



Cisco Spaces Configuration Guide

First Published: 2018-12-18

Last Modified: 2024-03-04

Americas Headquarters

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

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

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

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

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

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

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

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

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

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)

© 2024 Cisco Systems, Inc. All rights reserved.



Preface

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



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

This document contains the following sections:

- [Audience, on page iii](#)
- [Document Organization, on page iii](#)
- [Document Conventions, on page v](#)
- [List of Acronyms and Abbreviations, on page v](#)
- [Communications, Services, and Additional Information, on page v](#)

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 Organization

Chapter Number	Chapter Title	Description
Chapter 1	Cisco Spaces Prerequisites	Provides information about various Cisco Spaces features and the prerequisites to deploy Cisco Spaces.

Chapter Number	Chapter Title	Description
Chapter 2	Get Started with Cisco Spaces	Provides an overview about Cisco Spaces and its features. This chapter also describes the process flow, system requirements, and how to start working with Cisco Spaces.
Chapter 3	Cisco Spaces Home	Provides information about about Cisco Spaces dashboard and its features.
Chapter 4	Cisco Spaces: SEE License Apps	Provides information about Cisco Spaces apps tied to SEE license.
Chapter 5	Cisco Spaces: ACT License Apps	Provides information about Cisco Spaces apps tied to ACT license.
Chapter 6	Cisco Spaces: SMART_OPERATIONS License Apps	Provides information about Cisco Spaces apps tied to SMART_OPERATIONS license.
Chapter 7	Cisco Spaces: SMART_VENUES License Apps	Provides information about Cisco Spaces apps tied to SMART_VENUES license.
Chapter 8	Location Hierarchy in Cisco Spaces	Provides information about how to define Cisco Spaces location hierarchy.
Chapter 9	Location Hierarchy 2.0 in Cisco Spaces	Provides information about Location Hierarchy 2.0 and its features in Cisco Spaces.
Chapter 10	Integration	Describes how to integrate with Cisco Catalyst Center (formerly known as Cisco DNA Center) and Service Now and other applications.
Chapter 11	Monitor	Provides information about the app details mentioned in the Monitoring section.
Chapter 12	Admin Management	Provides information about how to manage Cisco Spaces users, Cisco Spaces accounts, and Cisco Connected Mobile Experiences (CMX) accounts.
Chapter 13	Setup	Describes how to setup Wireless Network, Cisco Meraki Camera, Locations 7 Maps, Sensors, Data Export and other available features.

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 3](#)
- [Cisco Spaces Compatibility Matrix, on page 4](#)

System Requirements

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

Table 3: System Requirements

Item	System Requirements
Operating System	<ul style="list-style-type: none">• Microsoft Windows XP or a later version• macOS X 10.6 or a later version
Browser	Windows OS <ul style="list-style-type: none">• Firefox Version 30 or a later version• Chrome Version 34 or a later version• Safari Version 5.1.7 or a later version macOS <ul style="list-style-type: none">• 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 <i>Guidelines for Cisco Wireless Software Release Product Bulletin</i> 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)	<ul style="list-style-type: none"> • 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, see the [Cisco Spaces IP Addresses, on page 3](#).



Note For a default Cisco Unified Wireless Network installation, ports 80 and 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.

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 includes:

- **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, see [Cisco Software Licensing Guide](#).

For more information about enabling Cisco Smart License in Cisco Spaces, see [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)	<ul style="list-style-type: none"> Cisco Wireless Controller Native Cloud Connector - 8.3 or a later version (except 8.3.102 for Presence) <p>Note 8.3 is End-of-Life (EOL). We recommend that you migrate to one of the recommended releases as per the <i>Guidelines for Cisco Wireless Software Release Product Bulletin</i> at:</p> <p>https://www.cisco.com/c/en/us/products/collateral/wireless/wireless-controllers/bulletin-c25-738147.html</p> <ul style="list-style-type: none"> 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 3375 Appliance is not supported.

Compatibility Matrix for Location Service

For detailed information about Location Service compatibility matrix, see [Compatibility Matrix for Location Service](#).

Compatibility Matrix for Cisco Spaces: IoT Service (Wireless)

For detailed information about Cisco Spaces: IoT Service (Wireless) compatibility matrix, see, [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 10](#)
- [Cisco Spaces License Packages, on page 11](#)
- [Log In, on page 12](#)
- [Single Sign-On for Cisco Spaces, on page 13](#)
- [Start Working with Cisco Spaces, on page 15](#)
- [Idle Timeout for Cisco Spaces, on page 17](#)
- [Migrate Data from Cisco Prime Infrastructure to Catalyst Center, on page 17](#)
- [Cisco Spaces Documentation, on page 17](#)

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. It covers various verticals of business such as retail, manufacturing, hospitality, healthcare, education, financial services, enterprise workspaces, and so on. Cisco Spaces also provides solutions for monitoring and managing the assets in your premises.

The following are the major features of Cisco Spaces:

- A common platform for managing visitor engagements, assets and resources, and beacons.
- A single setup section to complete all the platform setups.
- Support to display promotions and offers to the customers connecting to your SSIDs.
- Support to target the customers individually or as a group based on their location, tag, visit frequency, visit duration, and so on using rules.
- Support to engage with multiple wireless networks simultaneously.
- Provision to view your business performance.
- App to create captive portals, and to display them to the customers based on rules.
- App to send notifications to the customers when they are in your business premises.

- App to inform the employees when customers are near your business premises.
- App to group the customers, and create tags.
- Provision to add third party partner apps.
- Support to import location hierarchy in the same structure as in your wireless network.
- Provision to create Cisco Spaces users with different privileges and location access.
- Provision to monitor the performance status of Cisco Spaces and its apps and latencies.

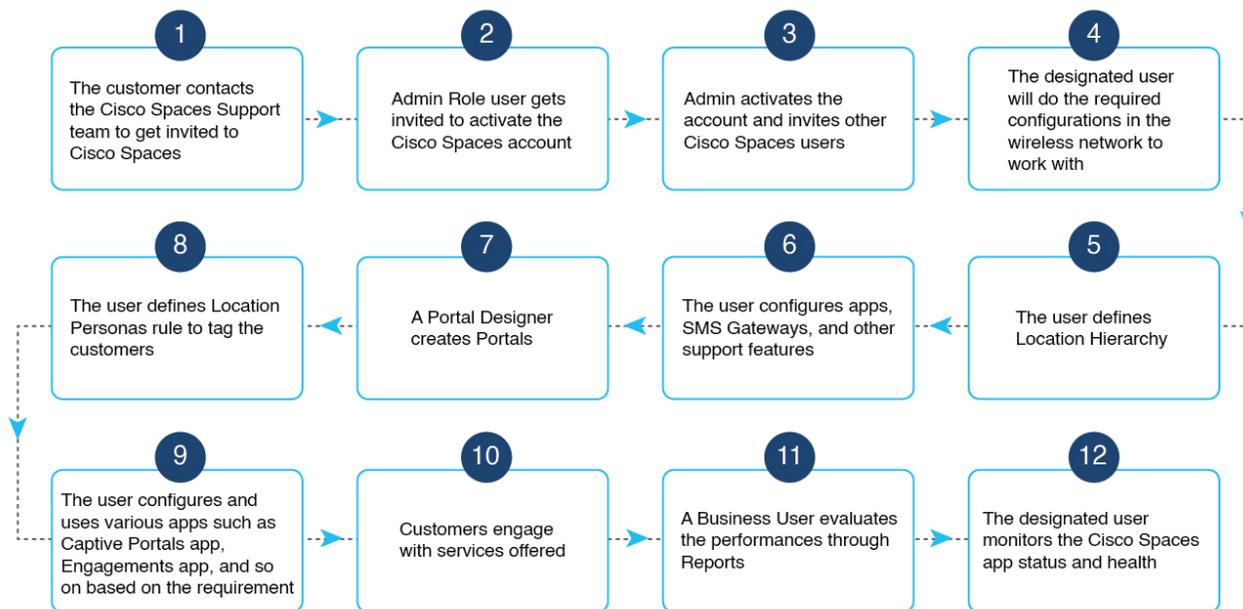
In the ABC shopping mall, to get free Wi-Fi, the customers must connect to an SSID once they enter the mall. ABC wanted to provide a personalized experience to each customer who connects to the Wi-Fi based on their purchase history and visit frequency. After installing Cisco Spaces, ABC could collect 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 1: Process Flow for Cisco Spaces



Cisco Spaces License Packages

The Cisco Spaces License package supports the following six licenses:

- **SEE**: This is the basic license version for Cisco Spaces.
- **ACT**: This license works based on the number of Access Point (AP) provisioned for the Cisco Spaces account. The number of APs used in the Location Hierarchy are considered as the license count.
- **EXTEND**
- **SMART_OPERATIONS**: This license works in the same way as the existing **SEE** license with some additional entitlements. The **SMART_OPERATIONS** license includes all the access privileges under the **SEE** license along with access to the following apps:
 - Asset Locator
 - IoT Explorer
- **SMART_VENUES**: This license works in the same way as the existing **SEE** license with some additional entitlements. The **SMART_VENUES** license includes all the access privileges under the **SEE** license along with access to the following apps:
 - Captive Portals
 - Engagements
 - Location Personas
 - Profile Rules
- **SPACES UNLIMITED**: Cisco Spaces accounts with **UNLIMITED** license include all the entitlements similar to an existing **ACT** license.

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.

Cisco Spaces is available in the following six license packages namely,

The features available for your account depends on the type of Cisco Spaces license package you own. In the Cisco Spaces dashboard, the apps are displayed based on the license type for which they will be available.

For information about features included in the Cisco Spaces See, Extend, and Act licenses, see the [Cisco Spaces Data Sheet](#).



Note Cisco Spaces users can now choose any of these licenses for a location using the **Split License** feature.

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

For more information about CCI, see [Login and Account Help](#).

Step 1 Go to [Cisco Spaces](#) and click **Login**.

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.

Step 2 In the **Email** field, enter your Cisco Spaces account email ID and click **Continue**.
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 Cisco Spaces pop-up window, from the **Select Customer** drop-down list, select a customer.

Step 7 Click **Proceed**.

Cisco Spaces dashboard window is displayed.

Note

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

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.

To enable SSO for your Cisco Spaces account, you will need to provide the following information to the Cisco Spaces [support team](#):

- 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:

Unit Dashboard Admin Role: Provides full admin permission to the List user for the selected account

bullet
5

Unit 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.

-
- 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/login>
 - CallBack URL from your IDP to Cisco Spaces: <https://dnaspaces.io/api/tm/v1/account/login/callback>

You need to configure your IDP metadata to return the **firstName**, **lastName** and **email** fields as below:

```
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 [Cisco Spaces Prerequisites](#) mentioned in [System Requirements](#), on page 1.



Note Initially, you must contact 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.

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

Step 1 Log in to Cisco Spaces.

Note You can enable Single Sign-On for Cisco Spaces. For more information see, [Single Sign-On for Cisco Spaces](#), on page 13.

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, see [Configuring Cisco Meraki for Cisco Spaces](#).
- **Cisco Unified Wireless Network with Cisco CMX**: For connecting Cisco Spaces with Cisco AireOS Controller through Cisco CMX, see [Connecting Cisco Spaces to Cisco Wireless Controller through Cisco CMX](#), on page 49.
- **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, see 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 61](#) section.
- **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, see [Connecting Cisco Spaces to Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller using Cisco Spaces: Connector, on page 79](#).
- **Using Cisco Embedded Wireless Controller:** For configuring a Cisco Unified Wireless Network using Cisco Embedded Wireless Controller, see [Configuring Mobility Express to work with Cisco Spaces, on page 80](#).

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, see [Managing Cisco Spaces Users, on page 347](#).
- Step 4** Import the location hierarchy defined in your wireless network to Cisco Spaces. For more information on configuring the location hierarchy, see [Location Hierarchy in Cisco Spaces](#).
- 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, see the “SSIDs” section.
- Step 6** Define Location Personas Rules to tag customers. For more information on creating a Location Personas Rule, see 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, see 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, see 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, see 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, see 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.

Support to Change Password after Expiry Date

Cisco Spaces allows you to change your password even after your password is expired. After entering your credentials when you click the **Continue** button, a pop-up window to change the password appears.

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.

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.

You can also view the documentation, announcements, deployment guides, use cases and support information from the **Spaces LaunchPad** section. To do this, click the **Spaces LaunchPad** icon that is available at the bottom-right in Cisco Spaces UI.



PART **III**

Cisco Spaces Home

- [Cisco Spaces Dashboard, on page 21](#)
- [Cisco Spaces: Apps, on page 35](#)
- [Partner App Management, on page 41](#)
- [Configuring Cisco Wireless Controllers and Cisco Catalyst 9800 Series Controllers for Cisco Spaces, on page 45](#)
- [Configuring Cisco Meraki for Cisco Spaces, on page 91](#)



CHAPTER 3

Cisco Spaces Dashboard

- [Cisco Spaces Navigation, on page 21](#)
- [Cisco Spaces Dashboard, on page 21](#)
- [Cisco Spaces Features, on page 24](#)
- [User Profile, on page 27](#)
- [Viewing Cisco Spaces Account Details, on page 28](#)
- [Cisco Smart License, on page 29](#)

Cisco Spaces Navigation

When you login to Cisco Spaces dashboard, the Cisco Spaces apps are displayed on the Cisco Spaces Home page. The apps are displayed under the license type for which they are available. You can access other features of Cisco Spaces such as **Location Hierarchy**, **Monitor**, **Admin Management**, and **Setup** using the three-line menu icon displayed at the top-left of the Dashboard. You can navigate to the Home page by clicking **Cisco Spaces** displayed at the top-left of the dashboard or using the **Home** option the three-line menu.

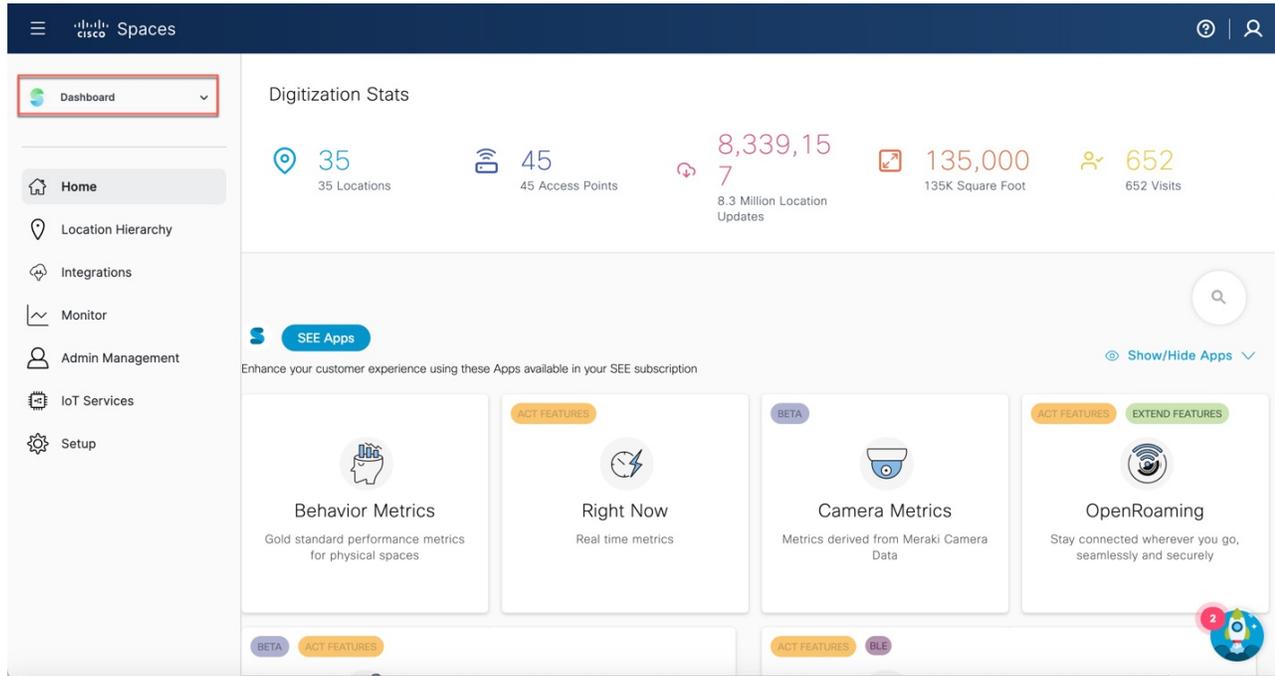
An app launcher (Grid) icon appears at the top-right of the dashboard using which you can easily navigate from one app to another app. When you click the app launcher icon, it lists all the Cisco Spaces apps activated for the user. From an app you can navigate to the home page by clicking **Cisco Spaces** displayed at the top-left of the dashboard.

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 2: 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, Digitization Stats and various applications available as per your subscription.

Menu Bar

Click the **Menu** icon () at the left of the menu bar to access the following menu items:

- App Search - **Dashboard** drop-down list
- Location Hierarchy
- Integrations
- Monitor
- Admin Management
- IoT Services
- Setup

Icons

Click the icons at the right 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 Information > License Units Consumed . For more information, see User Profile, on page 27 .

Apps Search

This app search option is available in the left navigation pane in the **Dashboard** drop-down list. The **Dashboard** drop-down list displays all the applications that are available in your Cisco Spaces subscription.

Digitization Stats

The Cisco Spaces dashboard displays the cumulative statistics values for locations, APs, location updates from your network and location visits.

The information in the **Digitization Stats** section displays as a single row.

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.

OpenRoaming SDK Profile

Cisco Spaces now supports configuration of OpenRoaming Wi-Fi profile using the **Menu** () **Integrations > Cisco Spaces SDK > Configure Profile** window. You can create a customer specific profile for a particular tenant based on the values you provide in the **Configure Profile** window.

Prior to this enhancement, the profile used to be updated manually in the backend.

Cisco Spaces Features

The major features of Cisco Spaces dashboard includes:

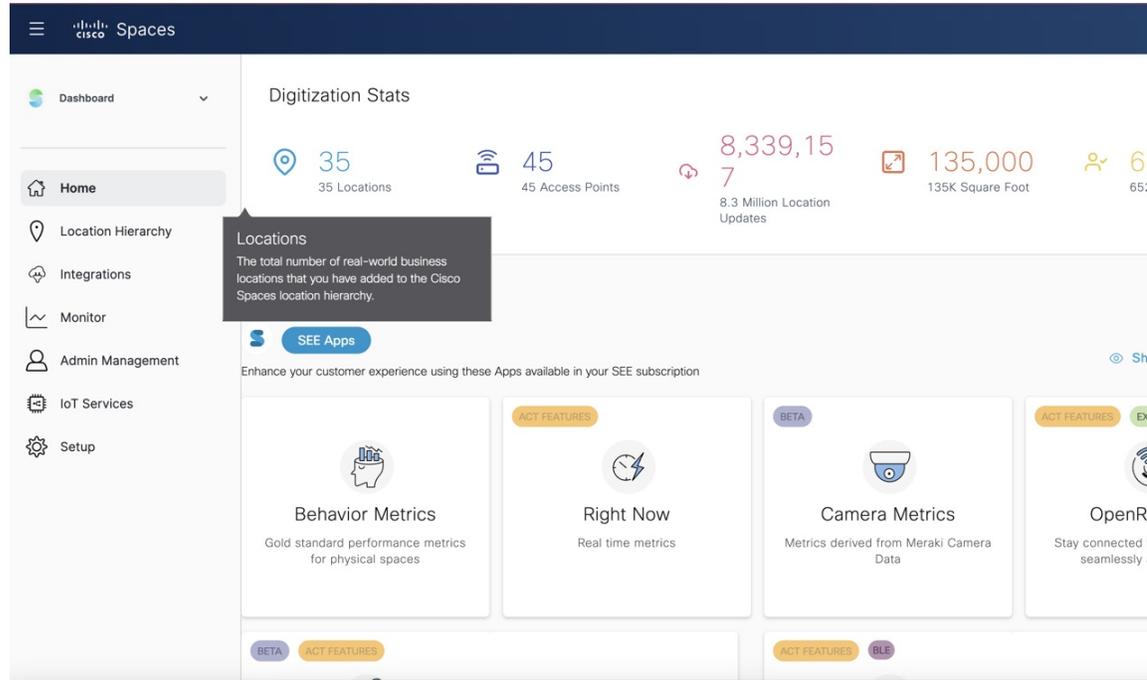
Digitization Stats

In the Cisco Spaces dashboard, the **Digitization Stats** area displays the following cumulative statistics values. You can view the **Digitization Stats** as a single row.

- **Locations:** The total network locations configured in Cisco Spaces for various wireless networks.
- **Access Points:** The total number of APs added to Cisco Spaces
- **Location Updates:** The total number of location updates received from the wireless networks from the date of deployment of Cisco Spaces.
- **Square Foot:** The total area configured for network locations in the **Location Info** option in Location Hierarchy . However, if total area is not configured for network locations in the Location Hierarchy, then the Square Foot value will be displayed based on number of APs.
- **Visits:** The total number of visits (including repeated visits of unique visitors) that occurred in your business locations from the date of deployment of Cisco Spaces.

**Note**

- If a location is removed from the location hierarchy, the corresponding **Location Updates** and the **Visits** counter values are still retained in the **Digitization Stats** area.
- You can now click or hover your cursor on any counter to view the tooltip with the corresponding information.
- If data is not available for the counters, the tooltip displays a warning message as shown in the following image:



Overview of Cisco Spaces Apps

In the Cisco Spaces Home page, you can view all available applications. Use the **Dashboard** drop-down list to search apps.

The apps available in Cisco Spaces are tied to various **Cisco Spaces License Packages**. In the Cisco Spaces home page, you can view the app tiles segregated according to your Cisco Spaces account license.

The following apps are available under **SEE** license:

- Behavior Metrics
- Right Now
- Camera Metrics
- OpenRoaming
- Location Analytics
- Detect and Locate

- Impact Analysis

The following apps are available under **ACT** license:

- Proximity Reporting
- Space Manager
- Space Experience

The following apps available under **SMART OPERATIONS** license:

- Asset Locator
- IoT Explorer

The following apps are available under **SMART VENUES** license.



Note For a Cisco Spaces account tied to **SMART VENUES** license, all apps under **SEE** license is available.

- Captive Portals
- Engagements
- Location Personas

The following apps are available under **EXTEND** license:

- IoT Device Marketplace

Location Hierarchy

The Location Hierarchy feature enables you to define your business locations in Cisco Spaces. You can import the locations in the same structure in which they are defined in your wireless network. The apps such as **Engagements**, **Captive Portals**, and **Location Personas Rules** depend on the location hierarchy defined. Cisco Spaces provides universal account, and you can add the locations of multiple wireless networks to the location hierarchy.

The APs that you can add to the location hierarchy depends on the type of Cisco Spaces license you own.

For more information, see “Location Hierarchy in Cisco DNA Spaces”.

Monitor

The Monitor section enables you to monitor the performance status of Cisco Spaces, and its apps. It also displays the app latencies and anomalies. For more information, see the “Monitoring” section.

Admin Management

The **Admin Management** feature enables you to create Cisco Spaces users. You can restrict the privileges for each user based on their role. For more information, see the “Managing Cisco DNA Spaces Users and Accounts” section.

Setup

Wireless Networks and Camera

Wireless Network

Displays features and instructions to connect Cisco Spaces to a particular wireless network through various methods. For more information, see [Setting Up Cisco Spaces to Work with Various Wireless Networks](#).

Camera

Displays features and instructions to configure Cisco Meraki Camera to work with Cisco Spaces.

Map Service

Map Service enables you to upload the map of locations for Cisco CMX tethering.

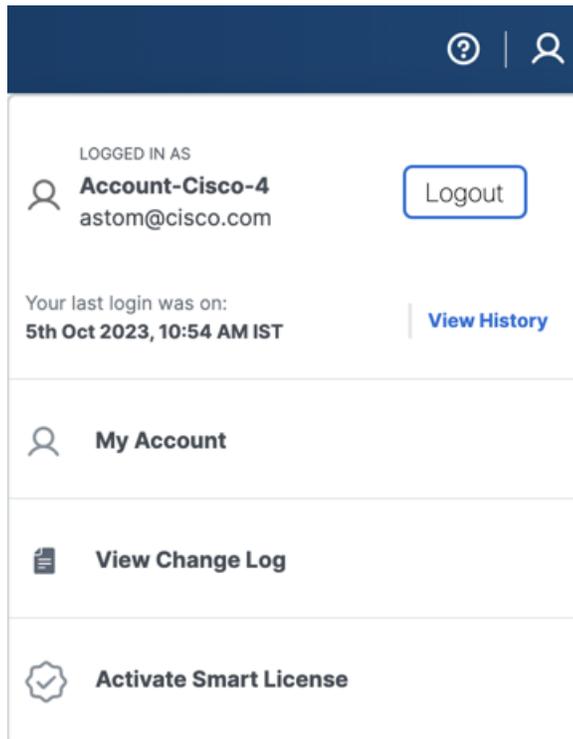
Wireless Network Status

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.

User Profile

The **User Profile** option () in the top-left of the Cisco Spaces dashboard helps to view account, smart licenses and logout options.

Figure 3: User Profile



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

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

- **My Account:** Click to display the **My Account** window. For more information, see [Viewing Cisco Spaces Account Details, on page 28](#).
- **View Change Log:** Click to open the **Change Log** tab that displays the activity details of all the users in a particular account. For more information, see [Viewing Cisco Spaces Account Details, on page 28](#).
- **Activate Smart License:** Click to activate Smart License. For more information, see [Activate Smart License, on page 29](#).

Viewing Cisco Spaces Account Details

Use the **My Account** window to view the Cisco Spaces profile details, account activity, and other account related information. 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 the failed attempt account activity details such as IP address, date and browser in which the account activity failed.
- **License Information:** 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 the change log details such as user activity, time, app, section and user. Click the **Filter** option to filter log details.

Cisco Smart License

Cisco Smart License is a flexible licensing model that streamlines the way you activate and manage software. The solution allows you to easily track the status of your license and software usage trends.

Smart License support in Cisco Spaces allows you to view and manage Cisco Spaces software license for your Cisco Smart Account. To enable Cisco Smart License in Cisco Spaces, you must have a smart account that is configured with Cisco Smart Software Manager (CSSM). In the Cisco Spaces dashboard, choose **Profile Icon** > **Activate Smart License** to activate Cisco Smart License.

You can also activate Cisco Smart License from **My Accounts** > **License Information** tab.

**Note**

To enable smart licenses in Cisco Spaces, you must have a smart account configured with Cisco. For more information about Cisco Smart License, see [Smart Software Licensing](#).

Activate Smart License

- Step 1** Log in to [Cisco Spaces](#).
- Step 2** In the Cisco Spaces dashboard, choose **Profile Icon** () > **Activate Smart License**. The **Terms and Conditions** window is displayed.
- Step 3** Read the terms and condition statements and click **Accept Terms and Conditions**. The **Smart License Configuration** window is displayed.
- Step 4** Click the **Yes, I have** radio button if you already have an account in the Cisco Smart Software Manager (CSSM).

If you do not have an account in the CSSM, click the **No, I don't have** radio button and proceed to view the instructions to create an account in CSSM.

Step 5 Click **Next**.

Step 6 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.

Step 7 Click **Next** after you have generated the token.

Step 8 In the **Product Instance Token** field, paste the generated token.

Step 9 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 **My Accounts** window under **License Information** tab.

- Note**
- After the Cisco Smart License activation, you can 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 or downgrade the Cisco Spaces license. To do this, choose **Profile Icon > License Info > Select License Level**. For more information, see [Update License Information, on page 30](#).

Update License Information

Use the **License Information** tab in the **My Accounts** window to manage your Cisco Spaces licenses. The following licenses are available:

- Cisco Spaces See
- Cisco Spaces Act
- Cisco Spaces Extend
- SMART OPERATIONS
- SMART VENUES
- SPACES UNLIMITED

You can renew authorization and registration, re-register and de-register Cisco Spaces smart licenses.

Step 1 Log in to [Cisco Spaces](#).

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

The **My Account** window is displayed.

Step 3 Click the **License Information** tab.

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

Figure 4: License Usage

The screenshot displays the Cisco Spaces user interface for license management. The user is logged in as '13may_cicd'. The 'License Information' tab is active, showing the current license tier as 'ACT'. A table titled 'LICENSE USAGE' provides a summary of device and location counts: 5 Access Points, 0 Webex Devices, 15 Meraki Cameras, 42 Locations, and 0 Building Units. The compliance status is 'OutOfCompliance'. Below this, the 'SMART SOFTWARE LICENSE' section indicates the license is 'Registered' as of 07-Jul-2023, but the overall 'License Compliance' is 'Out of Compliance'.

Step 4 To upgrade or downgrade the license, click **Change**.

The **Select License Level** window is displayed. Your current plan is indicated by a green tick mark. The upgrade or downgrade possibilities are also indicated in the **Select License Level** window.

The 'Select License Level' dialog box presents four options for license tiers. The 'UNLIMITED' tier is currently selected, indicated by a green checkmark. The tiers are:

- EXTEND**: View and understand realtime and historical behavior of people & assets in your properties through our analytics apps suite.
- UNLIMITED**: This plan will convert your devices to SQFT metering. Our top tier Package that includes everything in Spaces from all license types including our Smart workspaces offering.
- SMART_VENUES**: View and understand realtime and historical behavior of people & assets in your properties through our analytics apps suite.
- SMART_OPERATIONS**: View and understand realtime and historical behavior of people & assets in your properties through our analytics apps suite.

- Select the plan you would like to upgrade or downgrade.
A warning message is displayed with license upgrade or downgrade information.
- Check the **I accept the terms and conditions** checkbox to proceed.
- Click **Change Plan**.
A success notification message is displayed.
- To view the latest license details, click **Login** and log in to Cisco Spaces.

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

Figure 5: Smart Software

SMART SOFTWARE LICENSE
To view and manage Cisco Spaces software license for your Cisco Smart Account, go to Smart Software Manager

SMART LICENSE STATUS Actions

Registration Status: Registered
07-Jul-2023

License Compliance: Out of Compliance

ACCOUNT DETAILS

Smart Account Name: [REDACTED]
Virtual Account: [REDACTED]
Product Instance Name: [REDACTED]

ACCESS POINT INFORMATION Last updated: 0 mins ago Refresh

Active APs
44

Smart License Usage

License (version)	Description	Count	Status	Expiry Date
Cisco Spaces ACT Cloud (1.0)	Cisco Spaces ACT Cloud	44	Out of Compliance	04-Dec-2023

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.

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

- **Renew Authorization:** Click to renew Cisco Spaces smart license authorization.

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 to reflect in Cisco Spaces.

- **Renew Registration:** Click to renew Cisco Spaces smart license registration.

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.

- 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.

- **De-register:** Click to de-register Cisco Spaces smart license in the 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.

Step 8 In the **Access Point Information** 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:** Displays the license version.
 - **Description:** Displays the license description.
 - **Count:** Displays the number of active access points.
 - **Status:** Displays the license status.
 - **Expiry Date:** Displays the expiry date of the smart license.
-



CHAPTER 4

Cisco Spaces: Apps

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

In Cisco Spaces, apps are available as per the following license subscriptions:

- SEE
- ACT
- SMART_OPERATIONS
- SMART_VENUES
- SPACES UNLIMITED
- EXTENT
- [Overview of Cisco Spaces Apps, on page 35](#)
- [Cisco Spaces: SEE License Apps, on page 36](#)
- [Cisco Spaces: ACT License Apps, on page 37](#)
- [Cisco Spaces: SMART_OPERATIONS Apps, on page 37](#)
- [Cisco Spaces: SMART_VENUES Apps, on page 38](#)
- [Partner Apps, on page 39](#)
- [IoT Device Marketplace Application, on page 39](#)

Overview of Cisco Spaces Apps

In the Cisco Spaces Home page, you can view all available applications. Use the **Dashboard** drop-down list to search apps.

The apps available in Cisco Spaces are tied to various **Cisco Spaces License Packages**. In the Cisco Spaces home page, you can view the app tiles segregated according to your Cisco Spaces account license.

The following apps are available under **SEE** license:

- Behavior Metrics
- Right Now
- Camera Metrics
- OpenRoaming

- Location Analytics
- Detect and Locate
- Impact Analysis

The following apps are available under **ACT** license:

- Proximity Reporting
- Space Manager
- Space Experience

The following apps available under **SMART OPERATIONS** license:

- Asset Locator
- IoT Explorer

The following apps are available under **SMART VENUES** license.



Note For a Cisco Spaces account tied to **SMART VENUES** license, all apps under **SEE** license is available.

- Captive Portals
- Engagements
- Location Personas

The following apps are available under **EXTEND** license:

- IoT Device Marketplace

Cisco Spaces: SEE License Apps

In Cisco Spaces, **SEE** subscription is the basic license version. The apps available under **SEE** subscription are:

- **Behaviour Metrics:** The **Behavior Metrics** 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.
- **Right Now:** The **Right Now** app provides you the Right Now report that shows the details of visitors currently present at your locations. Using the **Right Now** 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.
- **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.

- **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.
- **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, see [Cisco Spaces Detect and Locate Configuration Guide](#).
- **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.

Cisco Spaces: ACT License Apps

In Cisco Spaces, **ACT** subscription is the basic license version. The apps available under **ACT** subscription are:

- **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, see [Cisco Spaces Proximity Reporting 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.

Cisco Spaces: SMART_OPERATIONS Apps

In Cisco Spaces, **SMART_OPERATIONS** subscription works in the same way as the existing **SEE** license with some additional entitlements. The **SMART_OPERATIONS** license includes all the access privileges under the **SEE** license along with access to the following apps:

- **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, see [Cisco Spaces Asset Locator Configuration Guide](#).
- **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**, see [Cisco Spaces IoT Services Configuration Guide](#).

Cisco Spaces: SMART_VENUES Apps

In Cisco Spaces, **SMART_VENUES** the subscription works in the same way as the existing **SEE** license with some additional entitlements. The **SMART_VENUES** license includes all the access privileges under the **SEE** license along with access to the following apps:

- **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, see [Create or Modify Tags, on page 263](#).

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, see [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 **ACT** license users. For the **SEE** 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.



CHAPTER 5

Partner App Management

- [Overview of App Center, on page 41](#)
- [Activate an App, on page 42](#)

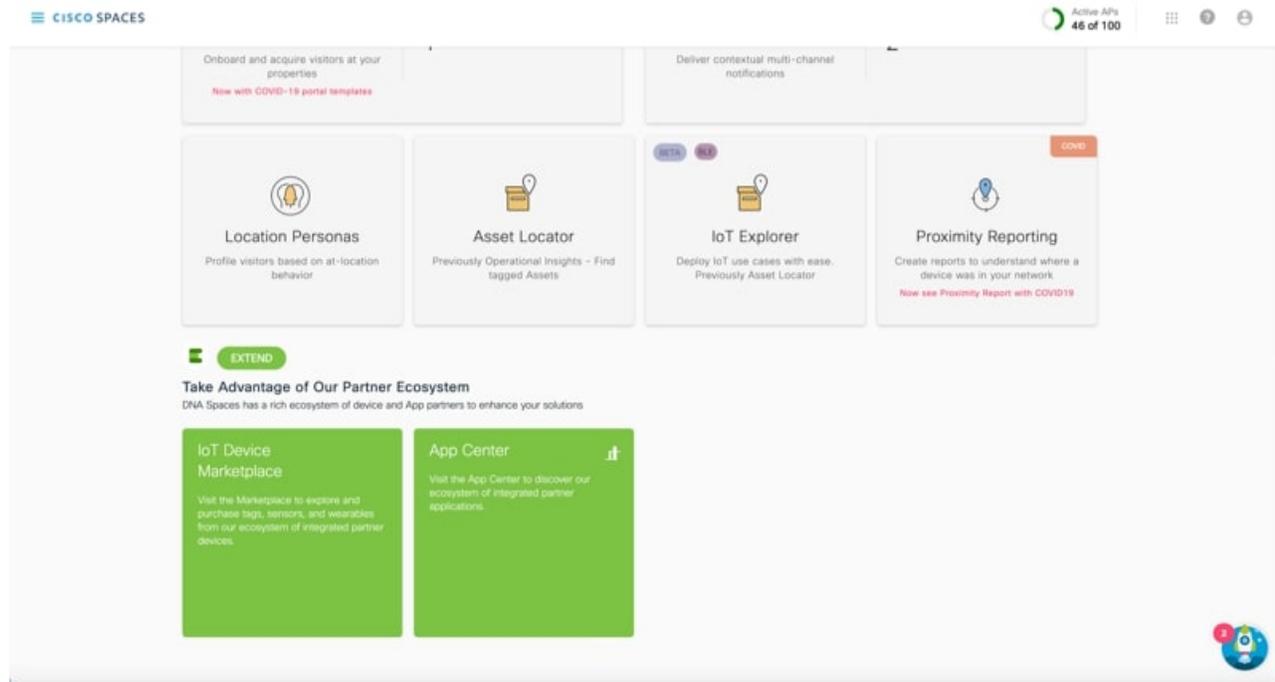
Overview of App Center

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 only available for Cisco Spaces Extend licenses.

Figure 6: 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, see [Overview of the Cisco Spaces - Partner Ecosystem](#) online help.

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 **App Center** in Cisco Spaces - Dashboard.

You must activate the app from **App Center** 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 Firehose APIs. These APIs checks for the device status and then events are triggered accordingly. For more information, see [Firehose API](#).

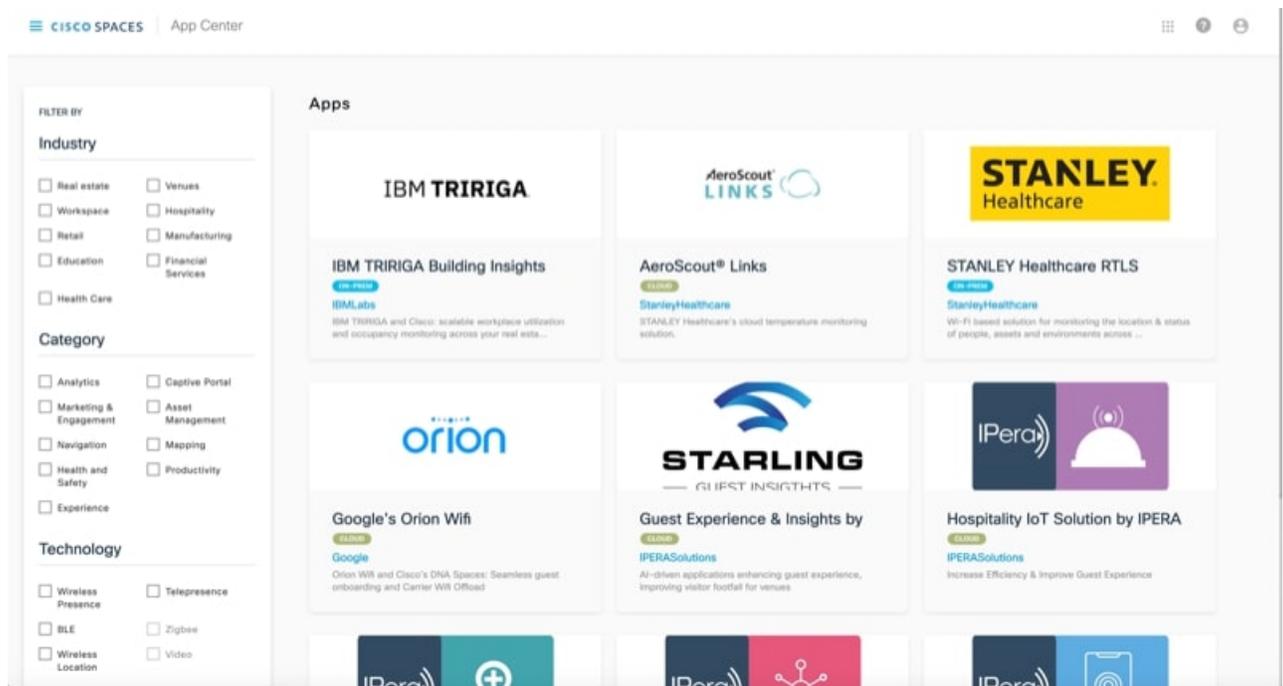
When a Cisco Spaces partner adds a new event to an already activated app, it will be sent through Firehose APIs only when the customer subscribes to the new event by accepting the permissions. Prior to this enhancement, customer permission was not required for new events.

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.

Step 1 In the Cisco Spaces dashboard, click **App Center**.

The App Center 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 7: 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 Cisco Wireless 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 46](#)
- [Connecting Cisco Spaces to Cisco Wireless Controller through Cisco CMX, on page 49](#)

- [Connecting Cisco Catalyst 9800 Series Wireless Controller or Cisco Wireless Controller to Cisco Spaces Using WLC Direct Connect or Cisco Spaces: Connector, on page 61](#)
- [Cisco Spaces Scale Benchmark, on page 90](#)

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 6: Connectors-Feature Support

Features/Apps	Cisco Spaces Connector	Cisco WLC Direct Connect (Recommended only for small scale deployments) ¹	Defining the Location Hierarchy for Cisco AireOS/ Cisco Catalyst Wireless Controller with Cisco CMX	Wired Devices	Configuring Cisco Meraki for Cisco Spaces
		Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect Connecting Cisco Spaces to Cisco Catalyst 9800 Series Wireless Controller Using Cisco WLC Direct Connect			
Cisco Spaces Dashboard	Supported	Supported	Supported	Not Supported	Supported
Captive Portals	Cisco Spaces: Captive Portal App	Cisco Spaces: Captive Portal App	Cisco Spaces: Captive Portal App	Not Supported	Cisco Spaces: Captive Portal App
Engagements	Cisco Spaces: Engagements App	Cisco Spaces: Engagements App	Cisco Spaces: Engagements App	Not Supported	Cisco Spaces: Engagements App
Location Personas	Cisco Spaces: Location Personas App	Cisco Spaces: Location Personas App	Cisco Spaces: Location Personas App	Not Supported	Cisco Spaces: Location Personas App

Features/Apps	Cisco Spaces Connector	Cisco WLC Direct Connect (Recommended only for small scale deployments)¹ Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect Connecting Cisco Spaces to Cisco Catalyst 9800 Series Wireless Controller Using Cisco WLC Direct Connect	Defining the Location Hierarchy for Cisco AireOS/ Cisco Catalyst Wireless Controller with Cisco CMX	Wired Devices	Configuring Cisco Meraki for Cisco Spaces
Location Analytics	Cisco Spaces: Location Analytics App	Cisco Spaces: Location Analytics App	Cisco Spaces: Location Analytics App	Not Supported	Cisco Spaces: Location Analytics App
Impact Analysis	Cisco Spaces: Impact Analysis App	Cisco Spaces: Impact Analysis App	Cisco Spaces: Impact Analysis App	Not Supported	Cisco Spaces: Impact Analysis App
Camera Metrics	Cisco Spaces: Camera Metrics App	Cisco Spaces: Camera Metrics App	Cisco Spaces: Camera Metrics App	Not Supported	Cisco Spaces: Camera Metrics App
Behaviour Metrics	Cisco Spaces: Behavior Metrics App	Cisco Spaces: Behavior Metrics App	Cisco Spaces: Behavior Metrics App	Not Supported	Cisco Spaces: Behavior Metrics App
RightNow WiFi	Cisco Spaces: Right Now App	Cisco Spaces: Right Now App	Cisco Spaces: Right Now App	Supported	Cisco Spaces: Right Now App
RightNow Video	Cisco Spaces: Right Now App	Cisco Spaces: Right Now App	Cisco Spaces: Right Now App	Not Supported	Cisco Spaces: Right Now App
Open Roaming²	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

Features/Apps	Cisco Spaces Connector	Cisco WLC Direct Connect (Recommended only for small scale deployments) ¹ Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect Connecting Cisco Spaces to Cisco Catalyst 9800 Series Wireless Controller Using Cisco WLC Direct Connect	Defining the Location Hierarchy for Cisco AireOS/ Cisco Catalyst Wireless Controller with Cisco CMX	Wired Devices	Configuring Cisco Meraki for Cisco Spaces
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 90 .	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**, see [Cisco Spaces: OpenRoaming Configuration Guide](#).

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:

-
- 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:

-
- 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:
- 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.
 - Choose the **On Mac Filter Failure** radio button.
 - In the **Preauthentication ACL** area, from the **IPv4** drop-down list, choose the ACL previously defined.
 - 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:

- From the **HTTP Access** drop-down list, choose **Disabled**.
- From the **HTTPS Access** drop-down list, choose **Enabled**.
- From the **WebAuth SecureWeb** drop-down list, choose **Disabled**.
- 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:

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:

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:

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, see the [Create SSIDs in Cisco Wireless Controller](#), on page 50.

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, see the [Create Access Control Lists](#), on page 52.

Configure the Virtual Interface

To configure the virtual interface, perform the following steps:

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 53

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:

- 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:

- 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 ACL** area, from the **WebAuth FlexACL** 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:

-
- 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:
- In the **Access Control List Name** field, enter a name for the new ACL.
Note You can enter up to 32 alphanumeric characters.
 - 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** If you want to provide social authentication for your portal, you must also configure the wall garden ranges for social authentication. To know the wall garden ranges that you must configure for social authentication, see 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:

- Step 1** Choose **Controller > Interfaces**.
- Step 2** Click the **Virtual** link.
- Step 3** In the **Interfaces > Edit** window that appears, enter the following parameters:
- In the **IP address** field, enter the unassigned and unused gateway IP address, if any.
 - 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:

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** 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:

- 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:
- In the Cisco Wireless Controller dashboard, choose **Security > Access Control Lists**.
 - Click **More Actions** for the Access Control List configured for Cisco Spaces.
 - Click **Add Remove URL**.
 - Enter a social URL name, and click **Add**.
 - 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”.

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.

- To import the locations based on Access Point prefix, see [Importing the Locations using Access Point Prefix, on page 287](#)
- To import the locations using Map Services, see [Importing Locations to the Location Hierarchy Using Map Services, on page 289](#)

What to do next

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

- [Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication](#)
- [Configuring Cisco Wireless Controller 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 are done 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 at least 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:

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 nmosp cloud-services on Cisco Catalyst 9800 Series Controller to communicate with Cisco Spaces Cloud over HTTPS.

- a. (config)#nmosp cloud-services server url <URL>
- b. (config)#nmosp cloud-services server token <Customer JWT TOKEN>
- c. (config)#nmosp 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)#nmosp 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 nmosp 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 brief summary of active/inactive Cisco CMX cloud connections, execute the following command:

```
#show nmosp 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 nmosp 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, see [Defining the Location Hierarchy for Cisco Catalyst 9800 Series Wireless Controllers or Cisco Wireless Controller \(without Cisco CMX\)](#), on page 286.
- 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:

- Step 1** In the Cisco Spaces dashboard, configure a Cisco Catalyst SSID. For more information on configuring the SSIDs, see the [Importing the SSIDs for Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller](#) 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 wlangs, 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:

Step 1 In the Cisco Spaces dashboard, configure a Cisco Catalyst SSID. For more information on configuring the SSIDs, see the [Importing the SSIDs for Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller](#) 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:

- 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 Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller](#) 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.lidn.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 DNA 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 referring the procedure mentioned in [Cisco DNA Spaces: Connector Configuration Guide](#)
- After connecting Cisco AireOS Controller to Cisco Spaces, configure RADIUS authentication and internet provisioning as described in [Configuring Cisco Wireless Controller 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 [Cisco Spaces: Captive Portal App, on page 163](#)
- If social authentication is required for captive portal, configure social authentication as described in [Configuring Cisco Wireless Controller for Social Authentication, on page 60](#)
- If you want to send notifications using Cisco Spaces, configure the engagement rules based on the procedure mentioned in chapter [Cisco Spaces: Engagements App, on page 243](#)

Cisco Catalyst 9800 Series Wireless Controller with Cisco DNA 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 DNA 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 66](#)
 - [Configuring Cisco Catalyst 9800 Series Wireless Controller GUI \(Local Mode\) for Captive Portals and Engagements Apps, on page 70](#)
 - [Configuring Cisco Catalyst 9800 Series Wireless Controller GUI \(Flex Mode or Mobility Express\) for Captive Portals and Engagements Apps, on page 74.](#)
- 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 [Cisco Spaces: Captive Portal App, on page 163](#)
- If you want to send notifications using Cisco Spaces, configure the engagement rules based on the procedure mentioned in chapter [Cisco Spaces: Engagements App, on page 243](#)

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:

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:

-
- 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:
- In the **Server IP Address** field, enter the IP address of the radius server.
 - In the **Shared Secret** field, enter your radius secret key.
 - 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:

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	325248125252525	0.0.0.0/0.0.0.0	Any	Any	Any	Any
Permit	0.0.0.0/0.0.0.0	325248125252525	Any	Any	Any	Any
Permit	525253925252525	0.0.0.0/0.0.0.0	Any	Any	Any	Any
Permit	0.0.0.0/0.0.0.0	525253925252525	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:

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:

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:

-
- 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 Cisco 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 62.

