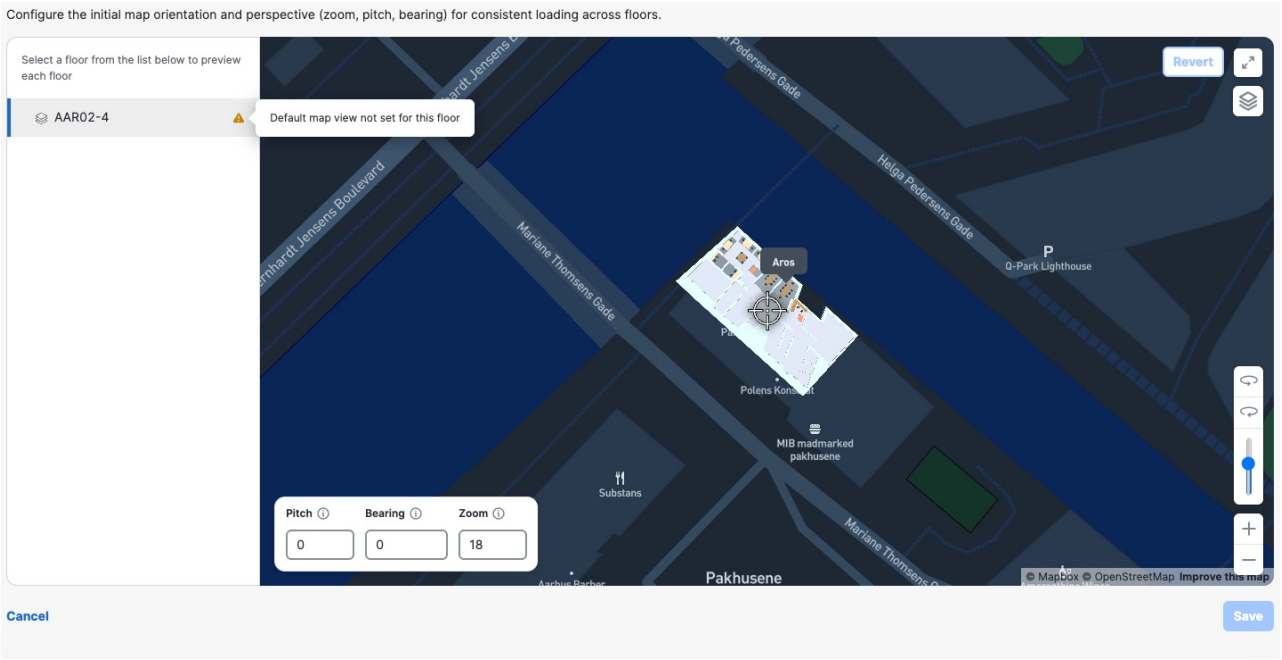
Step 4 In the Buildings area, locate the building for which you want to configure the default map view.

Step 5 In the **Actions** column, click the More Options icon (...) for the required building, and choose **Set default map view**.
The **Set Default Map View** window is displayed.

Step 6 Adjust the map view as required, and configure the following values:

a) **Pitch**: Specifies the tilt angle of the map view.
b) **Bearing**: Specifies the rotation angle of the map view.
c) **Zoom**: Specifies the zoom level of the map view.

Figure 74: Set default map view



Note A warning icon is displayed next to the floor when the default map view is not configured for that floor.

Step 7 Click **Save**.

Catalyst Center Map Export

In **Locations & Maps**, the **Digital Maps** feature (**Setup** > **Locations & Maps** > **Digital Maps**) lets you export building maps (published version) to Cisco Catalyst Center.

The option to export is available only for buildings with a published map.

The map export feature works only if the APs are placed under the **Setup** > **Device Placement** option.

Export Building Maps to Catalyst Center

Before you begin

The **Export** option is not available in these scenarios:

- When using an older version of the Cisco Spaces dashboard UI. We recommend that you switch to the beta version of the dashboard to access this feature.

  For locations where Access Points (APs), configured via the **Device Placement** feature, are not placed using PRO maps.

The Rich Map must not be in any of these statuses:

- Processing
- Error
- Cancelled
- Review
- Deleted

To support network planning and monitoring, you can export the published version of a building's digital map from Cisco Spaces to Catalyst Center.

Use the **Export to Catalyst Center** feature in Cisco Spaces to seamlessly transfer building maps to Catalyst Center.

Use the **Export to Catalyst Center** to export building maps (published version) to Catalyst Center.

You start the export from the building row action menu after the building map is in a supported published state.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed with the **Locations** tab selected.

Step 3 Click the three dots next to a building and select **Export to Catalyst Center** to process the map.

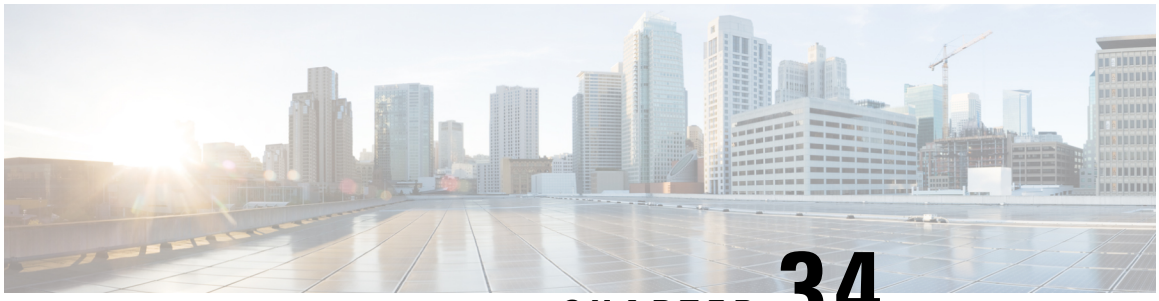
When the export starts, the UI shows a processing state while it prepares the ZIP package. After the export completes successfully, the **Download** option is displayed.



Note If the export cannot complete for the selected building, an error message is displayed indicating that the building is not currently supported for this export action.

Step 4 Click **Download** to save the processed digital map (in ZIP format) for the selected building.

Step 5 Follow the instructions in the pop-up window to import the map hierarchy into Catalyst Center.



CHAPTER 34

Set Up Meraki Camera

This chapter provides information about the configurations required in Cisco Spaces for Meraki Camera.

- Prerequisites, on page 353
- Set up Cisco Spaces to Work with Cisco Meraki Camera, on page 355
- Configure a Meraki Camera, on page 355
- Edit the Trip Wire for a Camera, on page 358
- Manage Camera Configuration, on page 359

Prerequisites

To set up your Meraki Camera, you must connect Meraki Video Cameras to Cisco Spaces so Cisco Spaces can receive Meraki video analytics data.

You can use the Cisco Meraki configuration to support visitor count and camera-driven analytics use cases within Cisco Spaces applications.

When the camera widget is not already available, you must first enable the camera experience from the **Setup** > **Camera** before continuing with the Cisco Meraki connection flow.

For new Meraki camera onboarding, use Meraki API Key or Meraki Integration. Use Meraki Login only if the account is already connected to Cisco Spaces through Meraki Login.

Before You Begin

Make sure you have:

- Access to Cisco Spaces
- A valid Meraki API key
- Meraki cameras with MV Sense licenses
- Permission to connect or manage Meraki synchronization
- Camera networks already configured in Meraki Dashboard

Before starting the camera configuration workflow, make sure the Cisco Meraki camera environment is ready for integration.

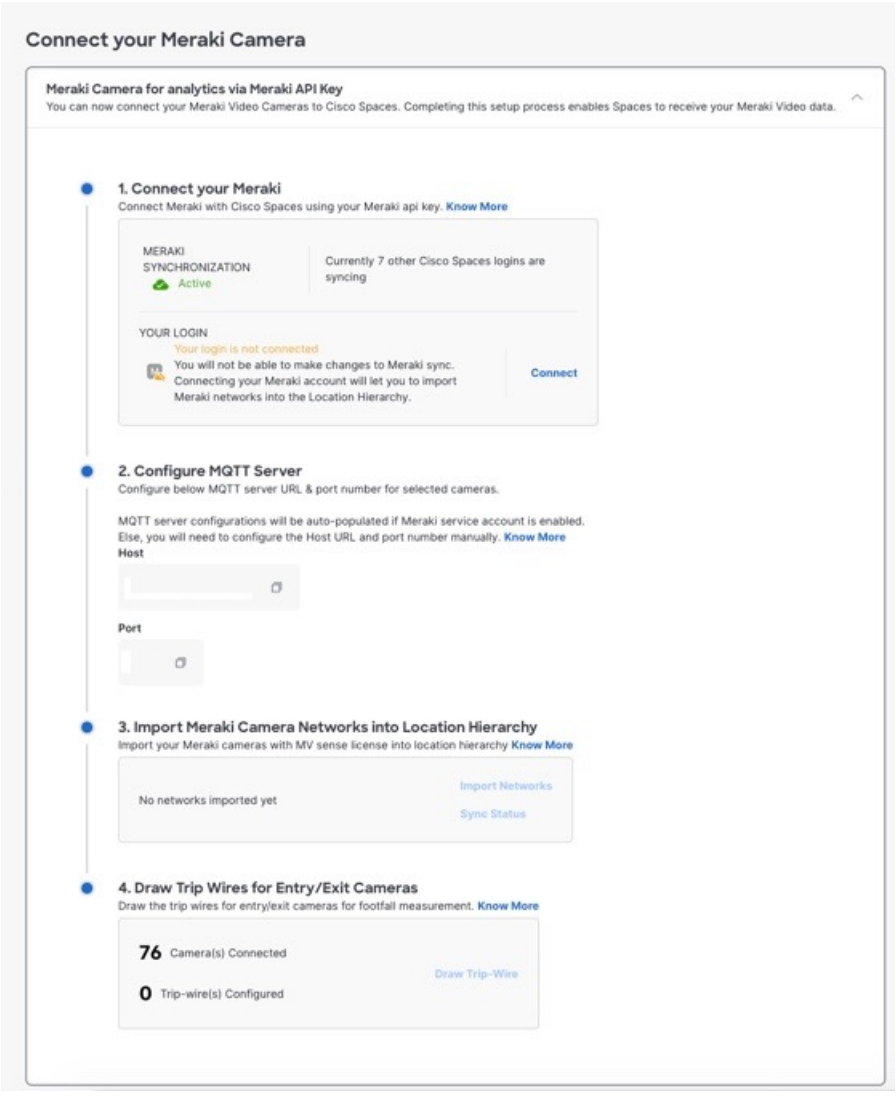
1. The camera is enabled in Meraki.
2. The required Meraki MV Sense license is available.

