

# Cisco Spaces Federal Support Configuration Guide

**First Published:** 2025-04-03

**Last Modified:** 2026-06-23

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

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

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

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

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

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

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

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

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

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

© 2026 Cisco Systems, Inc. All rights reserved.



# Preface

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

This document contains the following sections:


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


## Audience

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

Other target audience includes portal designers and access code managers.

## Document Conventions

This document uses the following conventions:

***Table 1: Document Conventions***

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

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

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

# List of Acronyms and Abbreviations

***Table 2: List of Acronyms and Abbreviations***

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

# Communications, services, and additional information

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

## Cisco Bug Search Tool

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

## Documentation feedback

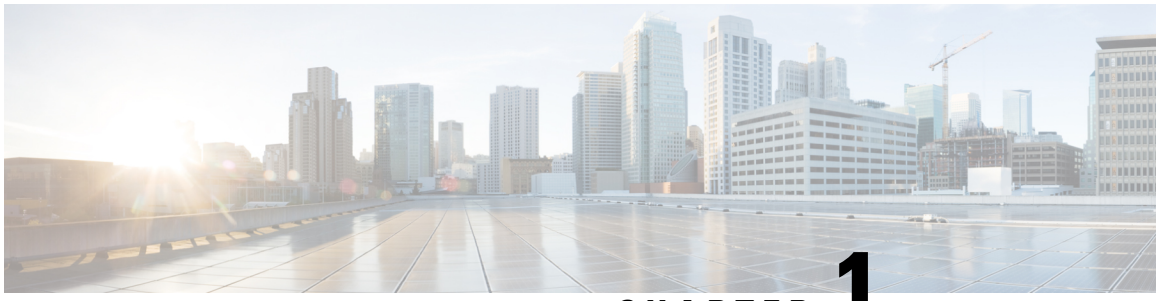
To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



PART I

# Prerequisites


- Cisco Spaces Prerequisites, on page 1



CHAPTER 1

# Cisco Spaces Prerequisites

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

This chapter contains the following sections:


- System Requirements, on page 1
- Bandwidth Requirements to Deploy Cisco Spaces, on page 2
- Accessible Ports and IP Addresses, on page 2
- Cisco Spaces IP Addresses, on page 3


## System Requirements

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

***Table 3: System Requirements***

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

| Item | System Requirements |
|---|---|
| Cisco AireOS Wireless Controller | 8.3 or a later version<br>**Note**<br>8.3 is End-of-Life (EOL). We recommend that you migrate to one of the recommended releases as per the *Guidelines for Cisco Wireless Software Release Product Bulletin* at:<br>https://www.cisco.com/c/en/us/products/collateral/wireless/wireless-controllers/bulletin-c25-738147.html |
| Cisco Connected Mobile Experiences (CMX) - this is required only for Cisco AireOS/Catalyst Controllers used with Cisco CMX. | 10.6 or a later version |
| Cisco Spaces: Connector (Only applicable for Cisco AireOS/Catalyst Controllers) | • vCPU: 2/4/8<br>• RAM: 4/8/16 GB<br>• 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<br>60000 clients | Cisco Wireless Controller Direct Connect | 250 Kbps |
| 5000 APs<br>60000 clients | Cisco Spaces: Connector | 4 Mbps |

# Accessible Ports and IP Addresses

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

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

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

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

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

# Cisco Spaces IP Addresses

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

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

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

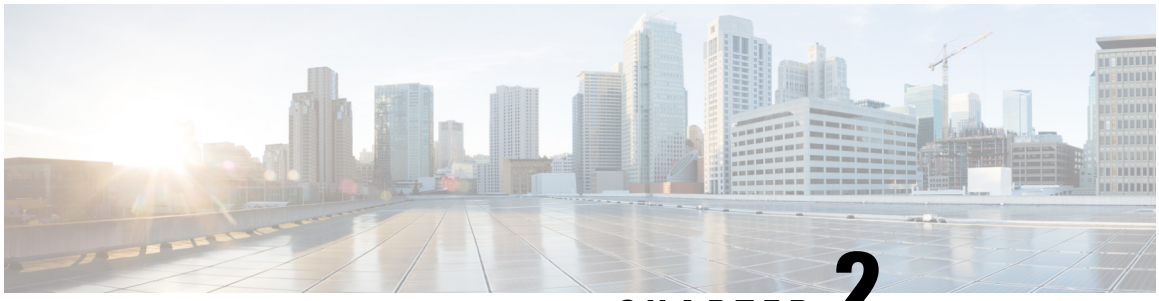
Certain domain names must also be allowed in a customer's infrastructure for the Cisco CMX instances that are deployed in a customer's network to be able to communicate with the Cisco Spaces analytical and notification servers. To know the domain names that should be allowed in the Cisco Spaces dashboard,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



PART II

# FedRAMP Secure Configuration


- FedRAMP Secure Configuration, on page 7



CHAPTER 2

# FedRAMP Secure Configuration

This chapter provides an overview of Cisco Spaces FedRAMP requirements for secure configuration.