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 80.

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:

- 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 62.

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:

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 Cisco 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 62.

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 8.10.150.0 for Cisco Spaces, perform the following steps:

- 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:
- From the **ACL Type** drop-down list, choose **IPv4**.
 - In the **ACL name** field, enter a name for the ACL.
 - Click **Add URL Rules**.
- The **Add /Edit URL ACLs** window appears.
- In the **URL** field, enter splash page URL domain.
 - From the **Action** drop-down list, choose **Permit**.
 - 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 if 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 **Management > 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:

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 Cisco 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 62.

Cisco Spaces Scale Benchmark

Table 7: 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
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 91](#)
- [Configuring Cisco Meraki for RADIUS Authentication, on page 92](#)
- [Configuring Cisco Meraki for Notifications and Reports, on page 94](#)
- [Configuring Cisco Meraki for Social Authentication, on page 94](#)
- [Manually Configuring SSIDs for Cisco Meraki, on page 95](#)
- [Configuring Scanning API in Cisco Meraki, on page 96](#)

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:

-
- 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 Meraki 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:

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:

-
- 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:

- 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:
- From the **Analytics** drop-down list, choose **Analytics is enabled**.
 - From the **Scanning API** drop-down list, choose **Scanning API enabled**.
 - 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:

- 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 8: Social Networking Domain Names

Facebook	Twitter	LinkedIn	
*.facebook.com	*.twitter.com	*.linkedin.com	
*.fbcdn.net	*.twimg.com	*.licdn.net	
*.akamaihd.net		*.licdn.com	
*.connect.facebook.net			

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:

-
- 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:
- Click **Home > Captive Portals > SSIDs** to import the Meraki SSID to Cisco Spaces. A splash page URL is generated in the Cisco Spaces Dashboard.
 - 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:

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.



PART **IV**

Cisco Spaces: SEE License Apps

- [Cisco Spaces: Behavior Metrics App, on page 99](#)
- [Cisco Spaces: Right Now App, on page 109](#)
- [Cisco Spaces: Camera Metrics App, on page 123](#)
- [Cisco Spaces: OpenRoaming App, on page 127](#)
- [Cisco Spaces: Location Analytics App, on page 129](#)
- [Cisco Spaces: Impact Analysis App, on page 143](#)



CHAPTER 8

Cisco Spaces: Behavior Metrics App

This chapter describes the Behavior Metrics app and reports.

- [Overview of Behavior Metrics, on page 99](#)
- [View the Behavior Metrics Report, on page 99](#)
- [Benchmarks, on page 101](#)
- [Report Tabs, on page 102](#)
- [Behavior Metrics \(Business Metrics\), on page 102](#)
- [Workspaces Vertical \(Behavior Metrics\), on page 105](#)
- [Education Vertical \(Behavior Metrics\), on page 107](#)
- [Pin a Location, on page 108](#)

Overview of Behavior Metrics

The **Behavior Metrics** 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 **Behavior Metrics** 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 Behavior Metrics Report

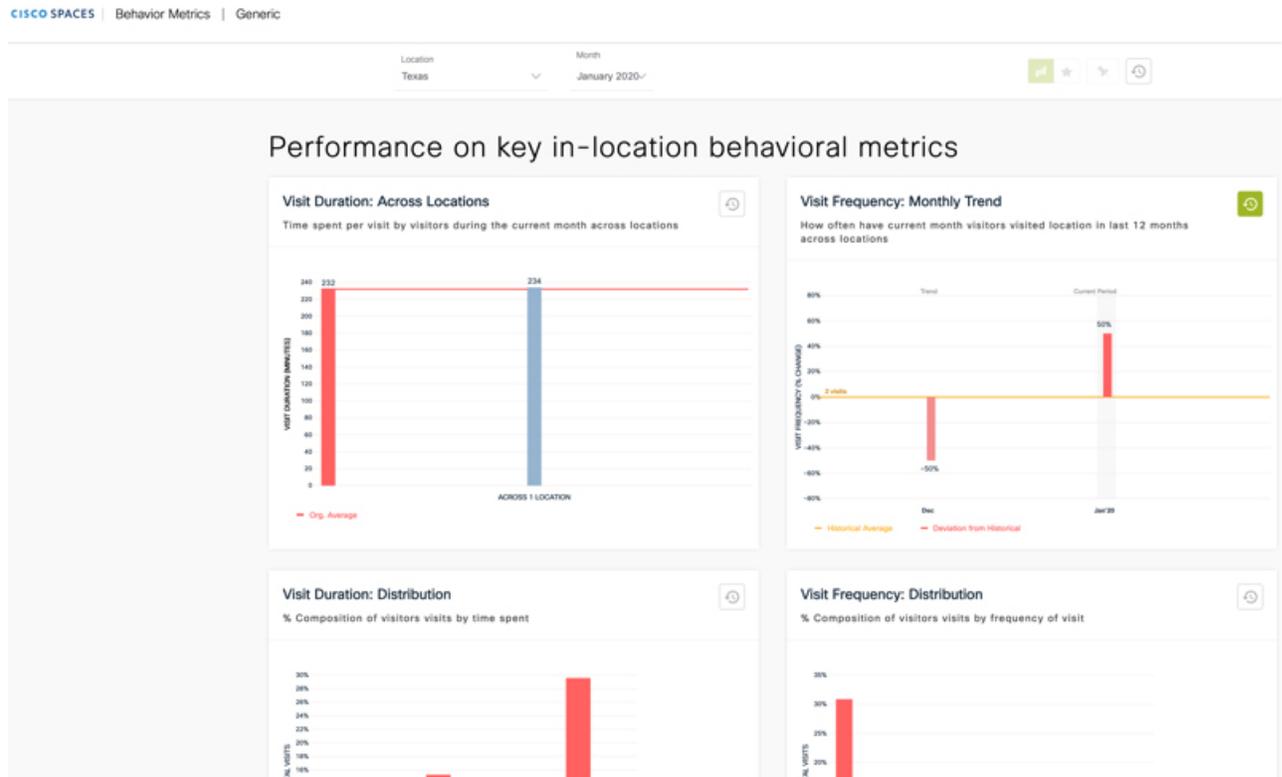
In the Behavior Metrics app, a minimum of 100 visits at each location level is required to display the chart data. Hence, only those locations with a significant amount of visit data are considered for visualisation in the charts.

To view the various reports in the Behavior Metrics app, perform the following steps:

Step 1 In the Cisco Spaces dashboard, click **Behavior Metrics**.

The Behavior Metrics report is displayed.

Figure 8: Behavior Metrics Report



Step 2 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 **Behavior Metrics** at the top of the **Behavior Metrics** window. For the **Workspaces** vertical, the title **Workspaces** displays along with **Behavior Metrics**. 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 Francisco” is filtered in the location hierarchy, the “Average Visit Duration” for Cisco San Francisco 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 Behavior Metrics 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 Behavior Metrics 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.

Behavior Metrics (Business Metrics)

Performance Benchmarking: Performance on Core Metrics related to Peers



Note The Behavior Metrics report for the **Workspaces** vertical is different from the following one. For information on the Behaviour Metrics report for the **Workspaces** vertical, see [Workspaces Vertical \(Behavior Metrics\)](#), on page 105.

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 (Behavior Metrics)

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 **Behavior Metrics** 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 (Behavior Metrics)

Cisco Spaces supports a new vertical called **Education** in the **Behavior Metrics** 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 Behavior Metrics 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:

-
- Step 1** In the **Behavior Metrics** window, click the **Pin Locations**.
 - Step 2** In the **Pin Locations** window, select the locations that you want to pin.
 - Step 3** Click **Apply**.
-



CHAPTER 9

Cisco Spaces: Right Now App

This chapter describes about the **Right Now** app.

- [Right Now Overview, on page 109](#)
- [Right Now on WiFi, on page 109](#)
- [Right Now on Camera, on page 112](#)
- [Density Rules, on page 115](#)
- [Settings, on page 121](#)

Right Now Overview

The **Right Now** app provides you the Right Now report that shows the details of visitors currently present at your locations. Using the **Right Now** 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 **Right Now** 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.

Right Now on WiFi

The Right Now on WiFi 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 Right Now WiFi 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 Right Now Wifi.

The **Right Now** app is available for SEE, ACT, and EXTEND license types.

**Note**

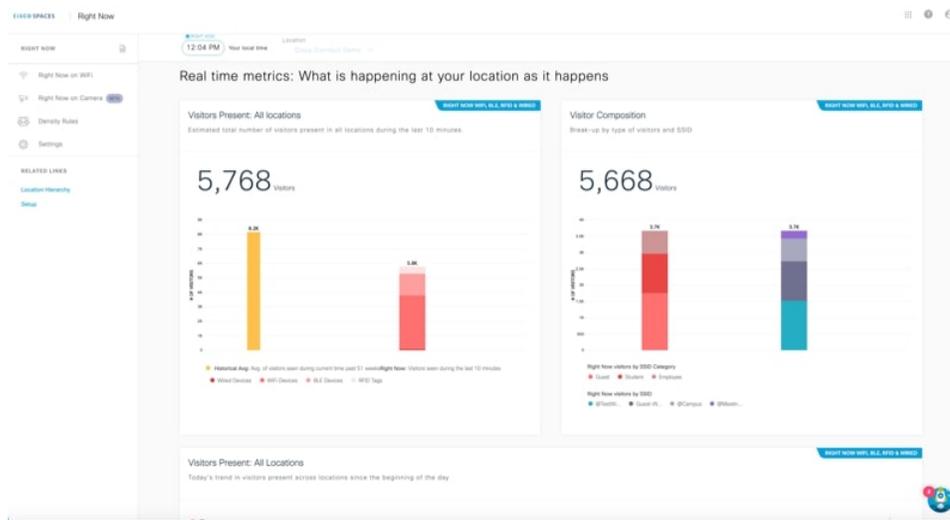
- If a location is removed or modified in the location hierarchy or timezone is changed, the existing **Presence** chart count is reset.
 - For BLE processing:
 - BLE group information should be received as part the IoT updates
 - RSSI value should be greater than -85
 - For probing devices:
 - **Cisco 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.
- For wired device processing: Contact [Cisco Spaces support](#) to configure the IP addresses for switches in the backend.

Viewing the Right Now Report

To view the Right Now report, perform the following steps:

-
- Step 1** In the Cisco Spaces Dashboard, choose **Right Now**.
The **Right Now** window appears.
- Step 2** From the **Location** drop-down list, choose the desired network location.
The Right Now report for the selected network location is displayed.

Figure 9: Right Now on Wi-Fi



The local time of your system is displayed under the **Right Now** section at the top of the report.

The Right Now report displays the following 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 see 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 Right Now report.
- The average value for the last 51 weeks is shown as historical data for each chart in the report.

Right Now on Camera

The Right Now on Camera option shows the Right Now 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, see [Setting up Cisco Spaces to Work with Cisco Meraki Camera, on page 369](#).

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 **Right Now** app is refreshed every 30 seconds and takes approximately three minutes to update the latest count on the report window.



Note The Right Now Report supports Cisco Meraki MV93 Cloud-Managed Smart Camera.

Viewing Right Now Report for Meraki Camera

To view the Right Now report for Meraki Camera, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Right Now**.
The **Right Now** window appears.
- Step 2** Click the three-line menu icon displayed at the top-left of the window, and choose **Right Now on Camera**.
The **Right Now on Camera** window appears with the Right Now report for Meraki Camera.

Figure 10: Right Now on Camera Report



Step 3 If required, from the **Location** drop-down list, choose 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 the following 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.
- **# of people present:** 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"
- **#of people present: 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. In such cases, you can pin upto three locations to view the current presence count for the locations of your choice. 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" .

Note The option to pin location will be available only if the number of locations are more than or equal to 15.

- **# 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. In such cases, you can pin upto three cameras to view the current presence count for the cameras of your choice. This graph will appear only for network, floor and zone level locations.

Note The option to pin cameras will be available only if the number of Cameras are more than Six.

- **# 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. In such cases, you can pin upto three camera zones to view the current presence count for the camera zones of your choice. This graph will appear only for network, floor and zone level locations.

Note The option to pin camera zones will be available only if the number of Camera Zones are more than Six.

- **Cumulative Footfall during the day:** Displays a line graph that shows the total footfall during each hour of the day on which the Right Now 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 current 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 you are viewing the **Right Now on Camera** 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.

- **Presence: By Location:** 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.

For information on pinning a location, camera, or camera zone, see [Pinning a Location, Camera, or Camera Zone, on page 114](#).

What to do next

You can go back to the **Right Now** report using the **Right Now on WiFi** option in the three-line menu that appears at the top-left of the window.

Pinning a Location, Camera, or Camera Zone

To pin a location, camera, or camera zone, perform the following steps:

-
- Step 1** In the **Right Now on Camera** window, click the **Pin** icon displayed at the top right of the window. The **Pin** window appears.
- Step 2** Do the following based on your requirement:
- To pin a location, in the **Pin Location** area, select the check box for the locations that you want to pin, and click **Apply**. The locations selected will be displayed in the **Pinned Locations** area. You can pin a maximum of 3 locations.

- To pin a camera, in the **Pin Cameras** area, click the **Cameras** tab, and select the check box for the cameras that you want to pin, and click **Apply**. The cameras selected will be displayed in the **Pinned Cameras** area. You can pin a maximum of 3 cameras.
- To pin a camera zone, in the **Pin Cameras** area, click the **Camera Zones** tab, and select the check box for the camera zones that you want to pin, and click **Apply**. The camera zones selected will be displayed in the **Pinned Camera Zones** area. You can pin a maximum of 3 camera zones.

Note You can search for a particular location, camera, or camera zone using the **Search** option displayed in the respective area.

Density Rules

Density Rule enables you to track the density of unique devices or visitors in your business locations. This option is available only for the **ACT** license.

The **Density Rule** option allows you to create rules that triggers 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 to send notifications through SMS, e-mail, 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:

-
- Step 1** In the Cisco Spaces dashboard, choose **Right Now**.
The **Right Now** 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 meter. 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 adjacent 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 choose "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 DNA 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 occupancy limit for each location in the [Adding the Information of a Location](#) window 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 choose "more than", "less than" or "between" from the first drop-down list, and you can manually enter the "percentage" or can choose the "percentage" 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. For more information on creating the location hierarchy, see the [Defining the Location Hierarchy](#) section.

You can again filter the locations based on the metadata defined for the selected location, or its parent or child locations. For more information on configuring the metadata for the locations, see the [Adding Metadata for a Location](#) section. You can either apply the rule for the locations with a particular metadata or exclude the locations with a particular metadata. For more information on filtering the locations, see the [Filtering by Location](#).

Step 7 In the **Schedule** area, specify the period for which you want to apply the rule.

- 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.
- 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.
- 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.

- 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 adjacent 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, see [Notification Type for a Business User, on page 258](#).

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 **Right Now** report using the **Right Now 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:

Step 1 In the Cisco Spaces dashboard, click **Right Now**.

The **Right Now** 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 triggered 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 occurred.
- **count of people:** Total number of people that were available in the location when the activity occurred
- **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:

Step 1 In the Cisco Spaces dashboard, click **Right Now**.

The **Right Now** 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 **Test Rule** icon that appears at the far right of the Density rule that you want to test.
The **Test the Rule** window displays.
- Step 5** Click **Yes** to trigger a notification on the selected channels.
A notification is triggered and a success message is displayed.
- Step 6** Click **Continue**.
-

Modifying a Density Rule

To modify a Density rule, perform the following steps:

- Step 1** In the Cisco Spaces dashboard, click **Right Now**.
The **Right Now** 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 **Edit Rule** icon that appears at the far right of the Density rule that you want to modify.
- Step 5** Make necessary changes.
- Step 6** 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:

- Step 1** In the Cisco Spaces dashboard, click **Right Now**.
The **Right Now** 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 **Pause Rule** icon that appears at the far right of the Density rule that you want to pause.
- Step 5** 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:

Step 1 In the Cisco Spaces dashboard, click **Right Now**.

The **Right Now** 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 **Make Rule Live** icon that appears at the far right of the Density rule that you want to restart.

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

Step 1 In the Cisco Spaces dashboard, click **Right Now**.

The **Right Now** 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 **Delete Rule** icon that appears at the far right of the Density rule that you want to delete.**Step 5** In the dialog box that appears, click **Delete Rule**.

The Density Rule gets deleted.

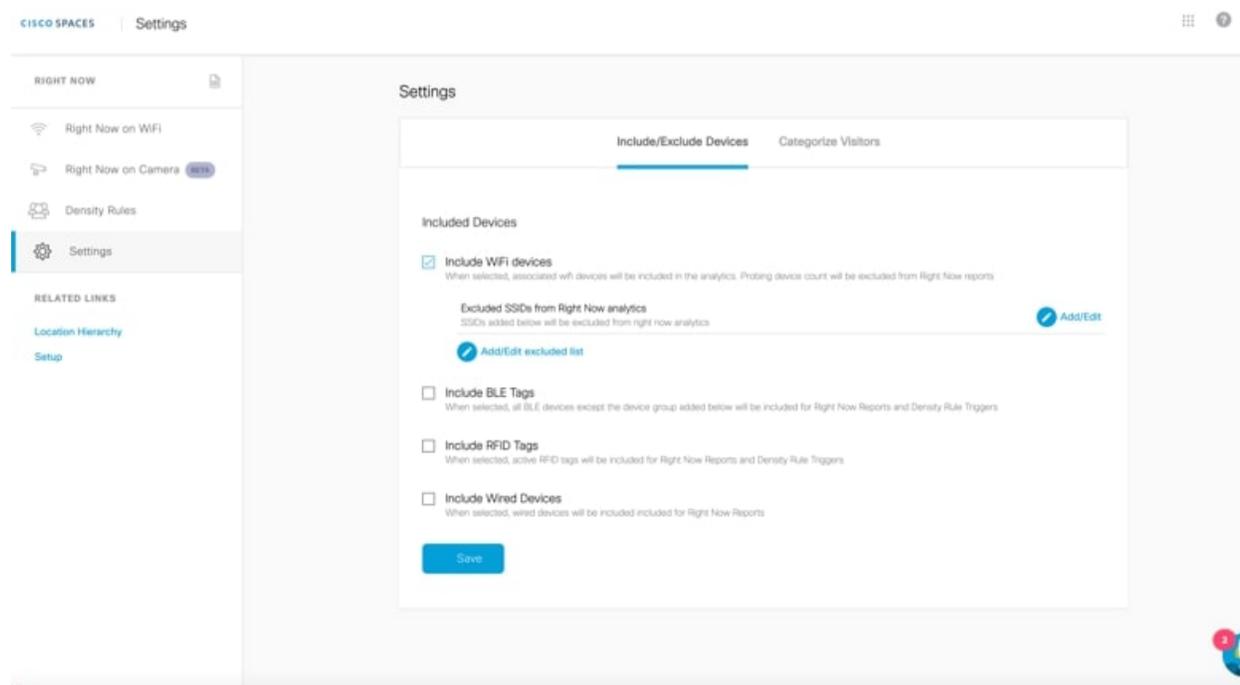
What to do next

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 **Right Now** app reports. The **Settings** menu includes the **Include/Exclude Devices** and **Categorize Visitors** tabs.

Figure 11: Right Now - 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 Right Now reports:

- Wi-Fi devices option is included by default and you cannot deselect the same.
To exclude devices connected to specific SSIDs from the Right Now analytics, click **Add/Edit** or **Add/Edit excluded list** and select the desired SSIDs from the **Exclude SSIDs** list.
- BLE Tags: To include BLE tags in the Right Now reports, select **Include BLE Tags**.
To exclude specific device groups from the Right Now 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 Right Now reports, select **Include RFID Tags**.
- Wired Devices: To include wired devices as part of active visitors in the Right Now 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 Right Now report.

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



CHAPTER 10

Cisco Spaces: Camera Metrics App

This chapter describes the Camera Metrics app.

- [Camera Metrics, on page 123](#)
- [Viewing the Camera Metrics Report, on page 124](#)

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 [Setting up Cisco Spaces to Work with Cisco Meraki Camera, on page 369](#).
- 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** data show up till the network/building locations and to view the data you must have configured the camera under these network/building locations.

Authentication Support for Camera Message Queuing Telemetry Transport (MQTT) Brokers

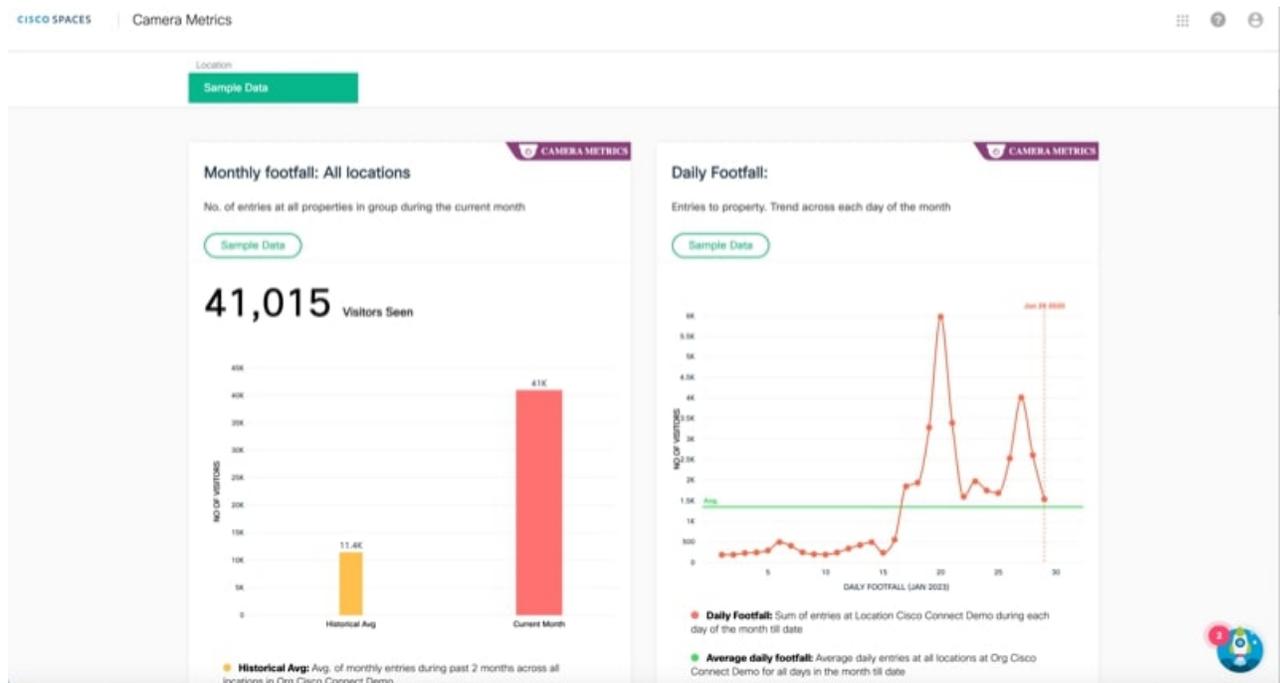
Cisco Spaces cloud is updated to support password-based authentication for receiving MQTT updates from Cisco Meraki cameras. The background network synchronization process will automatically update the authentication details to the Cisco Meraki dashboard.

Viewing the Camera Metrics Report

To view the Camera Metrics report, perform the following steps:

- Step 1** In the Cisco Spaces dashboard, click **Camera Metrics**.
The Camera Metrics report for the current month is displayed.

Figure 12: 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.



CHAPTER 11

Cisco Spaces: OpenRoaming App

- [Overview of OpenRoaming App, on page 127](#)

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, see [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 129](#)
- [View Location Analytics Report, on page 130](#)
- [Compare Reports, on page 133](#)
- [Create Custom Report, on page 134](#)
- [Add Widget, on page 138](#)
- [Share Location Analytics Custom Report, on page 141](#)

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

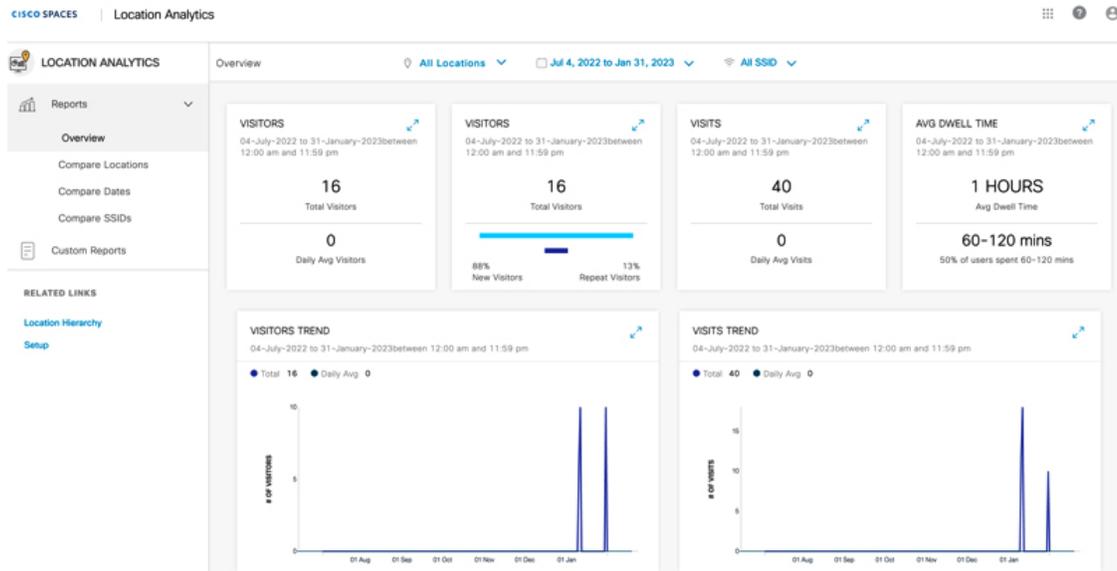
Click **Reports** on the left panel to expand the list and click **Overview** to view the reports. The **Overview** window displays visits, visitor details and dwell time distribution data in both tile and graphical format. You can click the arrow icon on the tile to view the details in graphical format.

Custom Reports

Choose **Location Analytics App > Custom Reports** to view, save and share 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, see [Compare Reports, on page 133](#).

Figure 13: 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 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.

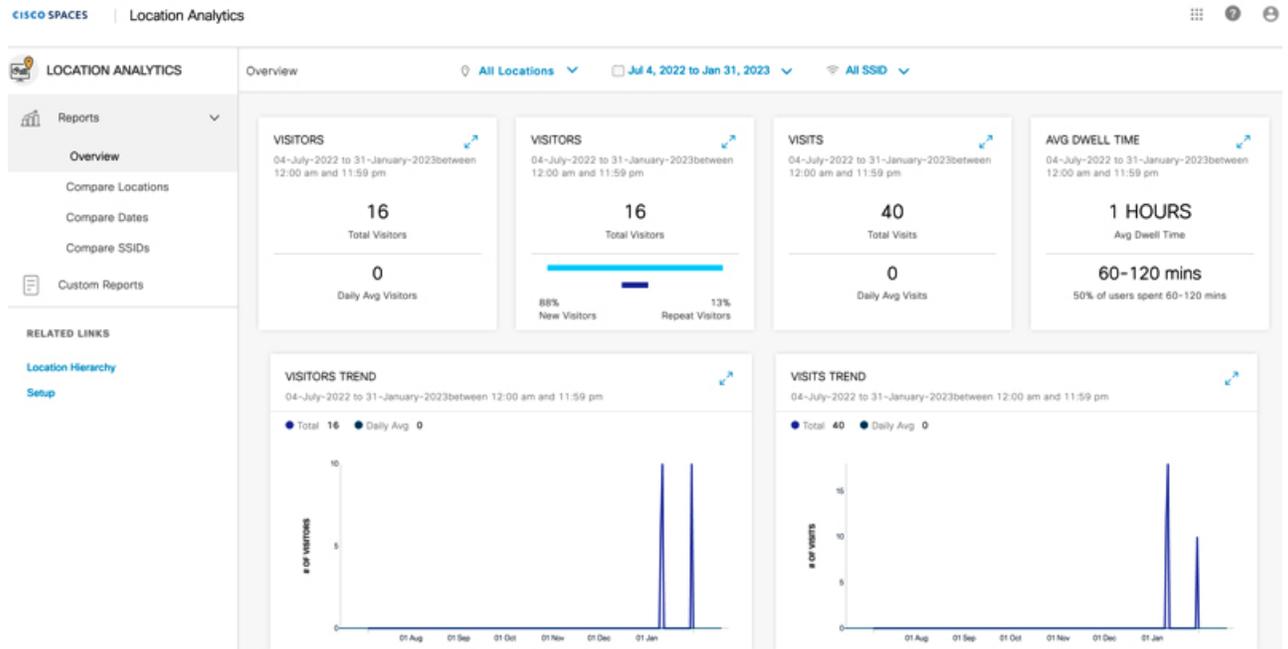
- Visitors Trend
- Visits Trend
- Dwell Time Distribution

View Location Analytics Report

Step 1 In the Cisco Spaces dashboard, click the **Menu** icon () and choose **Home**.

Step 2 In the **SEE** apps area, click **Location Analytics**.

The **Overview** window in the Reports menu is displayed by default.



- 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 ACT license users; it is not available to the SEE 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 ACT license users can view the report for floors and zones. The SEE 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 9: 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

Date Range	Description
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 10: 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 <ul style="list-style-type: none"> • 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

Report Item	Description
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 ACT license users.

Note You can view the **Visitors Trend**, **Visits Trends** and **Dwell Time Distribution** 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**.

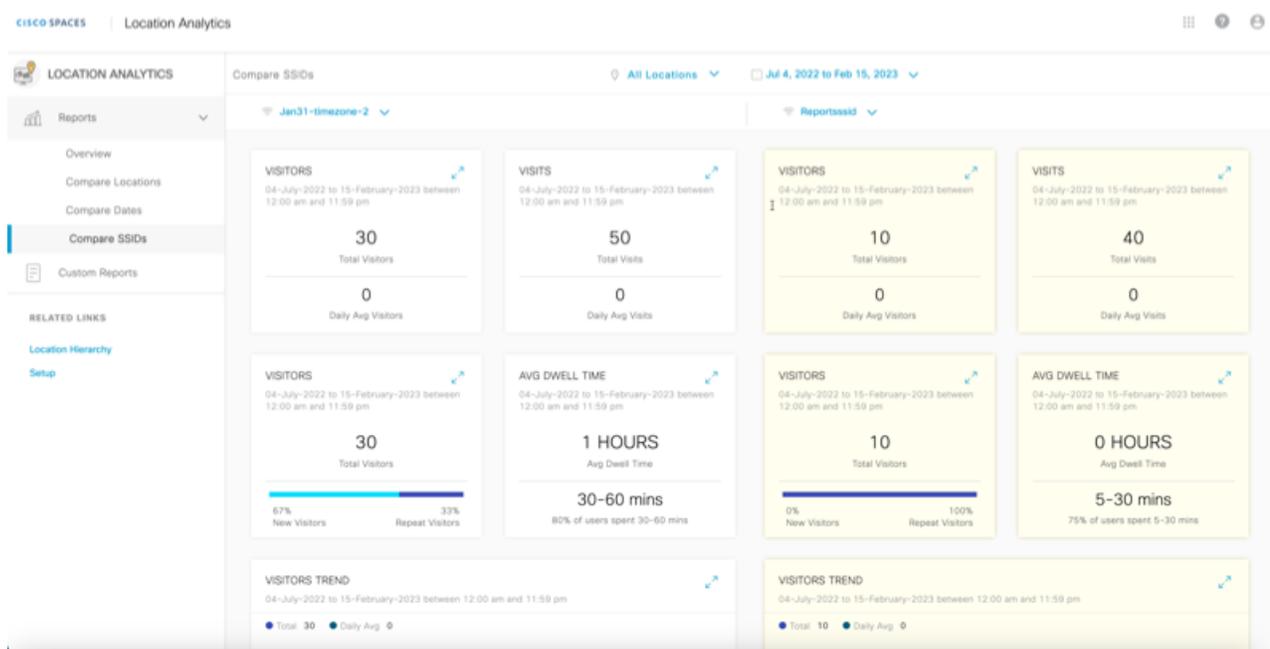
- **Compare Locations:** Use this tab to compare two location reports and view the visitors' trend. By default, two locations with most number of visitors are considered for the report. Visitor data must be available for atleast two network locations to display as charts. In the **Compare Locations** 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) against 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 14: 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.

- 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.

The screenshot shows the 'Create New Report' dialog box. It features a text input field for 'Report Name'. Underneath, a section titled 'Choose Report type' displays five report type options in a grid:

- Overview**: Use Metrics and Graph widgets to create an overview. Common Filters: Location and Date range. (This option is selected and highlighted with a blue border.)
- Compare Locations**: Compare two locations side by side.
- Compare Dates**: Compare two date ranges side by side.
- Compare SSIDs**: Compare two SSIDs side by side. (Marked with an orange 'ACT' badge.)
- Path Report**: Know where visitors come from Monthly Dwell Time Report and go to after a visit. (Marked with an orange 'ACT' badge.)

At the bottom right of the dialog, there are 'Cancel' and 'Next' buttons.

- 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 ACT license users)
- **Path Report**: This report type is available for ACT 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 available to search and select the required report filters.

Note ACT (Advanced) subscription customers are allowed to apply all filters (Location, SSID, Time Range and Visit Range) in the widgets. SEE (Base) 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 **ACT** license user. The **SEE** 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.

The screenshot displays the 'LOCATION ANALYTICS' interface. At the top, there are filters for 'All Reports' (45), 'Overview' (18), and 'Compare Locations' (7). A 'Create New Report' button is visible in the top right. Below the filters is a search bar and a table of reports.

<input type="checkbox"/>	Name	Type	No. of Widgets	Created	Last Updated	
<input type="checkbox"/>	port2	Path	1	January 30, 2023	January 30, 2023	...
<input type="checkbox"/>	Port	Path	1	January 30, 2023	January 30, 2023	...
<input type="checkbox"/>	PathReport	Path	1	January 23, 2023	January 23, 2023	...
<input type="checkbox"/>	asha	Overview	7	January 23, 2023	January 23, 2023	...
<input type="checkbox"/>	Path!	Path	1	January 12, 2023	January 12, 2023	...
<input type="checkbox"/>	CL1	Compare Locations	7	January 12, 2023	January 12, 2023	...
<input type="checkbox"/>	Default_1	Overview	7	January 12, 2023	January 12, 2023	...
<input type="checkbox"/>	Overview_Demo	Overview	8	January 12, 2023	January 12, 2023	...

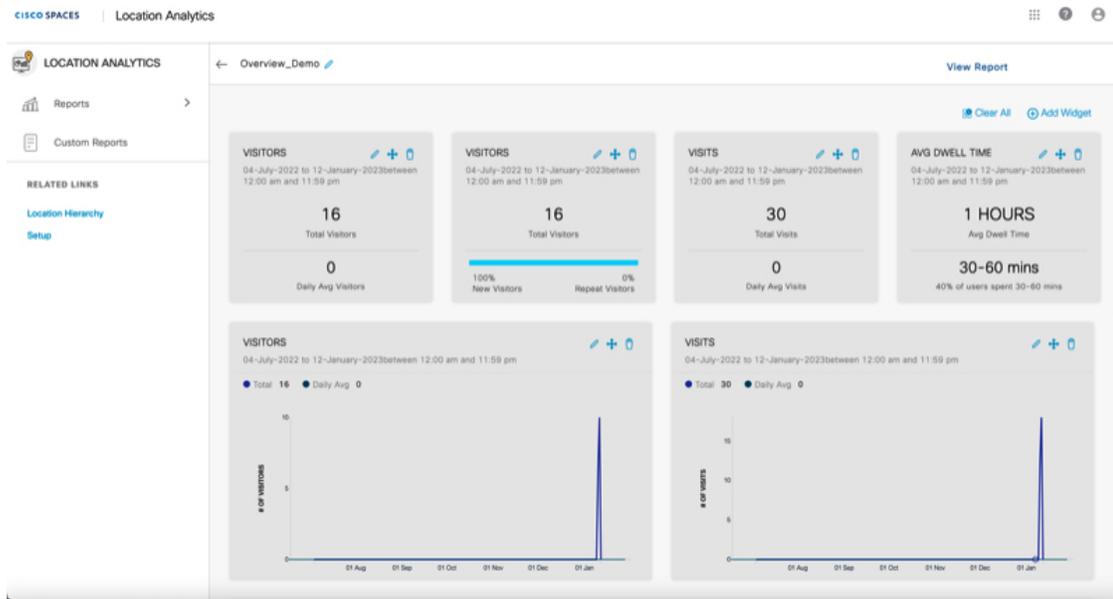
Note

- 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.

- Click **Share** to share the report with other users. For more information, see [Share Location Analytics Custom Report, on page 141](#).
- 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, see [Add Widget, on page 138](#).
- **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.

- 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 15: Add Widget

Add Widget

Name Your Widget *

Choose the widget you want to add

Visitors	Visits	Dwell
----------	--------	-------

Widget Information

Number of Visitors ∨

Visit Range

All Day (12am-11:59pm) ∨

Step 6

Enter the following information:

- Name Your Widget:** Enter the name for the new widget to be added.
- Choose the widget you want to add:** Click the widget that you wanted to add. The widget available are **Visitors**, **Visits** and **Dwell**.
- 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**
- 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.

Share Location Analytics Custom Report

The Share Custom Report feature in the Location Analytics app allows you to share reports with both Cisco Spaces users and non-Cisco Spaces users. Non-Cisco Spaces users must perform a one-time registration to access the reports. If you do not have the necessary permissions to access the report, request access from the administrator or the user who initiated the report.

You cannot access a report if it is deleted or revoked. Only an administrator or a sender can revoke a report.

Step 1 In the Cisco Spaces dashboard, choose **Location Analytics > Custom Reports**.

The **Custom Reports** window is displayed.

Step 2 Click a report from the available custom report list.

The selected report is displayed.

Step 3 Click **Share** displayed at the top-right of the window.

The **Share Report** window is displayed.

Step 4 Enter the following information:

- **Add Email:** Enter the email address of the recipient of the report. This is a mandatory field.
- **Add Message:** Enter your email message.

Note

- Use the **Preview** option to view how the report is shared with the recipient.
- Click the edit icon next to the report name to edit the name of the custom report.

Step 5 Click **Share**.

A success notification message is displayed. After the report is shared, the email address of the recipient is displayed in the right panel of the **Share Report** window. Select the check box next to the user and click **Delete** if you want to remove the recipient.



CHAPTER 13

Cisco Spaces: Impact Analysis App

This chapter describes how to work with the Impact Analysis app.

- [Impact Analysis Overview](#), on page 143
- [Adding an Impact Campaign \(Event\)](#), on page 144
- [Viewing an Impact Analysis Report](#), on page 145

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.

This app will be available for SEE, ACT, and Extend license types.

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:

-
- 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 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, 2019 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:

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.

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.



PART **V**

Cisco Spaces: ACT License Apps

- [Cisco Spaces: Smart Workspaces App, on page 149](#)
- [Cisco Spaces: Environmental Analytics App, on page 151](#)



CHAPTER 14

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 apps are tied to the **ACT** license.

- [Working with Cisco Spaces: Smart Workspaces, on page 149](#)

Working with Cisco Spaces: Smart Workspaces

To support **Cisco Smart Workspaces**, two new apps are added under the **ACT** license:

- **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 **Workspace Management** 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.

Room Occupancy Reports is a new feature that is introduced in the Cisco Spaces: Space Manager App. You can now 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.

- **Space Experience**: Use the **Space Experience** app to do the following:
 - 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, see [Cisco Spaces: Smart Workspaces Solution Guide](#).



CHAPTER 15

Cisco Spaces: Environmental Analytics App

- [Working with Cisco Spaces: App, on page 151](#)

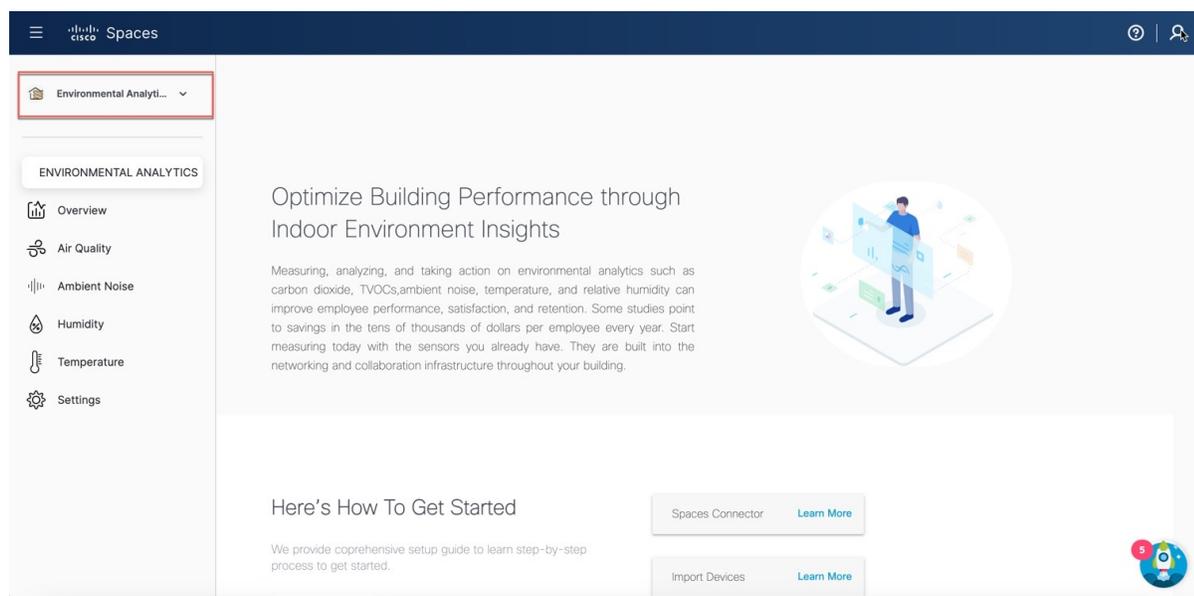
Working with Cisco Spaces: App

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.

Figure 16: Environmental Analytics App





Note Cisco Spaces Environmental Analytics app is tied to the **ACT** license.



PART VI

Cisco Spaces: SMART_OPERATIONS Apps

- [Cisco Spaces: Asset Locator App, on page 155](#)
- [Cisco Spaces: IoT Explorer App, on page 157](#)



CHAPTER 16

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 155](#)

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 17

Cisco Spaces: IoT Explorer App

- [Cisco Spaces: IoT Explorer, on page 157](#)
- [Working with Cisco Spaces: IoT Explorer, on page 157](#)
- [Temperature Monitoring: Use Case Overview, on page 158](#)
- [Asset Tracking: Use Case Overview, on page 159](#)
- [Presence Detection: Use Case Overview, on page 160](#)

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 ACT 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, see [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

-
- 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
- Set up alerts when an asset tag's battery needs replacing

Configure Tracking and Monitoring of Asset Location

- 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

- 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.