3. The camera and related network are ready for Cisco Spaces onboarding.

The Camera setup workflow has four high-level steps:

1. Connect your Meraki
2. Configure MQTT Server
3. Import Meraki Camera Networks into Location Hierarchy
4. Draw Trip Wires for Entry/Exit Cameras

Figure 75: Prerequisites



Set up Cisco Spaces to Work with Cisco Meraki Camera

Cisco Spaces uses Cisco Meraki Cameras to determine the number of visitors who enter and exit a location and the number of visitors currently present at the location. To use this feature, connect Cisco Meraki Cameras to Cisco Spaces through Meraki API Key or Meraki Integration. Meraki Login is supported only for accounts that are already connected to Cisco Spaces through Meraki Login. Make sure that the cameras are installed, can reach the Meraki cloud server, and have valid Meraki MV Sense licenses.

You can capture these details using the **Camera** feature:

- The total number of visits entering a location.
- The total number of visits leaving a location.
- The total number of visitors currently present at a location.



Note If a visitor exits the tripwire line and enters the tripwire line again, the new entry is counted as a separate visit.

You can view the visitor count using the **Camera Metrics** and **Live Occupancy** apps available in the Cisco Spaces dashboard.

Configure a Meraki Camera

Procedure

Step 1 In the Cisco Meraki dashboard, configure the cameras on the required Meraki network. For more information about configuring the cameras on the Meraki network, see Configuring Cameras.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Camera**.

The **Connect your Camera** window is displayed.

Step 3 Click **Get Started**.



Note If connected to the Cisco Meraki earlier, the widget corresponding to the connection method used is displayed automatically in the **Connect your Camera** window. In such cases, **Get Started** is not displayed. To connect to Cisco Meraki using the same connection method (Login, API Key) for configuring the Meraki camera, skip Step 4 to Step 6. However, to connect through the alternate connection method, add the corresponding widget using **Add New**. If widgets are added for both connection methods (through login and API key), **Add New** is disabled.

Step 4 Click **Select** to indicate the method that you wish to connect Cisco Meraki to Cisco Spaces.

The window displays the prerequisites for the selected method. For more information about the methods, see Setting Up Cisco Spaces to Work with Various Wireless Networks.

Step 5 Click **Continue Setup**.

In the **Connect your wireless network** window, a widget that allows connecting the camera is displayed.

The widget that is displayed depends on the method selected in Step 6. For the **Connect Via Meraki Login** method, the widget displayed is **Meraki Camera for analytics via Meraki Login**. For the **Connect via API Key** method, the widget displayed is **Meraki Camera for analytics via Meraki API Key**.

Step 6 In the expanded widget, click **Connect** displayed at Step 1.

If already connected to the Cisco Meraki network using the same connection method, the instruction for Step 1 is replaced with the message indicating that you are connected, and the **Connect** link is displayed. In such cases, skip this step.

a) For the **Meraki Camera for analytics via Meraki Login** widget, a window displays with fields to enter e-mail and password for login. Enter the login credentials, and click **Submit**. After connecting successfully, the content in Step 1 is replaced with the following message: `Connected as [e-mail using which you have connected].`

b) For the **Meraki Camera for analytics via Meraki API Key** widget, a window is displayed with an **API Key** field. Enter the API Key, and click **Submit**. After connecting successfully, the content in Step 1 gets replaced with the message `"Connected with [ masked API key]"`.

Step 7 Click **Import Networks** displayed in Step 2 in the **Connect your Meraki Camera** window.

If the camera network is already imported to the Location Hierarchy section, then skip Step 9 to Step 13.

Step 8 In the **Import Networks** window, select the parent location or root location under which you want to import the Meraki camera networks.

Step 9 From the **Choose Networks** area, select the check boxes for the Meraki networks that you want to import.

Step 10 Click **Import**.

The total number of Meraki networks and cameras that are imported are displayed.

Step 11 Click **Finish**.

The Meraki Camera configurations in Cisco Meraki will get automatically synchronized with Cisco Spaces. Typically, it gets auto-configured in 48 hours. If there is a delay, manually configure the MQTT server details in Cisco Meraki as explained in the following step.

Step 12 If want to manually configure the MQTT Server details in Cisco Meraki, perform the following:

The host and port of the MQTT server are account-specific and are displayed in Step 3 within the Cisco Spaces **Connect your Meraki Camera** window. You must configure these MQTT server details in Cisco Meraki.

a) Log in to the Cisco Meraki dashboard.

b) From the menu in the left pane of the dashboard, choose **Cameras** > **Cameras**.

c) In the **Name** field, click the link for the camera for which you want to configure the MQTT server.

The details of the selected camera are displayed. The **Video** tab for the camera is displayed by default.

d) Click the **Settings** tab, and click **Sense**.

e) To the right of Sense API, click **Enabled**.

f) Click the **Add or Edit MQTT Brokers** link.

g) In the **Edit MQTT Brokers** window, click **New MQTT Broker**.

h) In the **Edit MQTT Broker** window that is displayed, enter the following MQTT server details:

- **Host**: Enter the following host details:
  - For users hosted in the U.S. region: **`mqtt.dnaspaces.io`**
  - For users hosted in European region: **`mqtt.dnaspaces.eu`**
  - For users hosted in Singapore region: **`mqtt.ciscospaces.sg`**
- **Port**: Enter port as 1883. You must ensure that traffic from Cisco Meraki is allowed through the port 1883.

i) Click **Save**.

Step 13 To configure the entry or exit line for the camera, click **Draw Trip Wire** in Step 4 in the **Connect your Meraki Camera** window.

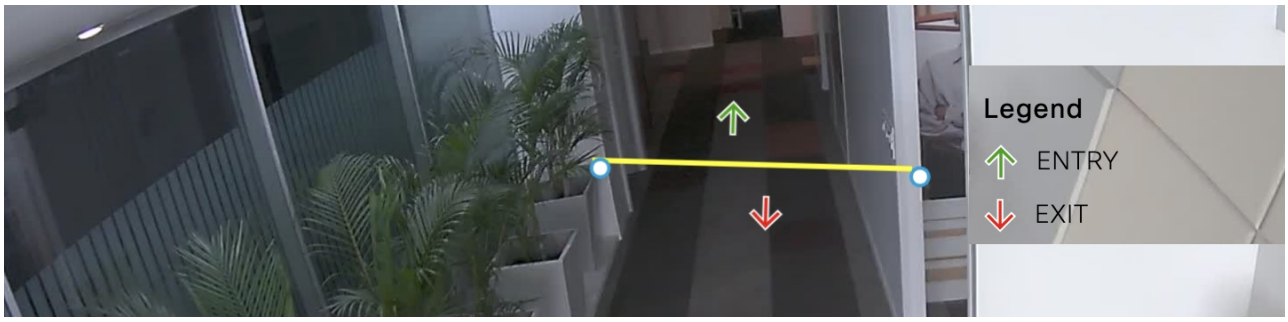
Note The camera metrics are calculated only at the location level. Ensure that there is a camera at every entrance to a location where metrics are desired and that the tripwire is drawn for each of those cameras. To ensure accuracy, cameras should be placed in close proximity to an entrance with a clear view of the entire entry or exit point. Tripwire should be drawn several feet off the floor at the point of entry or exit. Do not draw a tripwire for any cameras at a location that is not located at a location-level entry or exit point.

Step 14 In the **Draw Trip-Wire** window that is displayed, click **Select Locations**, choose the location in which the camera is configured, and click **Done**.

Step 15 In **Select a camera you wish to draw the trip-wire** area, select the radio button for the camera for which you want to set the trip wire, and click **Next**.

Step 16 Create the trip-wire by drawing a line on the camera preview image using +.

By default, the entry and exit arrows display in the middle of the tripwire. The green arrow represents the entry and the red arrow represents the exit. Ensure that the entry and exit arrows are pointing in the direction shown in the following image. If the arrows are not positioned properly, then click and hold the blue outlined dot at the end of the tripwire line and drag the mouse to rotate the line and arrow.



Note The tripwire functions only if the Cisco Meraki Service account is configured.

Step 17 Click both the endpoints of the line to configure the XY coordinates. After clicking the endpoints of the line, the XY coordinates for the entry and exit arrows are displayed automatically in the **Trip-wire status** area, and the status gets changed to **Set**. By default, the status will be **Not Set**.



Note The status will be changed to **Set** only if you click both endpoints of the line.

Step 18 Click **Finish**.

The camera is configured to use in Cisco Spaces.

What to do next

Cisco Spaces **Right Now** app also reports zone-level presence data, if you have configured camera zones in Cisco Meraki. To define zones for each camera, refer to Cisco Meraki documentation.

Edit the Trip Wire for a Camera

To edit the XY coordinates of the trip wire for a camera, perform the following steps:

Procedure

Step 1 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and select **Setup** > **Camera**.

The **Connect your Camera** window appears.

Step 2 In the **Connect your Camera** window, expand the Meraki camera connection widget.

Step 3 In Step 4: **Draw Trip Wire**, click **Draw-Trip Wire**.

Step 4 Click **Select Locations**, select the location where the camera is configured.

Step 5 Click **Done**.

Step 6 If needed, search for the camera and select it.

Step 7 Click **Next**.

Step 8 On the camera preview image, adjust the trip-wire line and entry or exit direction as required.

Step 9 Click **Finish**.
Success window appears.

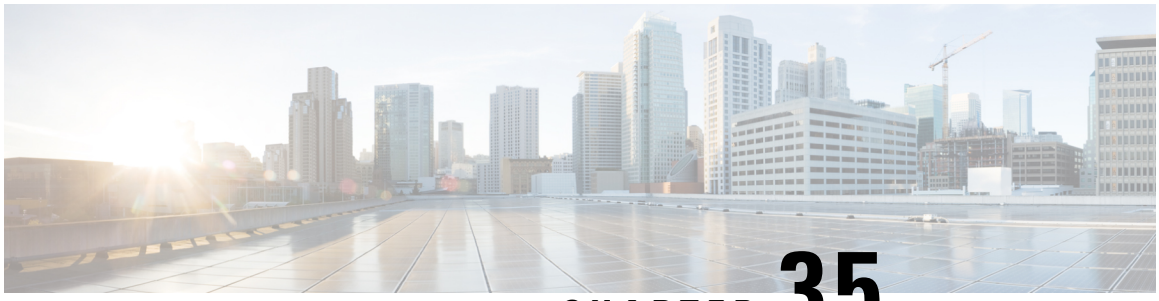
Step 10 Click **Continue** to return to the **Connect your Camera** window.

Step 11 Click **Go to camera list** to return to the **Draw Trip Wire** window.

Manage Camera Configuration

After setup is complete, manage the configured camera workflow from the **Setup** > **Camera** by performing these actions:

- Disconnect or remove an existing API key.
- Review the synchronization state using **Sync Status**.
- Reopen Draw Trip-Wire to update camera trip wires.
- Import additional camera networks as needed.



CHAPTER 35

Set Up Data Export

- Data Export, on page 361
- Spaces Data Export Source IP, on page 362
- Create Export Data, on page 362

Data Export

The Data Export feature in Cisco Spaces helps you to set up the automatic export of raw-level data as CSV files to any available storage destinations.