- Manage Dashboard Administrators and Permissions, on page 7
- Dashboard Admin Role, on page 7
- App Role, on page 8
- Custom Location-Restricted Role, on page 9
- Admin Management Workflows, on page 9
- User Management Workflows, on page 19
- Governance and Best Practices, on page 25


# Manage Dashboard Administrators and Permissions

This chapter explains the different permission levels within the dashboard and how to manage administrative users. Administrative users can log in to the dashboard to view and/or administer apps, locations, devices, and role-based access within the account.

### Admin Management

When you onboard to Cisco Spaces as a new user, the Cisco Spaces Support team will assist you in setting up your account details and fulfilling the initial-onboarding requirements. The Cisco Spaces Support team is responsible for creating the new account, generating the tenant ID, assigning the account number, and provisioning the appropriate license type.

When a new account is created, a **Default Admin Role** (**Dashboard Admin Role**) is automatically provisioned.

This role is assigned to the user email configured during account creation. The **Default Admin Role** is the top-level admin role for user and role management.

# Dashboard Admin Role

When a new account is created, the **Default Admin Role** (**Dashboard Admin Role**) is created and assigned to the user email used during account creation. This role acts as the top-level admin role for user/role management.

### Default Admin Role: Capabilities

A user with this role can:

- Invite new users with Default Admin Role and assign either Full Location or Restricted Location permissions.
- Invite new users and assign them to custom roles with location-based restrictions.
- Manage custom user roles, including changing user roles.
- Remove other Default Admin or custom-role users from account access.
- Create custom roles that either:
  - Mirror Default Admin Role access, or
  - Grant app-specific access and/or location-based restrictions.
- Manage role assignments, including creating role mappings, changing app/location access, and removing custom roles.
- Access all locations, devices, and Cisco Spaces apps entitled to the account license.



**Note** Users invited through the admin management section are considered full admins in the Cisco Spaces account for managing users and roles, regardless of whether their access is limited to specific applications or locations. Additionally, admins with restricted access retain the ability to invite unrestricted full admins.

### Default Admin Role: Limitations

A user with this role **cannot**:

- Delete or edit the Default Admin Role definition.
- Remove themselves from the account.
- Change the account license or subscription.

# App Role

App roles define what a user can do within the Cisco Spaces application, ranging from view-only access to full configuration and data management. A **Read-Only** app role allows users to access the app UI and view configurations, records, and details without making changes. A **Read/Write** app role enables users to access the app UI and add, edit, or delete app-related configurations and data, and also allows them to invite additional users (as Read-Only or Read/Write) using **User Management** option—restricted to the inviter's permitted location boundary.

### Read-Only app role

If the role grants **Read-Only** access to an app, you can:

- Access the app UI.

- View configurations, records, and details.

**Note** You cannot add, edit, or delete configurations/data.

#### Read/Write app role

If the role grants **Read/Write** access to an app, you can:

- Access the app UI.
- Add, edit, and delete data/configurations associated with that app.
- Invite other users using the **User Management** option as **Read-Only** or **Read-Write**, limited to the inviting user's permitted location boundary.

# Custom Location-Restricted Role

Users with location restrictions can:

- View, configure, and manage only the assigned locations.
- Perform data and operational actions limited to those locations.

Users with the custom location-restricted role cannot access locations outside their assigned scope.

# Admin Management Workflows

In Cisco Spaces, Admin Management Workflows are processes and procedures for managing administrative users and their roles. The range of these workflow tasks includes the addition of new admin users, the management of custom roles, the modification of user roles, the deletion of roles, and the revocation of user access.

These workflows aim to increase the security, organization, and efficiency of administration by defining the required steps to manage users and roles in your Cisco Spaces account.

This approach helps in ensuring that the access control of your Cisco Spaces account is appropriate, and the role permissions are followed, along with the management of location restrictions if necessary. By following these workflows, the administrators are able to control who has administrative access, manage roles according to the needs of the organization, and ensure the integrity and security of the administrative process.