PART **VII**

Cisco Spaces: SMART_VENUES Apps

- [Cisco Spaces: Captive Portal App, on page 163](#)
- [Cisco Spaces: Engagements App, on page 243](#)
- [Cisco Spaces: Location Personas App, on page 263](#)



CHAPTER 18

Cisco Spaces: Captive Portal App

This chapter describes how to create a captive portal using Cisco Spaces.

- [Creating and Managing Portal, on page 163](#)
- [Captive Portal Rule, on page 195](#)
- [Reports, on page 201](#)
- [SSIDs, on page 204](#)
- [Access Codes, on page 207](#)
- [User Management, on page 215](#)
- [Social Authentication for Portals, on page 215](#)
- [Configuring an SMS Gateway in Cisco Spaces, on page 218](#)
- [Certified Device List for Portals, on page 223](#)
- [Cisco Spaces Captive Portal Behavior, on page 225](#)
- [Authentication Steps for Customers, on page 229](#)
- [Smart Links and Text Variables for Captive Portals, on page 238](#)

Creating and Managing Portal

A portal is the user interface that appears when a Wi-Fi user connects to an SSID. You can create the captive portals using Cisco Spaces, and enhance the portals using the various portal modules provided by Cisco Spaces.

Cisco Spaces also allows you to have your own portals (Enterprise Captive Portals) to onboard end users who connect to Wi-Fi. For more information on Enterprise Captive Portals, see [Enterprise Captive Portals](#).

Prerequisites for Creating a Portal

- To specify the locations for which the portal is applicable, you must define the location hierarchy. For more information on defining the location hierarchy, see the [Defining the Location Hierarchy, on page 279](#) section.
- If you want to configure social authentication for the portal, you must do certain configuration in your social app, and then add that social app to Cisco Spaces. For more information on configuring for social authentication, see the [Social Authentication for Portals](#) section.

- If you want to configure SMS-based authentication for the portal, you must configure the SMS gateway. For more information on configuring the SMS gateway, see the [Configuring an SMS Gateway in Cisco Spaces, on page 218](#) section.

Bandwidth Requirements

For captive portals, we recommend a minimum bandwidth of 30Mbps for good end user experience.

The following table shows the response time for loading the captive portal based on the bandwidth.

Table 11:

Bandwidth	Number of Users	Response (In Seconds)
1 Mbps	1	5.86
	2	5.49
	3	5.40
	4	5.63
	5	5.92
2 Mbps	1	5.09
	2	5.10
	3	5.04
	4	5.25
	5	5.16
	6	5.23
	7	5.26
	8	5.30
	9	5.34
	10	5.40
	11	5.49

Bandwidth	Number of Users	Response (In Seconds)
5Mbps	5	4.92
	10	4.98
	11	5.05
	12	5.08
	13	5.11
	14	5.13
	15	5.17
	16	5.18
	20	5.25
7Mbps	25	5.13
	30	5.20
	31	5.23
	32	5.26
	33	5.29
	34	5.33
9Mbps	30	4.93
	35	4.98
	40	5.05
	41	5.07
	42	5.10
	43	5.13
	44	5.15
	45	5.17
	46	5.19
	47	5.15

Bandwidth	Number of Users	Response (In Seconds)
11 Mbps	35	4.68
	40	4.91
	50	5.05
	55	5.16
	56	5.18
	57	5.20
	58	5.24
	59	5.28
	60	5.25
	61	5.30

Sample Portals

Cisco Spaces provides sample portals for various authentication types.

- Email Authentication with Data Capture
- Inline SMS with password verification & data capture
- Inline Social Authentication
- SMS with password verification & data capture
- SMS with link verification
- Email authentication
- User Agreements

In addition, sample portals are provided to meet COVID-19 requirements.

To view and make a copy of the sample portal, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Home**.
- Step 2** In the window that appears, choose **Captive Portal**.
- Step 3** In the **Captive Portal** window that appears, choose **Portal** in the left pane.
- The sample portal for various authentication types are displayed at the bottom of the portal list.
- Step 4** Click the **Make a Copy** icon at the far right of the sample portal that you want.
- Step 5** In the portal wizard screen that appears, specify a name for the captive portal.
- Step 6** If required, do the necessary customizations to the portal configuration,

Step 7 Save the portal.

Creating a Portal

When defining a portal, you can also configure the locations for which the portal must be available.

To create a portal, perform the following steps:

Step 1 In the Cisco Spaces dashboard, choose **Home**.

Step 2 In the window that appears, choose **Captive Portal**.

Step 3 In the **Captive Portal** window that appears, choose **Portal** in the left pane.

Step 4 Click **Create New**.

The Portal wizard appears.

Step 5 In the **Portal Name** field, enter a name for portal.

Step 6 If you want this portal to be available only for certain locations, uncheck the **Enable this portal for all locations** check box.

Note By default, the **Enable this portal for all locations** check box is checked so that the portal will be available for all the location in the location hierarchy.

Step 7 Click **Next**.

The **Authentication** window appears.

Step 8 From the **Authentication Type** drop-down list, choose the authentication type that you want apply for the portal.

Based on the authentication type selected additional fields appear. For more information on various authentication types, see the [Configuring Authentication for a Portal, on page 171](#).

Step 9 After specifying the details for the authentication type, click **Next**.

The **Data Capture** window appears.

Note For the “Social Sign In” authentication, you will be directed to the “User Agreements” screen as there is no Data Capture for Social Sign In. For Social Sign In, skip step 10 to step 12.

Step 10 If you want to add Data Capture form for this portal, check the **Enable Data Capture** check box.

Step 11 Configure the Data Capture form. Add the fields required for the Data Capture form using the **+Add Field Element** button. For more information on adding fields to the Data Capture form, see the [Adding a Data Capture Form to a Portal, on page 178](#).

Step 12 Click **Next**.

The **User Agreements** window appears.

Step 13 In the **Terms & Condition Message** field, enter the “Terms & Conditions” for the portal.

Note By default, the **Enable Terms & Conditions** check box is checked. If you do not want to specify any “Terms & Conditions”, uncheck the **Enable Terms & Conditions** check box.

Step 14 If you want to display privacy policy along with the Terms & Conditions, check the **Enable Privacy Policy** check box, and in the **Privacy Policy** field that appears, enter the privacy policy.

If you specify the privacy policy, during customer acquisition, the privacy policy also appears along with the “Terms & Conditions”.

- Step 15** From the **How frequently do you want users to accept agreements** drop-down list, choose the frequency at which the customer must accept the “Terms & Conditions” to access the internet.
- Step 16** In the **User Accepts Terms In** area, choose how the “Terms & Conditions” must appear during customer acquisition.
- **1-Click**—Choose this option, if you want display only the **Terms & Conditions** link. If you select this option, during customer acquisition, the customer can proceed further by clicking the “Accept Terms and Continue” button.
 - **2-Click**—Choose this option, if you want to display a check box also along with the **Terms & Conditions** link. If you select this option, during customer acquisition, the customer has to select the check box, and click the **Accept Terms and Continue** button to proceed further.

Note The 2-Click option is provided in Cisco Spaces to meet the legal requirements of certain countries.

- Step 17** If you want to restrict the internet access to the customers below certain age, select the **Enable Age gating** check box, and then choose the required age gating method from the following:
- **Moderate**: If you choose this option, during customer acquisition, the customer has to acknowledge that the age is 16 or above to proceed further.
 - **Strict**: If you choose this option, during customer acquisition, the customer has to specify the month and year of the birth to access the internet. If the customer provides the age as less than 16, an alert message is shown, and the customer cannot proceed further to access the internet. However, the customer will be provided an option to change the age, if required.

- Step 18** Click **Save and Configure Portal**.

A message **Portal saved successfully** appears, and the **Portal** window opens with the portal modules on the left and portal preview on the right.

- Step 19** Add features to the portal using the [Portal Modules, on page 168](#).

- Step 20** Click **Save** to save the changes made to each module.

Note When creating the portal, you can save the portal after specifying the name and locations for the portal. The new portal gets listed in the **Portals** window. You can configure authentication type, Terms & Conditions, Data Capture form, and so on at any time later using the Edit Portal button for that portal.

Note To capture the details such as name, phone number, and so on of the customers connecting to the SSID using the captive portal, ensure that you add a “Data Capture form” in the captive portal. During customer acquisition (runtime), before provisioning the internet, the data capture form is displayed to the customer. The captured customer details are stored in Cisco Spaces.

Note A portal becomes live when you associate it with a Captive Portal Rule, and publish that rule.

Portal Modules

The following are the portal modules of Cisco Spaces:

- **Brand Name**—Define your brand name in the portal using this module. You can add the brand name as text or a logo image.

- **Welcome Message**—Add a welcome message in the portal using this module. You can configure to show different welcome messages for first time users and repeat users.
- **Notice**—Add a notice in the portal using this module. This helps you display notices to the portal users whenever required. You can set to provide the notice in the thicker text, text, or text with an image format.
- **Authentication**—Based on the authentication type selected when creating the portal, an Authentication module appears for the portal. The name of the module will be based on the authentication type. For example, if you have selected “SMS with link verification” as authentication type for a portal, the authentication module for that portal will be named as “SMS Authentication”. The Authentication module will have provision to configure the landing page URL for the portal. The Authentication module will not be available for the authentication type, “No Authentication”, if both “Data Capture” and “User Agreements” are not enabled.
- **Venue Map**— Add a label and icon for the Venue Map using this module. The venue map is uploaded in the portal from your wireless network based on the location.
- **Videos**—Add YouTube videos in the portal using this module. You can also add an appropriate caption and icon for the video section in the portal. You can also view the preview of the video when uploading.
- **Feedback**—Add the feedback questions in the portal using this module. You can add multiple choice and rating questions. This module also lets you customize the labels for the “Submit” button, “Thank You” message, and “Post Submission” button. You can also set whether the customers are to be provided a text box to add the comments. You can also specify the e-mail addresses and subject for feedback.
- **Help**—Add a help line number that the customer can contact for assistance using this module. You can customize the caption and icon for Help.
- **Get Apps**—Add apps to the portal using this module. You can add appropriate caption and icon for each app using this module.
- **Get Internet**—Add the external URL to which customer can navigate from the Get Internet section in the portal. To navigate to this URL, the customer has to accept the terms and conditions provided.
- **Promos & Offers**—Add the promotions and offers to display through the portal using this module. You can modify the title of the promotion. For each promotion you can add appropriate captions and images, and specify the URL to the promotion details. Promos are displayed as carousels.
- **Add Module**—Add customized content and menu items to the portal using this module. All the modules mentioned earlier are the default modules provided by Cisco Spaces. You can add additional items to a portal based on your requirements using the “Add Module” button.

Configuring a Language for a Portal

In Cisco Spaces, you can configure the language in which the module captions and static content in the portal are to display. To display the static content in any language other than English, you must upload the corresponding text to Cisco Spaces. Cisco Spaces does not support entering the content in any language other than English. The default language is set to English. You can change the default language.



Note You cannot translate the content prepared in one language to another using Cisco Spaces.

To configure a language in which the portal content is to display, perform the following steps:

-
- Step 1** To display the static content such as messages, country names, and so on in a language other than English, upload the key values in that language. For more information on uploading the key values for a language, see the [Uploading Static Content Key Values for a Language, on page 170](#)
- Step 2** Open the portal for which you want to configure the language.
- Step 3** Click the **Languages** (Globe) icon at the top of the **Portal** window.
The **Add Language** window appears.
- Step 4** Click **Add Language**.
- Step 5** In the search field that appears, enter the language.
If this language is supported by Cisco Spaces, then the language name appears in the drop-down list.
- Step 6** Click the **Add** button that appears adjacent to the language name.
The language gets added to the Added Languages list.
- Step 7** Click **Add**.
In the portal, now a drop-down list appears adjacent to the **Languages** icon, and the newly added language gets listed in that drop-down list.
- Step 8** From the drop-down list adjacent to the **Languages** icon, choose the language in which the static portal content is to display.
The captions of the modules are displayed in the chosen language.
-

Setting a Default Language

To set a default language, do the following:

-
- Step 1** In the portal, click the **Languages** icon at the top right of the window.
- Step 2** In the **Add Language** window, from the “Default Language” drop-down list, choose the default language.
- Step 3** Click **Add**.
-

Uploading Static Content Key Values for a Language

To set to display the static content in any language other than English, perform the following steps:

-
- Step 1** In the portal, click the **Languages** icon at the top right of the window.
- Step 2** In the **Add Language** window, click **Download** to download and save the template.
- Step 3** Open the template.
The template contains keys for various static messages and the message that appears if your language is English. The column for English has “en” as first row.

Step 4 In the column adjacent to the English column, enter the language identifier for the language in which you want to display the static content.

For example, if you want to display the content in Arabic, enter “AR” in the first row.

Step 5 In the remaining rows, enter the text that must appear for the corresponding key.

Step 6 Save the file.

Step 7 In the **Add Language** window, use the **Upload** button to upload the window.

Step 8 Click **Add**.

What to do next

To know how to display the static content in a language, see the [Configuring a Language for a Portal](#), on page 169.

The language code for various languages are shown in the following figure.

Figure 17: Language Code

```
[{"Abkhaz": "ab"}, {"Afar": "aa"}, {"Afrikaans": "af"}, {"Akan": "ak"}, {"Albanian": "sq"}, {"Amharic": "am"}, {"Arabic": "ar"}, {"Aragonese": "an"}, {"Armenian": "hy"}, {"Assamese": "as"}, {"Avaric": "av"}, {"Avestan": "ae"}, {"Aymara": "ay"}, {"Azerbaijani": "az"}, {"Bambara": "bm"}, {"Bashkir": "ba"}, {"Basque": "eu"}, {"Belarusian": "be"}, {"Bengali": "bn"}, {"Bihari": "bh"}, {"Bislama": "bi"}, {"Bosnian": "bs"}, {"Breton": "br"}, {"Bulgarian": "bg"}, {"Catalan": "ca"}, {"Chamorro": "ch"}, {"Chechen": "ce"}, {"Chichewa": "ny"}, {"Chinese": "zh"}, {"Chuvash": "cv"}, {"Cornish": "kw"}, {"Corsican": "co"}, {"Cree": "cr"}, {"Croatian": "hr"}, {"Czech": "cs"}, {"Danish": "da"}, {"Divehi": "dv"}, {"Dutch": "nl"}, {"Dzongkha": "dz"}, {"English": "en"}, {"Esperanto": "eo"}, {"Estonian": "et"}, {"Ewe": "ee"}, {"Faroese": "fo"}, {"Fijian": "fj"}, {"Finnish": "fi"}, {"French": "fr"}, {"Fula": "ff"}, {"Galician": "gl"}, {"Georgian": "ka"}, {"German": "de"}, {"Greek": "el"}, {"Guaraní": "gn"}, {"Gujarati": "gu"}, {"Haitian": "ht"}, {"Hausa": "ha"}, {"Hebrew": "he"}, {"Herero": "hz"}, {"Hindi": "hi"}, {"Hungarian": "hu"}, {"Interlingua": "ia"}, {"Indonesian": "id"}, {"Interlingue": "ie"}, {"Irish": "ga"}, {"Igbo": "ig"}, {"Inupiaq": "ik"}, {"Ido": "io"}, {"Icelandic": "is"}, {"Italian": "it"}, {"Inuktitut": "iu"}, {"Japanese": "ja"}, {"Javanese": "jv"}, {"Kalaallisut": "kl"}, {"Kannada": "kn"}, {"Kanuri": "kr"}, {"Kashmiri": "ks"}, {"Kazakh": "kk"}, {"Khmer": "km"}, {"Kikuyu": "ki"}, {"Kinyarwanda": "rw"}, {"Kyrgyz": "ky"}, {"Komi": "kv"}, {"Kongo": "kg"}, {"Korean": "ko"}, {"Kurdish": "ku"}, {"Kwanyama": "kj"}, {"Latin": "la"}, {"Luxembourgish": "lb"}, {"Ganda": "lg"}, {"Limburgish": "li"}, {"Lingala": "ln"}, {"Lao": "lo"}, {"Lithuanian": "lt"}, {"Latvian": "lv"}, {"Manx": "gv"}, {"Macedonian": "mk"}, {"Malagasy": "mg"}, {"Malay": "ms"}, {"Malayalam": "ml"}, {"Maltese": "mt"}, {"Marathi": "mr"}, {"Marshallese": "mh"}, {"Mongolian": "mn"}, {"Nauru": "na"}, {"Navajo": "nv"}, {"Nepali": "ne"}, {"Ndonga": "ng"}, {"Norwegian Nynorsk": "nn"}, {"Norwegian": "no"}, {"Nuosu": "ii"}, {"Southern Ndebele": "nr"}, {"Occitan": "oc"}, {"Ojibwe": "oj"}, {"Old Church Slavonic": "cu"}, {"Oromo": "om"}, {"Oriya": "or"}, {"Ossetian": "os"}, {"Panjabi": "pa"}, {"Persian": "fa"}, {"Polish": "pl"}, {"Pashto": "ps"}, {"Portuguese": "pt"}, {"Quechua": "qu"}, {"Romansh": "rm"}, {"Kirundi": "rn"}, {"Romanian": "ro"}, {"Russian": "ru"}, {"Sanskrit": "sa"}, {"Sardinian": "sc"}, {"Sindhi": "sd"}, {"Northern Sami": "se"}, {"Samoan": "sm"}, {"Sango": "sg"}, {"Serbian": "sr"}, {"Scottish Gaelic": "gd"}, {"Shona": "sn"}, {"Sinhala": "si"}, {"Slovak": "sk"}, {"Slovene": "sl"}, {"Somali": "so"}, {"Southern Sotho": "st"}, {"Spanish": "es"}, {"Sundanese": "su"}, {"Swahili": "sw"}, {"Swati": "ss"}, {"Swedish": "sv"}, {"Tamil": "ta"}, {"Telugu": "te"}, {"Tajik": "tg"}, {"Thai": "th"}, {"Tigrinya": "ti"}, {"Tibetan Standard": "bo"}, {"Turkmen": "tk"}, {"Tagalog": "tl"}, {"Tswana": "tn"}, {"Tonga": "to"}, {"Turkish": "tr"}, {"Tsonga": "ts"}, {"Tatar": "tt"}, {"Twi": "tw"}, {"Tahitian": "ty"}, {"Uyghur": "ug"}, {"Ukrainian": "uk"}, {"Urdu": "ur"}, {"Uzbek": "uz"}, {"Venda": "ve"}, {"Vietnamese": "vi"}, {"Walloon": "wa"}, {"Welsh": "cy"}, {"Wolof": "wo"}, {"Western Frisian": "fy"}, {"Xhosa": "xh"}, {"Yiddish": "yi"}, {"Yoruba": "yo"}, {"Zhuang": "za"}, {"Zulu": "Zulu"}]
```

Configuring Authentication for a Portal

To secure your portal from hacking or misuse, you can configure various authentication options for your portal. The customer is provided access only if the authentication is success.

You can authenticate the internet provisioning through SMS, e-mail, access code, or social networks such as Facebook, Twitter, or LinkedIn. Cisco Spaces supports the SMS gateway of the third party vendors for SMS authentication. You can configure to provide SMS authentication through “SMS with password verification” or “SMS with link verification”. For “SMS with password verification”, you can define a custom verification code for a portal or you can configure to auto-generate the verification code.

During customer acquisition, the authentication process is initiated when the customer click any menu item in the portal. However, you can configure for inline authentication also, so that the Authentication module will be shown in the captive portal. For more information on inline authentication, see the [Inline Authentication](#), on page 178.

Cisco Spaces supports the following authentication types:

- **SMS with password verification** — For this authentication type, validation of mobile number is mandatory. When the customer enters a valid mobile number, an SMS is sent to that mobile number, which contains a link and verification code. The customer can access the internet by providing the verification code in the SMS. The customer is not allowed to proceed further until the verification code is entered. Some use cases for this authentication type are SMS-based engagement campaigns, country specific requirements to verify the users connecting to internet, and so on. To know the authentication steps during customer acquisition, see [Steps for SMS with Password Verification Authentication, on page 231](#). For more information on configuring the “SMS with password verification”, see the [Configuring a Portal for SMS with Password Verification, on page 174](#) section.

SMS with link verification —For this authentication type, validation of mobile number is optional. When the customer provides a valid mobile number, an SMS is sent to that mobile number with verification link. The customer can complete the validation by clicking the verification link in the SMS. However, customer can skip the validation process and proceed further. This authentication type can be used if the validation of the mobile number is not mandatory . To know the authentication steps during customer acquisition, see [Steps for SMS with Link Verification Authentication, on page 229](#). For more information, see the [Configuring a Portal for SMS with Link Verification, on page 173](#) section.

Email — The customer has to provide a valid e-mail ID to access the internet. To know the authentication steps during customer acquisition, see [Steps for E-mail Authentication, on page 233](#). For more information on configuring e-mail authentication, see the [Configuring a Portal for E-mail Authentication, on page 176](#) section.

Social Sign In — The internet access is provided only if the customer is logged in to a social site configured for authentication. You must configure at least one social site to use this option. To know the authentication steps during customer acquisition, see [Steps for Social Authentication, on page 237](#). For more information on configuring the Social Sign In authentication, see the [Configuring a Portal for Social Sign In Authentication](#) section.

Access Code — The customer has to provide a valid access code to access the internet. To know the authentication steps during customer acquisition, see [Steps for Access Code Authentication, on page 235](#). For more information on configuring Access code authentication, see the [Configuring a Portal for Access Code Authentication, on page 176](#) section.

No Authentication — The internet access is provided without any authentication process. To know the authentication steps during customer acquisition, see [Steps for No Authentication with Terms and Conditions, on page 237](#). For more information on configuring a portal for No Authentication, see the [Configuring a Portal with No Authentication, on page 177](#) section.



Note The **Opt In** option is not available for the "Social Sign In" authentication type. You can configure the Data Capture form for all the authentication types, except “Social Sign In”. For more information on configuring the Data Capture form, see the [Adding a Data Capture Form to a Portal, on page 178](#). For more information on Opt In feature, see the “Opted In Option for Users” section .



Note For **SMS with link verification** and **SMS with password verification**, you can include additional information that needs to be passed to the SMS gateways. For example, if you want to send the SMS in a language other than English to your customers, provision is now available to include that information in the SMS sent to the SMS Gateways.

Configuring a Portal for SMS with Link Verification

To configure a portal for “SMS with link verification”, do the following:

-
- Step 1** When creating a portal, from the **Authentication Type** drop-down list, choose **SMS with Link verification**.
- Step 2** If you want to configure inline authentication for this portal, and display the “Data Capture form” and “User Agreements” in the home page, check the **Display Authentication, Data Capture, and User Agreements on portal home page** check box. For more information on inline authentication, see the [Inline Authentication , on page 178](#).
- Step 3** If you want the customers to provide an option to opt for receiving notifications, check the “Allow users to Opt in to receive message” check box.
- Step 4** If the “Allow users to Opt in to receive message” check box is checked, the following fields appear:
- **Opt in Message:** Enter an opt in message.
 - **Default Opt-In Check Box Behavior**
 - **Checked:** Click this option if you want the **Opt In** check box to be displayed as checked by default, during customer acquisition.
 - **Unchecked:** Click this option if you want the **Opt In** check box to be displayed as unchecked by default, during customer acquisition.
- Step 5** In the **SMS Text** field, enter the text message that must appear in the SMS sent to the customer.
- Note** To display the link through which the customer can access the captive portal, ensure that “{Link}” is not removed when editing the text message.
- Step 6** From the **Default Country** drop-down list, choose the country for which this setting is applicable.
- Step 7** From the **SMS Gateway** drop-down list, choose the SMS gateway.
- The SMS Gateways configured in the Settings option are available for selection. You can also use the **Demo Gateway** provided by Cisco that is chargeable.
- Note** For more information on configuring the SMS gateway, see the [Configuring an SMS Gateway in Cisco Spaces, on page 218](#).
- Step 8** Save the changes.
-

What to do next



Note Portals with **SMS with link verification** authentication type will have an authentication module named **SMS Authentication**. For more information on the Authentication Module, see the [Authentication Module, on page 178](#).



Note If you have not configured the authentication type when creating the portal, you can specify it at any time using the **Edit Portal** button for that portal in the **Portals** window.

Configuring a Portal for SMS with Password Verification

To configure a portal for “SMS with password verification”, perform the following steps:

-
- Step 1** When creating a portal, from the Authentication Type drop-down list, choose **SMS with password verification**.
- Step 2** If you want to configure inline authentication for this portal, and display user agreements on portal home page, check the **Display Authentication and User Agreements on portal home page** check box. For more information on inline authentication, see the [Inline Authentication](#), on page 178.
- Step 3** If you want the customers to provide an option to opt for receiving notifications, check the “Allow users to Opt in to receive message” check box.
- Step 4** If the “Allow users to Opt in to receive message” check box is checked, the following fields appear:
- **Opt in Message:** Enter an opt in message.
 - **Default Opt-In Check Box Behavior**
 - **Checked:** Click this option if you want the **Opt In** check box to be displayed as checked by default, during customer acquisition.
 - **Unchecked:** Click this option if you want the **Opt In** check box to be displayed as unchecked by default, during customer acquisition.
- Step 5** Click the required Password Type.
- **Auto Generated password**— To auto-generate the password for each authentication request. The auto-generated password is sent to the customer.
 - **Fixed Password**— To define a password for authentication. For all of the customers, this password is sent whenever there is an authentication request. In the “Password” field that appears when you click the “Fixed Password” option, enter the password that is to send to the customers.
- Step 6** In the **SMS field** field, enter the text that must appear in the SMS that is sent to the customer.
- Note** To display the link through which the customer can access the captive portal, ensure that “{Link}” is not removed when editing the text message. Similarly, to display the password in the message, ensure that the “{Password}” is not removed.
- Step 7** From the **Default Country** drop-down list, choose the country for which this setting is applicable.
- Step 8** From the **SMS Gateway** drop-down list, choose the SMS Gateway.
- The SMS Gateways configured in the Settings option are available for selection. You can also use the Demo Gateway provided by Cisco that is chargeable.
- Note** The **SMS Gateway** window appears where you can configure the required SMS gateway. For more information on configuring the SMS gateway, see the [Configuring an SMS Gateway in Cisco Spaces](#), on page 218.
- Step 9** Save the changes.
-

What to do next



Note Portals with **SMS with password verification** authentication type will have an authentication module named **SMS Authentication**. For more information on the Authentication module, see the [Authentication Module, on page 178](#).



Note If you have not configured the authentication type when creating the portal, you can specify it at any time using the **Edit Portal** button for that portal in the **Portals** window.

Configuring a Portal for Social Sign In Authentication

Cisco Spaces supports authentication through the following social networks:

- Facebook
- Twitter
- LinkedIn



Note To authenticate the access to the internet through a social network, you must configure the app for that social network in Cisco Spaces. You can configure the social app in Cisco Spaces through the Settings option. For more information, see the [Adding Social Apps for Social Authentication, on page 217](#).

To authenticate the access to a portal through social sign in, perform the following steps:

-
- Step 1** When creating a portal, from the Authentication Type drop-down list, choose **Social Sign In**.
The social networks that are supported by Cisco Spaces for authentication appear along with the configured social apps.
- Step 2** If you want to configure inline authentication for this portal, and display user agreements in the portal home page, check the **Display Authentication and Users Agreements on portal home page** check box. For more information on inline authentication, see the [Inline Authentication , on page 178](#).
- Step 3** Check the check box adjacent to the social networks through which you want to authenticate access to the internet.
The social networks configured in the Social Apps option under the Settings section will be available for selection. For more information on configuring the Social Apps, see the [Adding Social Apps for Social Authentication, on page 217](#).
- Step 4** Save the changes.
-

What to do next

- Portals with **Social Sign In** authentication type will have an authentication module named **Social Authentication**. For more information on the Authentication Module, see the [Authentication Module, on page 178](#).

- The **+Add** button takes you to the **Social Apps** window where you can configure the customized apps.
- If you have not configured the authentication type when creating the portal, you can specify it at any time using the **Edit Portal** button for that portal in the **Portals** window.

Configuring a Portal for E-mail Authentication

To configure a portal for e-mail authentication, do the following:

-
- Step 1** When creating a portal, from the **Authentication Type** drop-down list, choose **Email**.
- Step 2** If you want to configure inline authentication for this portal, check the **Display Authentication and User Agreements on portal home page** check box. For more information on inline authentication, see the [Inline Authentication](#), on page 178.
- Step 3** If you want to provide the customer an option to opt for receiving notifications, check the **Allow users to Opt in to receive message** check box.
- Step 4** If the **Allow users to Opt in to receive message** check box is checked, the following fields appear:
- **Opt in Message:** Enter an “opt in” message
 - **Default Opt-In Check Box Behavior**
 - **Checked**—Click this option if you want the **Opt In** check box to be displayed as checked by default, during customer acquisition.
 - **Unchecked**—Click this option if you want the **Opt In** check box to be displayed as unchecked by default, during customer acquisition.
- Step 5** Save the changes.

What to do next



Note Portals with **Email** authentication type will have an authentication module named **Email**. For more information on the Authentication Module, see the [Authentication Module](#), on page 178.

Configuring a Portal for Access Code Authentication

To configure a portal for the Access Code authentication, do the following

-
- Step 1** When creating a portal, from the **Authentication Type** drop-down list, choose **Access Code**.
- Step 2** If you want to configure inline authentication for this portal, and display user agreements on portal home page, check the **Display Authentication and User Agreements on portal home page** check box. For more information on inline authentication, see the [Inline Authentication](#), on page 178.
- Step 3** If you want the customers to provide an option to opt for receiving notifications, check the **Allow users to Opt in to receive message** check box.

- Step 4** If the **Allow users to Opt in to receive message** check box is checked, the following fields appear:
- **Opt in Message:** Enter an opt in message.
 - **Default Opt-In Check Box Behavior**
 - **Checked:** Click this option if you want the **Opt In** check box to be displayed as checked by default, during customer acquisition.
 - **Unchecked:** Click this option if you want the **Opt In** check box to be displayed as unchecked by default, during customer acquisition.

- Step 5** Save the changes.

You can create access codes and share it with your customers using the **Access Code** option displayed in the left pane of the **Captive Portals** app. For more information on creating and sharing the access codes, see [Access Codes, on page 207](#).

What to do next



Note Portals with **Access Code** authentication type, provided **Data Capture** or **User Agreements** is enabled. For more information on the Authentication module, see the [Authentication Module, on page 178](#).

Configuring a Portal with No Authentication

To configure a portal for No Authentication, perform the following steps:

- Step 1** When creating a portal, from the **Authentication Type** drop-down list, choose **No Authentication**.
- Step 2** If you want to display data capture and user agreements on portal home page, check the **Display Data Capture and User Agreements on portal home page** check box.
- Step 3** If you want the customers to provide an option to opt for receiving notifications, check the **Allow users to Opt in to receive message** check box.
- Step 4** If the **Allow users to Opt in to receive message** check box is checked, the following fields appear:
- **Opt in Message:** Enter an “opt in” message.
 - **Default Opt-In Check Box Behavior**
 - **Checked:** Click this option if you want the **Opt In** check box to be displayed as checked by default, during customer acquisition.
 - **Unchecked:** Click this option if you want the **Opt In** check box to be displayed as unchecked by default, during customer acquisition.
- Step 5** Save the changes.
-

Inline Authentication

In the Captive Portal, you can add authentication as an inline module along with other modules. That is, the authentication option is displayed before the customer click any link in the captive portal, thus reducing the number of clicks required to initiate the authentication process.

To configure inline authentication, in the Authentication screen, select the check box provided for configuring inline authentication.

For the **SMS with Link verification** and **SMS with password verification** authentication types, the authentication section will have a field to enter the mobile number, along with a Connect button. For Email authentication, the authentication section will have a field to enter the email ID. For social authentication, the authentication section will have relevant buttons for each social network configured for the portal, using which the customer can complete the authentication through that social network.

Authentication Module

When you select the authentication type for a portal, an authentication module is created for the portal based on the authentication type selected.

If you select the authentication type **No Authentication** or **Access Code** for a portal, that portal will not have an authentication module, if either “Data Capture” or “User Agreements” is not enabled.

The Authentication module will have a field to specify the alternate landing page for the portal.

Adding a Data Capture Form to a Portal

If you choose an authentication type other than **Social Sign In** for the portal, you can add a Data Capture form in the captive portal. You can add fields to the Data Capture form when creating the portal. You can configure the fields to capture the details such as first name, last name, mobile number, and so on of the customer. You can also add business tags based on which you can filter your customers.



Note The business tags defined in the Data Capture form are available in the “Add Tags” option available in the rules such as Captive Portal Rule, Engagement Rule, and Profile Rule.

To configure a Data Capture form in a captive portal, perform the following steps:

Step 1 When creating a portal, after specifying the Terms and Conditions, click **Next**.

The Data Capture screen appears.

Step 2 Enable the **Data Capture** check box.

Step 3 Click **Add Field Element**.

You can add the following field elements to the Data Capture form:

- **Title**—To specify how to address the customer. For example, Mr, Ms. If you configure this field, during customer acquisition (runtime), the titles, Mr and Ms will be available for selection in the Data Capture form for the customer.
- **Email**—To specify the e-mail ID of the customer.

- **Mobile Number**—To specify the mobile number of the customer. You can specify a default country for the mobile number so that during customer acquisition, the code for the default country is displayed in the data capture form.
- **First Name**—To specify the first name of the customer.
- **Last Name**—To specify the last name of the customer.
- **Gender**—To specify the gender of the customer.
- **Date of Birth**: To specify the date of birth of the customer. If you add the **Date of Birth** field, you are not allowed to select the **Moderate** option in the **Enable Age Gating** area in the **User Agreements** window.
- **Business Tags**—To provide an answer of customer's choice for the business tag question. This business tags help you in categorizing the customers.
- **Country Specific Fields**
 - ZIP/Postal Code—To provide the postal code of your address.
 - CPF—To provide the CPF (This is applicable only for Brazil).

Note The **Email** field element is not available for **Email** authentication as the e-mail information is already collected during authentication. The **Mobile Number** field element is not available for the **SMS with password verification** authentication as the customer has to provide the mobile number during authentication.

Step 4 Click the corresponding option to add the fields.

General Fields

- In the **Place Holder** field, enter the text that must appear as place holder for the field.
- Check the **Make this field mandatory** check box to make the field mandatory.

Element-Specific Fields

- For the **mobile number** field element, choose the default country so that the country code for this country appears in the data capture form during customer acquisition.
- For the **Zip/Postal Code** field element, from the **Country** drop-down list, choose the country, so that the data capture form allows the customer to add the postal codes of that particular country. To support the postal codes of more than one country, click **Add Country**, and add another country.
- For the Business Tag field element, you must configure the following additional fields:
 - In the **Name** field, enter a name for the business tag.
 - In the **Field Label** field, enter the question that you want to ask the customer.
 - Click **+Add Option**.
 - In the field that appears, enter an answer that you want to provide to the customers to opt.
 - Similarly, add the remaining answer choices also using the **+Add Option**.

Note You can delete an added option using the corresponding Delete icon.

Note When the customers access the Data Capture form during authentication process, the answers you specify are available in a drop-down list. They can choose the required value. You can use this value for filtering the customers in the proximity rules.

Step 5 Save the changes.

Note During customer acquisition, the value entered in the **CPF** field in the **Data Capture** form will be converted to the "000.000.000-00" format. The number will be formatted automatically as the user enters the CPF number value. So the captive portal users do not have to add dots or hyphen manually to maintain the required format.

Defining a Brand Name for a Portal

Cisco Spaces enables you to add your brand name in the portal using the Brand Name module. You can add the brand name as text or image. For example, you can use your company logo as a brand name.

To define a brand name in the portal, perform the following steps:

Step 1 Open the portal for which you want to define the brand name.

Step 2 Click the **Brand Name** module.

The **brand name** window appears.

Step 3 Choose the type of brand.

- a) If you choose **Text only**, in the **Brand Name** field that appears, enter the brand name.
- b) If you choose **Logo**, click the **Upload** button that appears, and upload the logo image.

Step 4 Click **Save**.

The brand name for the portal is successfully defined.

What to do next



Note If you are modifying a portal that is already associated with a published captive portal, click the **Save & Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the [Creating a Captive Portal Rule to Display Captive Portals, on page 196](#).

Adding a Welcome Message to a Portal

You can add a welcome message to a portal using the Welcome module. The welcome message added is displayed when a customer accesses your portal. You can configure to display different welcome messages for first time user and repeat user.

To add a welcome message to a portal, perform the following steps:

Step 1 Open the portal in which you need to add the welcome message.

- Step 2** Click the **Welcome Message** module.
The **Welcome Message** window appears.
- Step 3** In the **First time visitor welcome text** field, enter the welcome message that must appear when a customer accesses your portal for the first time. You can include the location details using the smart link variables. For more information on smart link, see the [Smart Links and Text Variables for Captive Portals, on page 238](#).
- Step 4** If you want to display a different welcome message for the repeat users, ensure that the **Add a custom message for Repeat Visitors** check box is checked, and in the adjacent text box, enter the welcome message for the repeat user. You can include the name and location details using the smart link variables. The variables “firstName” and “lastName” will be available for selection only if you have configured a Data Capture module in the portal with the fields, First Name and Last Name. The variables “firstName”, and “lastName” will be available for the authentication types other than “Social Sign In”. For more information on smart link, see the [Smart Links and Text Variables for Captive Portals, on page 238](#).
- Step 5** Click **Save**.
The welcome message is successfully defined for the portal.

What to do next



Note If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the [Creating a Captive Portal Rule to Display Captive Portals, on page 196](#).

Adding a Notice to a Portal

The Notice module enables you to provide notices in your portal. This module is useful when you want to pass any important information to your customers. You can add ticker and text notices. You can also add images along with text notices.

You can configure the date up to which the notice is to be displayed in the portal.

To add notices in a portal from the dashboard, do the following:

- Step 1** Open the portal in which you want to add notice.
- Step 2** Click the **Notice** module.
The **Notice** window appears.
- Step 3** Click the type of notice you want. The following options are available:
- **Ticker Text Only**—The notice appears in a moving text format. For **Ticker Text Only**, in the **Notice** field that appears, enter the notice text.
 - **Text Only**—The notice appears in the text format. For **Text Only**, in the **Notice** field that appears, enter the notice text.

- **Text with Image**—The notice appears as a text along with an uploaded image. For **Text with Image**, do the following:
 - In the **Notice** field, enter the notice text.
 - In the **Notice** image area, click the **Upload** button, and upload the image that must appear with the notice.

Step 4 In the **Hide After** field, choose the date up to which the notice is to display in the portal.

Step 5 Click **Save**.

The notice is successfully added to the portal.

What to do next



Note If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see [Creating a Captive Portal Rule to Display Captive Portals, on page 196](#).

Providing the Venue Details in a Portal

You can provide the venue details in a portal using the Venue Map module. You can define a label name, upload an icon image, and display a map for the venue using this module.

The default name of the module is Venue Map. The module name changes based on the changes you make in the Label field.

To add the venue details for a portal, perform the following steps:

Step 1 Open the portal in which you want to add the venue details.

Step 2 Click the **Venue Map** module.

The **VENUE MAP** window appears.

Step 3 In the **Label** field, enter the venue map label name that must appear in the portal.

Note The **Venuw Map** module name gets changed to the name you specify in the Label field.

Step 4 In the **Icon** area, upload the map icon that must appear adjacent to the map label using the **Upload** button.

Note You can delete the icon using the Delete icon.

Step 5 In the **Store Map** area, the map for this venue as in the wireless network appears.

Note The map appears only if the portal is associated with a location for which the map is defined in the wireless network (CUWN, Meraki). The map of the location where the customer is currently present is shown.

Step 6 Click **Save**.

The venue map is configured for the portal.

What to do next



Note If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the [Creating a Captive Portal Rule to Display Captive Portals, on page 196](#).

Uploading Videos to a Portal

You can upload the videos to Cisco Spaces portals using the Videos module. In this module, you can add a label and image for the area where the video appears in the portal, and specify the Youtube URL of the video.

The default name of the module is Videos. The module name changes based on the changes you make in the Label field.



Note You can show only the YouTube videos in your portal.

To upload videos to a portal, perform the following steps:

Step 1 Open the portal in which you want to upload the video.

Step 2 Click the **Videos** module.

The **VIDEOS** window appears.

Step 3 In the Label field, enter the label that must appear for the area where the video appears in the portal.

Note The Videos module name gets changed to the name you specify in the Label field.

Step 4 In the Icon area, upload the video icon that must appear adjacent to the video label using the **Upload** button.

Note You can delete the icon using the Delete icon.

Step 5 Click **Add a Video**.

Step 6 In the YouTube URL field that appears, enter the YouTube URL of the video that you want to display in the portal.

Step 7 Click **Save**.

The video is successfully uploaded to the portal.

What to do next

Note If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the [Creating a Captive Portal Rule to Display Captive Portals](#), on page 196.

Providing a Feedback Section in a Portal

The Feedback module in Cisco Spaces enables you to collect feedback from the customers of your portals. This module enables you to add multiple questions in the feedback section. These questions can be with multiple choice answers or rating-based answers. You can also provide a text box where the customers can add their comments.

To add a feedback section in a portal, perform the following steps:

-
- Step 1** Open the portal in which you need to add the feedback section.
- Step 2** Click the **Feedback** module.
The **FEEDBACK** window appears.
- Step 3** In the **Label** field, enter a name that must appear for the feedback section.
- Step 4** In the **Icon** area, upload the icon image that must appear adjacent to the feedback label using the **Upload** button.
- Step 5** In the **Question field**, enter a question for which you want the answer from the customer.
- Step 6** In the **Question Image** area, upload an image that must appear adjacent to the question using the Upload button.
- Step 7** In the **Question Type** area, choose any of the following:
- **Rating:** The customer can answer the question through rating.
 - **Multiple Choice:** The customer can answer from the multiple choices provided. If you have chosen this option, enter the multiple choice of answers in the Option 1 and Option 2 fields. If you want to provide more choices, add the choice options using the “Add option” button.
- Note** You can add more questions to the feedback section using the “Add question” button.
- Step 8** In the **Submit Button Label** field, enter the name for the submit button, using which the customer must submit the answer.
- Step 9** In the **Thank You/Success message** field, enter the message that must appear to the customer after the customer submits the answer.
- Step 10** In the **Post Submission button label** field, enter the name for the button that appears once the customer’s answer is submitted. This button leads the customer to the Cisco Spaces dashboard.
- Step 11** If you want to provide a text box for the customer to enter the comments, select the **Add a text box for additional comments from end user?** check box.
- Step 12** In the **Email to** field, enter the e-mail address to which the feedback is to be e-mailed.
- Step 13** In the **Email from** field, enter the **From** e-mail address to display to the receiver of the e-mail for the feedback e-mails.
- Step 14** In the **Email Subject** field, enter the subject for the e-mails with the feedback.
- Step 15** Click **Save**.

The feedback section is successfully created in the portal.

What to do next



Note If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the [Creating a Captive Portal Rule to Display Captive Portals, on page 196](#).

Adding a Help Option to a Portal

You can add a helpline in your Cisco Spaces portal using the Help module. The customers can use this helpline to contact you if they need any assistance. In this module, you can add a label and image for the area where the Helpline appears in the portal, and you can specify the number to contact if the customer needs any assistance.

The default name of the module is Help. The module name changes based on the changes you make in the Label field.

To add a Help option to a portal, perform the following steps:

Step 1 Open the portal in which you need to add a help option.

Step 2 Click the **Help** module.

The **HELP** window appears.

Step 3 In the **Label** field, enter the label that must appear for the area where the help line appears in the portal.

Note The Help module name gets changed to the name you specify in the **Label** field.

Step 4 In the **Icon** area, upload the help icon that must appear adjacent to the help label using the **Upload** button.

Note You can delete the icon using the Delete icon.

Step 5 In the **Contact** field, enter the help line number.

Step 6 Click **Save**.

The help option is successfully defined for the portal.

What to do next

Note If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the [Creating a Captive Portal Rule to Display Captive Portals, on page 196](#).

Adding Apps to a Portal

You can add apps to your Cisco Spaces portal using the Apps module. You can add apps from both iOS app store and Play Store. In this module, you can add a label and image for the area where the apps appear in the portal.

The default name of the module is Get Apps. The module name changes based on the changes you make in the **Button Label** field.

To add an app to a portal, perform the following steps:

-
- Step 1** Open the portal in which you need to add an app.
- Step 2** Click the **Get Apps** module.
The **GET APPS** window appears.
- Step 3** In the **Label** field, enter the label that must appear for the area where the app appears in the portal.
Note The **Get Apps** module name gets changed to the name you specify in the **Label** field.
- Step 4** In the **Icon** area, upload the app icon that must appear adjacent to the app label using the **Upload** button.
Note You can delete the icon using the Delete icon.
- Step 5** Click **Add an App**.
- Step 6** In the **Add App** area, do the following:
- From the **Platform** drop-down list, choose the app platform.
 - In the **App Store URL** field, enter the URL of the app store from which you want to add app.
 - In the **App URL Scheme** field, enter the URL scheme for your app that you receive when you install an app on your device.
 - To provide a different URL for the desktops and laptops, check the **Show this URL for Desktops and Laptops** check box.
 - If you have checked the **Show this URL for Desktops and Laptops** check box, enter the URL for desktops and laptops.
Note To add more apps, use the **Add an app** button.
- Step 7** Click **Save**.
The app is successfully added to the portal.
-

What to do next



Note If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the [Creating a Captive Portal Rule to Display Captive Portals, on page 196](#).

Providing Access to the Internet from a Portal

You can provide access to the internet from a portal using the Get Internet module. You can add an external URL to a portal using the Get Internet module. In this module, you can add a label and image for the area where the internet link appears in the portal.

The default name of the module is Get Internet. The module name changes based on the changes you make in the **Button Label** field.