Cisco Spaces captures a variety of data of users at the location including user acquisition data, user visit data, proximity rule match data, and so on.

Exports are provided as flat files (CSV) that are uploaded directly to the customer's storage destination. Optionally, this can be transferred over a VPN connection if the destination server is not accessible over the public internet. The upload frequency can be customized to suit customer requirements and the volume of data. This supports fully automated ingestion into customer systems.

For more information about routing the SFTP connection over VPN and additional details, contact Cisco Spaces support.

Note

- Customer acquisition data export does not support data for portals with the authentication types: **No Authentication** and **Access Code**.
- As part of the visits data export, visits with a duration of less than zero minutes (less than 0 min) are excluded. This removes invalid or transient visit records that could inflate visitor counts.

  Visits with a duration of more than 720 minutes are also excluded. This removes long-running, always-on device sessions that would otherwise inflate visitor counts.
- For the Cisco Spaces dashboard EXTEND license customer accounts, data export types such as Captive portal, and Engagement and Location Personas are not available for export.
- For ADVANTAGE license customer accounts, all data types are available for export.
- For ESSENTIAL (formerly known as SEE) license accounts, **Data Export** feature is restricted in the enhanced React version of Cisco Spaces.

Spaces Data Export Source IP

Data Export uses the following source IPs (based on region) to export data:

Region	Source IP(s)
.io	52.55.122.128 54.174.253.222 34.205.82.138 3.208.52.128 52.206.67.43 34.192.26.106 54.88.200.142
.eu	52.48.33.123 52.208.167.15 52.208.15.59 54.220.148.167 54.220.45.63
.sg	18.140.83.198 13.215.167.226 18.143.125.54 3.1.251.174

Create Export Data

Procedure

Step 1 In Cisco Spaces, click the **Menu** icon ( ) and choose **Setup** > **Data Export**.

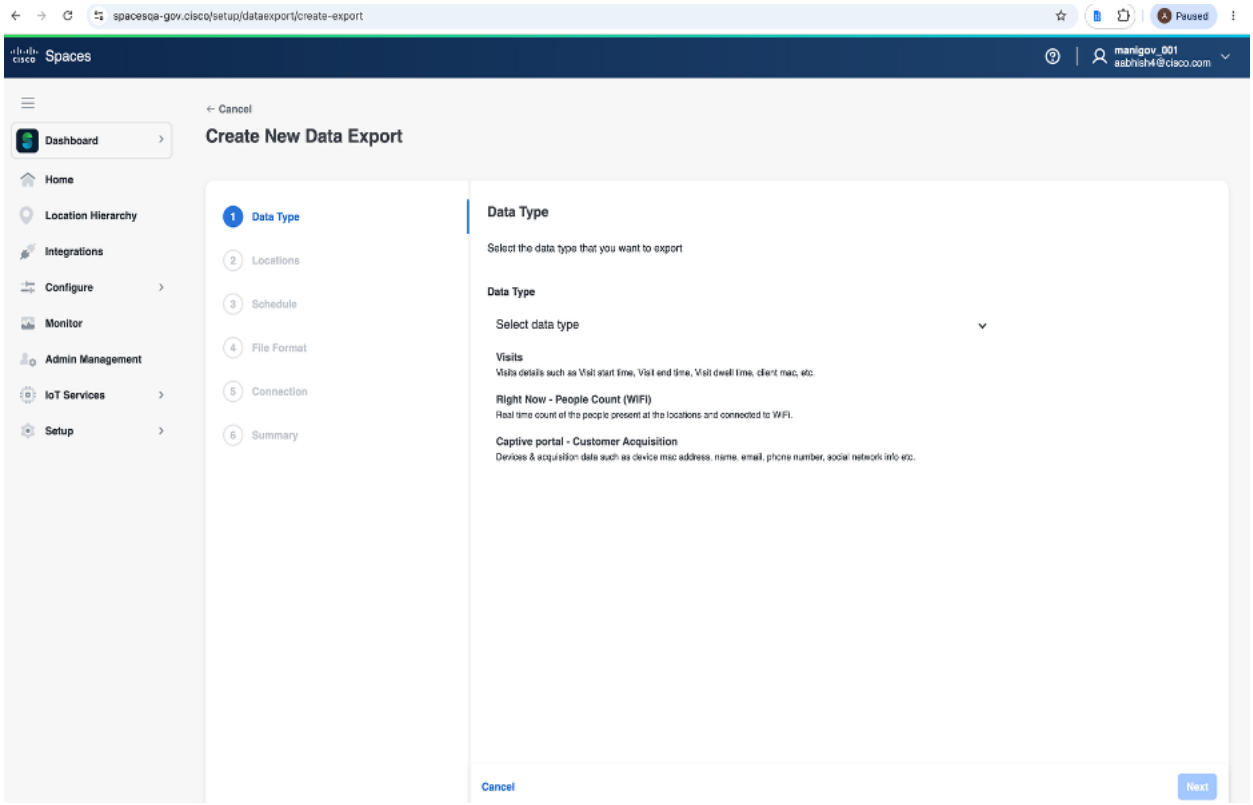
Step 2 Click **Create New Export**.

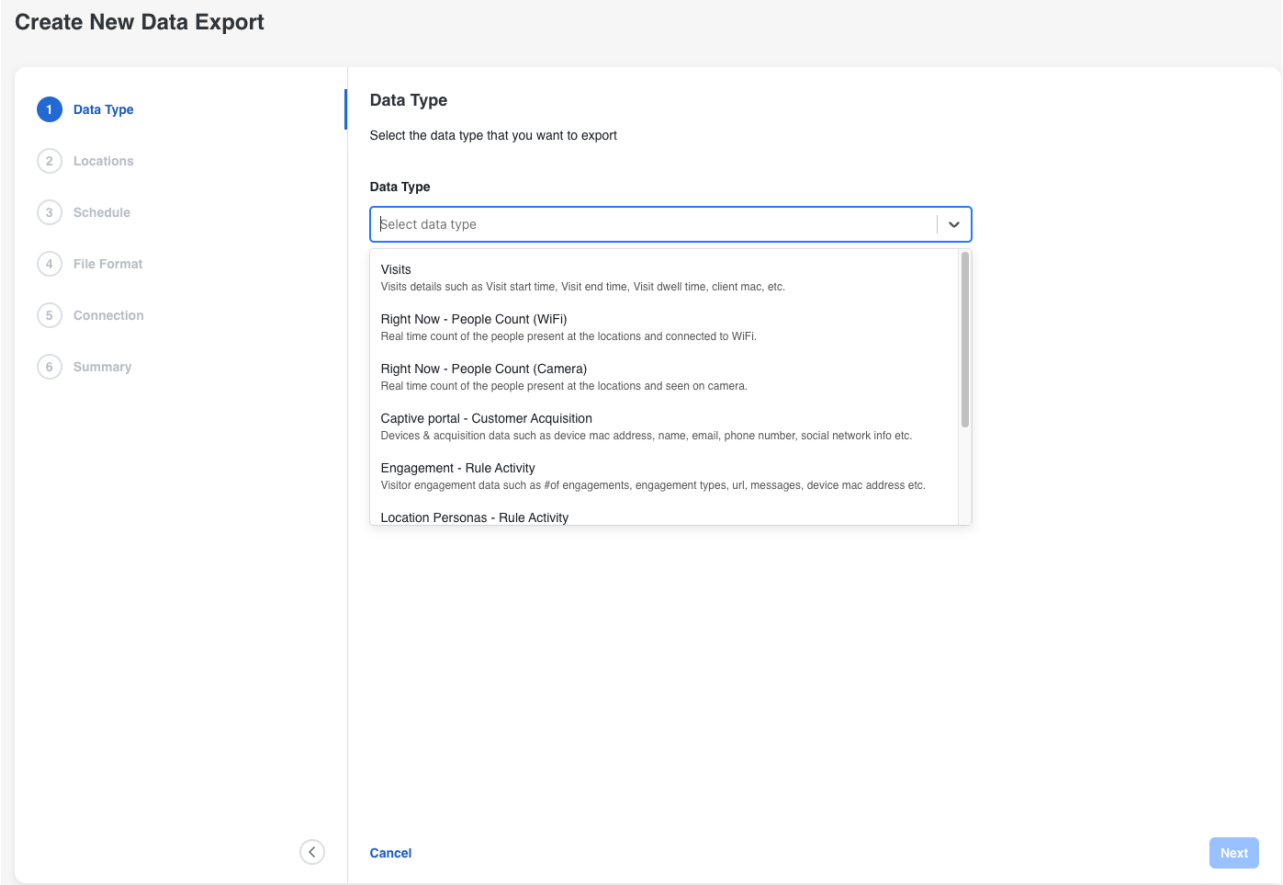
The **Create New Data Export** window is displayed with the following configuration options in the chronological order:

- **Data Type**
- **Locations**
- **Schedule**

- **File Format**
- **Connection**
- **Summary**

Figure 76: Create New Data Export





Step 3 From the **Data Type** drop-down list, select the data type.

The following data types are available:

Table 18: Data Types

Data Types	Description
Visits	Log Timestamp, Timezone, Local Date, Local Hour, Local Minute, Device ID, User ID, User Name, MAC Address, Visit Start Timestamp,Visit End Timestamp,Visit Duration, Location Information
Right Now - People Count (Wi-Fi)	Log Timestamp, Local Date, Local Hour, Local Minute, Associated Users Count, Estimated Probing Count, Estimated Density, Location Information
Right Now - People Count (Camera)	Log Timestamp, Local Date, Local Hour, Local Minute, People Presence Count, Location Information

Data Types	Description
Captive Portal - Customer Acquisition	Log Timestamp, Timezone, Local Date, Local Hour, Local Minute, Acquisition Type, Device ID, User ID, MAC Address, Acquisition Handle, Opt In, Phone Number, Email, First Name, Last Name, Gender,Age, Business Tag Name, Business Tag Value, Social Network, Social Network Profile URL, Social Network Picture, CPF Number, Location Information
Location Personas - Rule Activity	Log Timestamp, Timezone, Local Date, Local Hour, Local Minute, Device ID, User ID, MAC Address, Profile Tag Name, Rule Name, Location Information
Engagement - Rule Activity	Log Timestamp, Timezone, Local Date, Local Hour, Local Minute, Device ID, User ID, MAC Address, Engagement Type, Engagement Destination, Message, Rule Name, Location Information
Open Roaming - User Data	Log Timestamp, Timezone, Local Date, Local Hour, MAC Address, User Name,Status Type, Account Session ID, Acct Input Octets, Acct Input Packets, Acct Output Octets, Acct Output Packets, Profile Name, Device Class Tag, CUI User Name, App Reference ID, Location Information



Note When you create or edit a Visits export, use the **Include PII** toggle to control whether the export contains the **User Name** and **MAC Address** fields.

The toggle is enabled by default. When enabled, the generated Visits export includes User Name and MAC Address. When disabled, Cisco Spaces omits both fields from the generated file. Other selected Visits fields are not affected.