## Invite a New Admin User

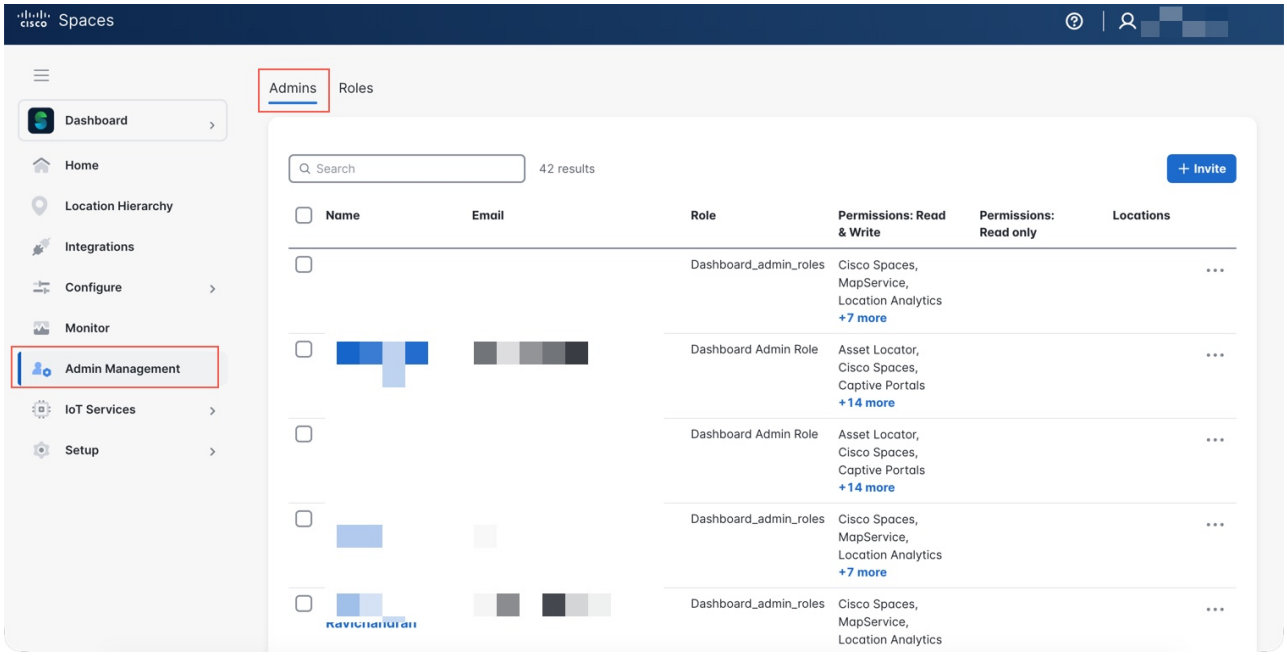
To enable administrators to securely add new users with appropriate permissions and access scope to the system, ensuring controlled and role-based access management.

This task guides administrators through the process of inviting a new admin user by specifying their email, assigning a role, and optionally setting location restrictions.

Follow these steps to invite a new admin user to Cisco Spaces:

### Procedure

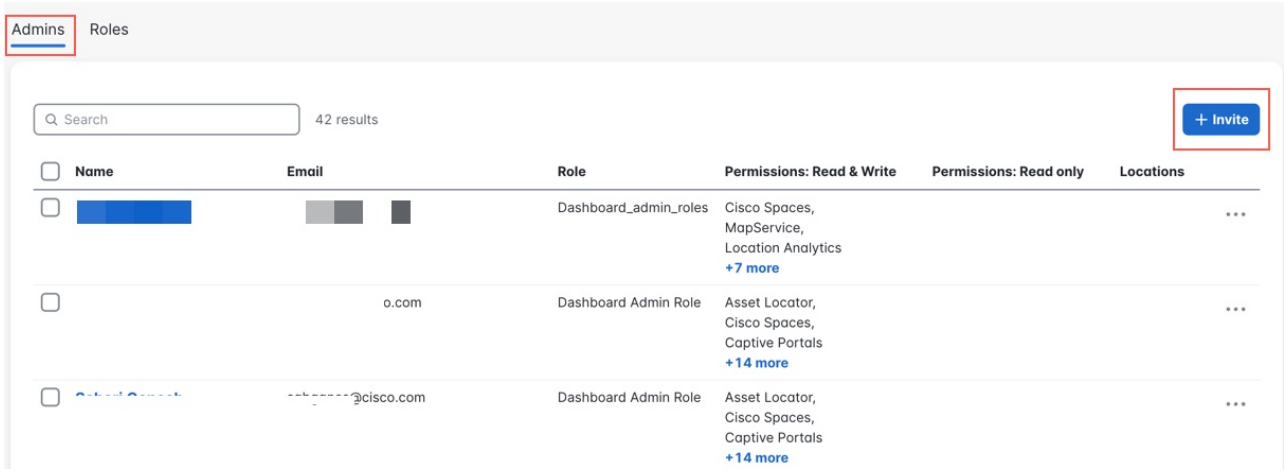
**Step 1** From the left pane, click **Admin Management**.




The **Admin Management** window is displayed.