Note If inline authentication is configured for the captive portal, the **Get Internet** module will not be shown during customer acquisition, even if it is configured. For more information on inline authentication, see the [Inline Authentication , on page 178](#).

To provide access to the internet from a portal, perform the following steps:

-
- Step 1** Open the portal in which you need to provide a link to the internet.
- Step 2** Click the **Get Internet** module.
The **GET INTERNET** window appears.
- Step 3** In the **Label** field, enter the label that must appear for the area where the internet link appears in the portal.
Note The **Get Internet** module name gets changed to the name you specify in the “Label” field.
- Step 4** Upload the icon that must appear adjacent to the internet link using the **Upload** button.
Note You can delete the image using the Delete icon.
- Step 5** To change the landing page, ensure that the **Change Landing page URL** check box is checked.
- Step 6** In the **Launch Page** field, enter the URL to connect to the internet from the portal.
- Step 7** Click **Save**.
An option to access the internet is successfully configured in the portal.
-

What to do next

Note If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the [Creating a Captive Portal Rule to Display Captive Portals, on page 196](#).

Adding Promotions and Offers to a Portal

The Promos & Offers module enables you add promotions and offers that you want to provide to the customers in your portal. You can add various promotion items in your portal that can be linked to different promotion URLs. The module enables you add a label, icon, and web URL for each promotion.



Note The promotions are displayed as carousels.

To add promotions and offers to a portal, perform the following steps:

-
- Step 1** Open the portal in which you want to add the promotions and offers module.
 - Step 2** Click the **Promos & Offers** module.
The **PROMOS & OFFERS** window appears.
 - Step 3** In the **Label** field, enter the label that must appear for the area in which the promotions and offers appear.
 - Step 4** Click **Add a Promotion**.
 - Step 5** In the **Promo Name** field, enter a name for the promotion link.
 - Step 6** In the **Promo Image** area, upload the icon that must appear adjacent to the promotion link using the **Upload** button.
 - Step 7** In the **Link Promo to URL** field, enter the URL that links to the promotion web page.
 - Step 8** Click **Save**.
The promotions and offers link is successfully added to the portal.
-

What to do next

Note You can add more than one promotion to your portal using the **Add a Promotion** button.



Note If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the [Creating a Captive Portal Rule to Display Captive Portals, on page 196](#).

Deleting a Promotion and an Offer for a Portal

Cisco Spaces enables you to remove a promotion from a portal after the required time line.

To delete a promotion from your portal, perform the following steps.

-
- Step 1** Open the portal from which you want to delete the promotion.
- Step 2** Click the **Promos & Offers** module.
- The **PROMOS & OFFERS** window appears with the promotions added to that portal.
- Step 3** Click the **Delete** icon that appears at the top right of the promotion that you want to delete.
-

Adding Custom Content and Menu Items to a Portal

The “Add Module” module enables you to add custom content and menu items in your portal according to your requirements. You can add various menu items to your portal that can be linked to different web pages. The module enables you add a label, icon, and web URL for each menu item. You can also enable a Back button, if the web page linked to is compatible.

To add a customized menu item to a portal, perform the following steps:

-
- Step 1** Open the portal in which you need to add custom menu item.
- Step 2** Click **Add Module**.
- Step 3** Choose any of the following:
- **Custom Content**—To include additional customized text in the portal.
 - **Menu Item**—To include Menu Items that links to a web page, in the portal.
- The custom module gets added to the portal module list, and opens the page for it. The fields that appears for the custom module depends on custom module type.
- Step 4** For “Custom Content”, enter the following details for the custom module.
- In the **HTML Module Name** field, enter a name for the module.
 - In the Rich field, add the content.
- Step 5** For **Menu Item** field, enter the following details for the custom module.
- a) In the **Label** field, enter the label that must appear for the custom menu item.
Note The Menu Item module name gets changed to the name you specify in the Label field.
 - b) In the Icon area, upload the icon that must appear adjacent to the menu item using the **Upload** button.
Note You can delete the icon using the Delete icon.
 - c) In the **Link to URL** field, enter the URL to which the menu item is to link.

Note You can enhance your URL using the smart link option. Click the **Add Variable** drop-down list to view the variables that you can add. For more information on creating a smart link, see the [Smart Links and Text Variables for Captive Portals, on page 238](#)

Step 6 To enable a back button in the linked web page, check the **Enable Back button** check box.

Step 7 Click **Save**.

The customized content or menu item is successfully added to the portal.

What to do next



Note The menu items added appear as text in the preview of the portal, but appear as links in the runtime.



Note If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see [Creating a Captive Portal Rule to Display Captive Portals, on page 196](#).

Exporting a Portal

Cisco Spaces enables you to export a portal created using the portal modules.

To export a portal, perform the following steps:

Step 1 Open the portal that you want to export.

Step 2 Click the **Eport Portal** icon at the top of the **Portal** window.

The Export Portal dialog box appears.

Step 3 Click **Download**.

Step 4 In the window that appears, do any of the following:

- a) To open the exported file directly, choose **Open**.
- b) To save the portal file on your computer, choose **Save File**.

The portal zip file is saved in the “Downloads” folder on your computer.

Note The portal is exported in the zip format.

Editing the Portal Style Sheet

The **Style Sheet Editor** option in Cisco Spaces enables you to update the style sheet of a portal. This helps you to change the font properties and outlook of your portal.

To edit a portal style sheet, perform the following steps:

-
- Step 1** Open the portal of which you want to edit the style sheet.
 - Step 2** Click **Stylesheet Editor** at the top of the **Portal** window.
 - Step 3** In the **CSS Editor** tab, make necessary changes in the style sheet.
 - Step 4** Click **Save**.
-

What to do next

You can upload the style sheet from an external source. For example, the CSS designed for another portal.

You can also download the style sheet to make necessary updates and upload the edited style sheet. For example, if you want a CSS designer to edit the portal, you can download the style sheet using the **Download CSS** button. After making the necessary changes to the style sheet, you can upload it to Cisco Spaces using the **Upload CSS** button.

Adding Assets to the Style Sheet

To improve the outlook of your portal, you can add assets such as images and fonts to the Stylesheet Editor of your portal. You can add image files such as jpeg, png, and tif. Edit your style sheet to incorporate these assets in the portal.

To add assets to a portal style sheet, perform the following steps:

-
- Step 1** Open the portal of which you want to edit the style sheet.
 - Step 2** Click **Stylesheet Editor**.
 - Step 3** Click the **Asset Library** tab.
 - Step 4** Drag and drop the asset file, or upload it using the **Choose File** button.

Note The maximum file size supported per attachment is 15 MB when you upload a new asset in the Asset Library of Captive Portals.

The file gets added to the assets list.

What to do next

You can copy the URL of an asset using the **Copy Asset url** button displayed for an asset at the bottom of the asset. To add this asset in your portal, add the URL in the style sheet in the appropriate location.

You can delete an asset using the delete icon displayed for the asset in the assets list.

Importing a Portal

Cisco Spaces enables you to import a portal from an external path. For example, if you want to enhance a portal using an external application, you can export the portal using the Export Portal icon, make necessary enhancements, and import the portal file to Cisco Spaces using the Import Portal option.

To import a portal, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Home**.
- Step 2** In the window that appears, click **Captive Portal**.
- Step 3** In the **Captive Portal** window, choose **Portal** in the left pane.
The **Captive Portal** window appears.
- Step 4** Click **Import Portal** at the top-right of the window.
- Step 5** In the **Import Portal** window that appears, do the following:
- In the **Portal Name** field, enter a file name for the portal.
 - Drag the drop the portal file to the window, or click the **Choose file** button, and choose the file that you want to import.
 - If you want this portal to be available for all the location, ensure that the **Add all locations to this portal** check box is checked. If you want the portal to be available only for the selected locations, uncheck the **Add all locations to this portal** check box, and select the locations for which the portal must be available.
The selected locations appear at the right side of the window.
- Step 6** Click **Import**.
-

What to do next



Note The portal is uploaded in the zip format.

Deleting a Portal

To delete a portal, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Home**.
- Step 2** In the window that appears, click **Captive Portal**.
- Step 3** In the **Captive Portal** window, choose **Portal** in the left pane.
The **Captive Portal** window appears with the list of available portals in Cisco Spaces.
- Step 4** Click the **Delete** icon that appears at the far right of the portal that you want to delete.
- Step 5** In the **Delete Portals** window that appears, click **Yes**.
The portal gets deleted from Cisco Spaces.

Note You can delete multiple portals simultaneously by selecting the check boxes adjacent to the portals that you want to delete, and clicking the **Delete** button that appears at the bottom of the window.

Note You cannot delete a portal that is associated with a captive portal rule.

Editing a Portal

To edit a portal, perform the following steps:

- Step 1** In the Cisco Spaces dashboard, choose **Home**.
 - Step 2** In the window that appears, click **Captive Portal**.
 - Step 3** In the **Captive Portal** window, choose **Portal** in the left pane.
The **Captive Portal** window appears with the list of available portals in Cisco Spaces.
 - Step 4** Click the **Edit** icon that appears at the far right of the portal that you want to edit.
 - Step 5** Make necessary changes and save the changes made for each module.
 - Step 6** To publish the changes, click the **Save and Publish** button for the portal.
-

Editing the Locations for a Portal

To edit the locations for a portal, perform the following steps:

- Step 1** In the Cisco Spaces dashboard, choose **Home**.
 - Step 2** In the window that appears, click **Captive Portal**.
 - Step 3** In the **Captive Portal** window, choose **Portal** in the left pane.
 - Step 4** In the **Captive Portal** window that appears, check the check box for the portal for which you want to edit the locations.
 - Step 5** Click **Add to Locations** that appears at the bottom of the window.
 - Step 6** In the **Add Locations to Portals** window that appears, select the locations for the portal, and click **Save Changes**.
 - Step 7** To publish the changes, click the **Save and Publish** button for the portal.
-

E-mailing a Portal Preview URL

You can e-mail the preview URL of a portal, so that the receiver can use this URL to preview the portal.

To e-mail the preview URL of a portal, perform the following steps:

- Step 1** Open the portal of which you want to e-mail the preview URL.
The portal appears.

- Step 2** Click the **Link** icon in the **Portal Preview** area at the far right of the window.
- Step 3** In the **Email Portal URL** field, enter the e-mail ID to which you want to e-mail the portal preview URL.
- Step 4** Click **Send**.
- A message appears stating the URL is sent to the e-mail address specified.
-

Previewing a Portal Using QR Code

Cisco Spaces enables you to preview the portal using the QR code for a portal. To use this feature, you need to have a QR code reader app installed on your mobile.

To scan the QR code of a portal, perform the following steps:

- Step 1** Open the portal of which you want to scan the QR Code.
- Step 2** Click the **Link** icon in the **Portal Preview** area at the far right of the window.
- Step 3** Open the QR code reader app on your mobile.
- Step 4** In the portal, focus the mobile on the area labeled **Scan with QR code reader on your mobile device**.
The mobile scans the QR code and displays the message whether to open the URL.
- Step 5** Click **Ok**.
The portal is opened in your mobile screen.
-

Previewing a Portal

Cisco Spaces enables you to view the outlook of the captive portal. Cisco Spaces enables you to preview each module in the captive portal separately. The default preview is of the Captive Portal home screen. The preview of authentication module simulates the customer acquisition (runtime) flow. The preview of modules appear as carousels.

To preview a captive portal, perform the following steps:

- Step 1** Open the portal of which you want to view the preview.
The preview of the portal home screen appears in the **Portal Preview** area.
- Step 2** Click the right arrow to navigate to the next screen.
-

Previewing the Portal in Various Devices

Cisco Spaces enables you to view the outlook of the captive portal in various devices. You can preview the portals for mobile, tablets, and laptops. Cisco Spaces enables you to preview each module in the captive portal separately. The default preview is of the Captive Portal home screen.

To preview a captive portal for a device, perform the following steps:

Step 1 Open the portal of which you want to view the preview in various devices.
The preview of the portal home screen appears at the devices are displayed in the right side of the portal
The **CSS Editor** window appears with device preview in the right pane.

Step 2 Do any of the following:

- To view the preview of the portal for mobile, click the tab for the mobile.
- To view the preview of the portal for tablet, click the tab for the tablet.
- To view the preview of the portal for laptop, click the tab for the laptop.

The preview of the captive portal home page for the selected device appears.

Step 3 To preview a particular module in the captive portal, from the adjacent drop-down list, select the module.

Note In the preview window, to view the preview of other devices, click the corresponding tabs. You can also scan the QR code, e-mail the portal URL, and change the orientation from the preview window.

Display, Hide or Reorder the Modules in a Captive Portal

The portal administrators can display or hide a module added to a portal by switching the ON/OFF toggle switch at the top left of the module. To reorder the modules, drag and drop the modules to the required location. The preview section reflects the changes.

Captive Portal Rule

The Captive Portal Rule enables you to manage the captive portal display and internet provisioning for the customers connecting to your SSIDs.

Using a Captive Portal Rule you can manage the captive portal display and internet provisioning in the followings ways:

- **Show Captive Portal**—When a customer filtered for the rule connects to the SSID configured for the rule, a captive portal is displayed. The customer can access the internet by clicking any menu item in the portal after completing the required authentication steps. You can configure to show different captive portals to the customers that suits them based on their location, number of visits, tags they belong to, number of visits made in your location, duration of their visits, and so on. You can restrict the duration for which internet must be provided for each session. Also, you can define the bandwidth required for the internet for this captive portal rule.
- **Direct Internet Access**—When a customer filtered for the rule connects to the SSID configured for the rule, the internet is provisioned immediately without any authentication process. The captive portal is not shown in this case.
- **Deny Internet Access**—When a customer filtered for the rule tries to connect to the SSID, connection cannot be established as internet is denied.

In addition, the Captive Portal rule enables you to do the following:

- Create tags or modify existing tags based on rule filtering.
- Send the details of the customers that are signed in to the captive portal to an external API.

In a Captive Portal rule, you can configure the actions to be performed, when the conditions defined are met. You can filter the customers for the rule based on various parameters such as locations, tags, number and duration of visits of the customers, app status, and so on.

This chapter describes how to create the captive portal rules.

Prerequisites for Creating a Captive Portal Rule

- To specify the locations for which the captive portal rule is applicable, you must define the location hierarchy. For more information on defining the location hierarchy, see the “Overview of Location Hierarchy” section.
- For the **CMX On Prem** option, ensure that all the required APs are added to the Cisco CMX.
- To specify the SSID for which you want to display the captive portal, you must import the SSIDs created in your wireless network system to Cisco Spaces. For more information on importing the SSIDs, see the [Importing the SSIDs from a Wireless Network, on page 205](#).
- To display a captive portal based on the captive portal rule, you must create the portal. For more information on creating the captive portal, see the [Creating and Managing Portal, on page 163](#).
- To specify the tags for which the rule is applicable, you must define the tags. For more information on creating the tags, see the "Creating or Modifying Tags Using a Location Personas App" section .
- 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 sent to the external API. For more information on configuring a data capture form, see the [Adding a Data Capture Form to a Portal, on page 178](#).
- RADIUS authentication is highly recommended for captive portals. RADIUS authentication is mandatory for **Seamlessly Provision Internet**, **Deny Internet**, and allowing users to define **Session Duration** and **Bandwidth**. To manage internet provisioning and RADIUS authentication, do the required configurations in your wireless network.
 - If your wireless network is Meraki, do the configurations mentioned in [Configuring Cisco Meraki for RADIUS Authentication, on page 92](#) .
 - If your wireless network is CUWN (Cisco AireOS), do the configurations mentioned in [Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication, on page 58](#).
 - If your wireless network is Cisco Catalyst 9800 Series Controller, do the configurations mentioned in [Captive Portal with RADIUS Server on DNA Spaces](#).

Creating a Captive Portal Rule to Display Captive Portals

Before creating a captive portal rule, ensure that all the prerequisites are met. To know the prerequisites for creating a captive portal rule, see the [Prerequisites for Creating a Captive Portal Rule , on page 196](#).

You can filter the customers for whom you want to apply the rule based on their location, whether the customer is an opted in or not opted in user, the tags the customers belong to, first time or repeat user, the number of visits made by the customer and so on. You can filter the locations in which the rule is to be applied based on the locations or the metadata associated with the locations. You can also apply the rule based on the number of visits made by the customer to the specified locations during the specified time. You can also configure to apply the rule only during a particular time with in a particular period, and only for certain days of a week.

The Captive Portal Rule also allows you to configure to provide direct internet connection when the customers filtered for the rule connects to your SSID. In this case, the captive portal is not displayed, but the customer will get access to the internet. You can also configure to deny the internet access to the customers filtered for a Captive Portal Rule.

Using a Captive Portal Rule, you can create new tags or modify existing tags with the customers filtered for the rule. The Captive Portal Rule also allows you send the details of the customers, connected to the SSID configured for the rule, to an external API.



Note If Cisco Wireless Controller is connected through Cisco CMX, ensure that all the required APs are added to the Cisco CMX for the Captive Portal rules to function. After defining the location hierarchy, if you are adding new APs to the Cisco CMX, the newly added APs get automatically displayed in the location hierarchy.

To create a captive portal rule to show a portal, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, click the **Captive Portal** app.
- Step 2** In the **Captive Portal** window that appears, click **Captive Portal Rule** in the left pane of the dashboard.
- Step 3** Click **Create New Rule** on the far right of the window.
- Step 4** In the **Rule Name** field, enter a name for the captive portal rule.
- Step 5** In the Sense area, perform the following steps:
- From the drop-down list after **When a user is on WiFi**, choose **WiFi**.
 - From the drop-down list after **and connected to**, choose the SSID for which you want to apply the rule.
- Note** The SSIDs are available for selection only if you have imported/configured the SSIDs. If the required SSID is not imported/configured, you can import/configure it using the **Configure SSID** button listed in the drop-down list. When you select the **Configure SSID** button, you are redirected to the **Import/Configure SSID** window. For more information on importing/configuring the SSIDs, see the [Importing the SSIDs from a Wireless Network, on page 205](#).
- 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 both Meraki and CUWN in a Captive Portal rule. For more information on creating the location hierarchy, see the [Defining the Location Hierarchy](#) section.
- You can again filter the locations based on the metadata defined for the selected location, or its parent or child locations. For more information on configuring the metadata for the locations, see the “[Defining or Editing Metadata for a Location](#)” section . You can either apply the rule for the locations with a particular metadata or exclude the locations with a particular metadata. For more information on filtering the locations, see the [Filtering by Location, on page 221](#).
- Step 7** In the IDENTIFY area, specify the type of customers for whom you want to apply the rule.

Note You can filter the customers for whom you want to apply the rule based on the on-boarding status of the customer, 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 Captive Portal rule is to apply, perform the following steps:

- a) If you want to filter the customers based on the on-boarding status of the customer, check the “Filter by On boarding Status” check box. If you want to filter the on-boarded customers (the customers who have completed the authentication process) for the rule, click the **Onboarded Visitor** radio button. If you want to filter the customers who have not on-boarded (the customers who have not completed the authentication process) for the rule, click the **Not Onboarded Visitor** radio button.
- b) If you want to filter the customer by the Opt In Status, check the **Filter by Opt-In Status** check box, and specify whether you want to filter the opted in users or not opted in users. For more information on opted in users, see the “Opted In Option for Users” section on page 6-5 .
- c) 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 rule must be applied or you can specify the tags for which the rule must not be applied. You can choose the best filtering method based on your requirement. For example, if you want to apply the rule for the customers in all the 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 apply the rule.

- To include the tags so that the rule is applied to the customers in the selected tags, use the **Add Tags** button for **Include**.
- To not apply the rule to the customers in the tags that are excluded, use the **Add Tags** button for **Exclude**.

For more information on using the tag filter, see the “Filtering by Tag” section.

- d) 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 for filtering. For more information on the visits and duration that you can configure, see the “Previous Visit Criteria” section .

Step 8 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 captive portal 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 captive portal 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 9 In the Actions area, configure the actions to be performed when the preceding conditions are met:

- a) To manage the internet provisioning for the customers filtered for the rule, choose the required option from the following:
 - **Show Captive Portal**—Choose this option to display a captive portal when the customers filtered for the Captive Portal rule connects to the SSID configured for the rule. From the **Select Captive Portal** drop-down list, choose the captive portal that you want to show when the conditions defined in this rule are met.

Note The portals that you have created for the chosen locations are available for selection. If you have not created the required portal, you can create it using the **Create Portal** button that is available in the **Select Captive Portal** drop-down list. When you select the **Create Portal** button, you are redirected to the **Create Portal** window. For more information on creating a portal, see the [Creating a Portal, on page 167](#).

- If you want to limit the period for which internet is to be provided for a session, check the **Session Duration** check box, and in the field that appears enter the session duration. You can specify the session duration in minutes, hours, or days.
- If you want to restrict the bandwidth for the internet provided for the customers based on this captive portal rule, check the Bandwidth check box, and in the bandwidth bar that appears, specify the bandwidth. You can define the bandwidth within a range of 1 kbps and 1 tbps.

Note The session duration defined here overrides the session expiry configuration in your wireless network such as Cisco Wireless Controller or Meraki. So, you can define more session duration for a captive portal than the one configured in your wireless network using this option.

- **Seamlessly Provision Internet:** Choose this option if you want to provide internet to your customers immediately after they connect to your SSID. In this case, the customer does not have to complete any authentication steps. To use this option, you must do certain configurations in your wireless network such as Cisco Wireless Controller or Meraki as mentioned in the [Prerequisites for Creating a Captive Portal Rule](#), on page 196. The data that is to be entered for this option depends on your wireless network.

- In the Rule/Policy Name field, enter a name for the policy. You must specify the same name that you have defined in the Wireless Network.

Note This field is not required for the Cisco Wireless Controller or Cisco 9800 Series Wireless Controllers.

- To specify the session duration, check the Session Duration check box, and in the **Enter Session Duration** field, mention the duration for which the you want to provide the internet access for each connection.
- To specify the bandwidth, check the Bandwidth the Limit check box, and specify the bandwidth using the bandwidth bar that appears. You can specify a maximum bandwidth of 1 tbps.

You can also use the **Show Manual Configuration** option to manually enter the bandwidth allowed for a Captive Portal Rule. This option enables you to configure the exact bandwidth you want to set rather than the predefined values. You can specify the bandwidth in KBPS, MBPS, GBPS, or TBPS.

Note The bandwidth field is not required for Meraki as the bandwidth configured in Cisco Meraki will be considered.

- **Deny Internet:** Choose this option if you want to deny the internet to the customers filtered for the rule when they try to connect to your SSID. In this case, the customers are not allowed to connect to the SSID.
- b) To create a tag for the customers who are filtered based on this captive portal rule or to add or remove the filtered customers from an existing rule, click the **Add Tags** button. For more information on using the tag filter, see the “Filtering by Tag” section ”.
 - c) If you want to send to an external API the details such as first name, last name, mobile number, and so on of the customers who have signed up to the captive portal configured for this rule, check the **Trigger API** check box, and do the necessary API configurations. For more information on API configurations, see [Trigger API Configuration for Notification](#).

Note The summary of the rule is shown on the right side of the window.

Step 10 Click **Save and Publish**.

The rule gets published and listed in the **Captive Portal Rules** window.

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 **Captive Portal Rules** window.

Use Case: Captive Portal Rule

XYZ is a business group that is engaged in different streamlines of business from mobile stores to supermarkets. XYZ has 5 mobile stores and 4 supermarkets at various locations in New York. The SSID name of XYZ in New York is XYZID. XYZ wants to show a captive portal C1, that displays the offers available for various items in the supermarket, when the customers connect to XYZID from XYZ's supermarkets. Similarly, a captive portal, C2, must be shown to customers who connect to XYZID from XYZ's mobile stores. The captive portal must be shown to the users who have not opted in.

Locations with super markets: L1, L2, L3, L4, L5

Locations with mobile stores: L7, L8, L9, L10

To achieve the preceding scenario, perform the following steps:

- Step 1** In the Cisco Wireless Controller, define the mode for access points, create the ACLs, and create the SSID, XYZID. For more information on the Cisco Wireless Controller configurations, see the [Importing the SSIDs for Cisco Meraki, on page 206](#).
- Step 2** Log in to Cisco Spaces.
- Step 3** Add XYZID to Cisco Spaces using the Import SSID option.
- Step 4** Create the location hierarchy for XYZ. In the location hierarchy, all the supermarkets and mobile store of XYZ in New York must be defined as locations under the location, New York. Add a location metadata for the locations L1, L2, L3, L4, and L5 with key as **StoreType** and value as **SM**. Add a location metadata for the locations L7, L8, L9, and L10 with key as **StoreType** and value as **MS**. For more information on defining the location metadata, see the “Defining or Editing Metadata for a Location” section.
- Step 5** Create portal **C1** for supermarket and portal **C2** for mobile stores. For more information on creating the portals, see the [Creating a Portal, on page 167](#).
- Step 6** In the Cisco Spaces dashboard, choose **Home**.
- Step 7** In the window that appears, choose **Captive Portal**.
- Step 8** In the **Captive Portal** window, choose **Captive Portal Rule** in the left pane.
- Step 9** Click **Create New Rule**.
- Step 10** In the **RULE NAME** enter the name, **R1**, for the captive portal rule.
- Step 11** From the **When a user is on** drop-down list, choose **WiFi**, and from the **add Connected to** drop-down list, choose **XYZID**.
- Step 12** In the Locations area, perform the following steps:
- Click the **Add Locations** button, and in the **Choose Locations** window that appears, select the location for New York, and click **Ok**.
 - Check the **Filter by metadata** check box, and click the **Add Metadata** button for Filter.
 - In the **Choose Location Metadata** window, choose the key, **StoreType**, and choose the value **SM**.

Note As the location metadata **StoreType** is defined for the locations that are under the location **New york**, it will be available for selection in the **Choose Location Metadata** window.

- Step 13** In the Identify area, check the **Filter by Opt-In Status** check box, and choose **Only for not opted-in Visitor**.
- Step 14** 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 this year.
- Step 15** In the Actions area, choose **Show Captive Portal**, and from the **Select Captive Portal** drop-down list, choose **C1**.
- Step 16** Click **Save and Publish** .
The rule gets published.
- Step 17** Similarly, create another rule, **R2**, for the Mobile Group, with the location metadata key as **StoreType** and value as **MS**, and the captive portal, **C2**.
- Now, when a customer visits XYZ's super market and connects to XYZID, **C1** is shown. When the same customer connects to XYZID from XYZ's mobile store, **C2** is shown.
-

Reports

Cisco Spaces provides the following captive portal reports:

By default, the report is provided for all the location for the last one year. You can filter the location and duration for the report.

To view the report, click **Reports** on the left pane of the **Captive Portal** window.

Device Onboarding

The Device Onboarding report provides information about the devices that have connected to your SSIDs. If a customer is connecting to your SSID from more than one device, each such device is counted to calculate the number of devices.

In the **Device Onboarding** report, the **Promos & Offers Performance** section includes promo views count. This feature enables you to track the number of view for a specific promotion along with the number of clicks.

Onboarding Journey

This section displays the count of unique devices for the selected location and period.

- **Connected to SSID:** The total number of unique devices that have connected to your SSIDs from the selected location during the time period specified.
- **Shown Captive Portal:** The total number of unique devices that have connected to your SSIDs, and got the captive portal loaded successfully, from the selected location during the time period specified.
- **Provisioned Internet:** The total number of unique devices that got internet provisioned from the selected location during the specified period. This metrics for all the locations from the date of deployment of Cisco Spaces is shown at the top of the report for **Total Unique Devices Provisioned Internet**.

Daily Trend: New v/s Returning Devices Connected to the SSID

This section displays the daily trend of the new and returning unique devices that have connected to your SSIDs from the location for the specified time period.

- **New Devices:** The total number of new unique devices that have connected to your SSIDs from the selected location during the specified time period. The percentage of new unique devices out of the total number of devices is also shown.
- **Returning Devices:** The total number of unique devices that have connected to your SSIDs from the selected location more than once during the specified period. The percentage of unique returning devices out of the total number of unique devices connected is also shown.

The graph represents the unique New v/s Returning devices connected from the selected location on each day of the specified period. X-axis of the graph represents the days in the selected period, and Y-axis represents the number of unique devices. The color indicators for new and returning unique devices are displayed at the top of the graph.

Menu Button Clicks in Captive Portal

This section displays the details of daily engagements of customers through promotions and offers. Daily engagement through promotions and offers is calculated based on the menu buttons that the customers have clicked during the specified period.

- **Menu buttons:** The total number of menu buttons that were clicked at least once from the selected location during the specified period.
- **Clicks:** The total number of clicks made in the captive portals from the selected location during the specified period.

Customer Acquisition

This report provides insights on the unique customers acquired newly from the selected location during the specified period, and the data (personal and demographic) collected from the acquired customers.



Note If a new customer connects to your location using multiple devices, and uses the same personal identity (mobile number, e-mail, or social ID), the customer is counted only once.

Customer Acquisition



Note This report will not count the customers who are acquired through the authentication types, "No Authentication" and "Access Code".

- **New Devices Connected to SSID:** The total number of new unique devices that have connected to your SSIDs from the selected location during the specified time period. The percentage of new unique devices out of the total number of devices is also shown.

- **News Customers Identified:** The total number of unique new customers that got acquired through any of personal identifiers such as mobile number, e-mail, or social ID from the selected location during the specified period. The percentage of new unique customers acquired out of the total new unique devices connected is also shown. This metrics for all the locations from the date of installation of Cisco Spaces is shown at the top of this report for “Customers Identified”.
- **Customers Opted In:** The total number of “unique new customers acquired” who have opted in for subscription from the selected location during the specified period. The percentage of opted-in “unique new customers acquired” out of the total number of “unique new customers acquired” is also shown. For more information on opted-in users, see the “Opted In Option for Users” section.
- **Completed Data Capture:** The total number of “unique new customers acquired through any of personal identifiers such as mobile number, e-mail, or social ID”, and have completed the data capture form from the specified location during the specified period. The percentage of “unique new customers acquired” who have completed the data capture out of the total number “unique new customers acquired” is also shown.

Daily Customer Acquisition

This section displays a bar graph that shows the count of “unique new devices connected to your SSIDs” and “unique new customers acquired through any of personal identifiers such as mobile number, e-mail, or social ID”, from the selected location during the specified period. It also shows the daily count of “unique new customers acquired” who have opted-in for subscription and completed the data capture. X-axis represents the days in the selected period. Y-axis represents the count. The color indicators are shown at the top of the graph. Mouse-over the graph to view the count for a particular day.



Note This report will not count the customers who are acquired through the authentication types, "No Authentication" and "Access Code".

Captured Data

This section displays the number of e-mail addresses, phone numbers, names, gender details, and so on captured from the selected location during the specified period.

- **Phone Number**—The total number of unique phone numbers captured from the specified location during the specified period.
- **Emails**—The total number of unique e-mail addresses captured from the specified location during the specified period.
- **Social ID**—The total number of unique social IDs captured, through social authentication, from the specified location during the specified period.
- **Names**—The total number of customers/devices from which the names (first name/last name) are captured from the specified location during the specified period.
- **Gender**—The total number of customers/devices from which gender is captured from the specified location during the specified period.

Customer Distribution

This section displays the profile details such as country, gender, and language captured newly from the selected location during the specified period.

Countries: Displays a pie chart with the percentage of customers from different countries out of the total number of customers for whom the country data is collected. The total number of countries is displayed at the center of the pie chart, The countries with highest number of customers are displayed below the pie chart with the count of customers. You can view all the countries, with at least one customer, by clicking the “Show All” button. Country names are derived based on the country code of the phone numbers specified during the authentication process.

Languages: Displays a pie chart with the percentage of customers who used various languages out of the total number of customers for whom the language data is collected. The languages that are used the most by customers are displayed below the pie chart with the count of customers. You can view all the languages, used at least by one customer, by clicking the “Show All” button. Language count is derived based on the language selected by the customer in the captive portal.

Gender: Displays a pie chart with the percentage of male, female, and "gender not specified" customers out of the total number of customers. The total percentage of the customers that has provided the gender details is displayed at the center of the pie chart. The count of the male, female, and unknown gender customers are displayed at the bottom of the pie chart.

SSIDs

The SSID refers to wireless network ID your customers connect to access the internet. You might be having multiple SSIDs for your business locations. Cisco Spaces allows to display different captive portals for same SSID or various SSIDs in your business locations based on your requirement.

The SSIDs are defined in the Wireless Network System. For example, Cisco Wireless Controller for Cisco Unified Wireless Network. To define the captive portals to be displayed for an SSID, you must import the SSID to Cisco Spaces.

The imported SSIDs will be shown in grid view. Each Meraki SSID will have a “Detail” link using which you can configure the SSID in Meraki. If required, you can delete the imported SSID for a wireless network from the grid.

The **Configure Manually** link for a **SSID** leads you to the manual configuration instructions for the corresponding wireless network. For example, the “Configure Manually” link for the Meraki SSIDs lead to the configuration instructions for Cisco Meraki.

Cisco Spaces enables you to delete the SSIDs even if they are not deleted from the wireless network such as Cisco Meraki. This will you to delete unwanted SSIDs during delay in network synchronization.

Prerequisites for Importing or Configuring the SSIDs

To import/configure the SSIDs to Cisco Spaces, you must do the following:

- Create the location hierarchy. For more information on creating the location hierarchy, see [Overview of Location Hierarchy](#).
- Create the SSIDs in the Wireless Network System.

- For creating the SSIDs for the CUWN, see the [Configuring Cisco Wireless Controllers and Cisco Catalyst 9800 Series Controllers for Cisco Spaces, on page 45](#) chapter.
- For creating the SSIDs for Meraki, see the [Enabling SSIDs in Cisco Meraki, on page 91](#) section .
- For Meraki, to import the SSIDs, Cisco Spaces and Meraki must be connected. The connection is usually established when defining the location hierarchy. You can also connect to Meraki using the Wi-Fi icon at the top right of the Cisco Spaces dashboard.

Importing the SSIDs from a Wireless Network

Before importing an SSID, ensure that the prerequisites are met. For more information on the prerequisites to import an SSID, see the [Prerequisites for Importing or Configuring the SSIDs, on page 204](#).



Note To create a captive portal rule for an SSID, you must import that SSID from the CUWN or Meraki.

Importing the SSIDs for Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller



-
- Note**
- For the Cisco AireOS Series Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller, you must manually add the SSIDs to Cisco Spaces.
 - For Cisco AireOS Series Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller with CMX, the SSIDs are configured in the Cisco Wireless Controller, not in the Cisco CMX.
 - The SSID name you specify in Cisco Spaces must match with the SSID name configured in the controller. You can view the SSID name in the controller dashboard.
 - 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.
-

To manually import the SSIDs to Cisco Spaces, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Home**.
 - Step 2** In the **My Apps** area, click **Captive Portal**.
 - Step 3** In the **Captive Portal** window that appears, choose **SSIDs** in the left pane.
 - Step 4** Click **Import/Configure SSID**.
 - Step 5** In the **Import/Configure SSID** window that appears, from the **Wireless Network** drop-down list choose **CUWN (CMX/WLC)**.
 - Step 6** In the SSID field, enter the name of the SSID you want to import, and click **Add**.

The imported SSID appears in the **SSIDs** window.

What to do next



Note As Cisco Spaces needs to synchronize with the controller to load the imported SSIDs, you may need to refresh the window to view the imported SSIDs.

Importing the SSIDs for Cisco Meraki

To create the Captive Portal rules for an SSID of Meraki, you must import that SSID from the Meraki network. After importing the SSIDs, in the Meraki dashboard, you must configure the SSID for working with Cisco Spaces.



Note You can import the SSIDs only for those locations that are imported to the location hierarchy.

To import the SSIDs, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Home**.
 - Step 2** In the **My Apps** area, click **Captive Portal**.
 - Step 3** In the **Captive Portal** window that appears, choose **SSIDs** in the left pane.
 - Step 4** Click **Import/Configure SSID**.
 - Step 5** In the **Import/Configure** window that appears, from the **Wireless Network** drop-down list, choose **Meraki**.
 - Step 6** From the Organization drop-down list, choose the organization of which you want to import the SSID.
The SSIDs enabled in Meraki for the selected organization are available for selection.
 - Step 7** Check the check box for the SSID that you want to import, and click **Import**.
The imported SSID appears on the **SSIDs** window.
 - Step 8** In the grid for that SSID, click the **Detail** link.
 - Step 9** On the window that appears, click **Activate** for the SSID to update the Cisco Spaces configurations for the SSID in Meraki.
The **SSID Configuration Sync** window appears with the SSID updates that need to be configured in Meraki.
 - Step 10** Click **Update**.
- Note** You can manually also configure the SSIDs in Meraki. To know how to manually configure the SSIDs in Meraki, see the “Manually Configuring SSIDs for Cisco Meraki” section.
-

What to do next



Note As Cisco Spaces needs to synchronize with the Meraki network to load the imported SSIDs, you may have to refresh the window to view the imported SSIDs.

Access Codes

Cisco Spaces enables you to control the internet provisioning in your business premises using access codes. You can create access codes for your various locations and restrict the internet access for these locations using the access codes. That is, the customers can access the internet only after providing an access code configured for that location. This section describes how to create and manage the access codes using Cisco Spaces.

To use this feature, you must configure access code authentication for your captive portals. For more information on configuring access code authentication for captive portals, see [Configuring a Portal for Access Code Authentication, on page 176](#)

Cisco Spaces enables you to share with the customers the access codes that you have created. You can specify the validity period for an access code. You can configure to have a single code value for an access code, or to change the code value weekly or monthly. You can manually specify the code values for an access code or choose to auto-generate. You can define the time for which the customers can access the internet using an access code. Cisco Spaces also enables you set the download and upload bandwidth limits for access codes, when accessing the internet using a particular access code.

You can define multiple access codes for a single location. For example, if you want to provide a high speed internet only for your platinum members, you can create an access code with maximum bandwidth and create another access code with limited bandwidth. You can then share the access codes based on the type of the customer.

To know the authentication steps for an access code authentication, see [Steps for Access Code Authentication, on page 235](#).

You can also create a single-use access code. Choose **Captive Portal > Access Code > Create Access Code** to create a new single-use access code. For more information, see [Create a Single-Use Access Code, on page 210](#).



-
- Note**
- Only a Cisco Spaces user with account admin or access code manager rights can create or manage the access code
 - Only a Cisco Spaces Account Admin user can invite a user as an Access Code Manager. The Access Code option is available in the Cisco Spaces dashboard only for an Account Admin or Access Code Manager account.
 - The **Session Duration** and **Bandwidth Limit** configured at the access code level will now be considered by the captive portal. During authentication, the values are passed to the controller and override any default settings done at the controller for session duration and bandwidth.
-

Creating an Access Code

To create an access code, perform the following steps:

Step 1 In the Cisco Spaces dashboard, click **Captive Portals**.

Step 2 In the left pane of the window that is displayed, click **Access Code**.

Note The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spaces user, see the [#unique_266](#).

Step 3 From the **Location** drop-down list, choose the location for which you want to define the access code.

Step 4 Click **Create Access Code**.

Step 5 In the **Create Access Code** window, click **Shared Access Code** tab.

Step 6 In the **Shared Access Code** tab, choose the type of access code that you want to create. The options are:

- **Fixed:** The code value remains the same till the time the access code is valid.
- **Weekly:** The code value for the access code changes every week
- **Monthly:** The code value for the access code changes every month.

The remaining fields that appear depends on the access code type that you have selected.

If you choose the access code type as **Fixed**, enter the following details:

- a) In the **Access Code Name** field, enter a name for the access code.
- b) If you want to define your own code values for the access code, check the **Set your own access code?** check box.
- c) In the **Access Code** field that appears, enter the code value.
- d) Specify the time for which the customer could access the internet using the access code by adjusting the **Limit session by time** bar. This time is for a single session.
- e) If you want to define a validity period for the access code, check the **Define a validity period for this access code** check box. Specify the start date and end date by clicking the respective buttons.
- f) If you want to limit the bandwidth when the customer accesses the internet using this access code, check the **Limit bandwidth** check box.
- g) Specify the maximum bandwidth that must be provided to the customer when accessing the internet using this access code by adjusting the **Bandwidth Limit** bar.
- h) Click the **Show More** link, and specify the upload and download limits.
- i) From the **Number of times access code can be used** drop-down list, choose the maximum number of times a customer can access the internet using this access code

If you choose the access code type as **Weekly**, enter the following details:

- a) In the **Access Code Name** field, enter a name for the access code.
- b) Specify how to generate the access code.
 - If you want to specify your own code values for all the weeks, check the **Upload access codes from the csv file** check box. You can download the access code template by clicking the link in the message box. After entering all the code values for all the required weeks in the template, you can upload the template as a csv file using the **Upload** button.

- If you want to generate the code values for all the weeks automatically, specify the period for which this access code is valid in weeks by adjusting the “Access Code Validity time period” bar.

Note The **Access Code Validity time period** bar will be available only if you have not selected the **Upload access codes from the csv file** check box. If you have selected the **Upload access codes from csv File** check box, the validity period is considered based on the number of code values entered in the csv file. For example, if you define three code values in the csv file, then the access code is valid for three weeks. The code values mentioned in the csv file are considered sequentially for each week.

- c) Specify the time for which the customer could access the internet using the access code by adjusting the **Limit session by time** bar. This time is for a single session.
- d) Click the **Start Date** button, and specify the date from which the access code is valid.
- e) If you want to limit the bandwidth when the customer accesses the internet using this access code, check the **Limit bandwidth** check box.
- f) In the **Bandwidth limit** bar that appears, specify the maximum bandwidth that must be provided to the customer when accessing the internet using this access code by adjusting the bar.
- g) Click the **Show More** link and specify the upload and download limits.
- h) From the **Number of times access code can be used** drop-down list, choose the maximum number of times a customer can access the internet using this access code.

If you choose **Monthly**, enter the following details:

- a) In the **Access Code Name** field, enter a name for the access code.
- b) Specify how to generate the access code.
 - If you want to specify your own code values for all the months, check the **Upload access codes from the csv file** check box. You can download the access code template by clicking the link in the message box. After entering all the code values for all the required months in the template, you can upload the template as a csv file using the **Upload** button.
 - If you want to generate the code values for all the months automatically, specify the period for which this access code is valid in months by adjusting the **Access Code Validity time period** bar.

Note The **Access Code Validity time period** bar will be available only if you have not checked the **Upload access codes from the csv file** check box. If you have checked the **Upload access codes from the csv file** check box, the validity period is considered based on the number of code values entered in the csv file. For example, if you define three code values in the csv file, then the access code is valid for three months. The code values mentioned in the csv file are considered sequentially for each month.

- c) Specify the time for which the customer could access the internet using the access code by adjusting the **Limit session by time** bar. This time is for a single session.
- d) Click the **Start Date** button, and specify the date from which the access code is valid.
- e) If you want to limit the bandwidth when the customer accesses the internet using this access code, select the **Limit bandwidth** check box.
- f) In the **Bandwidth limit** bar that appears, specify the maximum bandwidth that must be provided to the customer when accessing the internet using this access code by adjusting the bar.
- g) Click the **Show More** link, and specify the upload and download limits.
- h) From the **Number of times access code can be used** drop-down list, choose the maximum number of times a customer can access the internet using this access code.

Step 7 Click **Create**.

Create a Single-Use Access Code

To create a single-use access code, perform the following steps:

Step 1 In the Cisco Spaces dashboard, click **Captive Portals**.

Step 2 In the left pane of the window that is displayed, click **Access Code**.

Note The Access Code option is available in the Cisco Spaces dashboard only if you are a user with Cisco Spaces Account Admin or Access Code Manager privileges. For more information about creating a Cisco Spaces user, see [#unique_266](#).

Step 3 From the **Location** drop-down list, choose the location for which you want to define the access code.

Step 4 Click **Create Access Code**.

Step 5 In the **Create Access Code** window, click **Single Use Access Code** tab.

Step 6 In the **Single Use Access Code** tab, do the following:

- **Access code name:** Enter the name for the new single-use access code.
- **Access code type:** To select the access code type, click either the **Numeric** or the **Alphanumeric** radio button.
- **# of Access Code:** Enter the number of access codes that you want to create. The default value is 1.
- **# of Characters:** Enter the number of characters required in the access code. A single-use access code must include a minimum of three characters.
- **Limit session by time:** Use the slider bar to set the session limit time. The valid range is from 30 minutes to three months.
- **Define a validity period for this access code:** Enter the following dates, using the calendar, to set a validity period for the access code:
 - **Start Date**
 - **End Date**
- **Limit bandwidth:** Check the check box to limit the bandwidth to 1 Mbps.

Step 7 Click **Create**.

The generated access code is for one-time use only. If the access code has been used previously, the following error message is displayed:

```
invalid access code
```

The status of the new access code is shown as **Available** in the **View Access Codes** window. After the access code is used, the status changes to **Used**.

Viewing an Access Code

You can view all the access codes for a location of which the validity period has not yet expired.

To view the access codes defined for a location in the Cisco Spaces, perform the following steps:

Step 1 In the Cisco Spaces dashboard, click **Captive Portals**.

Step 2 In the left pane of the window that is displayed, click **Access Code**.

Note The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spaces user, see the [#unique_266](#).

Step 3 In the **Access Code** window that appears, from the drop-down list, choose the location for which you want to view the access codes.

The access codes defined for the location appears.

For the location selected, the total number of access codes available, the total number of expired access codes, and number of active and inactive access codes among them are displayed.

In addition, the following details of the access codes defined for the location are displayed:

- **Status:** Whether the access code name is active or not.
- **Name:** The name of the access code.
- **Code:** The code value for the access code name at the time of viewing the access code. The code value changes if it is set to change weekly or monthly.
- **Type:** The access code type. The access code type can be fixed, or that changes weekly or monthly.
- **Expiry Date:** The period for which the access code is valid.
- **Actions:** The actions such as edit, share, and delete that you can perform for an access code.