- For each data type, you must select the levels in **Location Hierarchy** and location information to include in the export.
- The location selection is based on the location type selected in the **Data Type** field.
- The location selection option is not available for the data types **Engagement**, **Captive Portal** and **Location Personas**.
- Cisco Spaces captures various user data at location including user acquisition data, user visit data, engagement rule match data, and so on.
- For custom data export, contact, Cisco Spaces support.

a) In the **Location Information** area, the following fields are displayed depending on the selected configuration. All these fields are optional and you can choose to select them to include in the data export.

- Location Name
- Location Type

- Hierarchy Path
- City
- State
- Country
- Capacity
- Area

The recent hour data for the selected data type is displayed in the sample export.

b) Use the **INCLUDE PII** toggle to choose whether Personally Identifiable Information (PII), such as MAC Address and username, is included in the export.

Note This option is available only if you select **Data Type** as **Visits** Export in the Create or Edit Export workflow. By default, the toggle is enabled, so the exported file includes the username and MAC Address fields. You can disable the toggle to exclude these fields from the export.

Cisco Spaces uses standardized values in the Location Type field of export files. Use the these values when processing exported location data:

Table 19:

Previous value	Current value	Description
cmxzone or merakizone	zone	Unified value for all zone types
meraki	org	Organization associated with a Cisco Meraki network
MSE	cmx	Location associated with Cisco CMX

Update downstream parsers, mapping, and validation rules to accept zone, org, and cmx.

c) Click **Next** to navigate to **Locations**.

Step 4 Check the **Enable this export for all locations** check box to select all available locations and click **Next** to navigate to **Schedule**.

If you want to select the locations to be exported individually, uncheck the **Enable this export for all locations** check box and select the locations.

Step 5 In the **Export Schedule** area, from the **Recurrence** drop-down list, select the export recurrence to schedule a data export. The export is scheduled based on the configured timezone.

The options are:

- **Hourly**: Select this option to schedule data export every hour. From the **Timezone** drop-down list, select the required timezone.
- **Daily**: Select this option to schedule data export on a daily basis. From the **Timezone** drop-down list, select the required timezone and also select the hour of the day when the data is to be exported.

- **Weekly**: Select this option to schedule data export on a weekly basis. Select the day and from the **Timezone** drop-down list, select the required timezone and also select the hour of the day when the data is to be exported.

Step 6 Click **Next** to navigate to **File Format**.

Step 7 In the **Delimiter** area, select the data separator symbol code preference.

The options are:

- **Pipe**
- **Comma**
- **Tab**
- **Custom character**: In the **Custom Character** field, enter the character of your preference. You can use any special character except /,\, &, ',".

Note For the options **Pipe**, **Comma**, and **Tab** you must provide additional inputs.

Step 8 In the **Compress export data**, select **Yes** or **No** if you need a compressed export.

Note We recommend that you select the compressed format for data export.

Step 9 In the **File Name Format** field, enter the filename prefix and select the format for date and time.

Step 10 From the **Select Date & Time Format** drop-down list, select the format.

Step 11 Click **Next** to navigate to **Connection**.

Step 12 In the **Connection Type** area, from the **Select Destination** drop-down, select the destination type.

Depending on the connection type selected, enter the configuration parameters. The available connection types are:

- SFTP
- Amazon S3
- Microsoft Azure Blob Storage
- Google Cloud Storage
- Box

a) Enter the following parameters if the connection type is **SFTP** server:

- **SFTP Host**: Enter the hostname or IP address of the server in the following format `hostname.server.com`.
- **Port**: Enter the port number you want to connect to the **SFTP** server.
- **Username**: Enter the username.
- **Use Password**: Choose this radio button and enter your password to connect to the **SFTP** server.

- **Use Private Key**: Choose this radio button to use the private key to connect to the **SFTP** server. You must use the **Upload Private Key** option to upload the private key and enter the passphrase.



Note

- You can either choose **Use Password** or **Use Private Key** based on the SFTP configuration to establish the connection.
- Password or passphrase selection is based on the SFTP server.
- We recommend that you use RSA private key because OpenSSH key based authentication is not supported.

- **Upload Path**: Enter the upload path for the export data.

b) Enter the following parameters if the connection type is **Amazon S3**:

- **Access Key**: Enter the access key for your Amazon S3 bucket.
- **Secret Key**: Enter the secret key for your Amazon S3 bucket.
- **Region**: From the **Region** drop-down list, select the region for your Amazon S3 bucket.
- **Bucket Name**: Enter the bucket name depending upon the selected region.
- **Upload Path**: Enter the upload path for the export data.

c) Enter the following parameters if the connection type is **Microsoft Azure Blob Storage**:

- **Account Name**: Enter the storage account name for the Microsoft Azure Blob Storage.
- **Account Key**: Enter the account key for your Microsoft Azure Blob Storage.
- **Container Name**: Enter the container name.
- **Upload Path**: Enter the upload path for the export data.

d) Enter the following parameters if the connection type is **Google Cloud Storage**:

- **Bucket Name**: Enter the bucket name.
- **Upload Path**: Enter the upload path for the export data.



Note You must add a data-out@dna-spaces.iam.gserviceaccount.com service account and provide role as **Storage Object Admin** in the Identity and Access Management (IAM) Service.

e) For the connection type **Box**, in the **Upload Path** field, enter the folder name created in **Box** for exporting the data and click **Authenticate**.

1. Ensure that a box account is available to authenticate Data Export.
2. Enter the same username and password credentials to authenticate to the box. Single sign-on (SSO) method for authentication is not supported.

Note After a successful authentication, provide full access to Cisco Spaces to access files in the box location. Click **Grant access to box** to grant full permission to Cisco Spaces to export the data.

Custom data export is currently not supported for box destinations.

Step 13 Click **Connect**.

If the connection is successful, the following message is displayed: `Connection Established`.

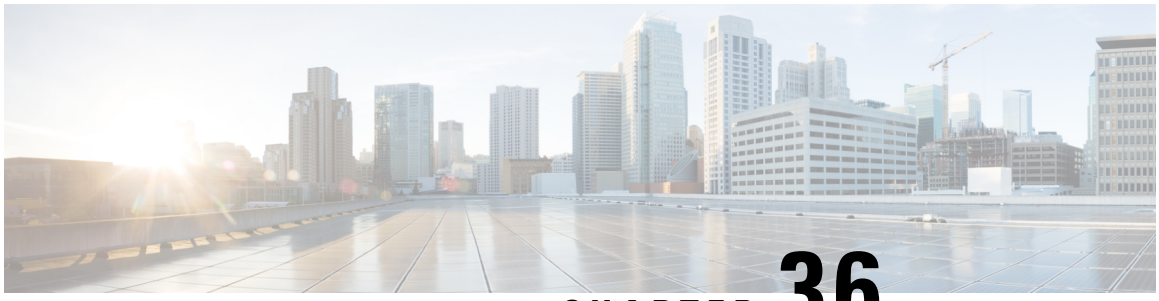
Step 14 Click **Next** to navigate to **Summary**.

Step 15 In the **Add a name to your data export** field, enter the name for the data export.

Step 16 Review the data export details and click **Export**.

A sample file is available in the upload path of the connection type once the export is configured.

In the **Create New Export** window, the data export details such as name, connection type, schedule, next export detail and the last successful export information are displayed.



CHAPTER 36

Set Up Cisco Webex

This chapter provides information on how to integrate Cisco Webex with Cisco Spaces.

- Integrate Cisco Webex, on page 371
- Set Up Cisco Webex, on page 372
- Generate an Activation Code, on page 373

Integrate Cisco Webex

The integration of Cisco Webex with Cisco Spaces enables Cisco Webex devices in the **Webex Control Hub** account to perform a cloud-to-cloud integration between **Webex Control Hub** and Cisco Spaces.

Note Cisco Webex integration supports only **Cisco Smart Workspaces** users.

This integration supports:

- Synchronization of Cisco Webex entities such as Cisco Webex workspaces, devices, workspace locations, and floor details from the **Webex Control Hub**. The synchronization process is scheduled at the backend every three hours after the token is configured in the Cisco Spaces dashboard. Choose **Setup** > **Webex** to configure the tokens.
- Cisco Webex devices to send device data such as temperature, air quality, occupancy, and so on, which is then used in **Cisco Smart Workspaces**.

As part of **Cisco Webex** integration, Cisco Spaces supports integration with persistent web app for **Cisco Webex** navigators. When a customer activates the control hub integration with Cisco Spaces, the necessary configuration supporting this integration is updated in the **Cisco Webex** control hub.

Note Currently, this integration is only available for **Cisco Smart Workspaces** users.

Set Up Cisco Webex

You can connect your Cisco Webex account to Cisco Spaces and then import the Cisco Webex networks into Location Hierarchy.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Webex**.

Step 3 In the **Connect your Webex** window, click **Connect**.

The Webex Token slider is displayed.

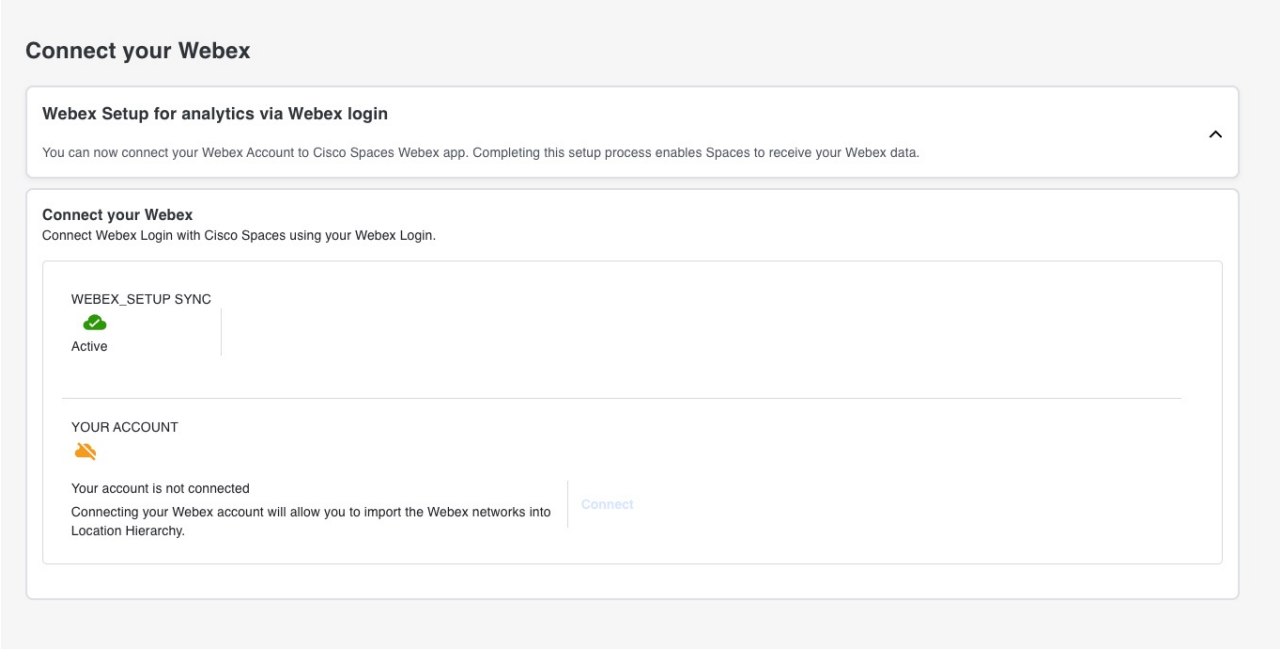
Step 4 In the **Enter or copy-paste your Webex Token** field, enter the Cisco Webex token.