**Step 2** Click the **Admins** tab.

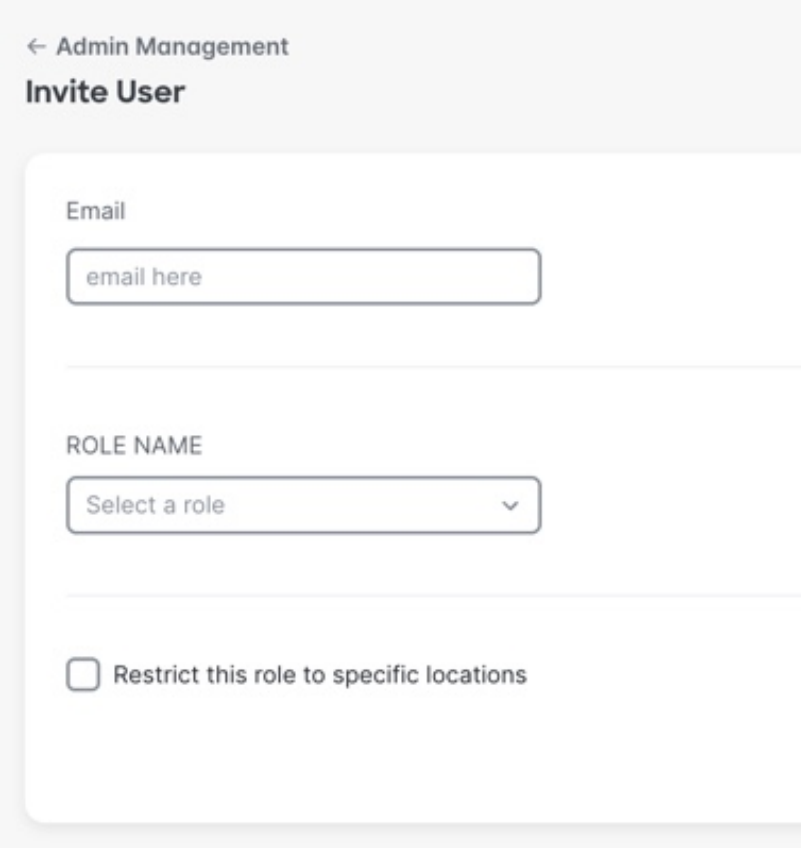
**Step 3** To invite a new admin user, click **Invite**.




The **Invite User** window is displayed.

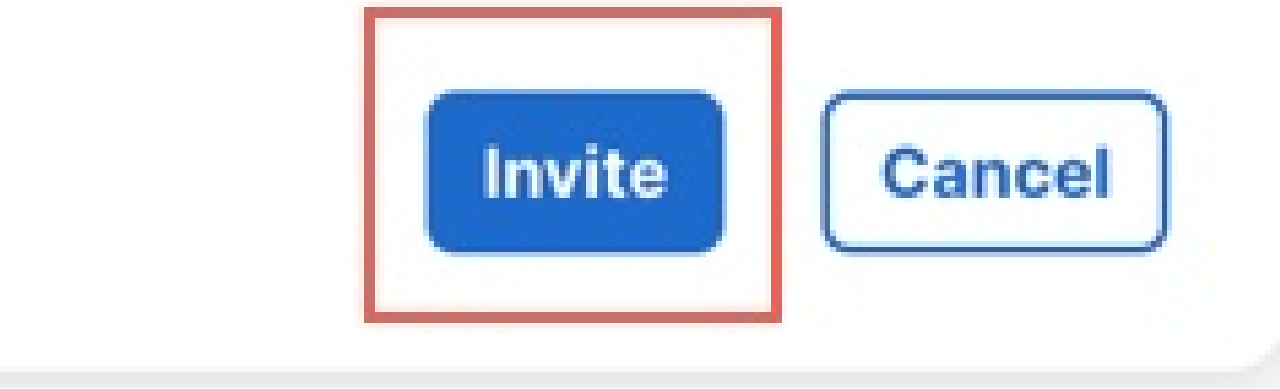
**Step 4** In the **Email** field, enter the new admin user's email address.

**Step 5** From the **Role Name** drop-down list, choose the role as **Default Admin Role** or custom role.




**Step 6** (Optional) Check the check box to enable location restriction and select the applicable locations.

**Step 7** Click **Invite** to send the invitation.




The invitation email is sent to the new user.

# Create a Custom Role

To allow administrators to define tailored roles that fit organizational needs, providing granular control over admin permissions and enhancing security through role customization.

This task explains how to create a custom admin role by naming it and selecting specific app permissions such as Read-Only or Read/Write.

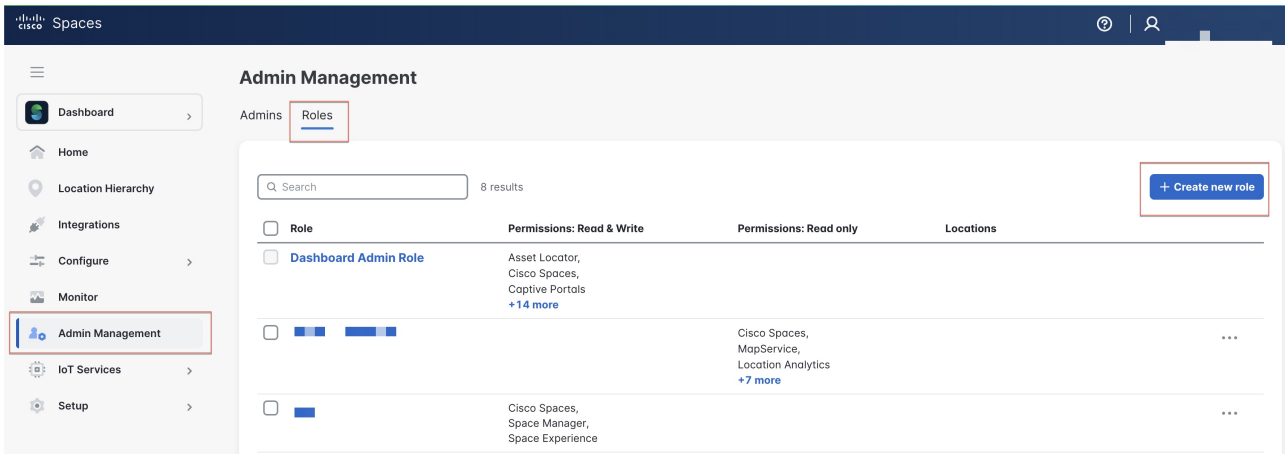
Follow these steps to create a custom admin role:

### Procedure

**Step 1** From the left pane, click **Admin Management**.

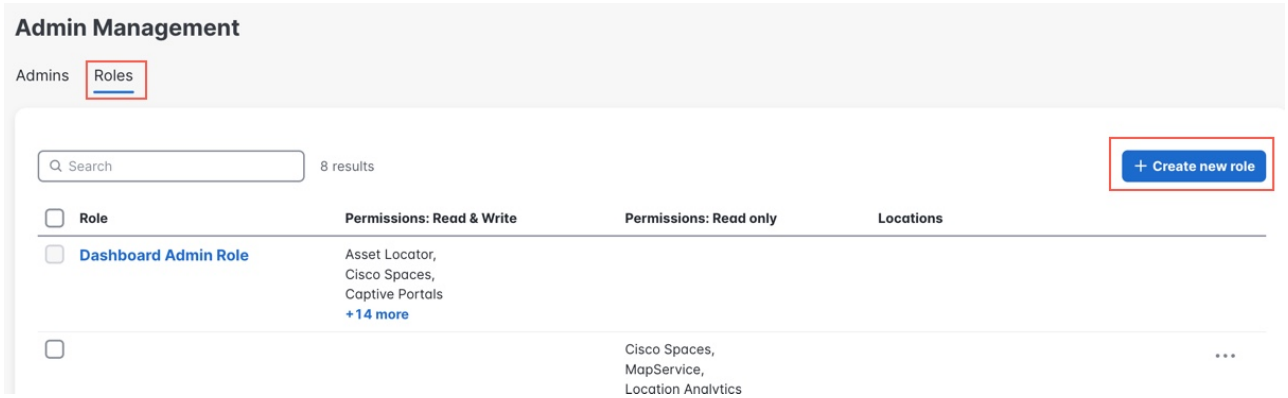
The **Admin Management** window is displayed.