Editing an Access Code

To edit an access code, perform the following steps:

Step 1 In the Cisco Spaces dashboard, click **Captive Portals**.

Step 2 In the left pane of the window that is displayed, click **Access Code**.

Note The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spaces user, see the [#unique_266](#).

Step 3 In the **Access Code** window that appears, select the location for which you want to edit the access code.

The access codes defined for that location appear.

Step 4 In the **Active Access Codes** area, for the access code that you want to edit, click the **Edit** button.

Step 5 Make necessary changes, and click **Update**.

Sharing an Access Code

Cisco Spaces enables you to share access codes with your customers.

To share an access code, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, click **Captive Portals**.
- Step 2** In the left pane of the window that is displayed, click **Access Code**.
- Note** The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spaces user, see the [#unique_266](#).
- Step 3** In the **Access Code** window that appears, select the location for which you want to share the access code. The access codes defined for that location appear.
- Step 4** In the **Active Access Codes** area, for the access code that you want to share, click the **Share** button.
- Step 5** In the **Share Access Code** window that appears, enter the e-mail ID of the person to whom you want to share the access code, and click **Invite**.
-

Deleting an Access Code

To delete an access code, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, click **Captive Portals**.
- Step 2** In the left pane of the window that is displayed, click **Access Code**.
- Note** The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spaces user, see the [#unique_266](#).
- Step 3** In the **Access Code** window that appears, select the location for which you want to delete the access code. The access codes defined for that location appear.
- Step 4** In the **Active Access Codes** area, for the access code that you want to delete, click the **Delete** button.
- Step 5** In the **Delete** window that appears, click **Yes** to confirm the deletion.
- Note** You can delete multiple access codes simultaneously. A check box will appear for each access code so that you can select multiple access codes at a time, and delete them simultaneously. You can also delete the expired access codes.
-

Deactivating an Access Code

To deactivate an access code, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, click **Captive Portals**.
- Step 2** In the left pane of the window that is displayed, click **Access Code**.
- Note** The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spaces user, see the [#unique_266](#).
- Step 3** In the Access Code window that appears, select the location for which you want to deactivate the access code. The access codes defined for that location appear.
- Step 4** Swap the “Status” toggle switch for the access code that you want to deactivate. If deactivated, the status button turns grey.
-

Reactivating an Access Code

By default, an access code is in the active mode when it is created. Once you deactivate it, you can activate it whenever required, provided the validity period for the access code is not expired.

To reactivate an access code, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, click **Captive Portals**.
- Step 2** In the left pane of the window that is displayed, click **Access Code**.
- Note** The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spaces user, see the [#unique_266](#).
- Step 3** In the **Access Code** window that appears, select the location for which you want to activate the access code. The access codes defined for that location appear.
- Step 4** Swap the “Status” toggle switch for the access code that you want to activate. If activated, the status button turns green.
-

Exporting Access Codes

Cisco Spaces enables you to export access codes created for a location to a .csv file or as a PDF.

To export the access codes defined for a location in the Cisco Spaces, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, click **Captive Portals**.
- Step 2** In the left pane of the window that is displayed, click **Access Code**.

Note The Access Code option will be available in the Cisco Spaces dashboard only if you are a Cisco Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco Spaces user, see the [#unique_266](#).

Step 3 In the **Access Code** window that appears, from the drop-down list, choose the location for which you want to export the access codes.

For the location selected, the total number of access codes available, total number of expired access codes, and number of active and inactive access codes among them are displayed.

Step 4 Do any the following based on the format required:

- To export the access codes as a PDF file, choose **Export > Export as PDF**.
- To export the access codes as a .csv file, choose **Export > Export as CSV**.

Step 5 In the window that appears, click **OK** to save the file.

The access codes get downloaded to the **Downloads** folder in your computer in the format specified.

Note Only the access codes that are active get exported.

What to do next

If you want to export expired access codes or if you want to export the access codes that are valid during a particular period, you can do it using the **Filter** option.

Filtering Access Codes to Export

To filter the access codes to be exported, perform the following steps:

Step 1 In the **Access Code** window, from the drop-down list, choose the location for which you want to export the access codes.

Step 2 Click **Filter**.

- **All Access Codes**: Exports all the access codes created for the selected location, including active and expired.
- **Filter by**: Exports the access codes based on the filter applied. You can choose to filter the access codes that expires on the current week, current month, or on a particular date range. Similarly, you can also filter the access codes that expired during current week, current month, or during a particular date range. You can simultaneously include both expired and active access codes using **Expires in** and **Expired** options.

Step 3 Click **Apply**.

The filtered access code gets displayed in the **Filtered Access Codes** window.

Step 4 Do any the following based on the format required:

- To export the access codes as a PDF file, choose **Export > Export as PDF**.
- To export the access codes as a .csv file, choose **Export > Export as CSV**.

Step 5 In the window that appears, click **OK** to save the file.

The access codes get downloaded to the **Downloads** folder in your computer in the format specified.

User Management

The **User Management** option allows you to invite Captive Portal users with the user roles, **Creative User** or **AccessCodeManager**. Only a user with read and write permission on Captive Portals app can invite other users using the **User Management** option.

- **Creative User:** This user can create, view, and edit the captive portals in the locations for which access rights are provided. This user will not have access to any other feature of Cisco Spaces. This role is basically for captive portal designers.
- **AccessCodeManager:** This user can create access codes and manage the access codes for the location for which access rights are provided. This user will have access only to the **Captive Portals** app. This role is basically for access code managers.

The roles are listed on the **Roles** tab. You cannot edit the roles from the **Roles** tab.

To define an Access Code Manager or Creative User, perform the following steps:

Step 1 In the Cisco Spaces dashboard, choose **Home**.

Step 2 Click **Captive Portals**.

Step 3 In the window that appears, click **User Management** in the left pane.

Note The **User Management** option will be available in the Cisco Spaces dashboard only for a user with read and write permission on Captive Portals app. For more information, see [#unique_266](#).

Step 4 Click **Invite User**.

Step 5 In the **Invite User** window, enter the e-mail address of the user whom you want to invite., and click **Next**.

Step 6 From the **Role** drop-down list, choose **Creative User** or **AccessCodeManager**.

Step 7 Click **Location**.

Step 8 In the **Location Hierarchy** area, check the check boxes for the locations for which you want to give access to this particular user.

Step 9 Click **Done**.

Step 10 Click **Send Invitation**.

An invitation is sent to the user. The user name gets listed in the **Users** tab. You can search for a user using the **Find Users** field.

Social Authentication for Portals

To enable social authentication for the portals, perform the following steps:

- [Configuring a Portal for Social Sign In Authentication, on page 175](#)

Configuring the Wireless Network for Social Authentication

For social authentication, you must do some configurations in your wireless network such as Meraki and CUWN. For more information, refer to the following links:

- [Configuring Cisco Meraki for Social Authentication, on page 94](#)
- [Configuring Cisco Wireless Controller for Social Authentication, on page 60](#)

Configuring the Apps for Social Authentication

The configuration required in the apps for the social-authentication through various networking sites is described in this section.

Facebook

To configure the Facebook app for the social-authentication, perform the following steps:

-
- Step 1** Go to developers.facebook.com.
- Step 2** From the **My Apps** drop-down list, choose the app that you want configure in Cisco Spaces for social-authentication.
- Step 3** Click **Settings**.
- Step 4** In the **App Domains** field, based on the region, enter the appropriate value from the list below:
- For US, enter `splash.dnaspaces.io`.
 - For EU, enter `splash.dnaspaces.eu`.
- Step 5** In the **User Data Deletion** field, enter the appropriate **Data Deletion Callback URL**, based on the region, from the list below:
- For US, enter `https://splash.dnaspaces.io/p/<CustomerAccountName>/fb_revoke`.
 - For EU, enter `https://splash.dnaspaces.eu/p/<CustomerAccountName>/fb_revoke`.
- Step 6** In the **Facebook Login Settings** tab, in the **Valid OAuth Redirect URIs** field, based on the region, enter the appropriate value from the list below:
- For US, enter https://splash.dnaspaces.io/p/facebook_auth.
 - For EU, enter https://splash.dnaspaces.eu/p/facebook_auth.
-

Twitter

To configure the Twitter app for the social-authentication, perform the following steps:

-
- Step 1** Log in to <https://developer.twitter.com/en/apps>.
- Step 2** Click the app that you want to configure in Cisco Spaces for social-authentication.
- Step 3** Click the **Settings** tab.
- Step 4** In the **Callback URL** field, enter the callback URL.
- Global Redirect URL: https://splash.dnaspaces.io/p/twitter_auth
 - Redirect URL for EU: https://splash.dnaspaces.eu/p/twitter_auth
- Step 5** Uncheck the **Enable Callback Locking** check box.
- Step 6** Check the **Allow this application to be used to Sign in with Twitter** check box.
- Step 7** To get information from Twitter, in the **Permissions** tab, do the following:
- In the **Access Permissions** area, select the **Read and write** radio button.
 - In the **Additional Permissions** area, check **Request email address from users**.

LinkedIn App

-
- Step 1** Log in to <https://www.linkedin.com/developers/>.
- Step 2** Click **My Apps** .
- Step 3** Click the app that you want to configure for the social-authentication.
- Step 4** Click **Authentication** .
- Step 5** In the Default Application Permissions area, select the **r_basicprofile** and **r-emailaddress** check boxes.
- Step 6** In the Authorized Redirect URLs field, enter the redirect URL, and click **Add**.
- Global Redirect URL: https://splash.dnaspaces.io/p/linkedin_auth
 - Redirect URL for EU: https://splash.dnaspaces.eu/p/linkedin_auth
- Step 7** In the **Settings** tab, configure the domain **splash.dnaspaces.io**.
- For the **EU** region, the domain is **splash.dnaspaces.eu**.

Adding Social Apps for Social Authentication

To manage authentication to the portals through the social network sites, you need to configure the corresponding social app in Cisco Spaces. For example, if you need to authenticate access to a portal for customers that are signed in to Facebook, you need to configure the Facebook app in Cisco Spaces. You can add the apps of the following social network sites to Cisco Spaces:

- Facebook
- Twitter

- LinkedIn

To configure the social apps in Cisco Spaces, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Home**.
- Step 2** In the window that appears, click **Captive Portal**.
- Step 3** In the **Captive Portal** window that appears, click **Settings** in the left pane.
- Step 4** In the **Settings** window, choose **Social Apps**.
- Step 5** Click the **Add** button corresponding to the social networking site for which you want to configure the app. The fields for configuring the app appear.
- Step 6** Enter the app name, app ID, and app secret key in the respective fields.
- Step 7** Click **Save**.
-

Configuring an SMS Gateway in Cisco Spaces

To send SMS notifications, and to manage the portal authentication through SMS, you must configure SMS gateways. Cisco Spaces enables you to use the SMS Gateways of third-party vendors. To configure an SMS gateway in Cisco Spaces, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Home**.
- Step 2** In the window that appears, click **Captive Portal**.
- Step 3** In the **Captive Portal** window that appears, click **Settings** in the left pane.
- Step 4** In the **Settings** window, choose **SMS**.
- Step 5** Click **Add SMS gateway**.
- Step 6** From the **SMS Gateway Type** drop-down list, choose the SMS Gateway type that you want to use. Additional fields appear based on the SMS Gateway type selected.

Cisco Spaces supports the following SMS Gateway types:

- REASON8
- SMPP
- WATERFALL
- MGAGE
- TWILIO
- PANACEA MOBILE
- DATAMETRIX
- TROPO
- NYY

- TRU
- PHIZZLE
- AWS_SNS
- PROXIMUS
- TELENOR

Step 7 In the additional fields that appear based on the SMS Gateway type selected, specify the required values.

Step 8 Click **Save**.

Note The SMS Gateways created appears for selection in the SMS Gateway drop-down list for “SMS with password verification” and “SMS with link verification” authentication options in the portal. These SMS gateways also are available for selection when configuring the SMS notifications in the Engagement Rule.

Managing Captive Portal Rules

You can pause a captive portal rule, and make it live again, whenever required. You can modify a captive portal rule, and delete it if required. You can also view the captive portal rules configured for a location.

Pausing a Captive Portal Rule

To pause a captive portal rule, perform the following steps:

Step 1 In the Cisco Spaces dashboard, choose **Home**.

Step 2 In the **My Apps** area, choose **Captive Portal**.

Step 3 In the **Captive Portal** window, choose **Captive Portal Rule**.

The captive portal rules created get listed.

Step 4 Check the check box for the captive portal rule that you want to pause.

Step 5 Click the **Pause** button that appears at the bottom of the window.

Step 6 In the window that appears, click **Pause Rule** to confirm the pause.

The captive portal rule is paused.

What to do next



Note To pause multiple captive portal rules, check the check boxes for the captive portal rules that you want to pause, and click the **Pause** button that appears at the bottom of the window.

Restarting a Captive Portal Rule

To restart a captive portal rule that is paused, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Home**.
- Step 2** In the **My Apps** area, choose **Captive Portal**.
- Step 3** In the **Captive Portal** window, choose **Captive Portal Rule**.
The captive portal rules created get listed.
- Step 4** Check the check box for the captive portal rule that you want to restart.
Click the **Make Live** button that appears at the bottom of the window.
-

What to do next



- Note** To restart multiple captive portal rules, check the check boxes for the captive portal rules that you want to restart, and click the **Make Live** button that appears at the bottom of the window.
-

Modifying a Captive Portal Rule

To modify a captive portal rule, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Home**.
- Step 2** In the **My Apps** area, choose **Captive Portal**.
- Step 3** In the **Captive Portal** window, choose **Captive Portal Rule**.
The captive portal rules created get listed.
- Step 4** Click the **Edit Rule** icon for the captive portal rule that you want to modify.
- Step 5** Make necessary changes.
- Step 6** 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 Captive Portal Rule

To delete a captive portal rule, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Home**.
- Step 2** In the **My Apps** area, choose **Captive Portal**.
- Step 3** In the **Captive Portal** window, choose **Captive Portal Rule**.

The captive portal rules created get listed.

Step 4 Click the **Delete Rule** icon that appears at the far right of the captive portal rule that you want to delete.

What to do next



Note To delete multiple captive portal rules, select the check box for the captive portal rules that you want to delete, and click the Delete button that appears at the bottom of the window.

Viewing the Captive Portal Rules for a Location

To view a captive portal rule for a location such as group, building, floor, and so on, perform the following steps:

- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
- Step 2** Click the location for which you want to view the captive portal rule.
- Step 3** Click the **Proximity Rule** tab.
- Step 4** Click the **Captive Portal Rule** tab.
The captive portal rules for the location gets listed.
-

What to do next



Note The **Proximity Rules** link for a location is enabled only if at least one proximity rule exists for that location.

Filtering by Location

For the Cisco Spaces Rules such as Captive Portal Rule, Engagement Rule, Location Personas Rule, and Density Rule, you can filter the locations in which you want to apply a rule. You can also filter the locations by the metadata defined for the selected locations.

To specify the locations in which you want to apply the rule, perform the following steps:

- Step 1** Click the **Add Locations** button.
- Step 2** In the **Choose Locations** window that appears, select the locations for which you want to apply the rule.
- Step 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.

Apply the rule for locations with a particular metadata

To apply the rule for locations with a particular metadata, perform the following steps:

-
- 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**.
-

Exclude the locations with a particular metadata

To exclude the locations with a particular metadata, perform the following steps:

-
- 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**.
-

Trigger API Configurations

To configure to send notifications or customer details to an external API using the Cisco Spaces rules, perform the following steps:

- From the Method drop-down list, choose the method for triggering API.



Note You can include the data such as first name, last name, and so on of the customer in the notification message or the customer details sent to the API by adding the smart link variables in the API URI or by adding 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 request parameters to include additional details such as first name, last name, mobile number, and so on of the customer. You can add the request parameter keys defined in your API, and mention the values for them using variables. The value can be a hard-coded value or a variable. When you click the “Value” field, the variables that you can add get listed. For more information on variables, see the [Smart Links and Text Variables for Captive Portals, on page 238](#). You can add more “get parameters” using the **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 form 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. When you click the “Value” field, the variables that you can add get listed. For more information on variables, see the [Smart Links and Text Variables for Captive Portals, on page 238](#). 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, a text box appears where you can mention the JSON data that is to send to the API. You can mention the JSON values for various JSON fields defined in your API. The value can be a hard-coded value or a variable. To add a variable as JSON, click the “JSON Data” text box. The variables get listed. Select the variable that you want to add. For more information on variables, see the [Smart Links and Text Variables for Captive Portals, on page 238](#).
- **POST BODY**—To send notification or customer details to the API using the POST BODY method. If you choose this method, an additional field appears where you can mention the content that must be sent to the API. You can add variables in the content. To add a variable as BODY, click the “Post Body Data” text box. The variables get listed.
 - In the URI field, enter the URI for the API. You can include additional details of the customers in the notification or customer data sent to the API using the smart links. Click the “URI” field to view the variables that you can add. For more information on variables, see the [Smart Links and Text Variables for Captive Portals, on page 238](#)



Note You can define custom variables for the methods, GET, POST FORM, POST BODY, and POST JSON. When you click on a variable field for a method, a **Add Custom Variable** button is displayed along with the pre-defined variables. For the POST BODY method, currently there is no custom variable support for POST BODY DATA field. However, the URI field will not have custom variable support.



Note Only those data that you have configured to capture using the Data Capture form in the portal are included.

Certified Device List for Portals

The following table lists the devices and operating systems that are tested and certified for the portals.

Table 12:

Device	OS Version	Browser/ Captive Network Assistant (CNA) (where site loads and works fine)
Mobile Device		

Device	OS Version	Browser/ Captive Network Assistant (CNA) (where site loads and works fine)
Moto G2	6.0	CNA and Google Chrome
Sony Xperia SP	4.3	Google Chrome
Samsung S2	4.1.2	Google Chrome
Samsung Galaxy S5	6.0.1	Google Chrome
Samsung S6	6.0.1	Google Chrome
Micromax	5.0 and 4.4.4	Google Chrome
Google Nexus 6	6.0.1	CNA and Google Chrome
Moto X Play	6.0.1	Google Chrome
iPhone 4s	7.1.2	CNA Safari
iPhone 5s	9.3.5 and 9.3.4	CNA, Safari
iPhone 6	9.3.4	CNA, Safari
iPhone 6s	9.3.4	CNA, Safari
iPhone 6 Plus	9.3.2	CNA, Safari
Huawei Honor	6.0.1 and 6.0	Google Chrome
Huawei P8	5.0.1	Google Chrome
Microsoft Lumia 950	Windows 10	CNA and Native Browser
Nokia Lumia 1320	Windows 8.1	CNA and Native Browser
iPads/Tablets		
Samsung Galaxy Tab2	4.1.2	Google Chrome
Samsung Galaxy Tab 3 Neo	4.2.2	Google Chrome
iPad Mini	8.3	CNA and Safari
iPad 2	9.3.2	CNA and Safari
Laptops/Desktops		
Windows Lap HP ProBook	Windows 7	Chrome/ Firefox/IE
Windows Lap Lenovo	Windows 10	Chrome/ Firefox/IE
Macbook Pro 13-inch	Mac OS X EI Capitan 10.11.6	CNA

Device	OS Version	Browser/ Captive Network Assistant (CNA) (where site loads and works fine)
Macbook Pro 13-inch Retina display	Mac OS X EI Capitan 10.11.6	CNA

Cisco Spaces Captive Portal Behavior

The captive portal behavior for various devices is as follows:

Apple iOS 7.x to 11.x

When a customer connects to an SSID configured with the captive portal URL, the Captive Network Assistant (CNA) window appears. The CNA loads and displays the content for the portal.

When the customer click any menu or link in the portal, a Log In screen appears with the content based on the authentication type configured for the portal. For more information on configuring the authentication for portal, see the [Configuring Authentication for a Portal, on page 171](#). The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the [Authentication Steps for Customers, on page 229](#). After completing the required authentication steps, Cisco Spaces sends a request to the wireless network (CUWN, Meraki) to provision internet for that particular device. After successful provisioning of the internet, the CNA window is dismissed, and the Mobile Safari is opened. The web page for the menu or link that customer the clicked earlier appears in the Mobile Safari.



Note For iOS11.0 to 11.3, after internet provisioning, the CNA window will not close automatically. A message is displayed that asks the customer to close the CNA window by clicking the Done button.

Alternatively, if CNA is bypassed, and the customer accesses any URL that is not in allowed list (not in Access Control List or Walled Garden Range) using the Mobile Safari or Chrome browser, then the customer is redirected to the configured captive portal URL. The browser loads and displays the content for the captive portal. When the customer click any menu or link in the portal, the Log In screen appears where the customer has to complete the authentication steps as described earlier to provision the internet.



Note After the internet is provisioned, the customer can navigate through any of the menus or links in the portal without any more authentications.



Note If any error occurs during the internet provisioning, the captive portal re-appears.



Note If you configure the authentication module as an inline module in the captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see the [Inline Authentication](#) , on page 178.

Android 5.x and Later (Using CNA)

When the customer connects to an SSID configured with a captive portal URL, an option to 'Sign in to {SSID name}' appears in the notification area. On clicking the notification, devices with Android 5.x or later launches the CNA window. The CNA loads the content from the portal URL and displays the portal. When the customer click any menu or link in the portal, a Log In screen appears with the content based on the authentication type configured for the portal. For more information on configuring the authentication for portal, see the [Configuring Authentication for a Portal](#), on page 171. The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the [Authentication Steps for Customers](#), on page 229. After completing the required authentication steps, Cisco Spaces sends a request to the wireless network (CUWN, Meraki) to provision internet for that particular device. After successful provisioning of the Internet, the CNA window is dismissed.

Alternatively, the customer can ignore the notification and go ahead using the native or Chrome browser. When the customer accesses any URL that is not in allowed list (not in Access Control List or Walled Garden Range), the customer is redirected to the configured captive portal URL. The browser loads and displays the content for the captive portal. When the customer click any menu or link in the portal, the Log In screen appears where the customer has to complete the authentication steps as described earlier to provision the internet. After successful provisioning of the internet, the web page for the menu or link that customer clicked earlier appears.



Note After the internet is provisioned, the customer can navigate through any of the menus or links in the portal without any more authentications.



Note If any error occurs during the internet provisioning, the captive portal re-appears.



Note If you configure the authentication module as an inline module in th captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see the [Inline Authentication](#) , on page 178.

Android 4.x and Earlier

When the customer connects to an SSID configured with a captive portal URL, an option to 'Sign in to {SSID name}' appears in the notification area. On clicking the notification, devices with Android 4.x or earlier launches the default browser. The browser tries to load a URL that is generated by the device. As this URL is not in allowed list (not in Access Control List or Walled Garden Range), the customer is redirected to the

captive portal. When the customer click any menu or link in the portal, a Log In screen appears with the content based on the authentication type configured for the portal. For more information on configuring the authentication for portal, see the [Configuring Authentication for a Portal, on page 171](#). The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the [Authentication Steps for Customers, on page 229](#). After completing the required authentication steps, Cisco Spaces sends a request to the wireless network (CUWN, Meraki) to provision internet for that particular device. After successful provisioning of the internet, the web page for the menu or link that customer clicked earlier appears in the same browser.



Note After the internet is provisioned, the customer can navigate through any of the menus or links in the portal without any more authentications.



Note If any error occurs during the internet provisioning, the captive portal re-appears.



Note If you configure the authentication module as an inline module in th captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see the [Inline Authentication , on page 178](#).

Windows Phone

When the customer connects to an SSID configured with a captive portal URL, the Captive Network Assistant (CNA) appears. The CNA loads and displays the content for the captive portal URL. When the customer click any menu or link in the portal, a Log In screen appears with the content based on the authentication type configured for the portal. For more information on configuring the authentication for portal, see the [Configuring Authentication for a Portal, on page 171](#). The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the [Authentication Steps for Customers, on page 229](#). After completing the required authentication steps, Cisco Spaces sends a request to the wireless network (CUWN, Meraki) to provision internet for that particular device. After successful provisioning of the Internet, the CNA window is dismissed.



Note If any error occurs during the internet provisioning, the captive portal re-appears.



Note If you configure the authentication module as an inline module in th captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see the [Inline Authentication , on page 178](#).

Windows PCs and Laptops

After successfully connecting to an SSID configured with a captive portal URL, when the customer browses any URL that is not in allowed list (not in Access Control List or Walled Garden Range), the customer is redirected to the captive portal page configured for that SSID. When the customer click any menu or link in the portal, a Log In screen appears with the content based on the authentication type configured for the portal. For more information on configuring the authentication for portal, see the [Configuring Authentication for a Portal, on page 171](#). The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the [Authentication Steps for Customers, on page 229](#). After completing the required authentication steps, Cisco Spaces sends a request to the wireless network (CUWN, Meraki) to provision internet for that particular device. After successful provisioning of the internet, the web page for the menu or link that customer clicked earlier appears in the same browser.

For windows 10, when the customer connects to an SSID configured with a captive portal URL, the Captive Network Assistant (CNA) appears. The CNA loads and displays the content for the captive portal URL. When the customer click any menu or link in the portal, a Log In screen appears with the content based on the authentication type configured for the portal. For more information on configuring the authentication for portal, see the [Configuring Authentication for a Portal, on page 171](#). The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the [Authentication Steps for Customers, on page 229](#). After completing the required authentication steps, Cisco Spaces sends a request to the wireless network (CUWN, Meraki) to provision internet for that particular device. After successful provisioning of the Internet, the CNA window is dismissed.



Note After the internet is provisioned, the customer can navigate through any of the menus or links in the portal without any more authentications.



Note If any error occurs during the internet provisioning, the captive portal re-appears.



Note If you configure the authentication module as an inline module in th captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see the [Inline Authentication , on page 178](#).

Macbook

When the customer connects to an SSID configured with a captive portal URL, the Captive Network Assistant (CNA) window appears. The CNA loads and displays the content for the captive portal. When the customer click any menu or link in the portal, a Log In screen appears with the content based on the authentication type configured for the portal. For more information on configuring the authentication for portal, see the [Configuring Authentication for a Portal, on page 171](#). The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the [Authentication Steps for Customers, on page 229](#). After completing the required authentication steps, Cisco Spaces sends a request to

the wireless network (CUWN, Meraki) to provision the internet for that particular device. After successful provisioning of the internet, the web page for the menu or link that customer clicked earlier appears in the default browser of the customer. Apart from the link that the customer has clicked, the browser opens another tab with the home page that is in CNA.

Alternatively, the customer can dismiss the captive portal window and go ahead using the browser. When the customer accesses any URL that is not in allowed list (not in Access Control List or Walled Garden Range), the customer is redirected to the configured captive portal URL. The browser loads and displays the content for the captive portal URL. When the customer click any menu or link in the portal, the Log In screen appears where the customer has to complete the authentication steps as described earlier to provision the internet. After successful provisioning of the internet, the web page for the menu or link that customer clicked earlier appears in the same browser.



Note After the internet is provisioned, the customer can navigate through any of the menus or links in the portal without any more authentications.



Note If any error occurs during the internet provisioning, the captive portal re-appears.



Note If you configure the authentication module as an inline module in th captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see the [Inline Authentication](#) , on page 178.

Authentication Steps for Customers

The authentication steps that a customer has to complete to provision the internet for various authentication types are as follows:

Steps for SMS with Link Verification Authentication

To complete the “SMS with link verification” authentication, perform the following steps:

-
- Step 1** In the captive portal, click/tap any menu item.
- Step 2** In the Log In screen that appears, enter the mobile number.
- Note** If a Data Capture module is configured, the data capture form appears along with the mobile number field.
- Step 3** Enter the mobile number, and all the mandatory fields in the Data Capture form, and press Accept Terms and Continue. The internet is provisioned, and a SMS with a link to access the portal is sent to the mobile number provided.
- Step 4** Click the link in the SMS for finger print verification.
For more information on fingerprint verification, see the [Fingerprint Verification](#), on page 231.

Note If the customer does not click the link in the SMS within a time frame, a “Skip” button appears. The customer can click the “Skip” button to proceed further without fingerprint verification. When the customer tries to access the internet next time, a blank “mobile number” field is shown to provide the mobile number again. This occurs for every internet access until the customer completes the fingerprint verification.

Authentication Steps for a Repeat User for SMS with Link Verification

The authentication steps for a repeat user for various scenarios are as follows:

- **Completed the fingerprint verification (Data Capture module is not configured):** When the customer click/tap any menu item, internet is provisioned.
- **Completed the fingerprint verification (Data Capture module is configured, the Data Capture form is filled):** When the customer click/tap any menu item, internet is provisioned.
- **Completed the fingerprint verification, but Data capture form is not filled or partially filled (for non mandatory fields):** When the customer click/tap any menu item, internet is provisioned. However, the data capture form is shown if there is any change in the data capture form.
- **Not completed the fingerprint verification, but filled the Data Capture form:** When the customer click/tap any menu item, the mobile number field appears along with the pre-filled Data Capture form. The customer has to enter the mobile number again for accessing the internet. This continues for all the internet access attempts until the customer completes the fingerprint verification.
- **Mobile number verification process was not completed during previous internet access:** If the verification process is not complete within a limited time, the internet is provisioned even for invalid mobile numbers. For such a repeat user, when the captive portal loads, and the customer click any menu item or link in the portal, the log in screen appears with the mobile number field. The customer has to enter a valid mobile number.
- **The Data Capture module is configured, and the registration details are outdated:** When the captive portal loads, and the customer click any menu item or link in the portal, the registration form appears with the previously filled data. The customer can update the form, and press Connect to get access to the internet.

The following are some of the scenarios when the registration details become outdated:

- **Added new mandatory fields:** Added a new mandatory field in the Data Capture module. For example, you configured the Data Capture module without a Gender field. The customer completes registration. Later on, you added the Gender field to the Data Capture module and marked it as mandatory.
- **Optional field becomes mandatory:** Modified the Data Capture module to make an optional field that the customer skipped during registration as a mandatory field. For example, you have configured a Data Capture module with the last name as optional. The customer connected to the SSID and completed the registration without mentioning the last name. Now, you modified the Data Capture module and made the last name mandatory for registration.
- **Modified the choice options:** Removed or replaced a choice option that was available for selection. For example, you have configured a mandatory business tag “Age Criteria” with choice options as “Child” and “Adult”. The customer completes registration by selecting Age Criteria as Child. Later on, you modified to display the choices as “Kids”, and “Adult”.



Note In all the above scenarios, if there is any change in the Terms and Conditions defined, the “Accept Terms and Continue” button is displayed. The customer must press the “Accept Terms and Continue” button to get access to the internet or to move to the next authentication step.

Fingerprint Verification

When a customer provides the mobile number for the “SMS with link verification” authentication, a message with a link is sent to the mobile number provided, and the internet is provisioned. The Fingerprint verification happens when the customer click the link in the message. If the customer is not clicking the link within a pre-defined time, a temporary page with a “SKIP” option is shown to the customer. The customer can click the Skip option to access the internet without fingerprint verification.

The fingerprint verification status for various scenarios is as follows:

- When the customer click the link in the message, if fingerprint matches, then customer acquisition will happen and the customer will be redirected to the portal page. The customer will be considered as repeat user on next visit.
- When the customer click the link in the message, if the fingerprint verification fails (For example, if the customer opens the link in a different browser than the one used for initiating the SMS authentication, then the fingerprint verification fails.), a confirmation page appears for the customer. If the customer click “Confirm”, the customer acquisition will happen, and the customer will be redirected to the portal page. The customer will be considered as repeat user on next visit.
- When the customer click the link in the message, if fingerprint verification fails, a confirmation page appears for the customer. If the customer click “Cancel”, the customer will be considered as first time user on next visit, and the log in screen appears with a blank mobile number field.
- If the customer click “Skip” in the temporary page displayed, the customer is considered as first time user on next visit, and the log in screen appears with a blank mobile number field.

Steps for SMS with Password Verification Authentication

To complete the “SMS with password verification” authentication, perform the following steps:

-
- Step 1** In the captive portal, click/tap any menu item.
- Step 2** In the Log In screen that appears, enter the mobile number.
- Step 3** If the customer wants to unsubscribe from receiving notifications, uncheck the **Opt In to Receive notification** check box.
- Note** The “Opt In to receive notification” check box appears in the Log In screen only if you have selected the “Allow users to Opt in to receive message” check box in the Authentication screen when configuring the authentication details for the portal.
- Step 4** Press **Accept Terms and Continue**.
- Step 5** In the screen that appears, enter the verification code received through the SMS.
- Step 6** Press **Verify**.

After successful verification of the verification code, the Data Capture form appears, if Data Capture is enabled.

Step 7 Enter all the mandatory fields in the Data Capture form, and press **Connect**.

Note If all the fields are optional, there will be two buttons **Skip** and **Connect**. The customer can click the **Skip** button to proceed without filling the data. If the customer click **Skip**, the data capture form will appear for that customer only if there is any change in the form.

After successful registration, the internet provisioning process is initiated, and the internet is provisioned.

Note If the Data Capture module is not enabled, the internet is provisioned immediately after the verification code validation.

Authentication Steps for a Repeat User for SMS with Password Verification

The authentication steps for a repeat user for various scenarios are as follows:

- **Data Capture is not configured:** When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.
- **Data Capture is configured, and tge customer completed the registration:** When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.
- **Data Capture is configured, and the registration details are outdated:** When the captive portal loads, and the customer click any menu item or link in the portal, the Data Capture form appears with the previously filled data. The customer can update the form, and press the “Connect” button to get access to the internet.

The following are some of the scenarios when the registration details become outdated:

- **Added new mandatory fields:** Added a new mandatory field in the Data Capture form. For example, you configured the Data Capture form without a Gender field. The customer completes registration. Later on, you added the Gender field to the Data Capture form and marked it as mandatory.
- **Optional field becomes mandatory:** Modified the Data Capture form to make an optional field that the customer skipped during registration as a mandatory field. For example, you have configured a Data Capture form with the last name as optional. The customer connected to the SSID and completed the registration without mentioning the last name. Now, you modified the Data Capture form and made the last name mandatory in the form.
- **Modified the choice options:** Removed or replaced the choice options that was available for selection. For example, you have configured a mandatory business tag “Age Criteria” with choice options as “Child” and Adult”. The customer completes registration by selecting Age Criteria as “Child”. Later on, you modified to display the choices as “Kids”, and “Adult”.
- **Entered invalid e-mail ID during previous log in:** When the captive portal loads, and the customer click any menu item or link in the portal, the Data Capture form appears with the invalid e-mail ID mentioned during previous login. The customer has to enter a valid e-mail ID to proceed further.



Note In all the above scenarios, if there is any change in the Terms and Conditions defined, the **Accept Terms and Continue** button is displayed. The customer must press the **Accept Terms and Continue** button to get access to the internet, or to move to the next authentication step.

Steps for E-mail Authentication

To complete the e-mail authentication, perform the following steps:

Step 1 In the captive portal, click/tap any menu item.

Step 2 In the Log In screen that appears, enter the e-mail ID.

Step 3 If the customer wants to unsubscribe from receiving notifications, uncheck the **Opt In to Receive notification** check box.

Note The **Opt In to Receive notification** check box appears in the Log In screen only if you have checked the **Allowed users to Opt in to receive message** check box for the **Email** authentication type when configuring the authentication details for the portal.

Step 4 Press **Accept Terms and Continue**.

If the e-mail ID entered is valid, the internet is provisioned.

Step 5 If the Data Capture is enabled in the Authentication screen of the captive portal, a Data Capture form appears when the customer press **Accept Terms and Continue**.

Step 6 Enter all the mandatory fields in the Data Capture form, and press **Connect**.

Note If all the fields are optional, there will be two buttons **Skip** and **Connect**. The customer can click the Skip button to proceed without filling the data. If the customer click "Skip", the Data Capture form will appear for the repeat user only if there is any change in the form.

The internet provisioning process is initiated, and the internet is provisioned.

Authentication Steps for a Repeat User for Email Verification

In Cisco Spaces, as part of the authentication workflow for a new user, you need to enter the email address only once. All domain related validations and MX records checks are cached for specific duration and same checks are not repeated for other users from the same domain within the cached duration.

For example, if 10 users are connected to Captive Portal at same time and enter their email addresses that belongs to the same domain (xyz@abc.com), then the domain validation and MX records check will happen only once for the specified caching duration. However, SMTP connection and mailbox checks are performed for all 10 users to verify whether the user ID is valid or not.

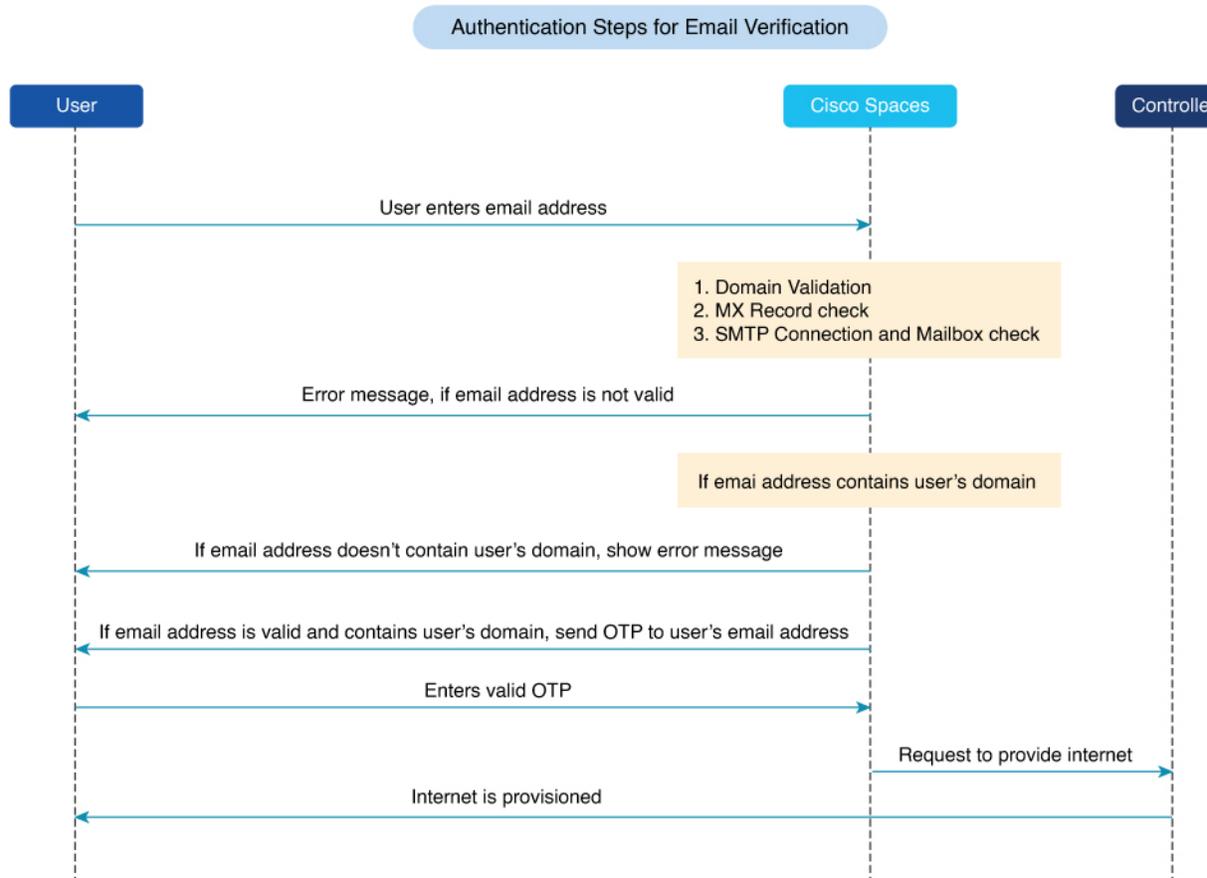
To make a SMTP connection:

1. Establish a socket connection to SMTP server and verify the response.
2. Run the **ELHO** command and verify the response.
3. Run the **MAIL FROM** command and verify the response.
4. Run the **RCPT TO** command and verify the response.



Note As part of the Captive Portal new user onboard workflow, the email address of a user is recorded only once. You are still allowed to authenticate to Cisco Spaces if Cisco Spaces did not receive response from the mailbox check. However, you must enter the email address again on the subsequent visit. As part of the mailbox check process Cisco Spaces will never send email request to the email address provided by the user.

Figure 18: Authentication Workflow



Authentication Scenarios

The authentication steps for a repeat user for various scenarios are as follows:

- **Entered invalid e-mail ID during previous log in:** When the captive portal loads, and you click any menu item or link in the portal, the log in window is displayed with an invalid email ID mentioned during the previous login. You must enter a valid email ID to proceed further.
- **Data Capture is not enabled:** When the captive portal loads, and you click any menu item or link in the portal, the internet is provisioned.
- **Data Capture is enabled, and the customer completed the registration:** When the captive portal loads, and you click any menu item or link in the portal, the internet is provisioned.

- **Data Capture is enabled, and the registration details are outdated:** When the captive portal loads, and you click any menu item or link in the portal, the Data Capture form is displayed with the previously filled data. You can update the form, and click **Connect** to get access to the internet.

Registration Information

The following are some of the scenarios when the registration details become outdated:

- **Added new mandatory fields:** Added a new mandatory field in the **Data Capture** form. For example, you configured the **Data Capture** form without a **Gender** field. The registration process is complete. Later on, you added the **Gender** field to the **Data Capture** form and marked it as mandatory.
- **'Optional field becomes mandatory:** Modified the **Data Capture** form to make an optional field that the customer skipped during registration as a mandatory field. For example, you have configured a **Data Capture** form with the last name as optional. The customer connected to the SSID, and completed the registration without mentioning the last name. Now, you modified the **Data Capture** form and made the last name mandatory in the form.
- **Modified the choice options:** Removed or replaced a choice option that was available for selection. For example, you have configured a mandatory business tag **Age Criteria** with choice options as **Child** and **Adult**. The customer completes registration by selecting **Age Criteria** as **Child**. Later on, you modified to display the choices as **Kids** and **Adult**.



Note In all the above scenarios, if there is any change in the **Terms & Conditions** defined, the **Accept Terms and Continue** option is displayed. You must press the **Accept Terms and Continue** option to get access to the internet or to proceed to the next authentication step.

Steps for Access Code Authentication

To complete the Access Code authentication, perform the following steps:

-
- Step 1** In the captive portal, click or tap any menu item.
- Step 2** In the **Log In** window, enter the access code.
- Step 3** If the customer wants to unsubscribe from receiving notifications, uncheck the **Opt In to Receive notification** check box.
- Note** The “Opt In to receive notification” check box appears in the Log In screen only if you have selected the “Allow users to Opt in to receive message” check box in the Authentication screen when configuring the authentication details for the portal.
- Step 4** Press **Accept Terms and Continue**.
- Step 5** Press **Verify**.
- After successful verification of the access code, the Data Capture form appears, if Data Capture is enabled.
- Step 6** Enter all the mandatory fields in the Data Capture form, and press **Connect**.

Note

- If all the fields are optional, there will be two buttons **Skip** and **Connect**. The customer can click the **Skip** button to proceed without filling the data. If the customer click **Skip**, the data capture form will appear for that customer only if there is any change in the form.
After successful registration, the internet provisioning process is initiated, and the internet is provisioned.
- If the **Data Capture** module is not enabled, the internet is provisioned immediately after the access code validation.
- If you need to configure **Limit session by time** or **Limit bandwidth**, ensure that you have configured the Cisco Spaces Radius server for your network. To setup Cisco Spaces Radius server, see [Configuring Cisco Meraki for RADIUS Authentication](#) and [Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication](#).

Authentication Steps for a Repeat User for Access Code Authentication

The authentication steps for a repeat user for various scenarios are as follows:

- **Data Capture is not configured:** When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.
- **Data Capture is configured, and the customer completed the registration:** When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.
- **Data Capture is configured, and the registration details are outdated:** When the captive portal loads, and the customer click any menu item or link in the portal, the Data Capture form appears with the previously filled data. The customer can update the form, and press the “Connect” button to get access to the internet.

The following are some of the scenarios when the registration details become outdated:

- **Added new mandatory fields:** Added a new mandatory field in the Data Capture form. For example, you configured the Data Capture form without a Gender field. The customer completes registration. Later on, you added the Gender field to the Data Capture form and marked it as mandatory.
- **Optional field becomes mandatory:** Modified the Data Capture form to make an optional field that the customer skipped during registration as a mandatory field. For example, you have configured a Data Capture form with the last name as optional. The customer has connected to the SSID and completed the registration without mentioning the last name. Now, you modified the Data Capture form and made the last name mandatory in the form.
- **Modified the choice options:** Removed or replaced the choice options that was available for selection. For example, you have configured a mandatory business tag “Age Criteria” with choice options as “Child” and “Adult”. The customer completes registration by selecting Age Criteria as “Child”. Later on, you modified to display the choices as “Kids”, and “Adult”.
- **Entered invalid e-mail ID during previous log in:** When the captive portal loads, and the customer click any menu item or link in the portal, the Data Capture form appears with the invalid e-mail ID mentioned during previous login. The customer has to enter a valid e-mail ID to proceed further.



Note In all the above scenarios, if there is any change in the Terms and Conditions defined, the **Accept Terms and Continue** button is displayed. The customer must press the **Accept Terms and Continue** button to get access to the internet, or to move to the next authentication step.

Steps for No Authentication with Terms and Conditions

You can configure to provision the internet to the customers if they accept just the terms and conditions mentioned.

To complete the authentication that requires only the acceptance of the terms and conditions, perform the following steps:

-
- Step 1** In the captive portal, click/tap any menu item.
- Step 2** In the Log In screen that appears, press **Accept Terms and Continue**.
The internet provisioning process is initiated, and the internet is provisioned.
-

Authentication Steps for a Repeat User with Terms and Conditions Authentication

When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.



Note If there is any change in the Terms and Conditions defined, the “Accept Terms and Continue” button is displayed. The customer must press the “Accept Terms and Continue” button to get access to the internet or to move to the next authentication step.