You can get the token from the **Webex Control Hub**. For more information about generating an activation code, refer to Generate an Activation Code, on page 373.

Step 5 Click **Connect**.

The Cisco Webex synchronization status is displayed as **Active** for all active users in a specific tenant (account) if at least one user successfully connected their Cisco Spaces account with the Cisco Webex account while importing the Cisco Webex networks into **Location Hierarchy**.

Figure 77: Cisco Webex Synchronization Status



Generate an Activation Code

Use the Cisco Webex Control Hub to generate code.

Procedure

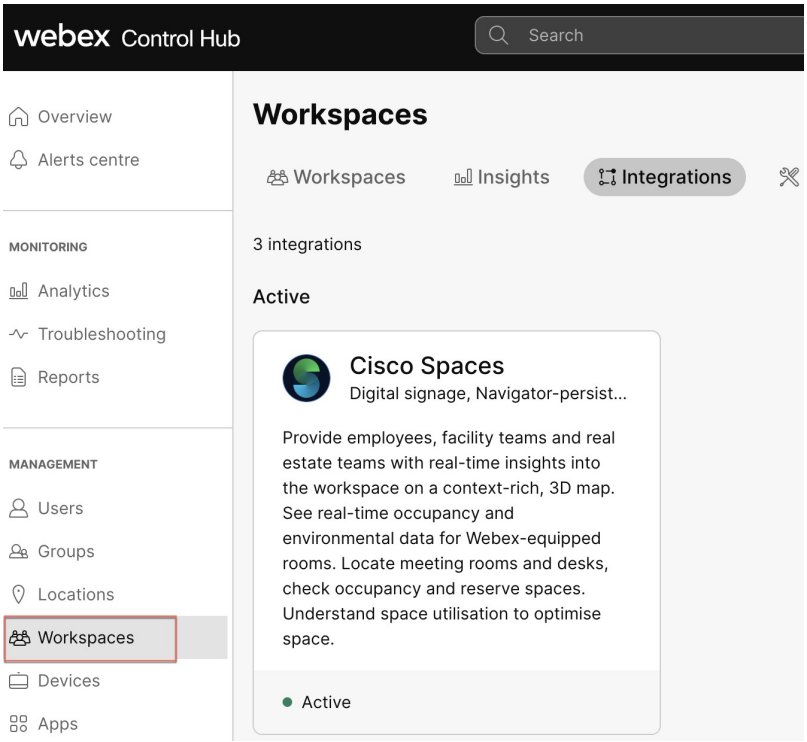
Step 1 Log in to Cisco Webex Control Hub.

Step 2 Enter your **Cisco Webex Control Hub** account email ID to sign in.

Step 3 In the **Cisco Webex Control Hub** dashboard, choose **Management** > **Workspaces**.

Step 4 Click the **Integrations** tab.

Figure 78: Cisco Webex Control Hub



Step 5 On the **Cisco Spaces** app tile, click **Details**.

The **Cisco Smart Workspaces** app integration details window is displayed.

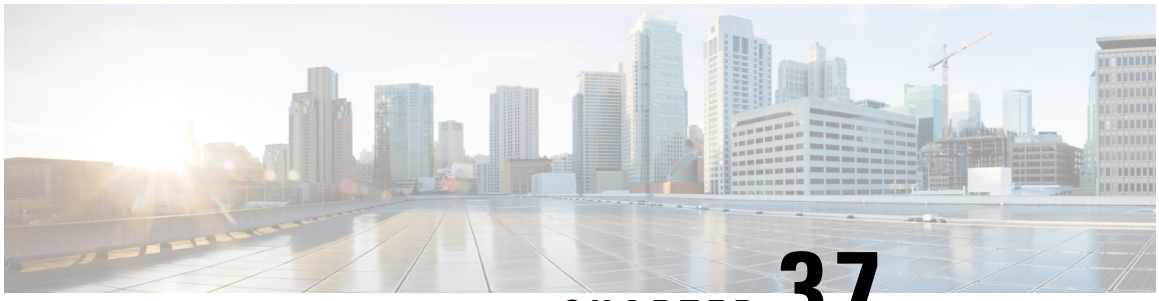
Step 6 At the top-right corner of the window, click **Activate**.

Step 7 Review the permissions requested by **Cisco Smart Workspaces** and check the **Terms and Conditions** check box.

Step 8 Click **Activate**.

Step 9 Use the **Copy to Clipboard** option to copy the activation code and paste the code in **Cisco Spaces** to integrate **Cisco Webex**.

The generated activation code's expiry details are displayed in the **Activate Integration: Cisco Smart Workspaces** window.



CHAPTER 37

Set Up pxGrid Cloud

- Activate pxGrid Cloud, on page 375
- Generate Cisco pxGrid Token (OTP), on page 376
- Activate App for Products, on page 376

Activate pxGrid Cloud

Cisco pxGrid Cloud is a new Cisco cloud offer that enables you to share contextual information between Cisco Identity Services Engine (Cisco ISE) and cloud-based solutions without compromising the security of your network. It provides a unified framework that enables seamless data integration between Cisco ISE and cloud-based solutions. It is secure and customizable, enabling you to share only the data that you want and consume only the contextual data that is relevant to your application.

Note You must have administrator privileges to Cisco ISE and Cisco pxGrid Cloud to perform the activation.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **pxGrid Cloud**.

The Activate pxGrid Cloud window is displayed. Click **View Documentation** to view additional instructions in the Cisco pxGrid Cloud Solutions guide.

Step 3 In the **Token** field, enter the token generated from the pxGrid Cloud application. Follow the on-screen instructions to generate the token. For more information about generating tokens, see Generate Cisco pxGrid Token (OTP), on page 376.

Step 4 Click **Activate pxGrid Cloud**.

A message indicating that the activation is successful is displayed.

Step 5 Click **Got it**.

Step 6 Click **Refresh to check status**. A green tick mark is displayed on the app tile indicating that the app is connected.

Proceed to activate the app for the product. For more information about activating apps for products, see Activate App for Products, on page 376. Follow the on-screen instructions to activate the product.

Generate Cisco pxGrid Token (OTP)

Procedure

Step 1 Log in to Cisco DNA Cloud.

Step 2 In the Cisco pxGrid Cloud portal, click the **Menu** icon ( ) and choose **App Store**.

Step 3 Click **My Apps**.

Step 4 In the **My Apps** window, choose the customer-specific application tile and click **Connect to App**.

The generated One Time Password (OTP) is displayed in the **OTP Generated** pop-up window.

Step 5 Use the **Copy** icon to copy the generated OTP.

The generated OTP is valid for 60 minutes.

Activate App for Products

Cisco pxGrid Cloud offers a plug-and-play deployment without requiring infrastructure changes to your network. Use the Cisco pxGrid Cloud portal to activate applications for your product.

Note Enable all the required scopes in Cisco ISE for a successful activation (stream creation). For more information, see Cisco pxGrid Cloud Solution Guide.

Procedure

Step 1 Log in to Cisco DNA Cloud.

Step 2 In the Cisco pxGrid Cloud portal, click the **Menu** icon ( ) and choose **App Store**.

Step 3 Click **My Apps**.

Step 4 In the **My Apps** window, choose the customer-specific application tile and click **Activate Product**.

The **Activate App for Products** window is displayed.

Step 5 To proceed, click **Let's Do it**.

The **Select an App** window is displayed. By default, the **App Name** field displays the application tile name selected in step 3. The compatible products and supported region details are also displayed.

Step 6 Click **Next**.

The **Select Product** window is displayed.

Step 7 From the **Product Type** drop-down list, select the product type for which you want to activate the selected app.

Step 8 From the **Product** drop-down list, select the product for which you want to activate the selected app.

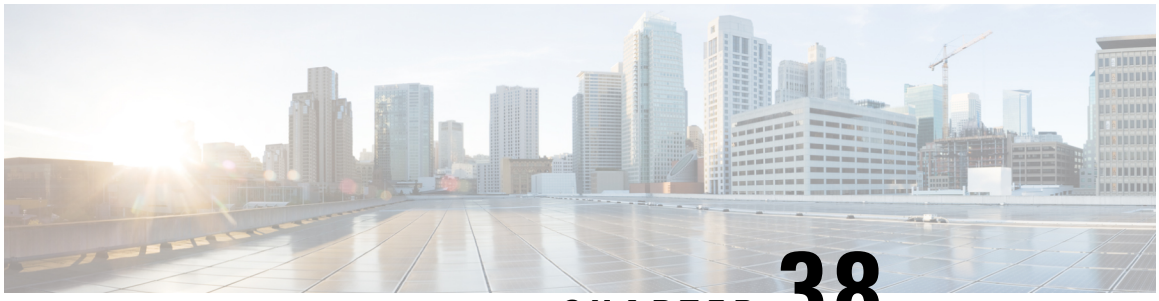
You can only select products that are registered in the **On-Prem Connections** window. You can also use the **Search** option to search for the product.

Step 9 In the **Configure App for Product** window, set the configuration scope.

Step 10 In the **Summary** window, review your settings and click **Activate App for Products**.

The app activation status is displayed as **Activated** in the **Product Activation** window.

Refresh the Cisco Spaces dashboard to view the successful integration status of Cisco pxGrid Cloud integration.



CHAPTER 38

Set Up Access Point Auto Location

- Access Point Auto Location, on page 379
- Prerequisites for AP Auto Location, on page 381
- Generate AnyLocate Measurement Data, on page 381
- Place Devices, on page 384
- Edit Device Placement, on page 387
- View AnyLocate Measurement Data Status, on page 388
- View APs, on page 389

Access Point Auto Location

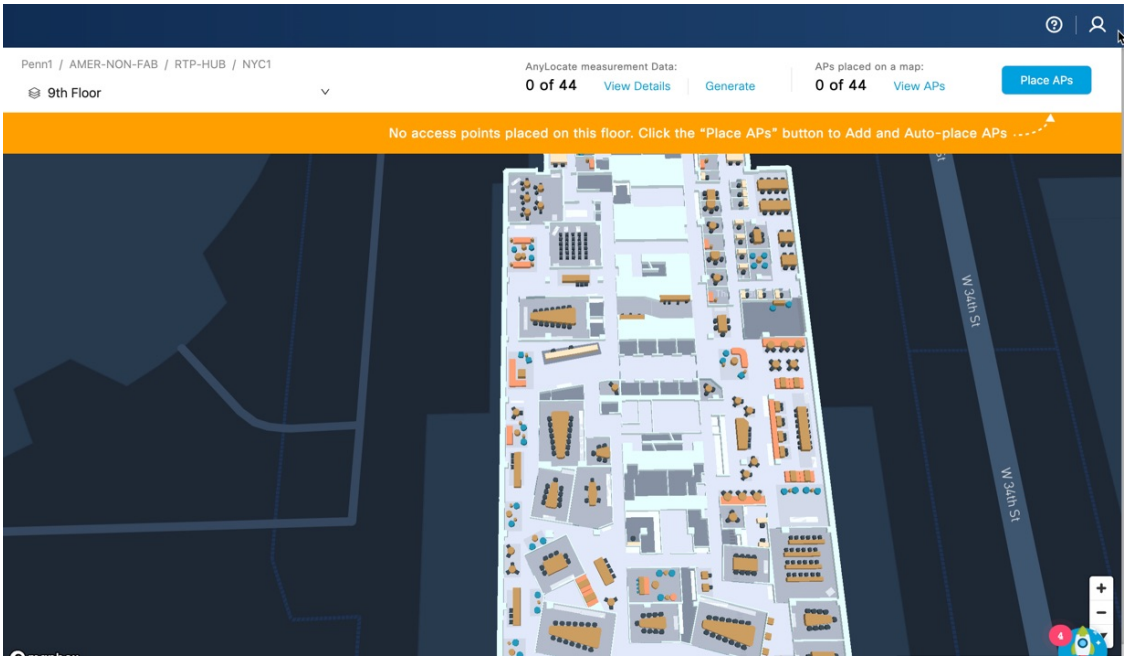
The Access Point Auto Location solution helps to effectively self-locate APs in a global coordinate by combining various ranging technologies and algorithms.

This solution delivers accurate, automated, up-to-date AP location leveraging Fine Timing Measurement (FTM) and Global Navigation Satellite System (GNSS) when available. If GNSS is not accessible, you must place a few manual anchors per each floor. This feature requires an AP density such that neighboring APs can hear each other at maximum power. The accuracy of the Access Point Auto Location feature depends on the building type and the distances between APs.

The configurations required for APs to enable the ranging orchestration are achieved using the **Access Point Auto Location** feature in Cisco Catalyst 9800 Series Wireless Controllers. For more information, see "Information About Access Point Auto Location Support" in the *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*.

In Cisco Spaces, to support the AP Auto Location solution, a new feature **Device Placement** is available under **Menu ( )** > **Setup** > **Device Placement**.

Figure 79: Device Placement



The AP Auto Location solution automatically locates your APs on a digital map in Cisco Spaces. After an administrator *anchors* several APs with known locations on the floor plan, this feature helps to determine the position of the remaining APs and automatically places them on the Rich Map. If APs have Global Positioning System (GPS) capabilities, the anchors may be automatically positioned on the map.

Restrictions for Access Point Auto Location

The feature is not supported on the **default-site-tag**.

Supported Platforms

The **AP Auto Location** feature is supported on the following platforms and versions:

Table 20: Supported Platforms and Versions

Product	Platform	Releases
Cisco Catalyst 9100 Family of Access Points	• Cisco Catalyst 9130 Series Access Points • Cisco Catalyst 9136 Series Access Points • Cisco Catalyst 9164 Series Access Points • Cisco Catalyst 9166 Series Access Points	Minimum required version is Cisco IOS XE 17.12.1 Preferred version is Cisco IOS XE 17.15.1

Product	Platform	Releases
Cisco Catalyst 9800 Series Wireless Controllers	Cisco Catalyst 9800 Series Wireless Controllers	Minimum required version is Cisco IOS XE 17.12.1 Preferred version is Cisco IOS XE 17.15.1
Cisco Spaces	Cisco Spaces: Connector 3	Location Service 3.1.0.94 or later



Note Along with the supported platforms, ensure that you also have a Cisco Spaces Cloud account.

Prerequisites for AP Auto Location

To successfully place the devices, ensure that the following prerequisites are met:

- Cisco Catalyst 9800 Series Wireless Controllers must be connected to the Cisco Spaces: Connector and both must be available in the Cisco Spaces cloud account. For more information, see "Connect Connector to Cisco Catalyst 9800 Series Wireless Controllers" in the *Cisco Spaces: Connector 3 Configuration Guide*.
- Rich maps must be available for the floors to place the AP. Use the **Locations & Maps** feature to add rich maps. For more information, see Setting up Locations and Maps.
- Site tags are mandatory for the floors. Use the Cisco Catalyst 9800 Series Wireless Controllers GUI to create site tags. The APs that you are placing in Cisco Spaces must be associated with the site tags. For more information about configuring site tags, see "Configuring a Site Tag" in the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide.
- Generate Fine Time Measurement (FTM) ranging data for APs. Click **View Details** to verify the ranging data availability and Generate AP to AP Ranging Data.

Generate AnyLocate Measurement Data

Before starting the AP Auto Location process, you must generate the AnyLocate Measurement data for the APs to automatically place the APs in Cisco Spaces. The ranging measurement process changes the AP channel in the selected area to a common channel and uses FTM to determine the distance between the APs. You need to run this process once, or when APs are moved or added to another environment.

Use Cisco Spaces to generate Fine Time Measurement (FTM) ranging data for APs to place them on the floor map. FTM ranging data is more resilient than RSSI and has better accuracy. Select a site tag and generate the ranging data for all APs associated with that site tag.

Before you begin

Use the Cisco Catalyst 9800 Series Wireless Controller GUI to achieve the following:

- Configuring Access Point Geolocation Derivation Using Ranging: To enable **Geolocation Derivation Using Ranging** and allow the corresponding AP to be part of the location services that use ranging to determine the geolocation of the AP.
- Configuring Access Point Ranging Parameters: To enable APs to support the FTM protocol.

Note

- The AnyLocate Measurement Data process is not supported for a default site tag.
- We recommend that you schedule the ranging process when the network is less busy as this process is disruptive. This process takes approximately 10 minutes to complete.
- The AnyLocate Measurement ranging process can be triggered per site tag basis and is not supported for a default site tag.

Procedure

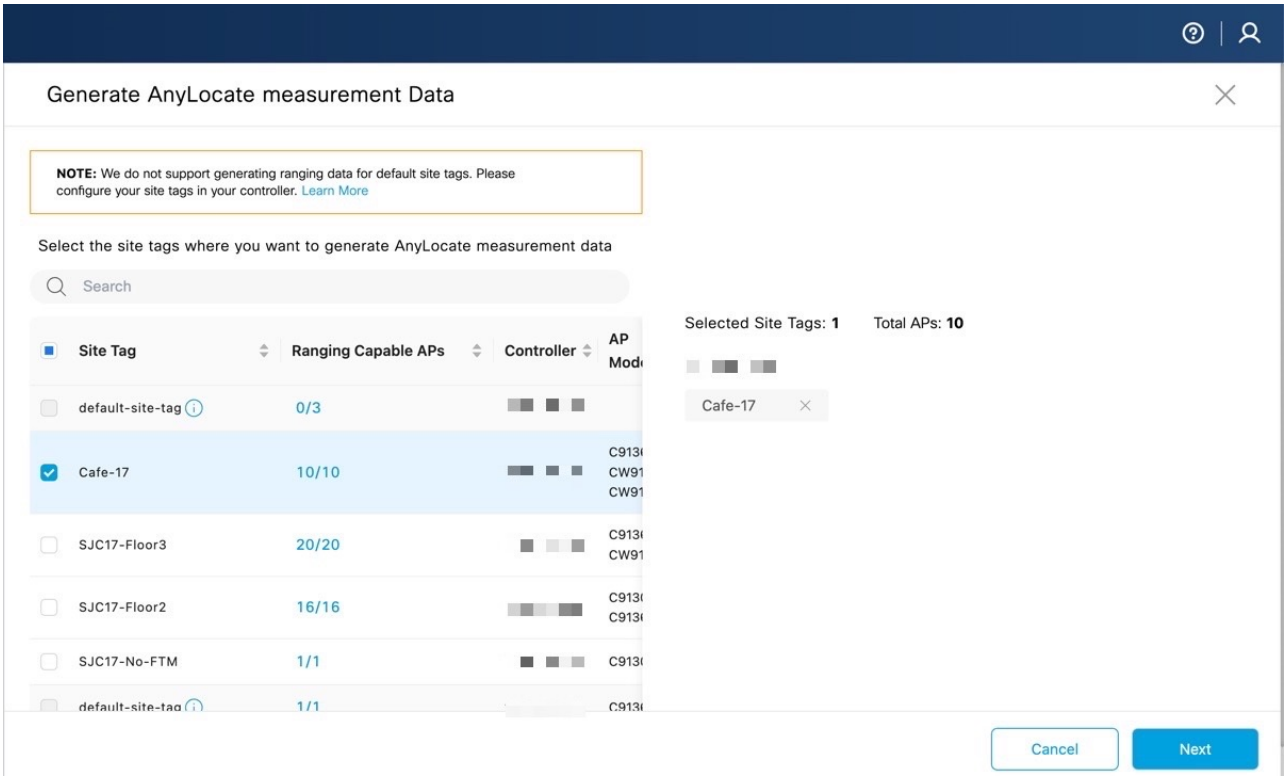
Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Device Placement**.

Step 3 In the **Device Placement** window, click **Generate**.

In a Day 0 configuration scenario, there is no AP ranging data available and you must click the **Generate** option displayed on the GUI to initiate the AP ranging data generation process. The **Generate AnyLocate measurement Data** window displays the site tags, number of ranging capable APs, controller, and AP model information.

Figure 80: Generate AnyLocate Measurement Data



Step 4 Select the site tags in the **Site Tag** column for which you want to generate the AnyLocate Measurement data.

The selected site tags and the corresponding controller details are displayed in the right side of the window. You can also check the **Site Tag** check box to select all site tags.

Note Generating ranging data for default site tags is not supported in Cisco Spaces.

Step 5 Click **Next**.

Step 6 Choose the scheduling option to generate AnyLocate Measurement data. The following options are available:

- **Schedule it for later**: Select this option to specify a date and time to generate AnyLocate Measurement data.
- **Generate Now**: Select this option to proceed with generating AnyLocate Measurement data.

Step 7 Click **Generate**.

Place Devices

Use the **Device Placement** feature to place the APs on the floor maps. Cisco Spaces uses various ranging technologies and algorithms to place the APs as per the global geographic coordinates. A site tag must be configured for each floor to place the APs successfully on the map.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Device Placement**.

Step 3 In the **Device Placement** window, from the **Floor** drop-down list, select the floor where you need to place the devices.