Steps for Social Authentication

To complete the social authentication for a portal, perform the following steps:

-
- Step 1** When the customer click any menu item or link in the captive portal, a screen appears with all the social sign in options available for the portal.
- Note** The Sign in option appears only for those social networks that are configured for the portal. For more information on configuring the social network for a portal, see the [Configuring a Portal for Social Sign In Authentication, on page 175](#).
- Step 2** Click the sign in option for the social network through which you want to complete the authentication. The log in page for the social network appears.
For example, click the sign in option for Linked In, then the log in screen for Linked In appears.
- Step 3** Enter the log in credentials for the social network, and press the log in button.

- Step 4** In the screen that appears, press **Allow**.
The redirect URI gets loaded, and the Terms and Conditions screen appears.
- Step 5** Press **Accept Terms and Continue**.
- Note** For Facebook and Twitter, it is not required to configure the redirect URI. The Redirect URI must be configured for Linked In. For more information on configuring the redirect URI for Linked In, see the [Configuring the Apps for Social Authentication, on page 216](#).
- Step 6** After provisioning the internet, a **Continue** window appears.
- Step 7** Press **Continue** to view the page for the link that you have clicked earlier.

Authentication Steps for a Repeat User with Social Authentication

When the captive portal loads, and the customer click any menu item or link in the portal, the options to connect with all the configured social networks appear. The social networks the customer has used earlier for authentication will be labeled as “Continue with [social network]”. For example, if the customer has used Facebook authentication earlier to access the internet through the captive portal, the option for Facebook will be labeled as “Continue with Facebook”. For the social networks that are not used earlier for authentication, a sign in option appears. For example, “Signin with LinkedIn”.

- If the customer continues to use a social network that was used earlier for authentication, the internet is provisioned without any authentication process. However, if there is any change in the Terms and Conditions, the Terms and Conditions screen is shown. Then, the customer must press the “Accept Terms and Continue” button to get access to the internet.
- If the customer signs in using a social network that was not used earlier for authentication, the customer has to complete the entire authentication process for that social network. If the customer has accessed the internet using social authentication through any of the social network, the Terms and Conditions screen is not shown during the authentication process. However, if there is any change in the terms and conditions, the Terms and Conditions screen appears during the authentication process. Then, the customer must press the “Accept Terms and Continue” button to get access to the internet.

Smart Links and Text Variables for Captive Portals

Smart Links

The Smart Link option enables you to provide your customers personalized web pages and messages. Using the Smart Link option, you can customize the URLs for the custom menu links in the captive portals to provide a personalized view. You can personalize your site pages for each user or group of users.

For example, you can configure the parameter “optedinstatus” for a custom menu item in your portal. Then you configure the web page for this custom menu item to display different content for “opted in” and “not opted in” users. When a customer who is an opted in user click the custom menu link in the captive portal, the content for the opted in user is shown. When a customer who is not an opted in user click the same custom menu link, the content for the not opted in user is shown.



Note To use these parameters to display the personalized view to the customers, you have to configure your web pages accordingly.

In the **Captive Portals** app, You can include the smart links in the following options:

- The links added in the custom menu items added to the portal.
- URL added in the **URI** field in Trigger API.

Text Variables

Using text variables, you can add personal details of the customers such as name, mobile number, gender, and so on in the messages sent to an API end point using **Trigger API**. By default, the message will have first name and last name of the customer. You can add additional customer details using the variables.

For example, assume that you have created an Trigger API notification and 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.

You can add variables in the following options:

- The message sent to an API end point using **Trigger API**.
- Welcome Messages for first time and repeat user.
- Notices added to the portal (Only backend support).

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 see the [Adding a Data Capture Form to a Portal](#) section.



Note The URL of the captive portal that is included in the “SMS with link verification” and” SMS with password verification” messages are not supported with the smart link feature.

Cisco Spaces provides certain predefined variables. You must use these variables to provide personalized view for you web pages and to add customer details in the notification messages.

You can include static and dynamic variables in a smart link or text.

The static parameters that you can include in the smart link or text are as follows:

Table 13: Static Variable List

Static Variable Name	Description
\$location or \$locationName	Name of the location for which the rule is triggered.
\$Address	The address configured for the location in the Location Info window in Location Hierarchy .

Static Variable Name	Description
\$State	The state configured for the location in the Location Info window in Location Hierarchy .
\$Country	The country configured for the location in the Location Info window in Location Hierarchy .
\$City	The city configured for the location in the Location Info window in Location Hierarchy .
\$TotalAreaValue	The total area configured for the location in the Location Info window in Location Hierarchy .
\$firstName (Not applicable for First Time Visitor in the Welcome module.)	First name of the customer.
\$lastName (Not applicable for First Time Visitor in the Welcome module.)	Last name of the customer.
The following variables are not applicable for the Welcome module, but only for Custom modules and Trigger API.	
\$email	E-mail address of the customer.
\$mobile	Mobilie number of the customer.
\$gender	Gender of the customer.
\$URL	URL link value.
\$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.

In additional, you can include the following dynamic variables in a smart link or text:

Table 14: 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, see the Adding a Data Capture Form to a Portal section.

Dynamic Variable Name	Description
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, see the Adding Metadata for a Location section.

To include a smart link in a URL, or variable in a text, perform the following steps:

-
- Step 1** Click anywhere in the URL field or text box or click the corresponding **Add Variable** drop-down list.
The variables that you can include get listed.
- Step 2** Choose the variables that you want to include.
-



CHAPTER 19

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 243](#)
- [Creating an Engagement Rule, on page 244](#)
- [Managing Engagement Rules, on page 251](#)
- [Engagement Rule Report, on page 253](#)
- **Visitor Engagement**, on page 254
- [Engagement URL, on page 254](#)
- [Previous Visit Criteria, on page 254](#)
- [Notification Types, on page 256](#)
- [Notification Frequency, on page 256](#)
- [Location Filter for an Engagement Rule, on page 256](#)
- [Notification Type for a Consumer, on page 257](#)
- [Notification Type for a Business User, on page 258](#)
- [Trigger API Configuration for Notification, on page 261](#)

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 94](#).

- 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 64](#)
- 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 66](#)
 - [Configuring Cisco Catalyst 9800 Series Wireless Controller GUI \(Local Mode\) for Captive Portals and Engagements Apps, on page 70](#)
 - [Configuring Cisco Catalyst 9800 Series Wireless Controller GUI \(Flex Mode or Mobility Express\) for Captive Portals and Engagements Apps, on page 74](#)
- 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, see the [Overview of Location Hierarchy, on page 275](#).
- To specify the tags for which the rule is applicable, you must define the tags. For more information on creating the tags, see the [#unique_306](#).
- 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, see the [Adding a Data Capture Form to a Portal, on page 178](#).

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.

To define an engagement rule to send notifications to the customers, perform the following steps:

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 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 different 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 rule, see the [#unique_308](#)

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 e-mail or SMS. For more information on the notification types, see [Notification Type for a Consumer, on page 257](#).

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:

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:
- Check the **Filter by Opt-In Status** check box, and choose **Only for opted-in Visitor**.
 - 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**.
 - From the following drop-down lists, choose **Atleast, 5 Times in This Year**.
- Step 9** In the **Schedule** area, do the following:
- 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.
 - Check the **Filter by days of the week** check box, and click **Sat** and **Sun**.
- Step 10** In the Actions area, do the following:
- From the **Notify** drop-down list, choose **Consumer**.
 - From the adjacent three drop-down lists, choose **Once in, 1**, and **Visits**, respectively.
 - Check the **Via Email** check box.
 - 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.
 - In the **Subject** field enter a subject for the email. If required, edit the message in the following text box.
 - 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, see 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:

- 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 different 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 rule, see the [#unique_308](#).

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:

- 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.
- 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 except 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.

- 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, see 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, see 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, see [Notification Type for a Business User, on page 258](#)

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, see 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:

-
- 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:
- Check the **Filter by Opt-In Status** check box, and choose **Only for opted-in Visitor**.
 - Check the **Filter by Tags** check box, and click the **Add Tags** button for Include.
 - 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:
- 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:
- From the Notify drop-down list, choose **Business**.
 - From the adjacent drop-down list, choose **Only Once**.
 - 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:

-
- Step 1** In the Cisco Spaces dashboard, click **Engagements**.
The **Engagements** window appear with all the engagements rules listed.
- Step 2** Click the **Pause Rule** icon that appears at the far right of the engagement rule that you want to pause.
- Step 3** In the window that appears, confirm pausing.
The engagement rule is paused.
-

What to do next



-
- Note** To pause multiple engagement rules, check the check box for the engagement rules that you want to pause, and click the **Pause** button that appears at the bottom of the page.
-

Restarting an Engagement Rule

To restart an engagement rule, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, click **Engagements**.
The **Engagements** window appear with all the engagements rules listed.
- Step 2** Click the **Make Rule Live** icon that appears at the far right of the engagement rule that you want to restart.
The engagement rule is restarted.
-

What to do next



-
- Note** To restart multiple engagement rules, check the check box for the engagement rules that you want to restart, and click the **Make Live** button that appears at the bottom of the window.
-

Modifying an Engagement Rule

To modify an engagement rule, perform the following steps:

Step 1 In the Cisco Spaces dashboard, click **Engagements**.

The **Engagements** window appear with all the engagements rules listed.

Step 2 Click the **Edit Rule** icon that appears at the far right of the engagement 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** 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:

Step 1 In the Cisco Spaces dashboard, click **Engagements**.

The **Engagements** window appear with all the engagements rules listed.

Step 2 Click the **Delete Rule** icon that appears at the far right of the engagement rule that you want to delete.

Step 3 In the window that appears, confirm deletion.

What to do next



Note To delete multiple engagement rules, check the check box for the engagement rules that you want to delete, and click the **Delete** button that appears at the bottom of the window.

Viewing an Engagement Rule for a Location

To view an engagement rule for a location such as group, building, floor, and so on, perform the following steps:

Step 1 Click the three-line menu icon at the top-left of the Cisco Spaces dashboard.

Step 2 Choose **Location Hierarchy**.

The **Location Hierarchy** window appears with the location hierarchy.

Step 3 Click the location for which you want to view the engagement rule.

- Step 4** Click the **Rules** tab.
- Step 5** Click the **Engagement Rule** tab.
- The engagement 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.

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 the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Home**.
- Step 2** In the My Apps area, choose **Engagements**.
- Click the rule for which you want to the Engagement Rule Report.
- Step 3** In the Filter area, choose the period for which you want to view the report.
- The report is filtered for the specified period.
- The Engagement Rule report has the following sections.
-

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 or e-mail notifications) 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.

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 253](#).

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.
 - **Hours**— To send the notification once in the number of hours 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 [Smarm Links and Text Variables for Engagements Rule and Density Rule](#) 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 254](#) 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 [Smarm Links and Text Variables for Engagements Rule and Density Rule](#) 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 254](#) 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, see the [Adding 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 [Smark Links and Text Variables for Engagements Rule and Density Rule](#) 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 254](#).

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 [Smark Links and Text Variables for Engagements Rule and Density Rule](#) 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 [Smarm Links and Text Variables for Engagements Rule and Density Rule](#) 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 254](#).

- 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.

Smarm 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 variables 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 see the [Adding 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 15: 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 Engagements Rule and Density Rule are as follows:

Table 16: 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, see the Adding 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. For more information on defining the location metadata, see the Adding Metadata for a Location section.

To include a smart link in the URL or text variable in the notification message, perform the following steps:

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, see [Smart Links and Text Variables for Captive Portals, on page 238](#)
 - 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 259](#)



CHAPTER 20

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 263](#)
- [Use Case: Location Personas Rule \(Profile Rule\), on page 265](#)
- [Managing Location Personas Rules, on page 268](#)
- [Location Personas Rule Report, on page 270](#)

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:

-
- Step 1** In the Cisco Spaces dashboard, click **Location Personas**.
- Step 2** In the **Location Personas** window that appears, click **Create New Rule**.
- Step 3** In the **Rule Name** field, enter a name for the Location Personas/Profile 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 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, see the [Location Filter for a Location Persons Rule, on page 267](#)

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, see the [Opted In Option for Users, on page 267](#).

- 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.

For more information on using the tag filter, see the [#unique_330](#).

- 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.

- d) If you want to filter the customers based on the customer's app status, check the **Filter by App Status** check box, and choose whether you want to filter the app user or non app user 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 the **Add Tags** button.
 - 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:

-
- 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 **Location Personas**.
- Step 4** In the **Location Personas** window that appears, 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, and select location A, and location C.
- Step 8** In the **Identify** area, do the following:
- Check the **Filter by Opt-In Status** check box, and choose **Only for opted-in Visitor**.
 - Check the **Filter by Previous Visits** check box, and click the **Add Locations** button, and add Location A, and Location C.
 - In the following fields, choose **At least, 10** times in, and **Date Range**, respectively.
 - In the date range fields, enter the start date and end date for the last two years.
- Step 9** 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 10** In the Actions area, do the following:
- Click the **Add Tags** button.
 - In the **Create Tags** window, Click **Create New Tag**.
 - 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 11** 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:

-
- 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:

-
- 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:

-
- 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 **OK**.

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:

-
- 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:

-
- 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 **OK**.
-

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:

-
- 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



Note To pause multiple Location Personas rules, check the check box for the Location Personas rules that you want to pause, and click the **Pause** button that appears at the bottom of the window.

Restarting a Location Personas Rule

To restart a Location Personas rule, perform the following steps:

-
- 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



Note To restart multiple Location Personas rules, check the check box for the Location Personas rules that you want to restart, and click the **Make Live** button that appears at the bottom of the window.

Modifying a Location Personas Rule

To modify a Location Personas rule, perform the following steps:

-
- 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:

-
- 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



Note To delete multiple Location Personas rules, check the check box for the Location Personas rules that you want to delete, and click the **Delete** button that appears at the bottom of the window.

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:

-
- 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:

-
- 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.



PART **VIII**

Location Hierarchy

- [Location Hierarchy in Cisco Spaces, on page 275](#)
- [Defining the Location Hierarchy, on page 279](#)
- [Managing the Location Hierarchy, on page 291](#)



CHAPTER 21

Location Hierarchy in Cisco Spaces

This chapter describes the structure of the location hierarchy in Cisco Spaces, and how to define the location hierarchy in Cisco Spaces.

- [Overview of Location Hierarchy, on page 275](#)
- [Prerequisites for Defining the Location Hierarchy, on page 277](#)
- [Displaying Cumulative Count in Location Hierarchy, on page 277](#)

Overview of Location Hierarchy

In Cisco Spaces, you can 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.

Each Cisco Spaces customer is provided with a default customer name (root name), and this customer name acts as the root location of the Cisco Spaces location hierarchy.

As Cisco Spaces provides universal account, you can import and manage the locations of multiple wireless networks. A proximity rule can include the locations of multiple wireless networks.

You can create proximity rules such as Captive Portal rule, Engagement rule, and Location Personas rule, and view access points, users, and child locations for any location in the location hierarchy. The number of access points, proximity rules, child locations, and users for each location in the location hierarchy are displayed against that particular location. For example, the number of proximity rules, child locations, and users for a group are shown against that group in the location hierarchy. The count of these location parameters are shown in cumulative manner.

Location Hierarchy automatically reflects the hierarchical structure defined in maps imported from **Cisco Prime Infrastructure** or **Cisco Catalyst Center**.

The **Cisco Spaces Dashboard** restricts the selective import of locations, like a campus, building, or floor, into the **Location Hierarchy** using the below methods:

- Add AP Zones
- Add Building
- Add Campus
- Add CMX zones
- Add Floor

Location Hierarchy supports Meraki MT. The configurations required for receiving the data from the MT sensors are updated using Cisco Spaces and Meraki integration. The MT sensors are automatically imported to **Location Hierarchy**.

The support for auto importing access points with model names starting with **CW** to **Location Hierarchy** (newly introduced by Cisco Meraki) is added. Before this release, support was only available for **MR** and **MX** access point models.

Cisco Meraki networks with **CiscoSpaces** tags are automatically imported into Cisco Spaces **Location Hierarchy** during the background synchronization process. The Meraki organization must be present in the **Location Hierarchy** to support the auto-import of these tagged networks. **CiscoSpaces** should be the tag name added in Cisco Meraki network.

**Note**

- If a location, like a campus, building, or floor, is deleted from **Location Hierarchy**, it can be added back to **Location Hierarchy** by uploading the previously uploaded map using **Map Service > Maps Upload**.
- As a Cisco Spaces customer, you can migrate from Cisco Prime Infrastructure based maps to Catalyst Center based maps in Cisco Spaces. To ensure a seamless migration to new maps in a way that does not impact the Location Hierarchy and existing Cisco Spaces data, we recommend that you reach out to the Cisco Spaces support team to validate the location hierarchy and ensure the data is carried over without any issues.
- We recommend that you use the Google Chrome Browser while working with maps. Map operations are best supported in Google Chrome. Map actions on other browsers are limited.

Cisco Smart Workspaces Support

The following features are introduced in **Location Hierarchy** to support the Cisco Smart workspaces use cases.

Location Hierarchy background synchronization now supports:

- Synchronization of the Meraki MT sensor devices in the Meraki networks or floor locations.
- Synchronization of Cisco Webex devices with meeting rooms and desks.

**Note**

During the background synchronization process, the Meraki Scanning API Notification URL for configuration template networks are updated automatically.

Camera Zone Support for Meraki Networks

In **Location Hierarchy**, for the newly added networks with camera zones in Meraki, zones are added to **Location Hierarchy** along with the networks.

For existing networks, the camera zones that are added, modified, or removed in Meraki are synchronized with the **Location Hierarchy** during the background synchronization process.



Note Currently, GUI support to display the camera zones in the Cisco Spaces dashboard is not available.

Prerequisites for Defining the Location Hierarchy

To define the location hierarchy in the Cisco Spaces dashboard, you must first define the required hierarchy structure in your wireless network such as Cisco Meraki, Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller. In addition, you must establish connection between Cisco Spaces and your wireless network.

- [Configuring Cisco Meraki for Cisco Spaces, on page 91](#)
- [Connecting Cisco Spaces to Cisco Wireless Controller through Cisco CMX, on page 49](#)
- [Connecting Cisco Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect , on page 62](#)
- [Connecting Cisco Spaces to Cisco Catalyst 9800 Series Wireless Controller Using Cisco WLC Direct Connect, on page 64](#)
- [Connecting Cisco Spaces to Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller using Cisco Spaces: Connector, on page 79](#)

Displaying Cumulative Count in Location Hierarchy

In the location hierarchy, the count of APs, Proximity Rules, and child locations for the locations will be shown as cumulative. The count for a location will be the total of its count and the count of all its child locations. For example, the total count of APs for a floor will be the sum total of APs for the floor and the APs for each zone under that floor.

The locations with zero count will not have a link to view the details. You can view the APs, Proximity Rules, Locations, and Users of a location by clicking that location. You can view the details of a location parameter only from the associated location.

For the proximity rules, only the unique rules are counted. For example, if two zones of a floor are included in an engagement rule, when counting the rule for the floor, that engagement rule will be counted only once.



CHAPTER 22

Defining the Location Hierarchy

- [Defining the Location Hierarchy, on page 279](#)

Defining the Location Hierarchy

Cisco Spaces supports the following wireless networks:

- **Cisco Meraki**
- **Cisco Wireless Controller with or without Cisco CMX**
- **Cisco Catalyst 9800 Series Wireless Controller**



Note For Cisco Wireless Controller without Cisco CMX and Cisco Catalyst 9800 Series Wireless Controller, you can ensure that appropriate data transfer happens between the Controller and Cisco Spaces using a Cisco Spaces: Connector.

Based on your wireless network, choose the required instructions from the following:

Defining the Location Hierarchy for Cisco Meraki

To import the Cisco Meraki locations, first you must add the Cisco Meraki Organization under the customer name. You can then import Meraki networks. When you import a Meraki network, its floors, and access points are also imported. You can group the access points and create zones at network or floor level. You can group the locations at customer name, or organization level. You can also rename the customer name.

A Meraki Network Location may contain one or more Meraki access points with Cisco Spaces-supported tags. When adding such a Meraki Network Location, only these tagged APs will be added to the Location Hierarchy. Currently, Cisco Spaces only supports the `Cisco-DNASpaces` tag.

If a Meraki Network Location with one or more Cisco Spaces-tagged APs is already added to the Cisco Spaces location hierarchy, then only these tagged APs will be added during the background network synchronization. Non-Cisco Spaces-tagged APs that exist in the location hierarchy for this network will be removed from their respective locations during the next background network synchronization.

However, if none of the APs in the Meraki network have Cisco Spaces-supported tags, then all the access points will be added to the Location Hierarchy. If such a Meraki Network Location having no tagged APs is

already added to the Cisco Spaces location hierarchy, then all the APs will be synchronized to the location hierarchy. There will be no change to the existing location hierarchy.

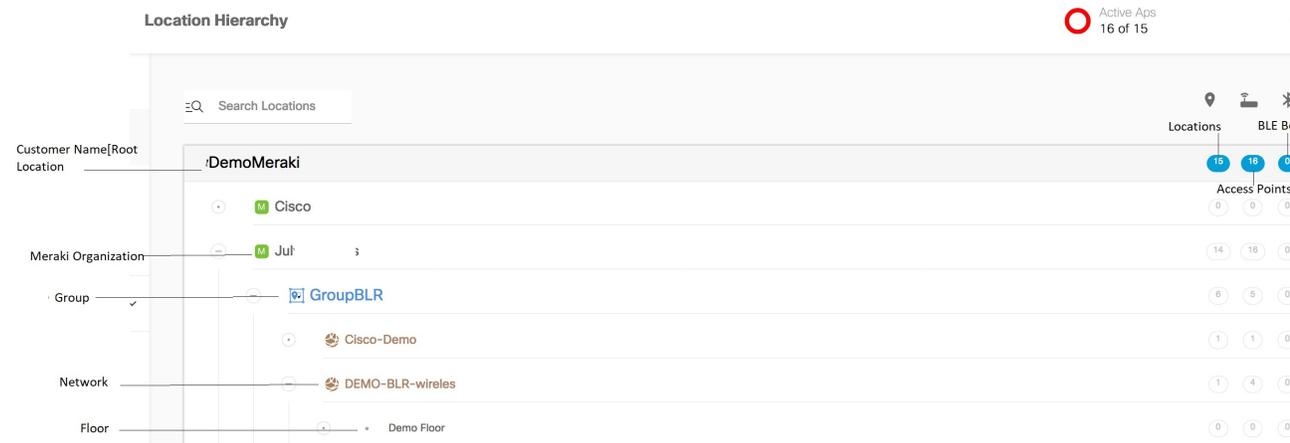
Before creating the location hierarchy, ensure that all the prerequisites are met. To know the prerequisites for creating the location hierarchy, see the [Prerequisites for Defining the Location Hierarchy, on page 277](#).

The location hierarchy for Cisco Meraki network is as follows:

Meraki > Organization > Network > Floor > Access Points.

The Location Hierarchy for Cisco Meraki is shown in the following figure.

Figure 19: Location Hierarchy for Meraki



If you do not have Meraki credentials you can import the locations using Meraki API keys. For more information on importing the locations from Meraki using the API keys, see [Importing Cisco Meraki Locations Using the API Keys, on page 282](#).

If you have the Meraki credentials, to import the Meraki locations to Cisco Spaces, perform the following steps:



Note After defining the location hierarchy, ensure that you define timezones for locations. The timezone defined affects the Cisco Spaces rules and reports.

Adding a Cisco Meraki Organization

To create the location hierarchy in Cisco Spaces, first you must add the Cisco Meraki Organization of which you want to import the locations to the location hierarchy.



Note Cisco Spaces enables you to add multiple Cisco Meraki Organizations to the location hierarchy so that you can connect to the multiple Meraki organizations simultaneously.

To add a Cisco Meraki Organization to the location hierarchy, perform the following steps:

Step 1 In the **Cisco Spaces** dashboard, choose **Location Hierarchy**.

- Step 2** In the **Location Hierarchy** window that appears, click **More Actions** for the customer name (root name).
- Step 3** Choose **Add a Wireless Network**.
- Step 4** From the **Wireless Network** drop-down list that appears, choose **Cisco Meraki**.
- Step 5** Enter the user name and password for your Meraki account, and click **Login**.
- Step 6** From the **Organization** drop-down list, choose the Cisco Meraki Organization from which you want to import the locations.
- Step 7** Click **Add**.
- The organization that is added gets listed in the location hierarchy.

Adding a Network to Cisco Meraki Organization

Cisco Spaces enables you to maintain the network, and floor structure followed for the location hierarchy in Cisco Meraki. After adding a Cisco Meraki Organization to the location hierarchy, you can import its networks, and the associated floors.

To import a network and its associated floors to the location hierarchy, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, click **Location Hierarchy**.
- Step 2** In the **Location Hierarchy** window, click the **More Actions** icon at the far right of the Cisco Meraki Organization for which you want to add the network.
- Step 3** Choose **Add Network**.
- Step 4** In the **Add Network** window, select the networks that you want to add to the location hierarchy.
- The **Add Network** window appears with all the available networks for that Cisco Meraki Organization.
- Step 5** Click **Add**.
- The networks added gets listed in the location hierarchy along with its associated floors.
- Note** In the Cisco Meraki application, ensure that the network name is not duplicated.

Creating Zones and Adding Access Points

You can group the access points of a network or floor using zones. You can create the zones at network or floor level.



Note You cannot modify the access points for a floor.

To create a zone for a network or floor, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
- Step 2** In the **Locations** window, click the **More Actions** at the far right of the network or floor under which you want to create the zone.

Step 3 Choose **Add Zone**.

Step 4 In the **Add Zone** window that appears, perform the following steps:

- a) In the **Zone Name** field, enter a name for the zone.
- b) In the **Select Access Points** area, check the check box for the access points that you want to add to the zone.
- c) Click **Add**.

What to do next



Tip Before creating the zones, locate the access points that you want to include in the zone in the Cisco Meraki dashboard.



Note When you add an access point of a network or floor to a zone, that access point will not be available for that network or floor. The access points added to a zone will not be available for other zones.

Importing Cisco Meraki Locations Using the API Keys

Use the **Setup > Wireless Networks** window to import Cisco Meraki locations for the first time using the API keys.

To import Cisco Meraki locations using the API keys, perform the following steps:

Step 1 In the **Location Hierarchy** window, click the **More Actions** icon for the customer name (root name), and click **Connect Wireless Networks**.

Step 2 In the **Connect your wireless network** window, click **Go to Setup**.

Step 3 In the **Connect your wireless network** window, click **+Add New**.

Step 4 Select Cisco Meraki as the wireless network.

The **Connect via Meraki API Key** wireless network is displayed.

Step 5 Click **Connect** to connect Cisco Meraki with Cisco Spaces using the API key.

The **Connect via API key** pop-up window is displayed.

Step 6 In the **API Key** field, enter the Cisco Meraki API key to fetch the network information and click **Connect**.

The network locations for that API key gets listed. The networks gets imported into Location Hierarchy.

Step 7 Enter the **Post URL** and **Secret Key** parameters to configure Meraki scanning API.

Step 8 Click **Import Networks** to import Cisco Meraki networks into Location Hierarchy.

The network locations gets listed in the **Locations Hierarchy** window. When you import a network, the floors and access points under it also imported.

Defining the Location Hierarchy for Cisco AireOS/ Cisco Catalyst

You can connect CiscoAireOS (Cisco Wireless Controller) and Cisco Catalyst (Cisco Catalyst 9800 Series Wireless Controller) to Cisco Spaces and import the location hierarchy using any of the following connectors: Cisco CMX, Cisco WLC Direct Connect, or Cisco Spaces: Connector.

Defining the Location Hierarchy for Cisco AireOS/ Cisco Catalyst Wireless Controller with Cisco CMX

Before creating the location hierarchy, ensure that all the prerequisites are met. To know the prerequisites for creating the location hierarchy, see the [Prerequisites for Defining the Location Hierarchy, on page 277](#).

Cisco Spaces supports only Cisco CMX 10.6 or later.



Note The **CMX on Prem** option in **Add a Wireless** window will not function any more. When connecting Cisco Spaces to Cisco AireOS/ Catalyst with Cisco CMX, for importing the location to location hierarchy, you can import the locations using CMX Tethering. CMX Tethering can be done by uploading map to Map Services or by configuring Token in Cisco CMX. After importing maps, the map data will reflect in the Location Hierarchy automatically.

The location hierarchy for Cisco AireOS Wireless Controller with a Cisco CMX installation is as following:

Cisco CMX Node > Campus > Building(network) > Floor > CMX Zone (if defined)



Note

- Due to the update in Map services, the location hierarchies imported newly after October 2020 will have only **Campus > Building > Floor > CMX Zone (if defined)** in the hierarchy. However, any updates made to the existing location hierarchy through map upload will maintain **CMX Node**
- For an existing location hierarchy, if you reimport the locations using Map Services, the overlapping APs (APs already existed in location hierarchy and is available in the map imported as well) will be moved to the map-based hierarchy. Therefore, the reports and proximity rules will be affected. . You also have to re-configure the proximity rules to display captive portals or to send notifications
- The **Cisco Spaces Dashboard** restricts the import of locations, under **Location Hierarchy > Add Wireless Networks**, using **CMX On-Prem** or **WLC Direct Connect > Import from Maps**.

The location hierarchy for Cisco AireOS/Catalyst Wireless Controller with Cisco CMX is shown in the following figure.

Figure 20: Location Hierarchy with Cisco CMX



Note After defining the location hierarchy, ensure that you define timezones for locations. The timezone defined affects the Cisco Spaces rules and reports.

Connecting Cisco Spaces to Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller Using CMX Tethering

If you are having Cisco CMX 10.6 or later, you can use the CMX tethering feature to connect Cisco Spaces to the controller, import locations and to configure the location updates for notifications and reports.

Cisco Spaces Network Sync Server supports AP synchronization for CMX Tethering. For CMX Tethering, the changes made to APs in Cisco Prime get updated in Cisco Spaces location hierarchy. To synchronize the AP changes, do any of the following:

- In Cisco CMX, click **SYSTEM**. In the dashboard that appears, choose **Settings > Controllers and Maps Setup > Import**. In the window that appears, provide Cisco Prime Username, Password and IP Address. Then click **Import Controllers and Maps** to get latest map changes. Click **Save**.
- Download updated map from Cisco Prime Infrastructure and upload it to Cisco CMX.
- Download updated map from Cisco Prime and upload it to Map Services in Cisco Spaces.

You can do CMX Tethering in the following ways:

CMX Tethering by Configuring Token in Cisco CMX

To configure CMX Tethering through token, perform the following steps:

- Step 1** In the Cisco Spaces dashboard, choose **Setup > Wireless Networks**.
- Step 2** In the **Connect your wireless network** window, click **Add New**.
- Step 3** Click **Select** for **Cisco AireOS/Catalyst**.
- Step 4** Click **Select** for **Connect Via CMX Tethering**.
The prerequisites for using this option are displayed.
- Step 5** Click **Continue Setup**.

The **Connect Via CMX Tethering** widget appears in the **Connect your wireless network** window.

Step 6 Expand the widget **Connect Via CMX Tethering** .

Step 7 Click **Create New Token** displayed at Step 2.

Step 8 In the **Create a new token** window, enter a name and description for the Cisco CMX Tethering.

Step 9 Click **Save**.

Step 10 Click **View Tokens** displayed at Step 2.

The Cisco CMX Tethering instance added gets listed.

Step 11 To generate a token for connecting the Cisco Spaces dashboard with Cisco CMX, in the **CMX Tethering Tokens** window, click the **Key** icon for the Cisco CMX Tethering instance for which you want to generate a token.

Step 12 Click **Copy**.

Step 13 Log into Cisco CMX.

Step 14 Choose **Manage > Cloud Apps**.

Step 15 In the **Cloud Applications** window that appears, click **Enable** in the **Actions** column for **Cisco Spaces**.

Step 16 In the window that appears, configure the token copied from Cisco Spaces dashboard.

When you configure CMX tethering using a token, the location map for the particular CMX node appears in the **Map Service** window and the locations appear automatically under **Location Hierarchy** of the Cisco Spaces dashboard.

- Note**
- If you delete a location from the **Location Hierarchy**, it will also be removed from **Map Service**.
 - To enable the **Cisco Spaces** service in Cisco CMX, you must have a Cisco Spaces account.
 - For Cisco CMX, you cannot add campus, building, and other child locations using **More Actions** in the location hierarchy. You must update the locations in **Setup > Map Service**. However, you cannot add zones (AP Zones). You can group or delete the locations from the location hierarchy. When you delete a location from the location hierarchy, that location gets removed from the **Map Service** also. For more information, see [Managing the Location Hierarchy for Cisco Wireless Controller with Cisco CMX](#) , on page 302.
 - If you want the location updates in Cisco Prime Infrastructure to get automatically synchronized in Cisco Spaces, you must click the **Map Sync** button in Cisco CMX.

CMX Tethering by Uploading the Location Map to Map Services

The configurations done in the external applications that are not 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.

You can export the maps from Cisco Prime Infrastructure or Catalyst Center. Maps exported from Cisco Prime Infrastructure or Catalyst Center, and imported into Cisco Spaces using **Map Service** will appear automatically under **Location Hierarchy**.

To import the locations to the location hierarchy by exporting the maps from Cisco Prime Infrastructure, perform the following steps:

Step 1 Log into Cisco Prime Infrastructure .

Step 2 In the **Settings/Getting Started** window, click the circle icon near the top left of the window (near the Cisco logo).

Step 3 In the window that appears, click **Maps** on the left pane.

Step 4 In the **Wireless Maps** area, click **Site Maps (Deprecated)**.

Note You can add new locations using the **Site Maps (New)** option.

Step 5 Click the drop-down list near **Go**, and choose **Export Maps**.

Step 6 Click **Go**.

Step 7 From the tree view of location maps, select the parent location (CMX node) that you want to export, and click **Export**.

Note Ensure that the **Include Map Information** check box is checked.

Save the location map on your computer.

Note You must download the map in the zip format and upload it in the Cisco Spaces in the same format.

Step 8 In the Cisco Spaces dashboard, choose **Setup > Map Service**.

Step 9 Click **Upload** at the top left of the window, and select the location map downloaded from Cisco Prime Infrastructure.

The location map gets uploaded to the **Map Service**.

Note You can add a CMX Zone in **Setup > Map Service** using the square icon (below the Expand Collapse icon) displayed in the map.

Step 10 In the Cisco Spaces dashboard, choose **Location Hierarchy**.

- The campuses and its associated buildings and floors that are available in the location map imported to **Map Service** are displayed.
- Maps exported from Cisco Prime Infrastructure and imported into Cisco Spaces using **Map Service** now appears automatically under **Location Hierarchy**.
- If you delete a location from **Location Hierarchy**, it will also be removed from **Map Service**.

Note

- For Cisco CMX, you cannot add campus, building, and other child locations using **More Actions** in the location hierarchy. You must update the locations in **Setup > Map Service**. However, you cannot add zones (AP Zones). You can group or delete the locations from the location hierarchy. When you delete a location from the location hierarchy, that location gets removed from the **Map Service** also. For more information, see [Managing the Location Hierarchy for Cisco Wireless Controller with Cisco CMX](#), on page 302.
- If you want the location updates in Cisco Prime to get synchronized in Cisco Spaces, you must upload the latest map to **Map Service**.

Defining the Location Hierarchy for Cisco Catalyst 9800 Series Wireless Controllers or Cisco Wireless Controller (without Cisco CMX)

You can connect a Cisco AireOS Wireless Controller (without CMX) or Cisco Catalyst 9800 Series Wireless Controller to Cisco Spaces using any of the following connectors:

- Cisco WLC Direct Connect
- Cisco Spaces: Connector

For more information on features supported by these connectors, see [Features Supported by Various Connectors](#), on page 46.

When you have connected the controller to Cisco Spaces using **Cisco WLC Direct Connect** or **Cisco Spaces Connector**, you can import the locations to the location hierarchy using any of the following methods:

- **Access Point Prefix:** If you are using this option, you can add only networks, groups, and zones in the location hierarchy.

For more information on connecting the Cisco Wireless Controller to Cisco Spaces, and importing the location hierarchy to the Cisco Spaces dashboard, see [Importing the Locations using Access Point Prefix](#), on page 287. Alternatively, you can also refer to the configurations steps for **Connect WLC/Catalyst 9800 Directly** in **Setup > Wireless Networks** of Cisco Spaces dashboard.

- **Importing from Maps:** This radio button is disabled now. Importing the locations through maps must be done now through **Setup > Map Service**. Using maps, you can import the locations in the same hierarchical structure as in Cisco Prime Infrastructure, Campus-Building-Floor. You must export the location map from Cisco Prime Infrastructure and upload the map to the **Map Service** option in the Cisco Spaces dashboard to view the locations in the location hierarchy. After importing maps to Cisco Spaces, the map data will reflect in the Location Hierarchy automatically. For more information on importing the locations using Map Services, see [Importing Locations to the Location Hierarchy Using Map Services](#), on page 289.

**Note**

- You can import APs as per the license limit when adding locations using the **Access Point Prefix** option (**Connect WLC/Catalyst 9800 Directly** or **Connect via Spaces Connector**).
- If the license limit was reached, APs over and above the license limit that were available under the controller were not synchronized with **Location Hierarchy**. Now, priority is given to the APs with a common prefix over the APs present under the **Unconfigured** location. Those APs that are present under the **Unconfigured** location are removed during the synchronization process, making way for the synchronization of the APs with a common prefix, under the controller.
- If you were using Cisco Spaces earlier with Cisco CMX, and if you are moving to use Cisco Spaces directly with Cisco Wireless Controller, the Reports and proximity rules will be affected. The Reports will be shown based on the new location configurations. You also have to re-configure the proximity rules to display captive portals or to send notifications
- For an existing location hierarchy, if you reimport the locations using Map Services, the overlapping APs (APs already existed in location hierarchy and is available in the newly imported map as well) will be moved to the map-based hierarchy. Therefore, the reports and proximity rules will be affected. You also have to re-configure the proximity rules to display captive portals or to send notifications.

Importing the Locations using Access Point Prefix

- Step 1** To import the locations to the Cisco Spaces, click the three-line menu icon at the top-left of the Cisco Spaces dashboard.
- Step 2** Choose **Location Hierarchy**.
- Step 3** In the **Location Hierarchy** window, click **More Actions** at the far right of the customer name(root name).
- Step 4** Click **Add a Wireless Network**.

- Step 5** From the **Wireless Network** drop-down list, choose **WLC Direct Connect**.
- Step 6** Click the **Access Point Prefix** radio button.
- The imported Cisco Wireless Controllers get listed.
- Note** The Cisco Wireless Controllers get listed only if you configure the Cisco Wireless Controller for importing them to Cisco Spaces.
- Step 7** Select the Cisco Wireless Controller, and click **Next**.
- This Cisco Wireless Controller will act as the primary Cisco Wireless Controller.
- Step 8** Select another Cisco Wireless Controller as the secondary controller, and click **Next**.
- Note** This feature helps you manage Cisco Spaces with a secondary Cisco Wireless Controller with the same APs if the primary controller is down.
- The secondary controller is optional. You can move to the next screen without selecting a secondary controller by clicking the **Skip** button.
- Step 9** Select the networks that you want to add.
- Note** Cisco Spaces will automatically group the APs based on the prefix of their names, and creates networks. The APs that are not grouped under a network will be listed under the name “Unconfigured”.
- Note** If you are not selecting a network, the APs in that network will be added to the location hierarchy under the name “Unconfigured”.
- Step 10** Click **Done**.
- The APs of the primary and secondary controllers selected will get listed in the location hierarchy.
- Step 11** In the location hierarchy, click the **More Actions** icon at the far right of the network, and click **Add Zone**.
- Step 12** In the window that appears, enter a name for the zone, and select the APs to be included in the zone.
- Step 13** Similarly, create all the required zones.
- Step 14** If you have created the location hierarchy earlier using the Cisco CMX, delete that location hierarchy, and re-configure the rules such as captive portal rules, engagement rules and location personas rules.

Note

- After defining the location hierarchy, ensure that you define timezones for locations. The timezone defined affects the Cisco Spaces rules and reports.
- When adding the APs in the Cisco Wireless Controller, follow proper naming conventions (with appropriate prefix) to ease auto-network creation in Cisco Spaces.
- In the Cisco Wireless Controller, if new APs are added to the Cisco Wireless Controller, those APs get automatically imported during the next Cisco Wireless Controller synchronization. If an imported AP is deleted from the Cisco Wireless Controller, the changes will be reflected in Cisco Spaces only after 48 hours.
- For Cisco Wireless Controller, Cisco Spaces enables you to group access points with different prefixes under a single network. After importing the networks to the location hierarchy, click the network to add the APs of multiple prefixes. In the location hierarchy, when you click a network location, a new **Access Points Prefix Used** option will be available in the **Location Info** tab to add APs of multiple prefixes to that network. After adding the prefix, the APs under the unconfigured network with the specified prefix will be moved under this network. The **Access Points Prefix Used** option will be available only for network locations. However, the **Access Points Prefix Used** option will not be available for the Unconfigured network.

What to do next

You can change the primary controller, and add more secondary controllers. You can also add APs of multiple prefixes to a single network. For more information, see the [Managing the Location Hierarchy for Cisco Wireless Controller or Cisco Catalyst 9800 Series Controller\(with WLC Direct Connect or Cisco Spaces: Connector\)](#), on page 305.

Importing Locations to the Location Hierarchy Using Map Services

If a Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller is connected to Cisco Spaces through **WLC Direct Connect** or **Cisco Spaces Connector**, you can import the locations to the location hierarchy using the Map Services. If you are using this option, you can import the locations in the same hierarchical structure, Campus- Building-floor .

**Note**

You can export the maps from Cisco Prime Infrastructure or Catalyst Center. Maps exported from Cisco Prime Infrastructure or Catalyst Center and imported into Cisco Spaces using **Map Service** appears automatically under **Location Hierarchy**.

To import the locations to the location hierarchy by exporting the maps from Cisco Prime, perform the following steps:

-
- Step 1** Log into Cisco Prime Infrastructure.
 - Step 2** In the **Settings /Getting Started** window, click the circle icon near the top-left of the window (near the Cisco logo).
 - Step 3** In the window that appears, click **Maps** on the left pane.
 - Step 4** In the **Wireless Maps** area, click **Site Maps (Deprecated)**.

Note You can add new locations using the **Site Maps (New)** option.

Step 5 Click the drop-down list near **Go**, and choose **Export Maps**.

Step 6 Click **Go**.

Step 7 From the tree view of location maps, select the parent location (CMX node) that you want to export, and click **Export**.

Note Ensure that the **Include Map Information** check box is checked.

Step 8 Save the location map on your computer.

Note You must download the map in the gzip format and upload it in the Cisco Spaces in the same format.

Step 9 In the Cisco Spaces dashboard, choose **Setup > Map Service**.

Step 10 Click **Upload** at the top left of the window, and select the location map downloaded from Cisco Prime Infrastructure. The location map gets uploaded to the **Map Service**.

Step 11 In the Cisco Spaces dashboard, choose **Location Hierarchy**.

- The campuses and its associated buildings and floors that are available in the location map imported to **Map Service** are displayed.
- Maps exported from Cisco Prime Infrastructure and imported into Cisco Spaces using **Map Service** now appears automatically under **Location Hierarchy**.
- If you delete a location from **Location Hierarchy**, it will also be removed from **Map Service**.

Note After defining the location hierarchy, ensure that you define timezones for locations. The timezone defined affects the Cisco Spaces rules and reports.

- If the locations are imported using **Map Service**, you cannot add campus, building, and other child locations using **More Actions** in the location hierarchy. You must update the locations in **Setup > Map Service**. However, you cannot add zones (AP Zones). You can group or delete the locations from the location hierarchy. When you delete a location from the location hierarchy, that location gets removed from the **Map Service** also. For more information, see [Managing the Location Hierarchy for Cisco Wireless Controller with Cisco CMX](#), on page 302.
-



CHAPTER 23

Managing the Location Hierarchy

- [Managing the Location Hierarchy, on page 291](#)

Managing the Location Hierarchy

Renaming a Customer

To rename a customer, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, click **Location Hierarchy**.
 - Step 2** In the **Location Hierarchy** window, click **More Actions** at the far right of the customer name.
 - Step 3** Click **Rename <root name>**.
 - Step 4** In the **Rename root** window that appears, enter the customer name you want.
 - Step 5** Click **Rename**.
-

Adding a Wireless Network

There are multiple methods to connect your wireless network with Cisco Spaces based on your wireless network deployment.

Cisco Spaces supports Cisco AireOS Wireless Controller (Cisco Wireless Controller), Cisco Catalyst 9800 Series Wireless Controller and Cisco Meraki. You can add multiple wireless networks to the location hierarchy using the **Connect Wireless Networks** option.

In the **Connect your wireless network** window, click Go to Setup to go to **Setup > Wireless Networks** to add your wireless network.

The following wireless network options are available:

- **AireOS Controller/Catalyst 9800 Wireless Controller:** Choose this for Cisco Aironet Access Points with Cisco Wireless Controllers or Cisco CMX On-Prem Tethering. This includes:
 - Via Spaces Connector: Need to install Cisco Spaces: Connector on a VM in order to connect your controller to Cisco Spaces.

- Connect Cisco Wireless Controllers directly: Wireless controllers require direct internet connectivity. Cisco AireOS Wireless Controller release 8.3 or later and Cisco Catalyst 9800 Series Wireless Controller release 16.10 or later is required.
- Connect via CMX Tethering: Cisco CMX Release 10.6 or later versions are supported while connecting via CMX Tethering.
- **Cisco Meraki:** Choose this for Cisco Meraki networks with Cisco Meraki Access Points. This includes **Connect via API key** method.



Note For more information on adding a Cisco CMX node, Cisco Meraki Organization, or Cisco Wireless Controller access points using the Add a Wireless Network option, see [Defining the Location Hierarchy, on page 279](#).