- Rich Maps are mandatory to place the APs. If rich maps are not available for a location, you cannot place the APs.
- Check the **Show Locations without Map** check box to filter and display locations without rich maps.

Step 4 In a Day 0 configuration scenario, a message is displayed indicating that no APs are placed on the floor. Click **Place APs** to place the devices.

The **Place APs** window is displayed with three sections: **Choose APs**, **Place APs** and **Review & Publish**.

Step 5 In the **Choose APs** section, check the check box corresponding to the cluster with APs to be placed in the specific floor.

Note

- By default, the **Automatically group neighbor APs** check box is checked and the APs are automatically grouped. Uncheck this check box to ungroup the APs and view them as a single list.
- All available AP clusters and the total AP count are displayed.
- For each cluster, you can view the controller, switch and site tag information.
- You can select multiple clusters to assign to a floor.
- APs with **default-site-tag** is excluded from the AP grouping.
- The AP grouping feature is available in the Connector May 2023 release. We recommend that you upgrade your **Connector** to the latest version to enable the AP grouping feature.

a) (Optional) Click and expand the AP cluster to view the APs available under the group neighbor.

The right panel displays the selected AP names and count. You can view the following AP information:

- Name
- AP Model
- MAC Address
- Controller
- Site Tag

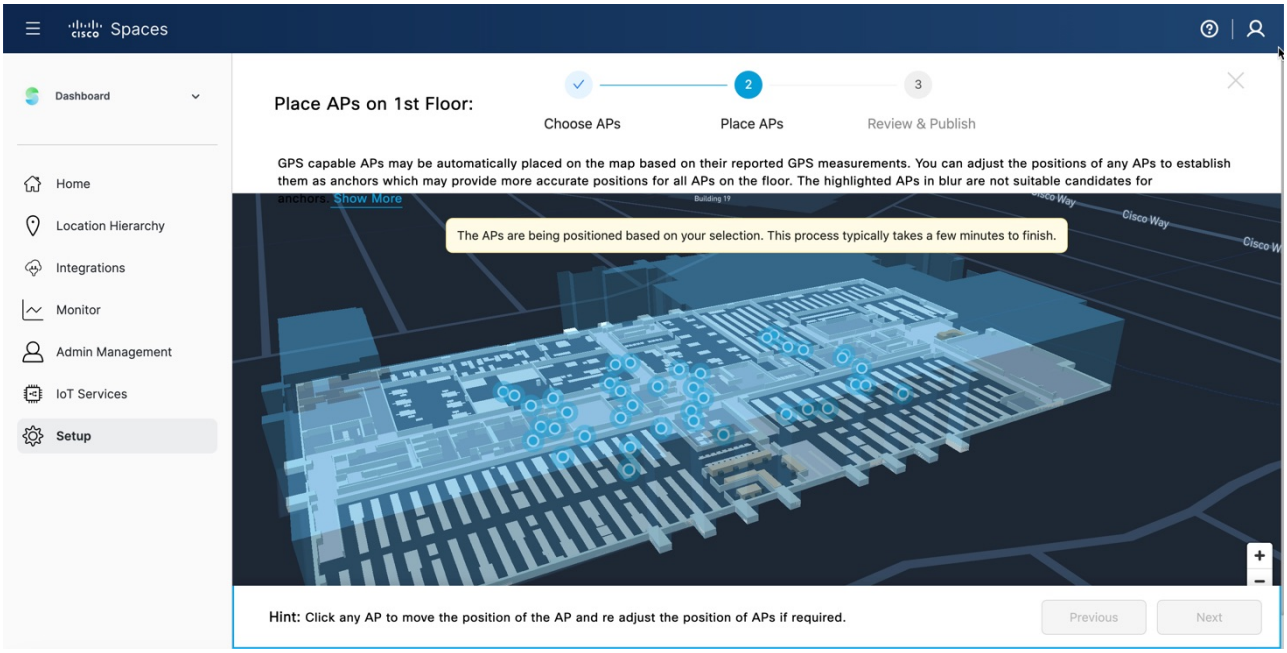
- Switch Name
- IP Address

b) (Optional) To search APs, enter the AP name in the **Search** field and click **Enter**.
c) (Optional) Click **Filter** to enter the filtering parameters to display the available APs.

Step 6 Click **Next**.

Step 7 In the **Place APs** section, you can view the APs getting placed automatically.

Figure 81: Auto-Place APs



When the APs are placed successfully, the following message is displayed: `The AP placement is complete for this floor. Please verify AP positions and make adjustments if needed or click "Next" to proceed.`

Note

- The APs highlighted in blue color are not suitable as anchors APs.
- All GPS capable APs are automatically placed on the map based on their reported GPS measurements. Adjust the positions of any APs to establish them as anchors to provide more accurate positions for all APs on the floor.
- If there are no GPS capable APs, the APs are placed based on the AP to AP relative positioning data.

a) Select the required AP and adjust the position manually.

Note The APs are color-coded as:

- Auto-placed APs in blue
- Manually adjusted APs in light green and dark green

APs with an additional GPS module attached are in dark green color. Click an AP to view the additional information in the right panel.

b) If you adjust the placement of 4 APs, a message is displayed to confirm the recalibration. Click **Recalibrate** to run the algorithm again to auto-place the APs.

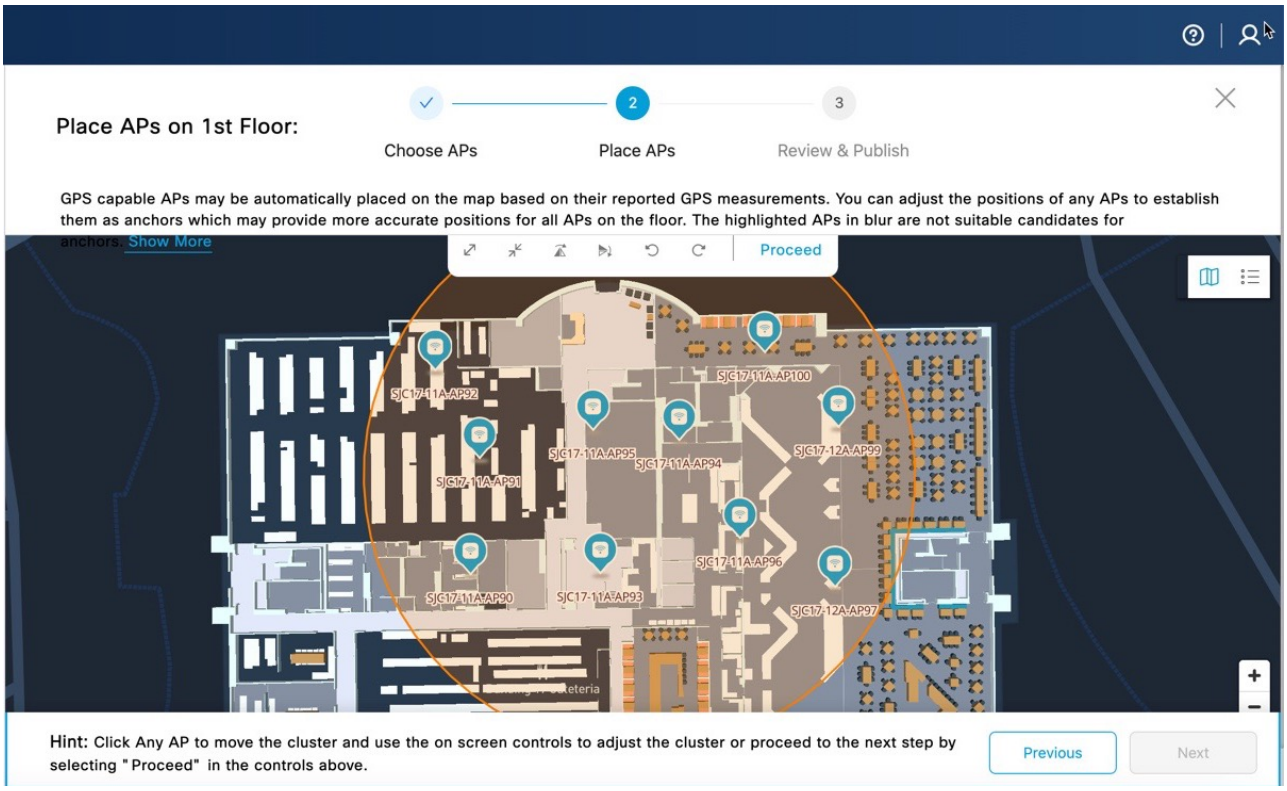
Click **Skip** to skip this step.

c) (Optional) To adjust the AP placements, use the controls (available on the top of the Rich map 

) to readjust the AP group position if required and click **Confirm Position/Proceed**.

You can flip or rotate the whole AP group and adjust the group placement. After you confirm the new placement, the AP group ring is not longer available.

Figure 82: Place APs Section



Step 8 Click **Next**.

Step 9 In the **Review & Publish** section, select an AP.

The **Access Point Details** slide-in window is displayed.

a) Edit the default AP height, modify AP specific parameters if required.

If you set the AP default height, all APs placed on the map inherit the same AP height parameter and the same is shared with the Cisco Spaces: Detect and Locate app.

b) Click **Save**.

Step 10 click **Publish**.

A pop-up message is displayed and click **Done**. You can view the placed APs in the Cisco Spaces: Detect and Locate app.

Edit Device Placement

Use the **Modify AP Placement** option to update the placement of APs on the floor. This option is enabled in the **Device Placement** window only if the selected floor has APs already placed on the floor map.

If there were any changes to the AP positioning, the **Device Placement** window displays a message and click **View** to display the **APs Notifications** slide-in window. You can review the APs that are either removed or moved from one floor to another and take the necessary action.

View the following AP details:

- AP Name
- Mac Address
- Reported Time
- Details
- Status
- Controller IP Address

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Device Placement**.

Step 3 In the **Device Placement** window, from the **Floor** drop-down list, select the floor where you need to edit the device placement.

Step 4 Click **Modify AP Placement**.

Step 5 In the **Choose APs** area, check or uncheck the check box against the required APs to update them.

The site tag associated with the floor is displayed along with the AP details such as the AP model, MAC address, controller, switch name, and so on.

The selected APs are displayed under the **Selected APs** section.

Step 6 Click **Next**.

Step 7 In the **Place APs** area, you can view the auto-placement of APs.

Cisco Spaces computes the AP location and places them on the floor map. View the rich map with the APs along with the calculated confidence percentage against each computed AP. You can manually adjust the AP placement if the calculated AP is not correctly placed.

Step 8 Click **Next**.

Step 9 In the **Review and Publish** area, verify the AP placement accuracy and click **Publish**.

View AnyLocate Measurement Data Status

AnyLocate Measurement data is required to process AP location. Generating measurement data might disrupt wireless connections for the APs participating in the ranging processes.

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Device Placement**.

Step 3 In the **Device Placement** window, click **View Details**.

The **AnyLocate Measurement Data Status** window is displayed. You can view the following AnyLocate Measurement data status:

- Ranging data generated for the number of APs and sites
- Number of APs with no site tags
- APs that do not support ranging data
- Number of site tags with a schedule for generating ranging data

Step 4 (Optional) Click **Manage / View History** to view the history of ranging data generation.

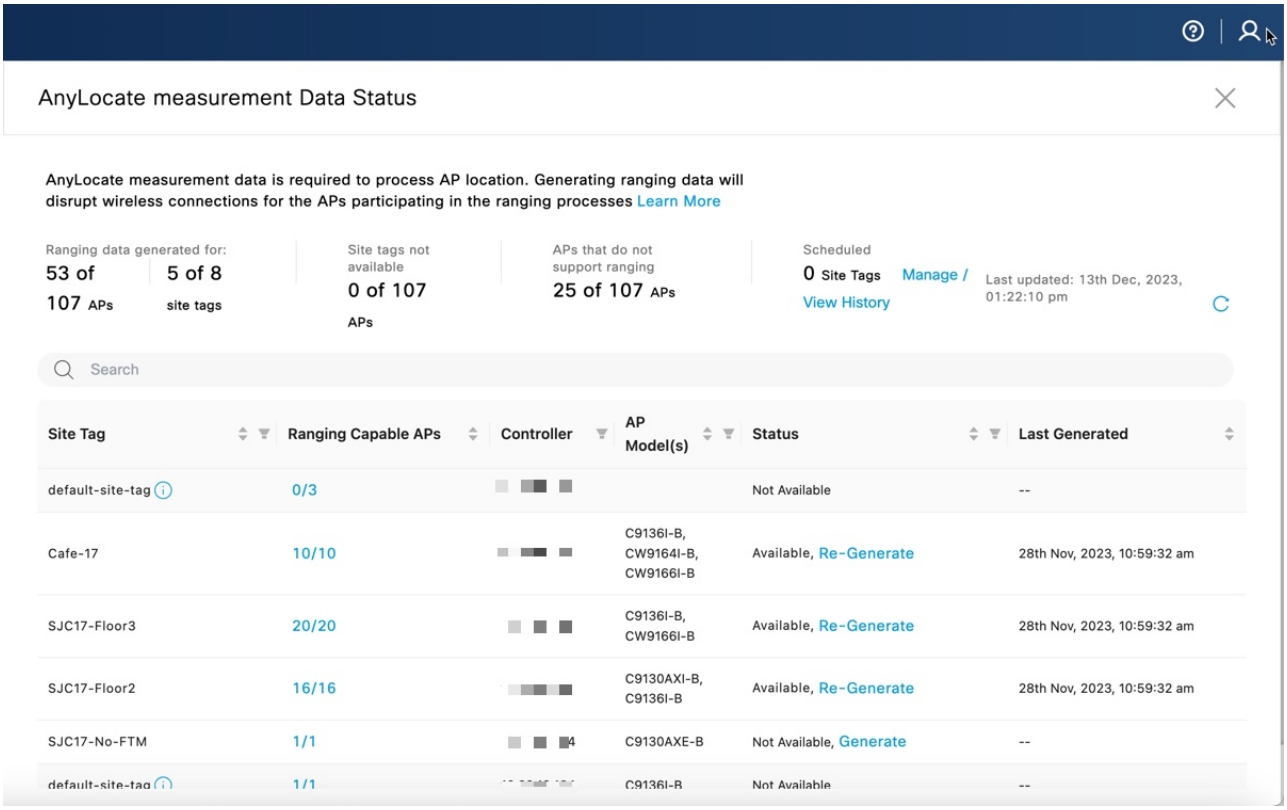
The **Ranging Data History** window displays both the executed and scheduled history status. Click **Cancel** to cancel the ranging data generation schedule.

Step 5 In the **AP to AP Ranging Data Status** window, view the following options:

- **Site Tag**: Displays the site tag. Default site tags are not supported for AP ranging data.
- **Ranging Capable APs**: Displays the number of APs capable of generating ranging data from the total number of APs placed on the floor. Click the number to view the details in the slide-in window.
- **Controller**: Displays the controller.
- **AP Model(s)**: Displays the AP models.
- **Status**: Displays the status of whether ranging data is generated or not. If ranging data is not generated for a site tag, the status is displayed as **Not Available**. You can click **Generate** to generate the data and proceed. If ranging data is already generated, the status is displayed as **Available**. You can click **Re-Generate** to regenerate the data if required.

- **Last Generated**: Displays the time stamp details of ranging data generation.

Figure 83: AnyLocate Measurement Data Status



Step 6 Click the **Close** ( ) icon to close the window.

View APs

Procedure

Step 1 Log in to Cisco Spaces.

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Device Placement**.

Step 3 In the **Device Placement** window, from the **Floor** drop-down list, select the floor to view the placed AP details.

Step 4 Click **View APs**.

The slide-in window is displayed with the details of the APs placed on the floor.

You can view the following AP to AP ranging data status:

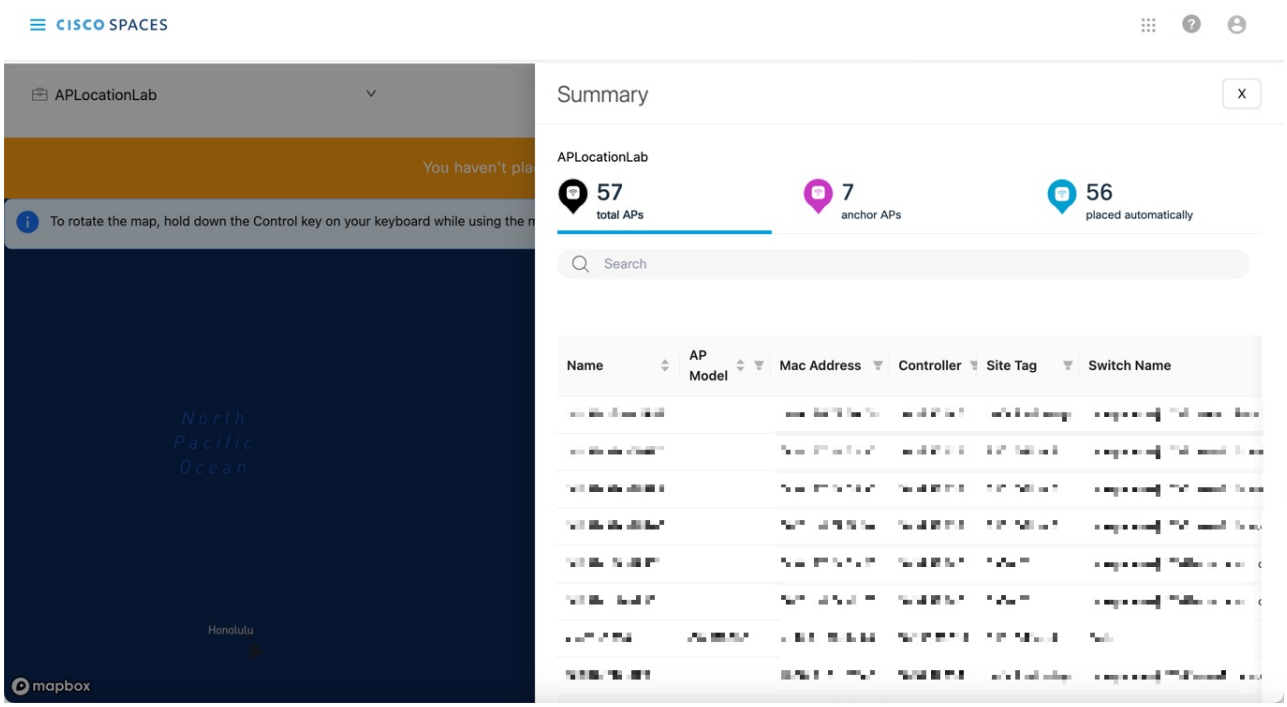
- Total number of APs

- Number of anchor APs
- Number of APs placed automatically

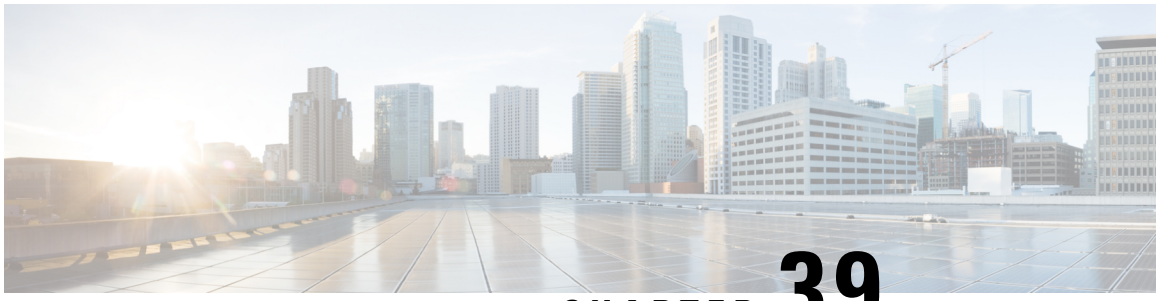
Step 5 View the following AP details:

- Name
- AP Model
- MAC address
- Controller
- Site Tag
- Switch Name

Figure 84: View AP Details



Step 6 Click the **Close** ( ) icon to close the slide-in window.



CHAPTER 39

Plugins

- Plugin Apps in Cisco Spaces, on page 391

Plugin Apps in Cisco Spaces

Plugins within Cisco Spaces serve as a platform service that standardizes the integration between Cisco Spaces and various third-party devices.

Plugins provides a platform service that enables standardized interconnection between Cisco Spaces and third-party devices or software. Through plugins, you can easily read data from external devices, access valuable context, and leverage calculated outputs from third-party software, all of which are integrated back into Cisco Spaces. This functionality helps organizations deliver new outcomes on top of their existing Cisco infrastructure.

Key Features

- **Standardized Interconnection**: Seamlessly connects Cisco Spaces with third-party devices and software.
- **Data Integration**: Enables easy data reading and context gathering from external devices.
- **Enhanced Outcomes**: Leverages third-party software to provide calculated outputs and insights.
- **Infrastructure Enhancement**: Builds additional value on top of existing Cisco infrastructure.

This capability allows organizations to leverage existing Cisco infrastructure while generating new, valuable outcomes through enhanced interoperability and data-driven insights. Plugins thus extend the functionality of Cisco Spaces by bridging external devices and software, enabling innovative applications and improved operational efficiency.

Available Plugins

The Available Plugins section includes the plugins that you can activate and start using. To activate a plugin, click **Activate**.

Note Activation and use of plugins require a **Spaces Advantage** license. Without this license, plugin functionality is not available.

A facility manager wants to integrate real-time location data from third-party UWB devices into Cisco Spaces for advanced analytics. By enabling the corresponding plugin (subject to license), they can visualize and act on this data within Cisco Spaces.