Adding Metadata for a Location

You can group the locations using metadata. You can use this metadata when defining the proximity rules. You can also use this metadata also for defining the brands for the **Behavior Metrics** app.

To add a metadata for a location, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
 - Step 2** In the **Location Hierarchy** window, click the **More Actions** icon for the location for which you want to add metadata.
 - Step 3** Click **Add/Edit Metadata**.
 - Step 4** In the **Add Metadata for <location>** window that appears, perform the following steps:
 - a) In the Key field, enter a metadata key.
 - b) In the value field, enter a value for the key.
 - c) Click **Save**.
-

What to do next



Note Similarly, add the metadata for other locations that must have this metadata.

Updating Metadata for a Location

To update the metadata for a location, perform the following steps:

-
- Step 1** In the **Location Hierarchy** window, click **More Actions** at the far right of the location for which you want to update the location metadata.
 - Step 2** Click **Add/Edit Metadata**.
 - Step 3** In the **Add Metadata for <location>** window that appears, click the metadata that you want to update.

Step 4 Make necessary changes, and click **Update** .

What to do next



Note You can delete a location metadata by clicking the Delete button for that metadata.

Defining or Changing the Time Zone for Locations

You can define the time zone for various locations in the location hierarchy. To define the time zone for a location, perform the following steps:

Step 1 In the Cisco Spaces dashboard, choose **Location Hierarchy**.

Step 2 In the **Location Hierarchy** window, click the location for which you want to define the time zone.

Step 3 On the **Location Info** tab, click **Edit** for **Location Data**.

The **Location Information** pop-up window appears.

Step 4 From the **Select Timezone** drop-down list, choose the time zone that you want to configure for this location.

Step 5 Click **Update**.

The time zone is defined for the location.

What to do next



Note The notifications are sent for the locations based on the configured time zones.

Adding the Information of a Location

You can specify the information such as address of each separately location in the location hierarchy.

To add the location information for a location, perform the following steps:

Step 1 Click the three-line menu icon at the top-left of the Cisco Spaces dashboard.

Step 2 Choose **Location Hierarchy**.

Step 3 In the **Location Hierarchy** window, click the location for which you want to add the information.

Step 4 On the **Location Info** tab, click **Edit** for **Location Data**.

Step 5 In the **Location Information** window that appears, enter the information for the particular location.

You can add the following information about the location:

- Brand
- Country
- State
- City
- Zip /Postal Code
- Address
- Time Zone
- Area in Square Feet or Square Meter
- Occupancy Limit (Max Capacity)

Step 6 Click **Update**.

The location information added will now get listed in the **Location Data** area on the **Location Info** tab.

Note If you are not specifying the location information for a location, that location will inherit the information of its parent location. Location information inherited from the parent location will appear in Orange. However, we recommend you to update the location information for each location.

Searching for a Location

You can search for a location in the location hierarchy using its name. To search for a location in the location hierarchy, perform the following steps:

Step 1 In the Cisco Spaces dashboard, choose **Location Hierarchy**.

The **Location Hierarchy** window appears.

Step 2 In the Search field, enter the name of the location that you want to search.

The location gets highlighted in the location hierarchy.

Searching for an Access Point

You can search for an access point using its name or MAC address.

To search for an access point in the location hierarchy, perform the following steps:

Step 1 In the Cisco Spaces dashboard, choose **Location Hierarchy**.

The **Location Hierarchy** window appears.

Step 2 In the Search field, enter the name or MAC address of the access point that you want to search.

The access point gets highlighted.

Managing the Maps for a Location

The maps are displayed by default based on the map configuration in the wireless network.

To view the map for a location, perform the following steps:

- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
- Step 2** In the location hierarchy, click the location for which you want to view the map.
- Step 3** Click the **Maps** tab.
The map appears in the **Maps** tab.
-

Managing the Access Points

You can add or remove access points to a zone.

Adding an Access Point to a Zone

To add access points to a zone, perform the following steps:

- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
- Step 2** In the location hierarchy, click the zone to which you want to add the access point.
- Step 3** Click **Modify Access Points**
- Step 4** Select the check box for the access point that you want to add.
- Step 5** Click **Add**.
The access point gets added to the zone.
-

What to do next



Note If there are no access points under that zone, the button name will be **Add Access Points**.



Note For Cisco Unified Wireless Network, to import the access points, the Cisco CMX must be publicly accessible. For a default Cisco Unified Wireless Network installation, the ports 80 and 443 must be open. For more information, see [Bandwidth Requirements to Deploy Cisco Spaces, on page 2](#).

Removing an Access Point from a Zone

To remove an access point from a zone, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
- Step 2** In the location hierarchy, click the zone from which you want to delete the access point.
- Step 3** Click **Modify Access Points**.
- Step 4** Uncheck the check box for the access point that you want to delete.
- Step 5** Click **Add**.
The access point gets deleted from the zone.
-

Viewing the Access Points for a Location

You can view the access points under each location. Ideally, the access points belong to a floor or zone.

To view the access points for a location, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
- Step 2** In the location hierarchy, click the location for which you want to view the access points.
- Step 3** Click the **Access Points** tab.
The access points associated with that location are displayed.
-

What to do next



Note The **Access Points** link for a location is enabled only if at least one access point exists for that location.

Managing the Groups

Cisco Spaces enables you to rename a group name, edit a group, and delete an independent group.

Creating Groups

Grouping enables you to create proximity rules specific to a set of locations. You can create groups at the higher levels in the location hierarchy.

For Cisco Unified Wireless Network, you can group the CMX nodes or campuses in the location hierarchy. For example, you can group the Campus 1 and Campus 2 under one group and Campus 3 and Campus 4 under another group. You can also create sub groups under these groups. For Meraki, you can group the Cisco Meraki Organizations or networks in the location hierarchy. For example, you can group the Network 1 and Network 2 under one group and Network 3 and Network 4 under another group. You can also create sub groups under these groups.

You can also create a group including the wireless network nodes of both Cisco Unified Wireless Network and Meraki. However, you cannot group the lower level locations of Cisco Unified Wireless Network and Meraki. For example, you cannot group a campus and a Meraki network.

To create a group for a location, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, click **Location Hierarchy**.
- Step 2** In the **Location Hierarchy** window, click **More Actions** at the far right of the location under which you want to add the group.
- Step 3** Click **Create Group**.
- Step 4** In the window that appears, perform the following steps:
- Enter a name for the group.
 - Select the locations that you want to add under this group.
- Note** The locations available for selection depends upon where you are adding the group in the location hierarchy. When you add a group under the customer name (root level), the first level locations (For example, CMX node, Cisco Meraki Organization) are available for selection. When you add a group under a CMX node, only the campuses under that CMX node are available for selection.
- Click **Add**.

What to do next



Tip If you want to have a parent group without any location, and sub groups with location, then you first create the parent group with all the required locations that must become the part of its sub groups. Then you create a sub group under the parent group. The locations added to the parent group are available for selection. Select the locations that you want to add under the sub group. Similarly, you can create more sub groups under the parent group.



Note You can add more locations to a group at any time.

Renaming a Group

To rename a group, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
 - Step 2** In the location hierarchy, click **More Actions** for the group that you want to rename.
 - Step 3** Click **Rename "group name"**.
 - Step 4** In the **Rename group** window that appears, enter the new name for the group.
 - Step 5** Click **Rename**.
-

Editing a Group

You can add or remove the locations from a group.

To edit a group, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
 - Step 2** In the location hierarchy, click **More Actions** for the group that you want to edit.
 - Step 3** Click **Edit group**.
 - Step 4** In the **Edit Group** window that appears, check the check box for the locations that you want to be part of the group.
 - Step 5** Click **Update**.
-

Deleting a Group

To delete a group, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
 - Step 2** In the location hierarchy, click **More Actions** at the far-right of the group that you want to delete.
 - Step 3** Click **Delete group**.
-

What to do next



Note To delete a group, first you have to delete the locations and sub groups under that group, if any.



Note You cannot delete a group that is associated with the proximity rules.

Managing the Zones

You can rename and delete the zones created for Cisco Unified Wireless Network or Meraki.

Renaming a Zone

To rename a zone, perform the following steps

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears.
- Step 2** In the location hierarchy, click **More Actions** for the zone that you want to rename.
- Step 3** Click **Rename "zone name"**.
- Step 4** In the **Rename-zone** window that appears, enter the new name for the zone.
- Step 5** Click **Rename**.
-

Deleting a Zone

To delete a zone, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears.
- Step 2** In the location hierarchy, click **More Actions** for the zone that you want to delete.
- Step 3** Click **Delete zone**.
- Note**
- When you delete a zone location from the **Map Service** UI, the same is deleted from **Location Hierarchy** as well.
 - You cannot delete any zone that is associated with the proximity rules.
-

Managing the Location Hierarchy for Meraki

You can rename, and delete the locations under Meraki.

Adding Floors to a Network

To add a floor to a network, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
- Step 2** In the **Location Hierarchy** window, click **More Actions** at the far right of the network under which you want to create the floor.
- Step 3** In the **Add Floor** window that appears, select the floor that you want to add under the network.
- Step 4** Click **Add**.
The floor gets added to the network.
-

Renaming a Cisco Meraki Organization

To rename a Cisco Meraki Organization, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
- Step 2** In the location hierarchy, click **More Actions** for the organization that you want to rename.
- Step 3** Click **Rename "Organization Name"**.
- Step 4** In the **Rename-Meraki** window that appears, enter the new name for the Cisco Meraki Organization.
- Step 5** Click **Rename**.
-

Deleting a Cisco Meraki Organization

To delete a Cisco Meraki Organization, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
- Step 2** In the location hierarchy, click **More Actions** for the Cisco Meraki Organization that you want to delete.
- Step 3** Click **Delete Organization**.
-

What to do next



-
- Note** To delete an organization, first you have to delete the locations and groups under that organization, if any.
-
- You cannot delete any organization that is associated with the proximity rules.

Renaming a Network

To rename a network, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
- Step 2** In the location hierarchy, click **More Actions** for the network that you want to rename.
- Step 3** Click **Rename "network name"**.
- Step 4** In the **Rename-location** window that appears, enter the new name for the location.
- Step 5** Click **Rename**.
-

Deleting a Network

To delete a network, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
- Step 2** In the location hierarchy, click **More Actions** for the network that you want to delete.
- Step 3** Click **Delete network**.
-

What to do next



Note To delete a network, first you have to delete the floors and access points under that network, if any.

- You cannot delete any network that is associated with a proximity rule.

Renaming a Floor

To rename a floor, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
- Step 2** In the location hierarchy, click **More Actions** for the floor that you want to rename.
- Step 3** Click **Rename "floor name"**.
- Step 4** In the **Rename-floor** window that appears, enter the new name for the floor.
- Step 5** Click **Rename**.
-

Deleting a Floor

To delete a floor, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
- Step 2** In the location hierarchy, click **More Actions** for the floor that you want to delete.
- Step 3** Click **Delete floor**.
-

What to do next



Note If the floor that you delete has any zone under it, that zone is moved under the network after the deletion of the floor.



Note You cannot delete any floor that is associated with a proximity rule.

Managing the Location Hierarchy for Cisco Wireless Controller with Cisco CMX

For Cisco Wireless Controller with Cisco CMX, you cannot add campuses, building, and other child locations using **More Actions** in the location hierarchy. You must update the locations in **Setup > Map Service**. However, you can rename, group, or delete the locations from the location hierarchy.

When you delete a location from the location hierarchy, that location gets removed from **Map Service** also. When you delete a location from **Map Service**, only the APs will be removed from the location hierarchy leaving the hierarchy structure as it is.

Renaming a CMX Node

To rename a CMX node, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
- Step 2** In the location hierarchy, click **More Actions** for the CMX node that you want to rename.
- Step 3** Click **Rename <Cisco CMX Node>**.
- Step 4** In the window that appears, enter the new name for the CMX node.
- Step 5** Click **Rename**.
-

What to do next

Note The renaming is not reflected in the Cisco CMX.

Deleting a CMX Node

To delete a CMX node from the location hierarchy, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
- Step 2** In the location hierarchy, click **More Actions** for the CMX node that you want to delete from the location hierarchy.
- Step 3** Click the option to delete the CMX node.
-

What to do next

Note To delete a CMX node, first you have to delete the locations and groups under that CMX node, if any.



Note You cannot delete a CMX node that is associated with the proximity rules.

Renaming a Campus

To rename a campus, perform the following steps

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
- Step 2** In the location hierarchy, click **More Actions** for the campus that you want to rename.
- Step 3** Click **Rename <campus name>**.
- Step 4** In the **Rename-campus** window that appears, enter the new name for the campus.
- Step 5** Click **Rename**.
-

Deleting a Campus

To delete a campus, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.

The **Location Hierarchy** window appears with the location hierarchy.

Step 2 In the location hierarchy, click **More Actions** for the campus that you want to delete.

Step 3 Click **Delecte campus**.

What to do next



Note To delete a campus, first you have to delete the locations under that campus, if any.



Note You cannot delete a campus that is associated with proximity rules.

Renaming a Building

To rename a building, perform the following steps:

Step 1 In the Cisco Spaces dashboard, choose **Location Hierarchy**.

The **Location Hierarchy** window appears with the location hierarchy.

Step 2 In the location hierarchy, click **Location Hierarchy** for the building that you want to rename.

Step 3 Click **Rename <building name>**.

Step 4 In the **Rename -network** window that appears, enter the new name for the building.

Step 5 Click **Rename**.

Deleting a Building

To delete a building, perform the following steps:

Step 1 In the Cisco Spaces dashboard, choose **Location Hierarchy**.

The **Location Hierarchy** window appears with the location hierarchy.

Step 2 In the location hierarchy, click **More Actions** for the building that you want to delete.

Step 3 Click **Delete building**.

What to do next



Note To delete a building, first you have to delete the floor or zones under that building, if any.



Note You cannot delete a building that is associated with a proximity rule.

Renaming a Floor

To rename a floor, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
 - Step 2** In the location hierarchy, click **More Actions** for the floor that you want to rename.
 - Step 3** Click **Rename "floor name"**.
 - Step 4** In the **Rename-floor** window that appears, enter the new name for the floor.
 - Step 5** Click **Rename**.
-

Deleting a Floor

To delete a floor, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.
 - Step 2** In the location hierarchy, click **More Actions** for the floor that you want to delete.
 - Step 3** Click **Delete floor**.
-

What to do next



Note If the floor that you delete has any zone under it, that zone is moved under the building after the deletion of the floor.

Managing the Location Hierarchy for Cisco Wireless Controller or Cisco Catalyst 9800 Series Controller (with WLC Direct Connect or Cisco Spaces Connector)

Adding Networks Automatically for a Primary Controller

If you have skipped to select the networks when importing the Cisco Wireless Controller, you can add the networks automatically at any time later.

To add network automatically for a Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
 - Step 2** In the **Location Hierarchy** window, click the **More Actions** icon for the wireless controller for which you want to add networks.
 - Step 3** Click **Edit**.
 - Step 4** In the **Edit Controller** window that appears, select the **Auto Network Creation** check box.
 - Step 5** Click **Done**.

The APs with similar prefix are grouped, and networks are formed automatically. The APs that are not added to the auto-created networks are listed under the network name “unconfigured”.

What to do next



-
- Note** Only the APs added to the wireless controller after configuring the auto network are grouped. Existing APs under the “unconfigured” network name will not be grouped automatically based on this configuration. However, if any new AP gets added to the wireless controller with the same prefix of an existing AP in the “unconfigured” network, then the existing AP gets grouped with the new AP added.
-

Manually Adding Networks for a Primary Controller

To manually add network for a Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
 - Step 2** In the **Location Hierarchy** window, click the **More Actions** icon for the cisco wireless controller for which you want to define the network.
 - Step 3** Click **Add Network**.
The **Add Network** window that appears.
 - Step 4** In the **Network Name** field that appears, enter a name for the network.
 - Step 5** In the **Access Point Prefix** field that appears, enter the prefix the APs must have to group under the network, and click **Fetch**.

The network get listed in the location hierarchy.

- Note** Multiple prefixes are supported for a wireless network. However, when you are adding a network, you can add the APs of only one prefix. If you want to add access points with another prefix to this network, you must edit the network after adding it. For more information on adding APs of multiple prefixes, see [Adding APs of Multiple Prefixes to a Network, on page 307](#).

- Step 6** Click **Done**.

The network will be created with the APs having the prefix mentioned.

Adding APs of Multiple Prefixes to a Network

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.

To add APs of multiple prefixes to a network of a Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, click the three-line menu icon at the top-left of the window.
- Step 2** Choose **Location Hierarchy**.
- Step 3** In the **Location Hierarchy** window, click the network to which you want to add APs of multiple prefixes.
- Step 4** In the **Location Info** tab, click **Edit** for **Access Points Prefix Used**.
- Step 5** In the **Edit Prefix** window that appears, in the **Prefix** field, enter the prefix.
The APs with the prefix entered get listed.
- Step 6** Click **Add Prefix**.
Now the newly added prefix gets listed under **Added Prefixes** in the right pane of the window. **Add Prefix** will be enabled only if there are APs with the Prefix entered.
- Step 7** Click **Save**.
After adding the prefix, the APs under the **unconfigured** network with this prefix will be moved to this network.
To delete a prefix, hover over that prefix under **Added Prefixes**, and click the **Delete** icon that appears.
- Note** 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.
-

Adding Additional Secondary Controller

If you have skipped to add a secondary controller when importing the Cisco Wireless Controller, you can add it any time later. Even if you have configured a secondary controller, you can add more than one secondary controllers.

To add a secondary controller for a Cisco Wireless Controller, perform the following steps:

-
- Step 1** In the Cisco Spaces dashboard, choose **Location Hierarchy**.
- Step 2** In the **Location Hierarchy** window, click the **More Actions** icon for the Cisco Wireless Controller for which you want to add secondary controller.
- Step 3** Click **Edit**.
- Step 4** In the **Edit Controller** window that appears, click **Add More** for Additional Controllers.
- Step 5** In the **Add additional controller** window that appears, select the Cisco Wireless Controller that you want to configure as secondary controller.

Note The Cisco Wireless Controllers similar to the primary controller (having same APs) will be top in the list.

Step 6 Click **Add**.

Now the newly configured Cisco Wireless Controller has become the secondary controller.

Note You can add more than one Cisco Wireless Controller as secondary controller. However, you can add only one at a time.

Deleting a Secondary Controller

To delete a secondary controller, perform the following steps:

Step 1 Click the three-line menu icon displayed at the top-left of the Cisco Spaces dashboard.

Step 2 Choose **Location Hierarchy**.

Step 3 In the location hierarchy, click the **More Actions** icon for the Primary Controller of which you want to delete the secondary Cisco Wireless Controller.

Step 4 Click **Edit**.

In the **Edit Controller** window that appears, the secondary controllers added for that PrimaryController will be listed under **Additional Controllers**.

Step 5 Click the **Delete** icon for the secondary controller that you want to delete.

Step 6 In the window that appears, confirm the deletion.

Now, the secondary controller is deleted.

What to do next



Note When you delete a secondary controller, the APs that are unique for this secondary controller (APs not in the primary controller or its other secondary controllers) also will be deleted.

Renaming the Primary Controller

To rename the primary controller, perform the following steps:

Step 1 In the Cisco Spaces dashboard, choose **Location Hierarchy**.

Step 2 In the location hierarchy, click the **More Actions** icon for the Cisco Wireless Controller that you want to rename.

Step 3 Click **Rename <cisco wireless controller>**.

Step 4 In the **Rename WLC** window that appears, enter the name required, and click **Rename**.

Now the name of the Cisco Wireless Controller is changed to the new name specified.

Note The name change is not reflected in the Cisco Wireless Controller.



PART **IX**

Location Hierarchy 2.0

- [Overview of Location Hierarchy 2.0, on page 313](#)



CHAPTER 24

Overview of Location Hierarchy 2.0

Location Hierarchy 2.0'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 are automatically reflected with Location Hierarchy 2.0.

In **Location Hierarchy** window, the default customer name (root location) is automatically selected and the **Map** tab displays the location on the map. An alert message is displayed if the time zone is not updated for that particular location.

The screenshot displays the Cisco Spaces Location Hierarchy interface. At the top, the header includes the Cisco Spaces logo, the page title 'Location Hierarchy - Beta', a 'Beta UI' toggle, and a status indicator for 'Active APs 46 of 100'. The left-hand pane features a search bar and a tree view of location hierarchies, with 'Cisco Connect Demo' selected. A tooltip for this location shows a warning: '1 Time zone data not available' and the message 'Time zone is not updated in this location.' The main content area shows a map of a street named 'Manas Chowk' with a blue location pin. Above the map, a summary table for the selected location is displayed:

Campus	Building	Group	Floor	Zone	Alerts
15	35	2	77	45	1

Below the map, there are tabs for 'Info', 'Network Devices', and 'Metadata'. A small notification icon with the number '2' is visible in the bottom right corner of the map area.

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 campuses, buildings, groups, floors and zones.

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 the connected network devices and running devices
- **Metadata:** Displays the configured metadata information

You can perform the following additional tasks in the **Location Hierarchy** window:

- **Search:** In the **Search** field, enter the location name and press **Enter**. You must provide a minimum of four letters as the search term. 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.
- **Delete:** Click the three dots next to the location and click **Delete Location** to delete the location from **Location Hierarchy**.



Note In the **Location Hierarchy 2.0** window, click the **Beta UI** toggle button to enable the new UI. If you enable **Location Hierarchy 2.0**, the feature is enabled for all the users available in the same account.

Location Hierarchy 2.0 shows rich maps, if they are available for a particular floor. The option to upload rich maps is currently managed by the Cisco Spaces support team. Click the **3D** toggle button to switch between 2D and 3D floor maps.

In **Location Hierarchy 2.0**, 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**.

- [View Location Information, on page 315](#)
- [Update Location Information, on page 319](#)
- [View the Network Devices, on page 321](#)
- [Configure Metadata, on page 322](#)

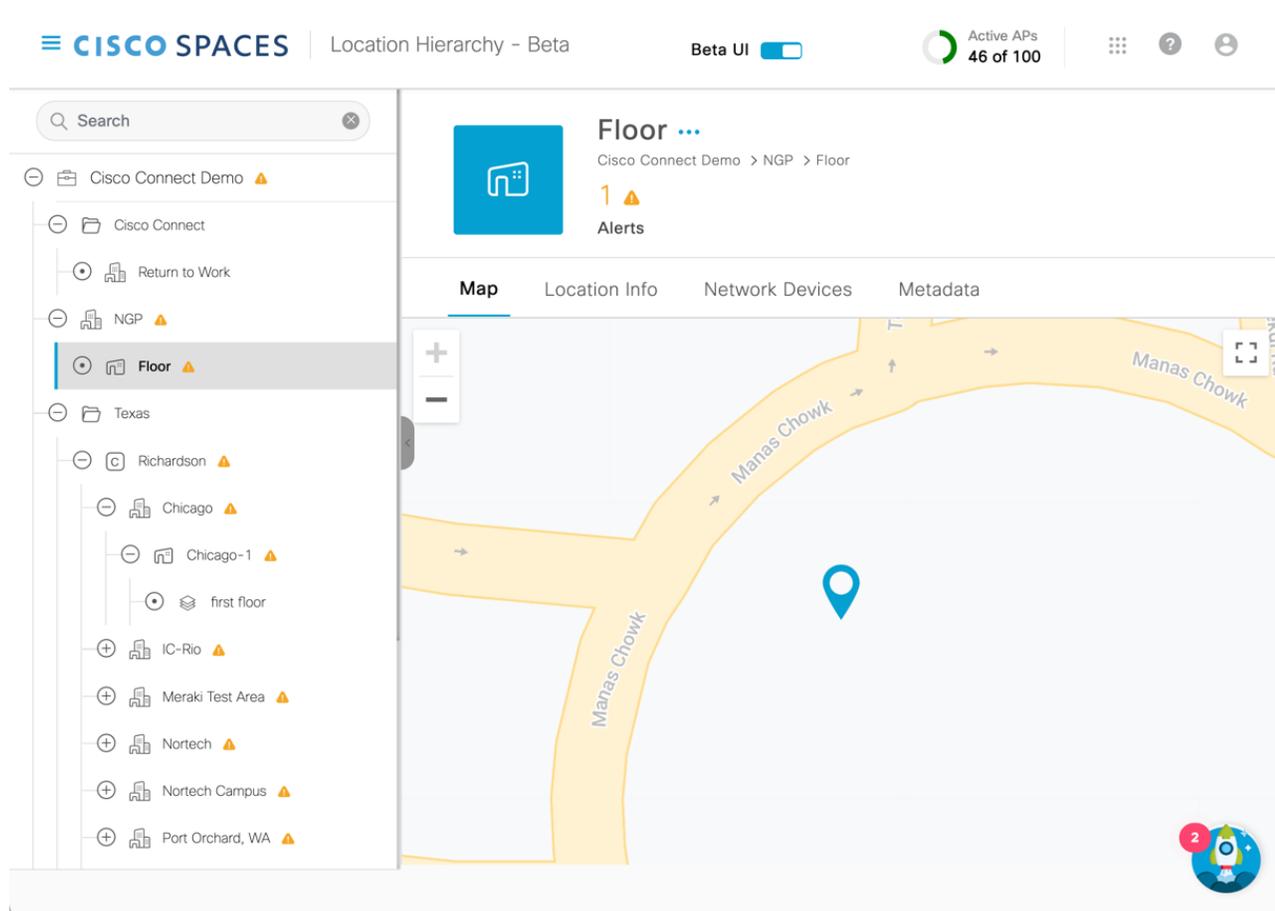
View Location Information

Use the **Map** tab (**Cisco Spaces dashboard** > **Menu icon** (☰) > **Location Hierarchy 2.0** > **Root Location**) to view the selected location, campus, building and floor information on the map.

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 plotter icon. You can click on the plotter icon 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 21: 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, see [Create a Zone, on page 316](#).

Depending on the location you select, view the following information:

- Organization
- Campus
- Building
- Floor
- Zone
- Alerts

Create a Zone

Use the **Map** tab to create Cisco CMX zones in **Location Hierarchy**.

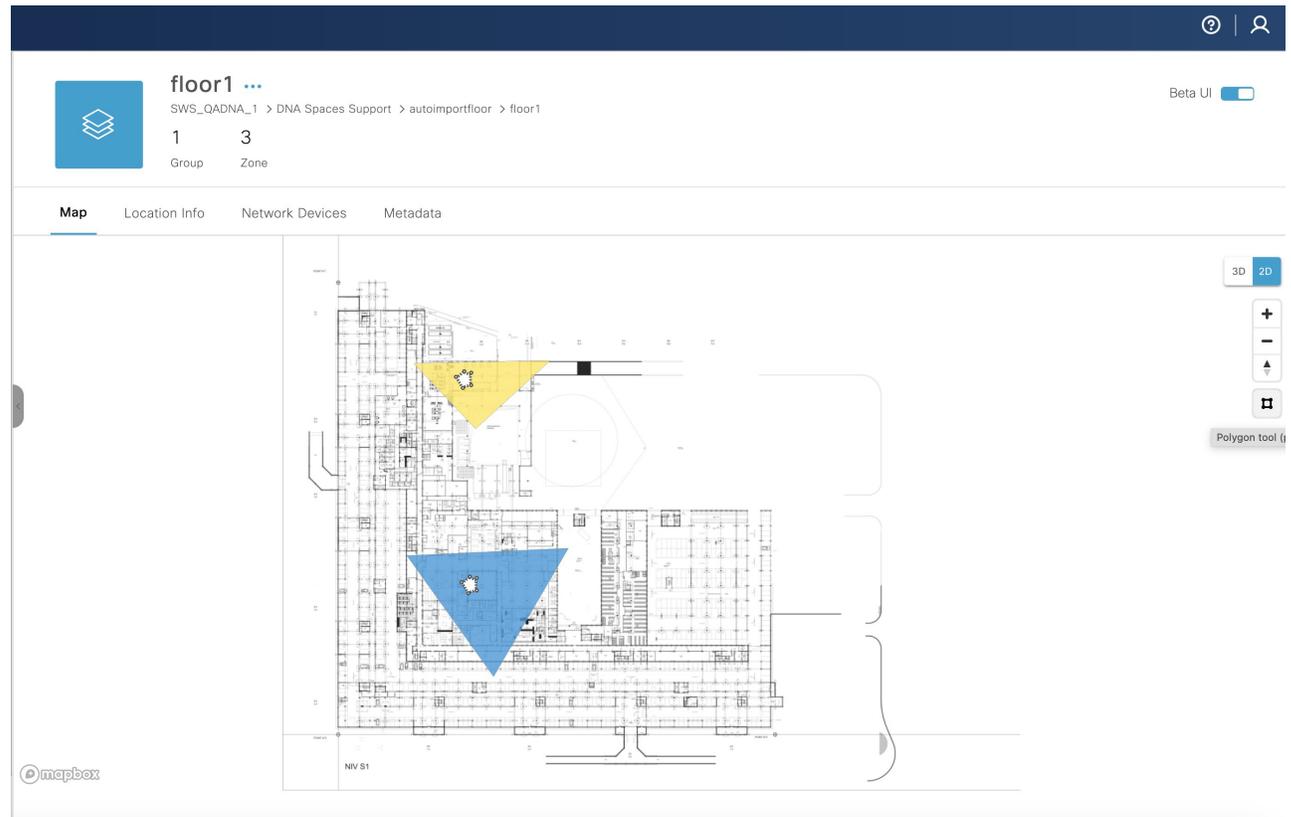
-
- Step 1** Log in to [Cisco Spaces](#).
- Step 2** In the Cisco Spaces dashboard, click the **Menu** icon (☰) and choose **Location Hierarchy**.
The **Location Hierarchy** window is displayed.
- Step 3** In the left pane, navigate to the required floor location.
The floor map is displayed.
- Step 4** Click the Polygon tool () on the map.
The cursor changes to a plus icon.
- Step 5** Click on 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 Cisco CMX zone is now listed as a new item under the floor hierarchy.
- Step 10** (Optional) Click the polygon icon on the map to update the zone details.
-

Create a Zone for a Floor Location

In Location Hierarchy 2.0 (Beta UI), 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.

-
- 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 22: 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 2.0** 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.

Split Licensing

Location Hierarchy in Cisco Spaces supports **Split Licensing**.

The accounts that are registered with Smart Licensing include an option to upgrade or downgrade the license type at building level and above. Use the **License Level Change** option available in the **Location Hierarchy** window.



Note To use **Split Licensing**, accounts must be registered with Smart Licensing.

Update Location Information

Use the **Location Info** tab (**Cisco Spaces dashboard** > **Menu icon (☰)** > **Location Hierarchy 2.0** > **Root Location**) to view and edit the location information.

For the selected location, the **Node Type** and **Network Reference** details are displayed.

Figure 23: Location Info Tab

The screenshot shows the Cisco Spaces interface for a location named 'Floor'. The breadcrumb path is 'Cisco Connect Demo > NGP > Floor'. There is one alert icon. The 'Location Info' tab is selected, showing 'Node Type: NETWORK' and 'Network Reference: Floor'. A note states: 'Note: Some location data fields are inherited from its parent location. Inherited fields are highlighted in orange color. We strongly recommended you to update the location data for each location separately to avoid discrepancy.' Below the note is a table of location data:

BRAND NA	TOTAL AREA NA	OCCUPANCY LIMIT (MAX CAPACITY) NA	
ADDRESS NA	LATITUDE 21.1458004	LONGITUDE 79.08815460000005	TIME ZONE NA
COUNTRY NA	STATE NA	CITY NA	ZIPCODE NA

Click **Edit** to update location information. For more information, see [Edit Location Info, on page 320](#).



Note The location data fields inherited from the parent location are highlighted in orange. We recommend that you update the location data for each location separately to avoid discrepancies.

Edit Location Info

- 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** Update the following location information as required:
- Location Name:** Edit the name of the location.
 - Brand:** Edit the name of the brand.
 - Total Area:** Edit the total area details.
 - Unit:** Select the unit for the total area entered. The options are **Square Feet** and **Square Meter**.
 - Occupancy Limit (Max Capacity):** Edit the occupancy limit/maximum capacity details.
 - Address:** Enter the address details and select from the displayed options. The selected address is plotted on the map displayed on the right side.
 - Latitude:** Displays the latitude of the selected address. You cannot edit this value.
 - Longitude:** Displays the longitude of the selected address. You cannot edit this value.
 - Time Zone:** Enter the search term in the **Search Timezone** field and search or select from the available options.
- 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:

- 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.

To delete a prefix, hover over that prefix under **Added Prefixes**, and click the **Delete** icon.

View the Network Devices

Use the **Network Devices** tab (**Cisco Spaces dashboard** > **Menu icon** (☰) > **Location Hierarchy 2.0** > **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 24: Network Devices tab

The screenshot shows the Cisco Spaces interface for 'Cisco Connect Demo'. The left sidebar displays a location hierarchy: Cisco Connect > Return to Work > NGP > Floor > Texas > Richardson > Chicago > Chicago-1 > first floor > IC-Rio > Meraki Test Area > Nortech > Nortech Campus > Port Orchard, WA. The main content area is titled 'Cisco Connect Demo' and shows statistics: 15 Campus, 35 Building, 2 Group, 77 Floor, 45 Zone, and 1 Alerts. Below these are tabs for Map, Location Info, Network Devices (selected), and Metadata. A summary states 'All the network devices under this node connected and running devices' with counts: 46 Access Points, 0 Cameras, and 0 Webex Devices. The 'Access Points' section includes a search table with the following data:

AP Name	MAC Address	Location
CMX-Security-AP-3-22f0.304d	34:db:fd:42:47:d0	Cisco Connect Demo > ... > Securit...
CMX-Security-AP-4-a83d.a4ac	c8:f9:f9:1a:6b:40	Cisco Connect Demo > ... > Securit...
CMX-Security-AP-2-2281.03fb	c0:25:5c:55:bf:00	Cisco Connect Demo > ... > Securit...

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.
- **Webex Devices:** Displays the connected Cisco Webex devices.

Configure Metadata

Use the **Metadata** tab (Cisco Spaces dashboard > Menu icon (☰) > **Location Hierarchy 2.0** > **Root Location**) to view the metadata information. If metadata is not configured yet, click **Add Metadata** to add metadata. For more information, see [Add Metadata, on page 323](#).

Figure 25: Metadata Tab

The screenshot shows the Cisco Spaces interface with the Location Hierarchy - Beta view. The left pane displays a tree structure of locations under 'Cisco Connect Demo', including 'Cisco Connect', 'Return to Work', 'NGP', 'Floor', 'Texas', 'Richardson', 'Chicago', 'Chicago-1', 'first floor', 'IC-Rio', 'Meraki Test Area', 'Nortech', 'Nortech Campus', and 'Port Orchard, WA'. The main pane shows the 'Cisco Connect Demo' dashboard with statistics: 15 Campus, 35 Building, 2 Group, 77 Floor, 45 Zone, and 1 Alerts. The 'Metadata' tab is selected, displaying a table with one entry: Metadata Key '12' and Value '43'. An 'Add Metadata' button is visible in the top right of the metadata section.

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

- 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**.
- 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**.

The new metadata keys and values are displayed under the **Metadata** tab. Click the **Edit** icon to update the key information.



PART **X**

Integration

- [Cisco Spaces SDK Integration, on page 327](#)
- [Cisco Catalyst Center \(formerly known as Cisco DNA Center\) Integration, on page 333](#)
- [Integrating Cisco Spaces with the ServiceNow Application, on page 335](#)



CHAPTER 25

Cisco Spaces SDK Integration

This chapter provides information on the integration of **Cisco Spaces Software Development Kit (SDK)**.

- [Cisco Spaces SDK Integration, on page 327](#)
- [Integrating Cisco Spaces, on page 327](#)

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** () > **Integrations** > **Cisco Spaces SDK**. This allows the customers to register their native app (iOS and/or Android) with Cisco Spaces.

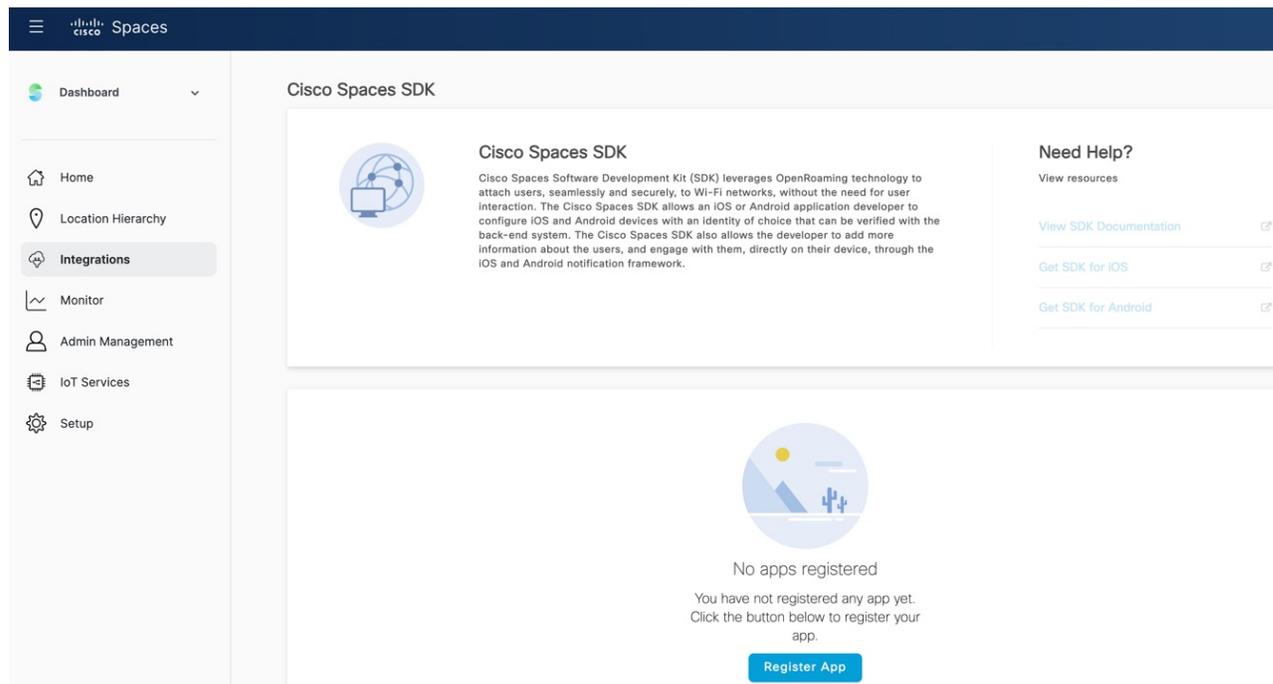
Integrating Cisco Spaces

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](#).

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** > **Cisco Spaces SDK**.
The Cisco Spaces SDK window is displayed.

Figure 26: 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
- Authentication

Figure 27: Register App Sections

Register App

1 Register Apps 2 Configure Profile 3 Push Notification 4 Authentication

Enter a name for your app

Enter App Name
This app name will be used for push notification channel selection while you create engagement rules

Configure app for iOS

Bundle Identifier
A Bundle ID or bundle identifier is a string that identifies your app on iOS. Every iOS application requires a bundle ID to work and it needs to be unique if the developer intends to publish it on the App Store. Usually, the bundle ID is in the form of the domain.your-company.app-name.

Configure app for Android

Enter Package Name
The package name is a unique name to identify an Android app. Generally, the package name of an app is in the format domain.your-company.app-name, but it is completely up to the app's developer to choose the name.

Cancel Previous Next

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

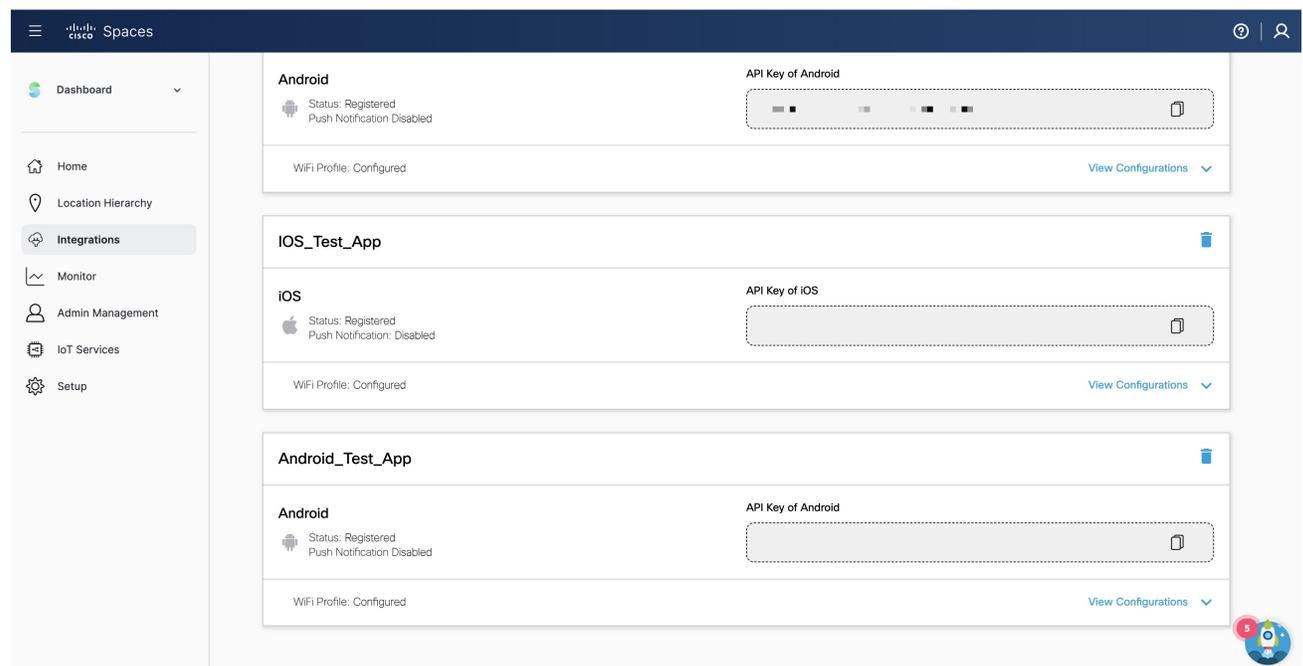
In the **Configure Profile** section, enter the following:

- **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.
- Enter the iOS App ID.
 - Click **Upload** to browse and upload the APNS P12 and Certificate.
 - Enter the APNS certificate password.
- Step 10** To enable push notifications for Android, check the **Enable Push Notification for Android** check box.
- Enter the Android App ID.
 - 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 **Authentication** section.
- In the **Enter Client ID** field, enter the apple account sign-in client ID.
 - 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 **Authentication** section.
- In the **Enter Client ID** field, enter the google account sign-in client ID.
 - 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 28: 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 26

Cisco Catalyst Center (formerly known as Cisco DNA Center) Integration

This chapter provides information on the integration of Cisco Spaces with Catalyst Center.

- [Overview, on page 333](#)
- [Integrate Cisco Spaces with Catalyst Center, on page 333](#)

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, see "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://dnspaces.io:443> for the initial activation. It may also require access to <https://dnspaces.eu:443> depending on your Cisco Spaces account region.

Integrate Cisco Spaces with Catalyst Center

To integrate Cisco Spaces with Catalyst Center, perform the following steps:

Step 1 Log in to [Cisco Spaces](#).

Step 2 In the window, click the **Menu** icon () and choose **Integrations**.

Step 3 In the Catalyst Center **Integration** window, click **Create Token**.

Step 4 In the **Create new token** pop-up window, enter the Catalyst Center instance name and click **Create Token**.

A success message is displayed indicating that the new token is created successfully and the token is displayed in the Catalyst Center **Integration** window.

Note The validity of the new token is two days.

Step 5 Click **Copy Token** and use this tenant token in Catalyst Center.

Step 6 Log into Catalyst Center.

Step 7 Click the **Menu** icon () and choose **System > Settings**.

Step 8 Click **CMX Servers/Cisco Spaces**.

Step 9 In the **CMX Servers/Cisco Spaces** window, under the Cisco Spaces section, click **Activate**.

Step 10 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, see the [Catalyst Center User Guide](#).



CHAPTER 27

Integrating Cisco Spaces with the ServiceNow Application

This chapter describes how to integrate Cisco Spaces with the **ServiceNow** application.

- [Integrating Cisco Spaces with the ServiceNow Application, on page 335](#)

Integrating Cisco Spaces with the ServiceNow Application

This chapter describes how to integrate Cisco Spaces with the **ServiceNow** application.

ServiceNow

Cisco Spaces can be integrated with the **ServiceNow** application so that you can auto transfer the data from Cisco Spaces apps to **ServiceNow** and avail its service offerings.



Note Currently the **ServiceNow** integration support is available only for Proximity Reporting.

Integrating Cisco Spaces with ServiceNow

To integrate Cisco Spaces with the **ServiceNow** application, perform the following steps::



Note Ensure that you have a **ServiceNow** account, and have created the required task IDs.

-
- Step 1** Choose the three-line menu icon displayed at the top-left of the Cisco Spaces dashboard.
 - Step 2** Choose **Integration > ServiceNow** .
 - Step 3** In the **ServiceNow Integration** window that appears, enter the ServiceNow URL, Client ID, and Secret Key for your **ServiceNow** account.
 - Step 4** Click **Register**.

- Step 5** Click **Authenticate** displayed at Step 2.
You are redirected to the **ServiceNow** log in window.
- Step 6** Enter your credentials, and click **Login**.
A message stating that Cisco Spaces would like to establish connection with **ServiceNow** is shown.
- Step 7** Click **Allow** to authenticate the integration.
Once successfully connected, the status **Active** is shown in the **ServiceNow Integration** window. You can disconnect at anytime using the **Disconnect** link.
- Step 8** Now in the Cisco Spaces app for which you want to use the **ServiceNow** application, configure the task ID. For example, in the **Proximity Reporting** app, to auto-transfer reports to the **ServiceNow** application, do the following:
- Open **Proximity Reporting**.
 - Click **Create Report**
 - In the **Look Up Summary** window, search for a user name or mac address for which you want to generate the report. For example, to view all the mac addresses starting with **00:**, enter **00:** in the **Search** field.
The mac addresses of all the devices found will be listed.
 - Check the mac addresses for which the report is to be generated.
 - In the **Time Range** area, specify the start date and end date of the period for which the report is to be generated.
 - Check **Auto-submit report data to ServiceNow task**.
Note The **Auto-submit report data to ServiceNow task** check box will appear only if you have authenticated the ServiceNow integration with Cisco Spaces as explained in Step 1 to Step 7.
 - In the **DiagnosticTask ID** field, enter the task ID created in the **ServiceNow** application.
Note The **DiagnosticTask ID** field will appear only if you have checked **Auto-submit report data to ServiceNow task**.
 - In the **Report Name** field, enter a name for the report.
 - Click **Generate Report**.
- Now when the report is generated, this report will be automatically transferred to the **ServiceNow** application, and the **ServiceNow** application will use this report to perform the task with respect to the task ID configured.
-



PART **XI**

Monitor

- [Monitoring and Support, on page 339](#)



CHAPTER 28

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**.

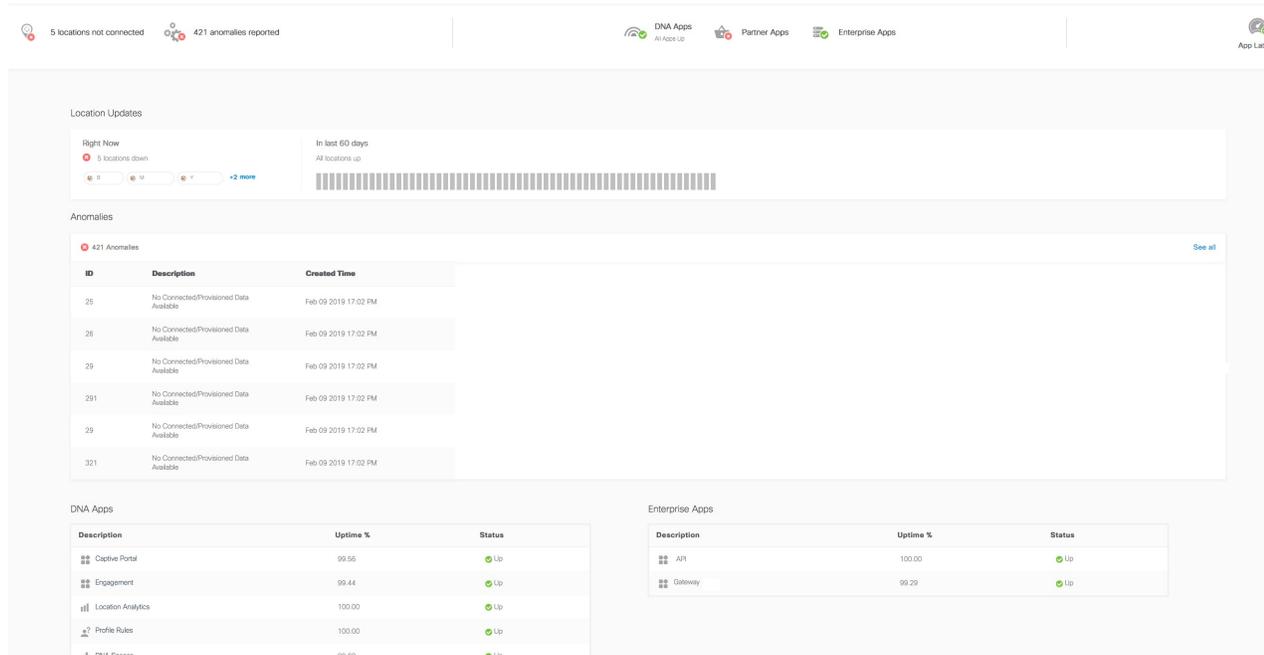
- [Monitoring, on page 339](#)
- [App Latency, on page 342](#)
- [Enterprise Apps, on page 342](#)
- [Partner Apps, on page 342](#)

Monitoring

This section describes Cisco Spaces health details that are displayed in the **Monitor** section.

The **Monitor** section of Cisco Spaces is shown in the following figure:

Figure 29: Monitor



The header of the monitoring section will be having the following details:

- **All Locations connected:** 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.
- **No Anomalies Reported:** Displays the current status of location updates and internet provisioning (this is applicable only if 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.
- **DNA Apps:** Displays the current status of Cisco Spaces apps. This section is marked as up if all the Cisco Spaces apps are currently active.
- **Partner apps:** Displays the current status of partner apps that you have integrated with Cisco Spaces. This section is marked as up if the partner apps that are integrated with Cisco Spaces are functioning as expected. This section will be marked as down, if you have not integrated any partner app with Cisco Spaces or if the partner apps are not functioning as expected.
- **Enterprise Apps:** Displays the current status of enterprise apps that you have integrated with Cisco Spaces. This section is marked as up if the enterprise apps that are integrated with Cisco Spaces are functioning as expected. This section will be marked as down, if you have not integrated any enterprise app with Cisco Spaces or if the enterprise apps are not functioning as expected.
- **App Latency:** This area displays the current latency status for the apps.

Location Updates

The locations for which the location updates are not happening currently are listed in this area. This area also displays a bar that shows location update status for the last 30 days. Each line in the bar represents a day of last 30 days. For days having location update issues the corresponding line in the bar appears in red.

Anomalies

This area displays the location updates issues and internet provisioning issues (this is applicable only if you have configured customer acquisition through captive portals) currently occurring in the locations. The total number of anomalies for your Cisco Spaces account will be listed.

The following details for each anomaly will be displayed:

- **ID**- The ID for anomaly.
- **Description**- Describes whether it is a location update or internet provisioning issue.
- **CreatedTime**- The time at which the anomaly is recorded.

DNA Apps

This area displays the status of the apps provided by Cisco Spaces for last 30 days. The following details of each Cisco Spaces app will be shown.

The status of the following apps will be shown:

- **Captive Portal**—Displays the status of the Captive Portal app.
- **Engagement**—Displays the status of the Engagement app.
- **Location Analytics**—Displays the status of the location updates for all your locations.
- **Location Personas**—Displays the status of the Location Personas app.
- **Cisco Spaces**—Displays the status of the Cisco Spaces domain. The status of the Cisco Spaces domain will be active only if all the associated apps are active.



Note Cisco Spaces domain will be marked as up, only if the domain is working for all the Cisco Spaces customers.

The following details will be shown for each app:

- **Description**— The name of the app.
- **Uptime %**— With in the last 30 days, the percentage of period for which the app was up. For example, if the app was active for all the last 30 days without any health issues, the **Uptime%** value will be 100 %.
- **Status**— Displays the current status of the app.

The following health properties will be considered to decide the status of the apps:

- **Captive Portal app**— Portal Health, Rule Engine Health, Subscriber Health, Email Verifier health, SMS Health, and database health.
- Cisco Spaces: Vault health, Dashboard health DMS health, TMS health.
- **Engagement app**— Dashboard health, Subscriber health, Server health, Location Receiver health, DMS health, Email Verifier health, SMS health, and Database health.
- **Location Analytics**— Dashboard health, Subscriber health, Server Health, Location Receiver health, and Database health.
- **Location Personas**— Dashboard Health, Subscriber Health, Server health, Location Receiver health, and Database health.

App Latency

This area displays the status of latencies associated with the apps for the last 30 days.

The following app latency details will be shown:

- **Description**— The name of the app. For example, Kafka server.
- **Latency**— During the last 30 days, the percentage of period for which the app latency status was up. For example, if the Kafka server has a app latency on 1 day during the last 30 days, the latency value will be 96.6 %.
- **Status**— The current status of the app latency.

Enterprise Apps

This area displays the status of the enterprise apps for the last 30 days.

The following enterprise app details will be shown:

- **Description**-Name of the Enterprise app.
- **Uptime Percentage**-During the last 30 days, the percentage of period for which the Enterprise app was up.
- **Status**- The current status of the enterprise app.

Partner Apps

This area displays the uptime and health status of all the apps you have activated. The overall status of partner apps is shown in the Summary section.

The following partner app details will be shown:

- **PartnerName**-Name of the partner.
- **AppName**-Name of the partner app.

- **Uptime %**-The percentage of period for which the partner app was up.
- **Status**- The current status of the partner app.



PART **XII**

Admin Management

- [Managing Cisco Spaces Users and Accounts, on page 347](#)



CHAPTER 29

Managing Cisco Spaces Users and Accounts

This chapter explains how to invite and manage Cisco Spaces users and accounts.

- [Managing Cisco Spaces Users, on page 347](#)
- [Managing the Cisco Spaces Accounts, on page 351](#)
- [Location-Based RBAC, on page 352](#)

Managing Cisco Spaces Users

Cisco Spaces provides users with different rights and privileges based on the role they perform.

In the Cisco Spaces dashboard, click the **Menu** icon (☰) and choose **Admin Management** to manage admin users and create roles.

The following tabs are available:

- **Admins:** Use the **Admins** tab to view the Cisco Spaces users and invite new administrators.
- **Roles:** Use the **Roles** tab to search for roles, create new roles and manage them.

Inviting 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 **SEE (Base)** license has access only to **DNA 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.

- **Asset Locator:** This role type provides access rights to the **Asset Locator** app.
- **DNA 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.
- **Detect and Locate:** This role type provides access rights to the **Captive Detect and Locate** app.
- **Proximity Reporting:** This role type provides access rights to the **Proximity Reporting** app.
- **MapService:** This role type provides access rights to **Map Service**.
- **Location Analytics:** This role type provides access rights to the **Location Analytics** app.
- **IoT Services:** This role type provides access rights to the **IoT Services** app.
- **Right Now:** This role type provides access rights to the **Right Now** 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.
- **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.
- **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 **DNA Spaces**. For example, you can create a role with read and write access to **MapServices** and Read Only access to **DNA 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 **DNA Spaces** service. For example, you can create a role with read and write access to **Location Analytics** and Read Only access to **DNA Spaces**. The Location Analytics tile is disabled for Cisco Spaces user accounts that do not have access to **Location Analytics**.

To invite a Cisco Spaces user, follow these steps:

-
- Step 1** In the **Cisco Spaces** dashboard, click the Menu icon (☰) and choose a **Admin Management > Admins** tab.
- 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, see [Creating a User Role, on page 350](#). The user roles defined are listed on the **Roles** tab.
 - After you select a role name, the permission type and app details are displayed in the bottom of the **Invite Admin** window.
- 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, check the check box against the required location from the Location Hierarchy. The selected location is displayed in the **Selected Locations** area.
 - c) Click **Done**.
- 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**.
-

Creating a User Role

To create a Cisco Spaces user role, follow these steps:

Step 1 In the **Cisco Spaces** dashboard, click the **Menu** icon (☰) and 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 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), see the role types described in [Inviting a Cisco Spaces User, on page 347](#).
- 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 **DNA Spaces** check box, and from the corresponding drop-down list choose **Read/Write**. Then check the **CaptivePortal** check box, and from the corresponding drop-down list choose **Read only**.

- d) Click **Create**.

The user role is available in the **Role Name** drop-down list of the **Invite Admin** window.

Editing Cisco Spaces User

A Dashboard Admin user with read and write permission 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.

To edit the user privileges of a Cisco Spaces user, follow these steps:

-
- Step 1** In the **Cisco Spaces** dashboard, click the **Menu** icon (☰) and choose **Admin Management**.
The **Admin** window is displayed with the list of e-mail IDs of the Cisco Spaces users.
- Step 2** Click the **Edit** icon at the far right of the e-mail ID of the user whom you want to edit.
The **Invite Admin** window is displayed.
- Step 3** 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, see [Creating a User Role, on page 350](#).
- Step 4** Click **Update**.
-

Deleting 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. A **Dashboard Admin Role** user can delete other users.

To delete an existing Cisco Spaces user, follow these steps:

-
- Step 1** In the **Cisco Spaces** dashboard, click the **Menu** icon (☰) and choose **Admin Management**.
The **Admins** window is displayed with the list of the Cisco Spaces users.
- Step 2** Click the **Delete** icon at the far right of the e-mail ID of the user whom you want to delete.
To delete multiple users, select the check box for the corresponding e-mail IDs, and click **Delete Admins** which displays on the top right of the window.
-

Managing the Cisco Spaces Accounts

This section describes how to manage the Cisco Spaces Accounts.

Changing the Cisco Spaces Password

We recommend that you change the Cisco Spaces password at frequent intervals to ensure more security for your application.

To change the password of your Cisco Spaces account, follow these steps:

-
- Step 1** In the **Cisco Spaces** dashboard, 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:
- In the **Current Password** field, enter the current password for your Cisco Spaces account.
 - In the **New Password** field, enter the new password that you want for your Cisco Spaces account.
 - In the **Confirm Password** field, reenter the new password for confirmation.
 - 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:

- 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 (RBAC) is now enhanced to support specific locations. Use the **Restrict this role to specific locations** option to support specific locations while creating a role (**Admin Management** > **Roles** > **Create Role**) and inviting user flows (**Admin Management** > **Invite Admin**).



PART XIII

Setup

- [Set Up Wireless Network, on page 355](#)
- [Set Up Wired Network, on page 363](#)
- [Set Up Map Service, on page 365](#)
- [Set Up Locations and Maps, on page 367](#)
- [Set Up Meraki Camera, on page 369](#)
- [Set Up Sensors, on page 373](#)
- [Set Up Data Export, on page 375](#)
- [Set Up Cisco Webex, on page 381](#)
- [Set Up pxGrid Cloud, on page 385](#)
- [Set Up Access Point Auto Location, on page 389](#)



CHAPTER 30

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 355](#)
- [Wireless Network Bars, on page 356](#)
- [Set Up Meraki API Key Method, on page 360](#)

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

Step 1 Log in to [Cisco Spaces](#).

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon () and 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 **Cisco AireOS/Catalyst** and **Cisco Meraki**.

- For **Cisco AireOS/Catalyst**, configurations for the following methods are available:
 - **Via Spaces Connector**: To connect Cisco Spaces to Cisco Wireless Controller using Cisco Spaces: Connector.
 - **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.
- For **Cisco Meraki**, configurations for the following methods 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** section 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 360](#).

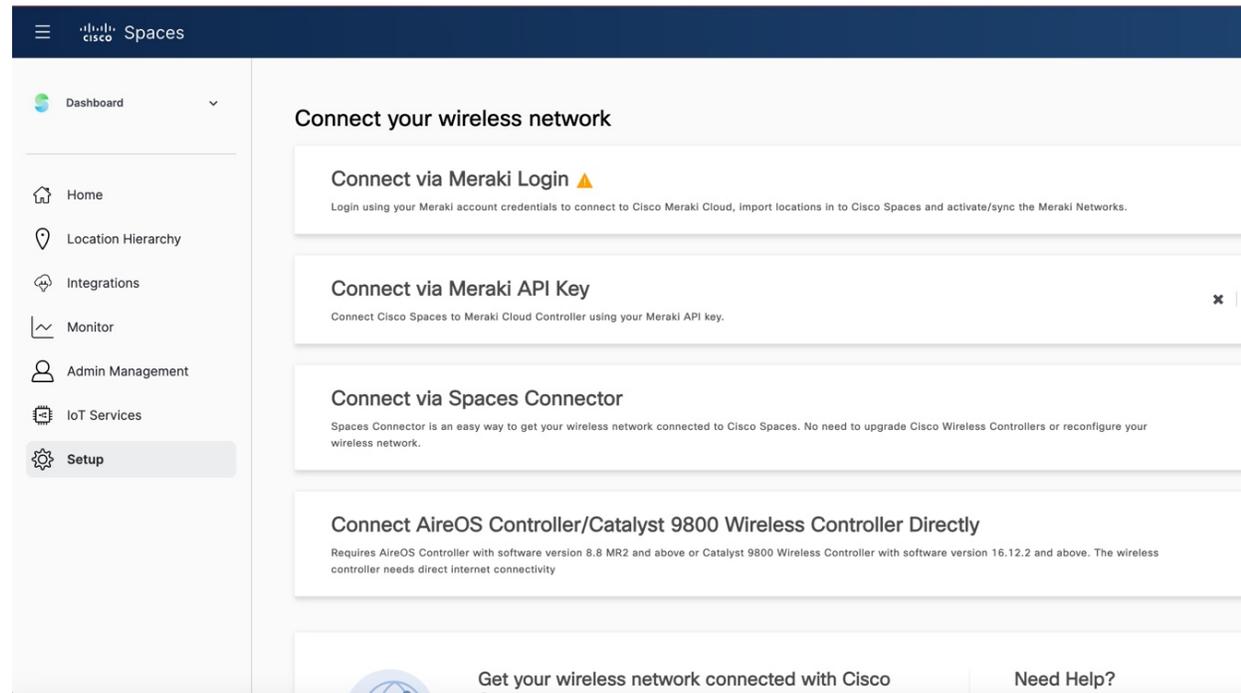
Note For new Cisco Spaces accounts, click **Get Started** option.

- 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 is displayed.
- Step 5** Click **Customize 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.
- 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 using the various methods are displayed.
- Step 8** Follow the on-screen instructions [Wireless Network Bars](#).
-

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 30: Wireless Network



The following tabs are displayed for Cisco Meraki based on your selection:

- **Connect via Meraki Login:** Use this option to connect to Cisco Meraki cloud using the Cisco Meraki account credentials and import locations in to Cisco Spaces and synchronize Cisco Meraki networks. Follow the on-screen instructions to connect Cisco Spaces to Cisco Meraki network.

Perform the following:

1. **Connect:** Connect Cisco Meraki with Cisco Spaces using your Meraki login credentials.
2. **Configure Meraki scanning API:** Cisco Meraki scanning APIs are automatically configured after importing the networks into the location hierarchy.
3. **Import Meraki Networks into Location Hierarchy:** Use the **Import Networks** option to import a Cisco Meraki organization and the related child locations to the location hierarchy.

For more information, see [Adding a Cisco Meraki Organization, on page 280](#).

- **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 that you use the **Connect via API Key** to connect your 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, see [Importing Cisco Meraki Locations Using the API Keys, on page 282](#).



Note The user count that is getting synchronized with Cisco Meraki 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 this option to connect Cisco Spaces to Cisco Wireless Controller using a Cisco Spaces: Connector.



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.
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.

For more information, see [Cisco Spaces: Connector Configuration Guide](#).

- **Connect AireOS Controller/Catalyst 9800 Wireless Controller Directly:** Use this option to connect Cisco Spaces to Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series 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 root certificate from the controller GUI
2. **Configure Token in AireOS Controller:** You can view token and controllers 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:** 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.

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/Catalyst	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.

-
- 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:
- In the **Connect our Meraki** pop-up window, paste the copied API token in the **API KEY** field.

Connect your Meraki



Connect via API key

Enter your Meraki API Key to fetch the network information

API KEY

Add API

Connect

- 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**.

CISCO SPACES Active APs
46 of 100

2 Configure Meraki scanning API

Configure below Post URL with URL validator and secret key and validate manually in Meraki dashboard to establish connection with DNA Spaces.

Post URL

`https://location.dnaspaces.io/notifications/Meraki/accountcisco4/<network_id>/<URLValidator>`

Secret Key

accountcisco4

0 networks configured

3 Import Meraki Networks into Location Hierarchy

Connect Meraki with DNA Spaces using the API key.

0 networks imported [Import Networks](#) [Sync Status](#)

[setup guide](#)
[Frequently Asked Questions](#)

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 web browser's address bar (Meraki URL), copy the `network_id` (after the `/n/`). For example https://xxx.meraki.com/your-net/n/network_id/.
- Step 10** Edit the post URL `<network_id>` to include your network ID.
- Step 11** From the **Location and Scanning** field, copy the `validator id`.
- Step 12** Edit the post URL `<URLValidator>` with the validator.
- Step 13** Click **Validate** to validate the post URL functions.
- Step 14** In the Cisco Spaces dashboard, from the **Import Meraki Networks into Location Hierarchy**, select **Import Networks**.
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.
-



CHAPTER 31

Set Up Wired Network

- [Set Up Wired Network](#), on page 363

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 both 2.x and 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.

For more information about setting up Cisco Spaces: **Connector**, see 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 32

Set Up Map Service

This chapter provides information about the features available in the **Map Service**.

- [Setting up Map Service, on page 365](#)

Setting up Map Service

Map Service in Cisco Spaces includes the following features to keep **Location Hierarchy** in sync with the imported map data:

- Maps exported from Cisco Prime Infrastructure or Catalyst Center and imported into Cisco Spaces using **Map Service** appears automatically under **Location Hierarchy**.
- When you import or synchronize maps from various sources: Catalyst Center, Cisco Prime Infrastructure or Cisco Meraki, support is extended to normalize and unify network hierarchies into a single business-orientated hierarchy.
- If you delete a location from **Location Hierarchy**, it will also be removed from **Map Service**.
- When you delete a zone location from the **Map Service** UI, the zone location is also deleted from **Location Hierarchy**.
- AP import restrictions have been implemented based on the AP license limits for the Cisco Spaces account.

The GPS markers warning message that is displayed in the **Import History** section shows the entire hierarchy in the **Import History** section for the floor with invalid GPS markers.

**Note**

- We recommend that you use Google Chrome Browser while working with maps. Map operations are best supported in Google Chrome. Map actions on other browsers are limited.
- If your locations have maps, create a map-based location hierarchy. However, if you have already created a location hierarchy through **WLCDirect > AP prefix**, **CMXOn-Prem Auto-Sync**, or **CMXManual Upload** and have imported the maps containing the overlapping APs, then the APs will be moved to a map-based hierarchy.
- If a location is deleted from **Map Service**, then only the corresponding access points are removed from **Location Hierarchy**.
- Map Service API performance is enhanced to get the import history and status.

Support for Map Hierarchy Migration from Cisco Prime Infrastructure to Catalyst Center: Cisco Spaces Location Hierarchy supports import of migration data with nested sites from Cisco Prime Infrastructure to Catalyst Center.

Support for Cisco DNA Center Nested Site Hierarchy: You can import or synchronize new sites from Catalyst Center to Cisco Spaces on top of the existing site hierarchy.

Support for Planned Access Point (AP) Import: You can import planned APs into Map Service.

Maps Upload

Click **Maps Upload** to upload maps from Cisco Prime Infrastructure or Catalyst Center. In the **Maps Upload** pop-up window, select the required option and click **Select File** and to upload the maps downloaded from the sources.



Note Click **Upload History** to view the map upload history details.

Cisco Catalyst Wireless 9164I Wi-Fi 6E Series Access Points (AP) Support

The Cisco Catalyst Wireless 9164I Wi-Fi 6E Series AP support is added in the **Map Service**.

You can import the Cisco Catalyst Wireless 9164I Wi-Fi 6E Series APs into Cisco Spaces using the **Map Service**.



CHAPTER 33

Set Up Locations and Maps

- [Setting up Locations and Maps, on page 367](#)

Setting up Locations and Maps

The Locations and Maps feature enables you to normalize and unify network hierarchies from various sources: Catalyst Center, Cisco Prime Infrastructure, and Cisco Meraki into a single business-orientated location hierarchy.

You can create a business-centric hierarchy in Cisco Spaces by uploading a Microsoft Excel (.xlsx) file containing location details. Moreover, the import from a Microsoft Excel (.xlsx) file allows you to add or update location metadata information for multiple locations at once.

The **Rich Maps** transforms flat floor plans into dynamic, interactive, and highly intuitive 3D rich maps. The **Rich Maps** feature in Cisco Spaces helps to logically deconstruct the Computer-aided design (CAD) files and extract data such as meeting room details, workplace desk information, amenities, and so on. You can attach them to the location hierarchy to discover additional use cases.



Note The Locations and Maps feature is enabled for all Cisco Spaces accounts.



CHAPTER 34

Set Up Meraki Camera

This chapter provides information about the configurations required in Cisco Spaces for Meraki Camera.

- [Setting up Cisco Spaces to Work with Cisco Meraki Camera, on page 369](#)

Setting up Cisco Spaces to Work with Cisco Meraki Camera

Cisco Spaces enables you to determine the number of visitors visiting your locations using a Cisco Meraki Camera. To avail this feature you must have a Meraki login and must have installed Cisco Meraki Cameras in your locations. Meraki Camera can be connected to the existing Cisco AireOS or Cisco Catalyst 9800 wireless controller-based network as long as the camera can reach the Meraki cloud server. Also, you must have valid Meraki MV Sense licenses.

You can capture the following 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 **Right Now** apps available in the Cisco Spaces dashboard.

Configuring a Meraki Camera

-
- 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 Meraki Organization (in which the Meraki Camera Networks are configured) that you want to import.

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 MQTT server details.
Host and port are displayed in Step 3 in the **Connect your Meraki Camera** window.
- 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.

Editing the Trip Wire for a Camera

To edit the XY coordinates of the trip wire for a camera, perform the following steps:

Step 1 Log in to [Cisco Spaces](#).

Step 2 In the Cisco Spaces dashboard, click the **Menu** icon () and choose **Settings > Camera**.
The **Connect your Meraki Camera** window is displayed.

Step 3 Click **View Cameras** displayed in Step 4 in the **Connect your Meraki Camera** window.
The Cameras imported into Cisco Spaces are displayed. You can filter to view the cameras for a particular location.

Step 4 Click the **Edit** icon that is displayed far-right of the camera for which you want to edit the tripwire.

Step 5 In the **Edit Trip Wire** window that is displayed, edit the tripwire details and click **Done**.



CHAPTER 35

Set Up Sensors

- [Sensors, on page 373](#)
- [Claim Sensors, on page 373](#)

Sensors

Use the **Setup > Sensors** option in the Cisco Spaces dashboard to claim the sensors into your wireless networks.

Claim Sensors

Use the MAC addresses of the sensors to claim them into the wireless network.

-
- Step 1** Log in to [Cisco Spaces](#).
- Step 2** In the Cisco Spaces dashboard, click the **Menu** icon () and choose **Setup > Sensors**.
- Step 3** Click **Claim Sensors**.
The **Claim Sensor(s)** slide-in pane is displayed.
- Step 4** In the **Enter a new tag** field, enter the MAC address of the sensor to claim.
- Step 5** Click **Enter**. Use comma (,) as a separator to add multiple MAC addresses and claim multiple sensors at the same time.
- Step 6** Click **Claim**.
The sensor details such as location, status, SSIDs and MAC address are displayed in the **Sensor Management** window.
To unclaim sensors, click the MAC address and click **Unclaim**.
-



CHAPTER 36

Set Up Data Export

- [Data Export, on page 375](#)
- [Create Export Data, on page 375](#)

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

- For the Cisco Spaces dashboard SEE license customer accounts, data export types such as Captive portal, and Engagement and Location Personas are not available for export.
 - For ACT license customer accounts, all data types are available for export.
 - Customer acquisition data export does not support data for portals with the authentication types: **No Authentication** and **Access Code**.
-

Create Export Data

- 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 31: Create New Data Export

Create New Data Export ×

1 Data Type 2 Locations 3 Schedule 4 File Format 5 Connection 6 Summary

Select data export type
Select the data type that you want to export

Data Type
- Select -

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
Engagement - Rule Activity	Log Timestamp, Timezone, Local Date, Local Hour, Local Minute, Device ID, User ID, MAC Address, Profile Tag Name, Rule Name, Location Information
Location Personas - 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

- 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.
- 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](#).

Step 4 Click **Next** to navigate to **Locations**.

Step 5 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 6 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 7 Click **Next** to navigate to **File Format**.

Step 8 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 9 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 10 In the **File Name Format** field, enter the filename prefix and select the format for date and time.

Step 11 From the **Select Date & Time Format** drop-down list, select the format.

Step 12 Click **Next** to navigate to **Connection**.

Step 13 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 14 Click **Connect**.

If the connection is successful, the following message is displayed: `Connection Established`.

Step 15 Click **Next** to navigate to **Summary**.

Step 16 In the **Add a name to your data export** field, enter the name for the data export.

Step 17 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 37

Set Up Cisco Webex

This chapter provides information on how to integrate Cisco Webex with Cisco Spaces.

- [Integrate Cisco Webex, on page 381](#)
- [Set Up Cisco Webex, on page 382](#)
- [Generate an Activation Code, on page 382](#)

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.

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.

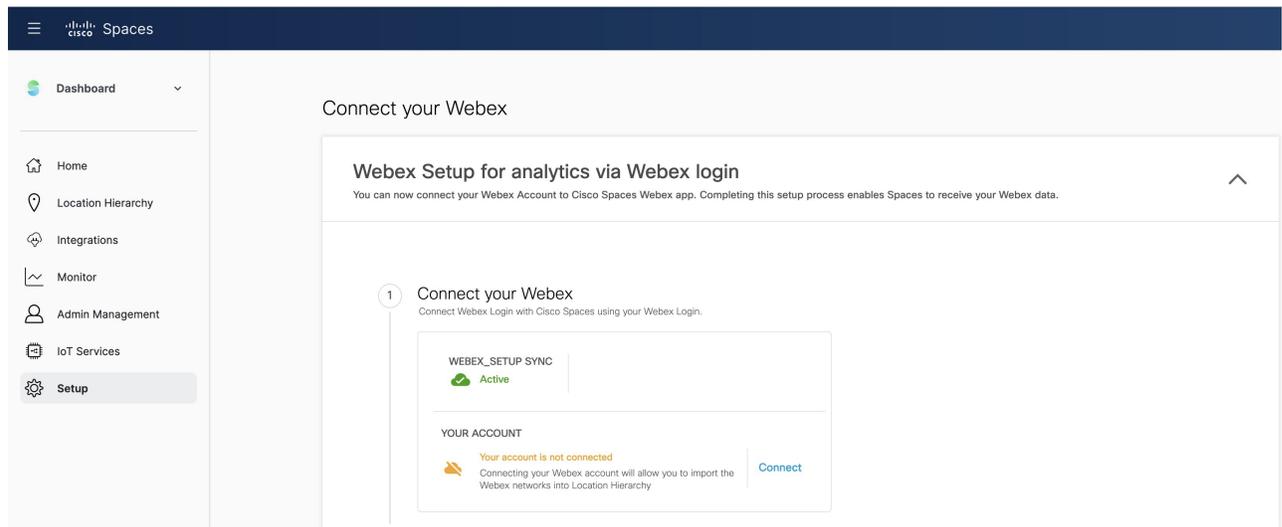
Step 4 In the **Enter or copy-paste your Webex Token** field, enter the Cisco Webex token.

You can get the token from the **Webex Control Hub**. For more information about generating an activation code, see [Generate an Activation Code, on page 382](#).

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 32: Cisco Webex Synchronization Status

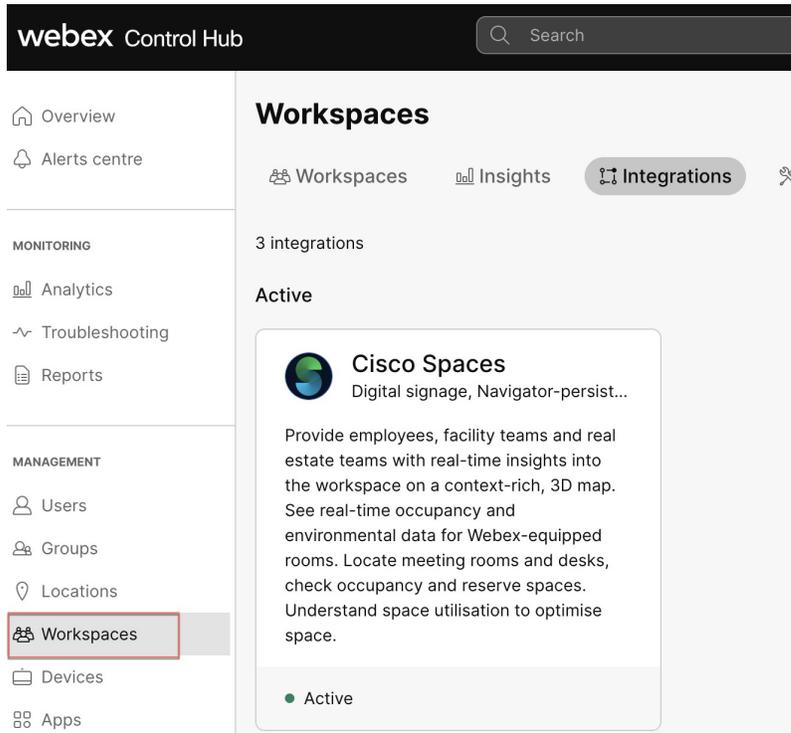


Generate an Activation Code

Use the [Cisco Webex Control Hub](#) to generate codes.

- 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 33: 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 38

Set Up pxGrid Cloud

- [Activate pxGrid Cloud, on page 385](#)
- [Generate Cisco pxGrid Token \(OTP\), on page 386](#)
- [Activate App for Products, on page 386](#)

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.

-
- 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 386](#).
- 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 386](#). Follow the on-screen instructions to activate the product.
-

Generate Cisco pxGrid Token (OTP)

-
- 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](#).

-
- 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 39

Set Up Access Point Auto Location

- [Access Point Auto Location, on page 389](#)
- [Prerequisites for AP Auto Location, on page 391](#)
- [Generate AnyLocate Measurement Data, on page 391](#)
- [Place Devices, on page 393](#)
- [Edit Device Placement, on page 396](#)
- [View AnyLocate Measurement Data Status, on page 397](#)
- [View APs, on page 398](#)

Access Point Auto Location

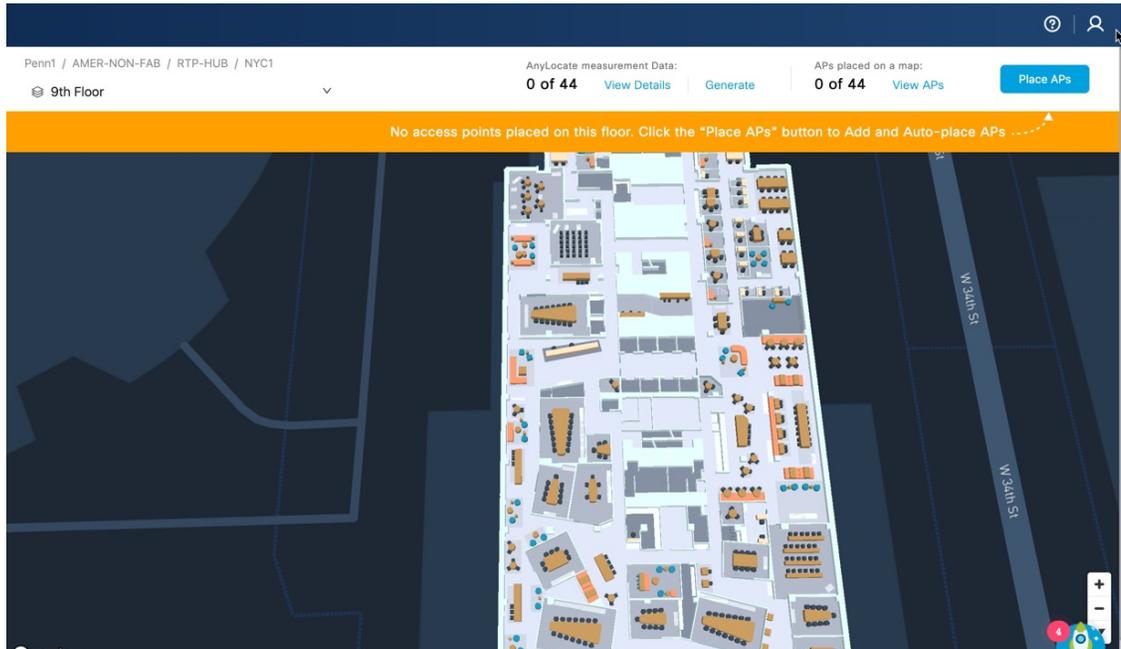
The Access Point Auto Location solution helps to effectively self-locate APs in a global coordinate by combining various ranging technologies and algorithms.

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 34: 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 19: Supported Platforms and Versions

Product	Platform	Releases
Cisco Catalyst 9100 Family of Access Points	<ul style="list-style-type: none"> • 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

Product	Platform	Releases
Cisco Catalyst 9800 Series Wireless Controllers	Cisco Catalyst 9800 Series Wireless Controllers	Cisco IOS XE 17.12.x
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 AnyLocate Measurement 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.

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 35: Generate AnyLocate Measurement Data

NOTE: We do not support generating ranging data for default site tags. Please configure your site tags in your controller. [Learn More](#)

Select the site tags where you want to generate AnyLocate measurement data

Search

Site Tag	Ranging Capable APs	Controller	AP Model
<input type="checkbox"/> default-site-tag	0/3		
<input checked="" type="checkbox"/> Cafe-17	10/10		C9131 CW91 CW91
<input type="checkbox"/> SJC17-Floor3	20/20		C9131 CW91
<input type="checkbox"/> SJC17-Floor2	16/16		C9131 C9131
<input type="checkbox"/> SJC17-No-FTM	1/1		C9131
<input type="checkbox"/> default-site-tag	1/1		C9131

Selected Site Tags: 1 Total APs: 10

Cafe-17

Cancel Next

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.

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.

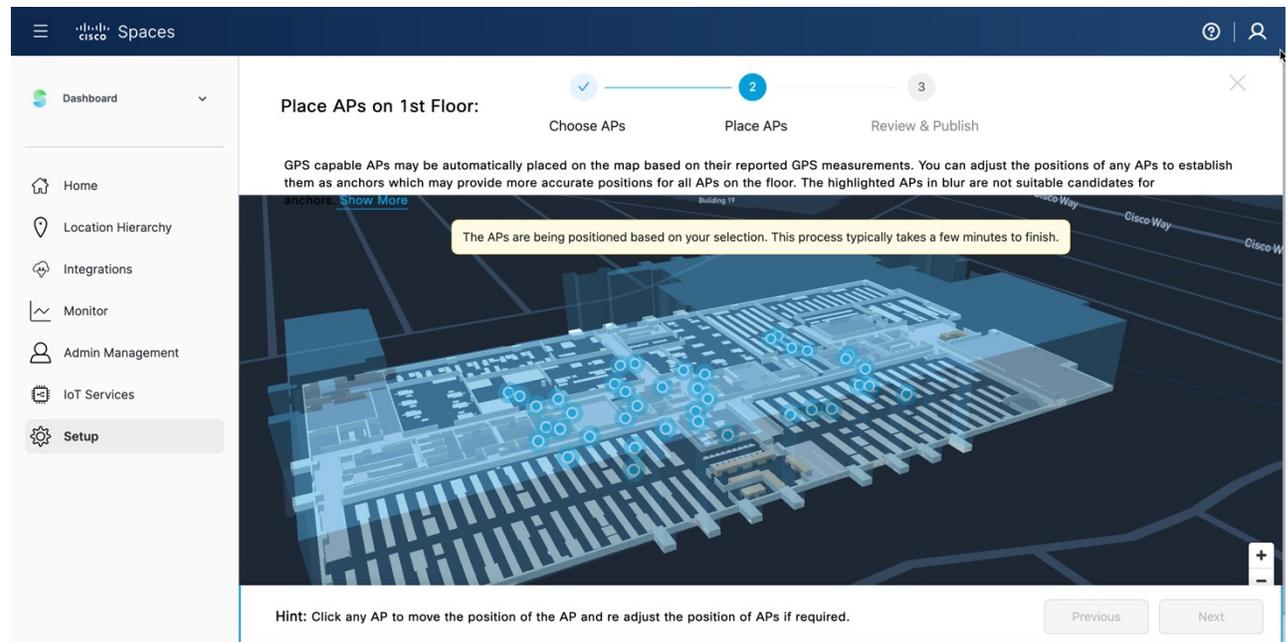
Step 6

Click **Next**.

Step 7

In the **Place APs** section, you can view the APs getting placed automatically.

Figure 36: 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.

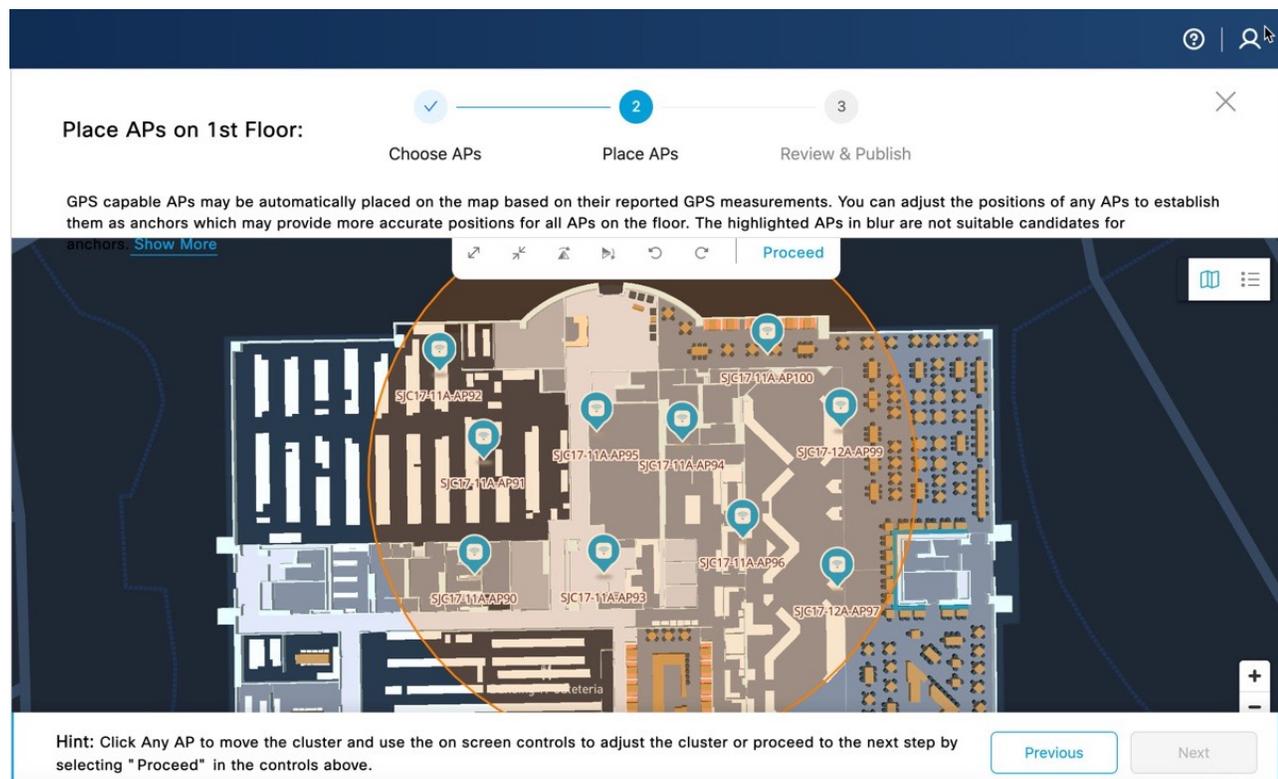
Click **Skip** to skip this step.

- 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 37: 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

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.

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 38: AnyLocate Measurement Data Status

AnyLocate measurement Data Status

AnyLocate measurement data is required to process AP location. Generating ranging data will disrupt wireless connections for the APs participating in the ranging processes [Learn More](#)

Ranging data generated for: **53 of 107 APs**, **5 of 8 site tags**

Site tags not available: **0 of 107 APs**

APs that do not support ranging: **25 of 107 APs**

Scheduled: **0 Site Tags** [Manage / View History](#) Last updated: 13th Dec, 2023, 01:22:10 pm

Search

Site Tag	Ranging Capable APs	Controller	AP Model(s)	Status	Last Generated
default-site-tag	0/3			Not Available	--
Cafe-17	10/10		C9136I-B, CW9164I-B, CW9166I-B	Available, Re-Generate	28th Nov, 2023, 10:59:32 am
SJC17-Floor3	20/20		C9136I-B, CW9166I-B	Available, Re-Generate	28th Nov, 2023, 10:59:32 am
SJC17-Floor2	16/16		C9130AXI-B, C9136I-B	Available, Re-Generate	28th Nov, 2023, 10:59:32 am
SJC17-No-FTM	1/1		C9130AXE-B	Not Available, Generate	--
default-site-tag	1/1		C9136I-B	Not Available	--

Step 6 Click the **Close** (✕) icon to close the window.

View APs

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 39: View AP Details

The screenshot shows the Cisco Spaces interface for 'APLocationLab'. On the left is a map of the North Pacific Ocean with 'Honolulu' marked. On the right is a 'Summary' panel with a close button (X). The summary shows 57 total APs, 7 anchor APs, and 56 placed automatically. Below the summary is a search bar and a table of AP details.

Name	AP Model	Mac Address	Controller	Site Tag	Switch Name
APLocationLab-001	AP-3502E-K9	9876 5432 1098	10.10.10.1	AP-001	SW-001
APLocationLab-002	AP-3502E-K9	8765 4321 0987	10.10.10.2	AP-002	SW-002
APLocationLab-003	AP-3502E-K9	7654 3210 9876	10.10.10.3	AP-003	SW-003
APLocationLab-004	AP-3502E-K9	6543 2109 8765	10.10.10.4	AP-004	SW-004
APLocationLab-005	AP-3502E-K9	5432 1098 7654	10.10.10.5	AP-005	SW-005
APLocationLab-006	AP-3502E-K9	4321 0987 6543	10.10.10.6	AP-006	SW-006
APLocationLab-007	AP-3502E-K9	3210 9876 5432	10.10.10.7	AP-007	SW-007
APLocationLab-008	AP-3502E-K9	2109 8765 4321	10.10.10.8	AP-008	SW-008
APLocationLab-009	AP-3502E-K9	1098 7654 3210	10.10.10.9	AP-009	SW-009
APLocationLab-010	AP-3502E-K9	0987 6543 2109	10.10.10.10	AP-010	SW-010

Step 6 Click the **Close** (X) icon to close the slide-in window.