**Step 2** Click the **Roles** tab.

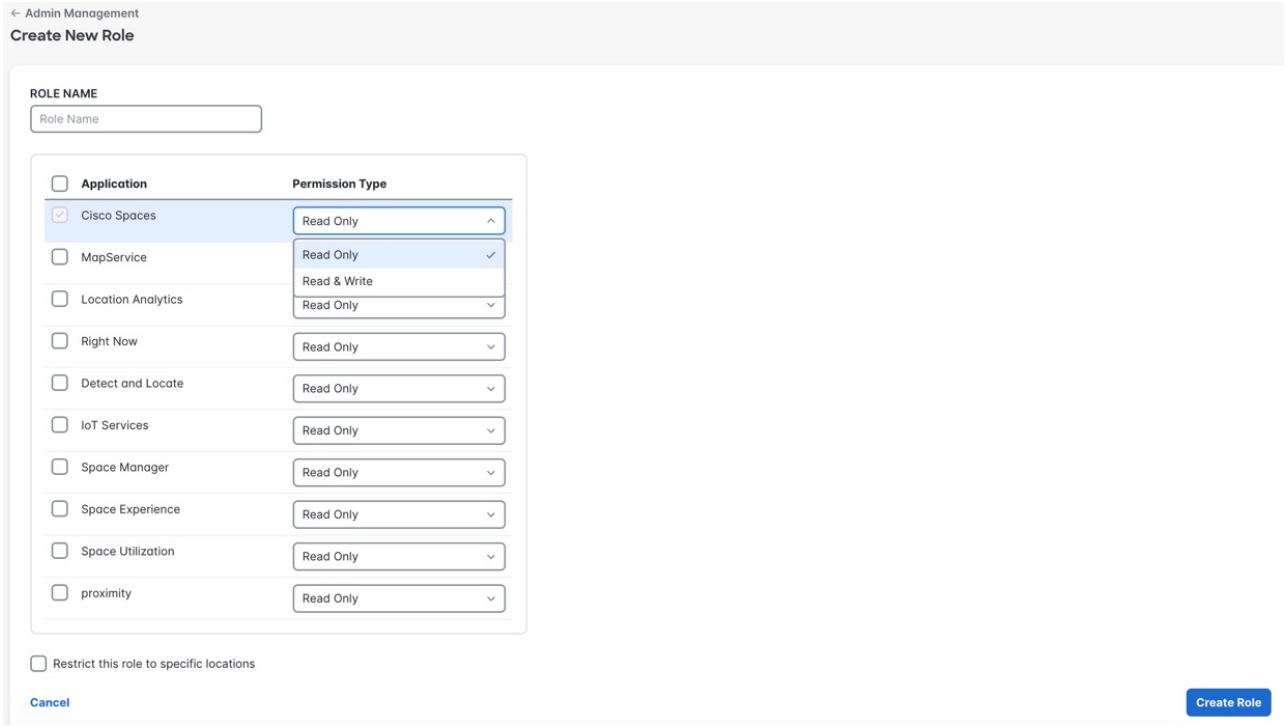



The **Roles** tab is displayed.

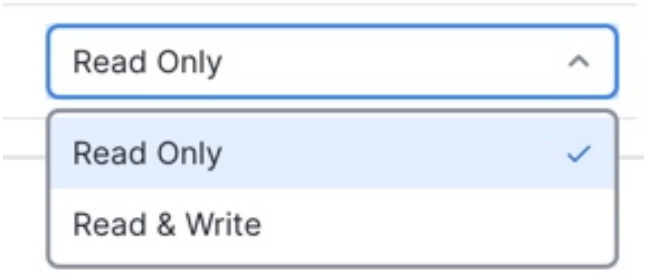
**Step 3** To create a new custom admin role, click **Create new role**.




**Step 4** In the **Role Name** field, enter a name for the new role.




**Step 5** From the **Permission Type** drop-down list, choose the permission type as either **Read Only** or **Read & Write**




access.

**Step 6** (Optional) Check the check box to enable location restriction and select the applicable locations.

**Step 7** Click **Create Role** to create the role.
The new custom role is created successfully.

# Edit User Role Assignment

To maintain accurate and up-to-date role assignments, ensuring that admin users have the correct permissions and access aligned with their responsibilities.

This task details the steps to modify an existing admin user's role and/or location scope.

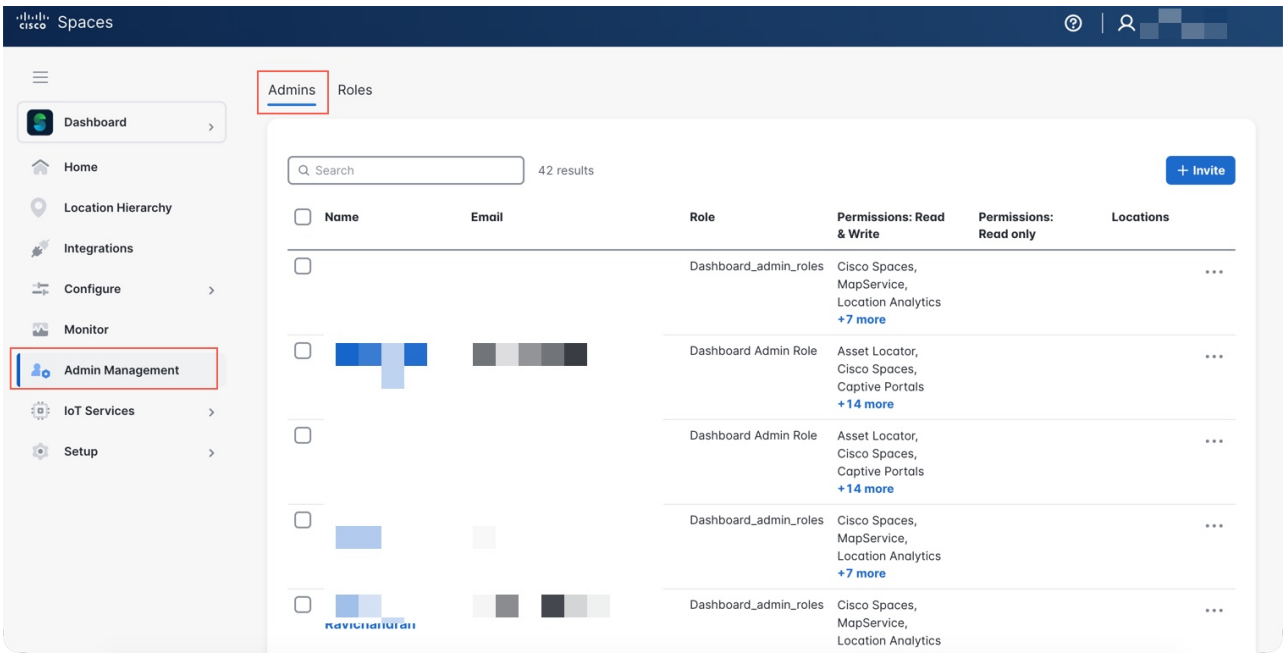
Follow these steps to edit the role assignment of an existing admin user:

### Procedure

**Step 1** From the left pane, click **Admin Management**.

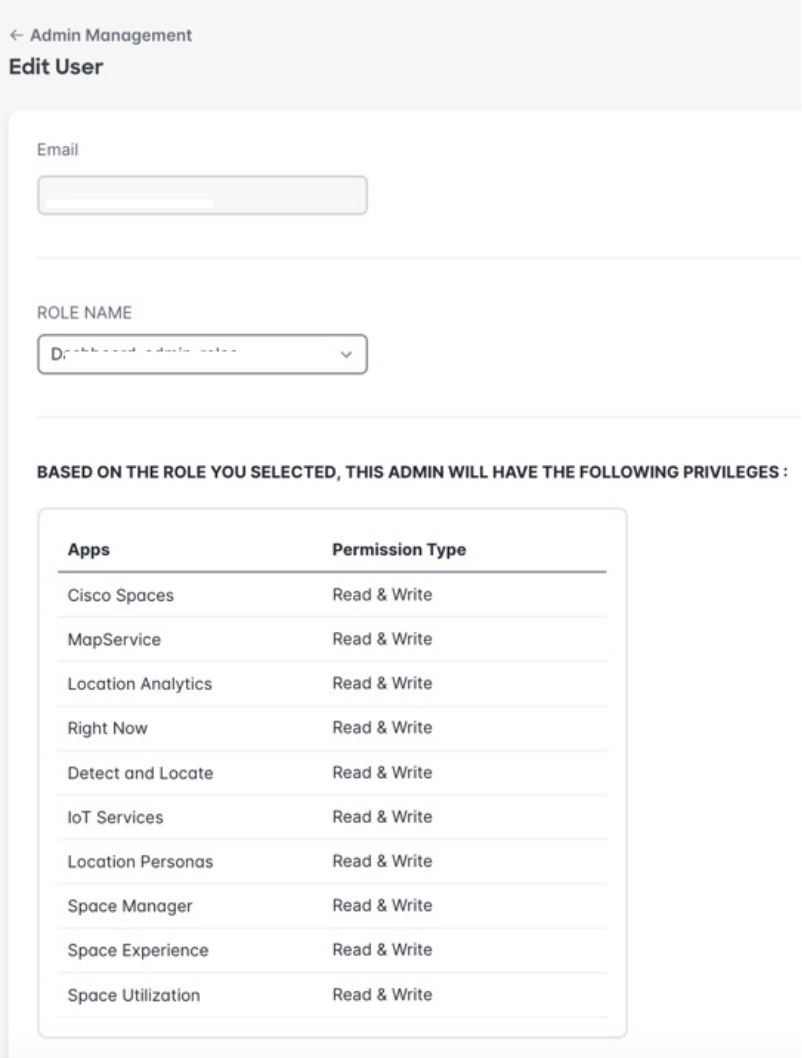
The **Admin Management** window is displayed.

**Step 2** Click the **Admins** tab.




**Step 3** Select the user whose role you want to edit and click **Edit**.

**Step 4** Update the user's role and/or location scope as needed.




**Step 5** Click **Update** to apply the changes.

# Delete Custom Role

To manage and clean up admin roles by removing obsolete or unnecessary roles while ensuring no user is left without appropriate access, maintaining system integrity.

This task describes how to delete a custom admin role and the importance of reassigning impacted users if necessary.

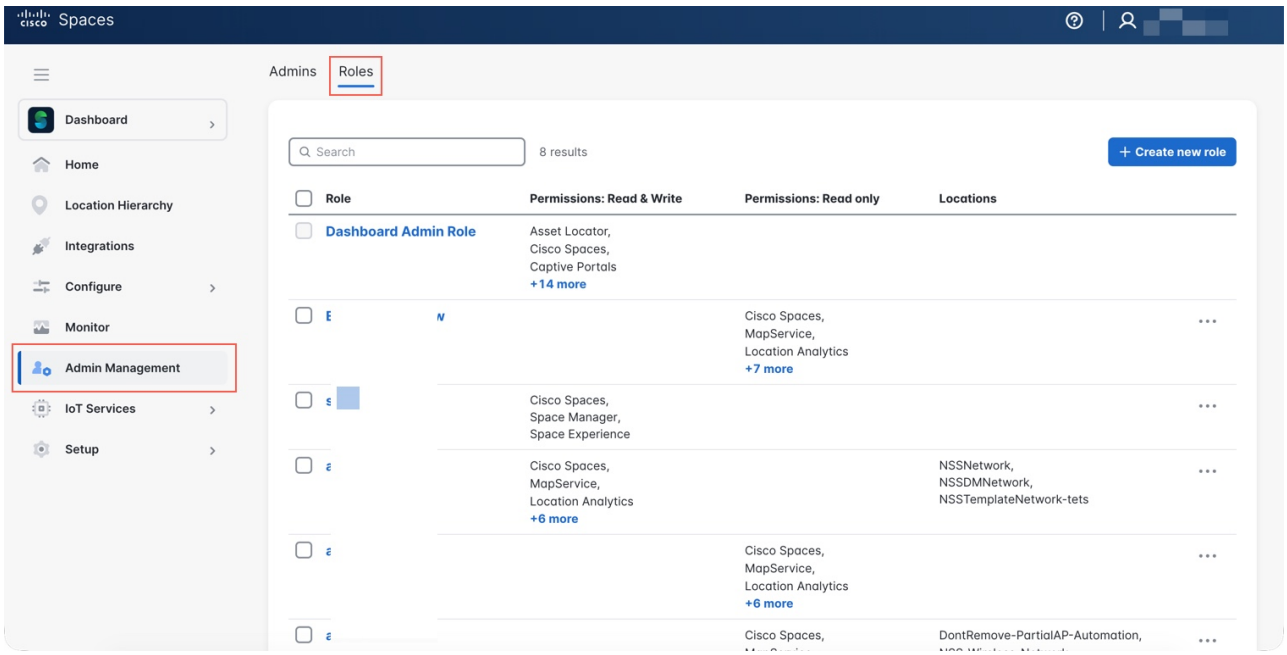
Follow these steps to delete a custom admin role:

### Procedure

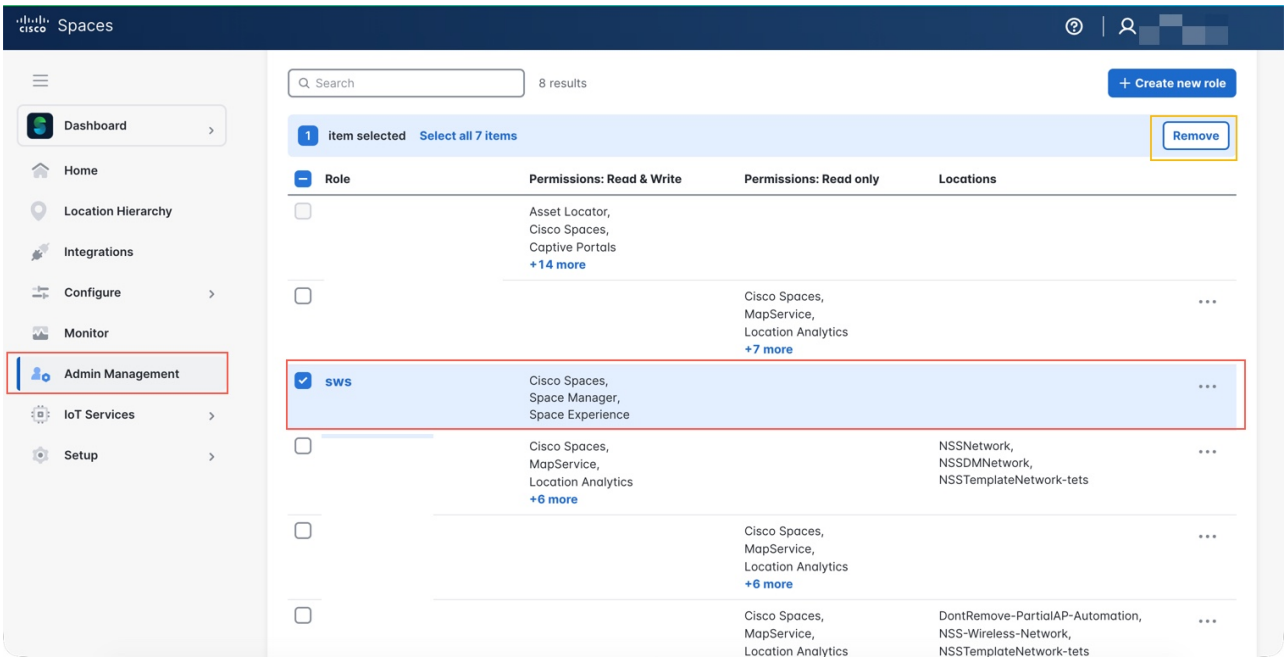
**Step 1** From the left pane, click **Admin Management**.

The **Admin Management** window is displayed.

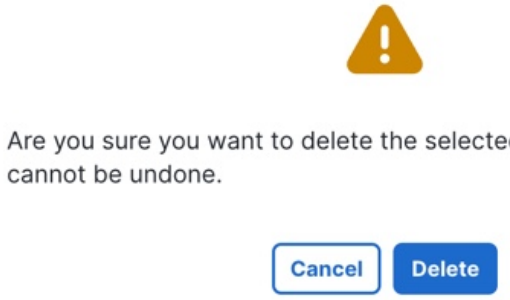
**Step 2** Click the **Roles** tab.




**Step 3** Select the custom role you want to delete.




**Step 4** Click **Remove** and confirm the deletion.




**Step 5** Ensure that any users impacted by this deletion are reassigned to other roles if required.

# Remove User Access

To securely revoke access for users who no longer require admin privileges, protecting the system from unauthorized access and potential security risks.

This task outlines the procedure to remove an admin user's access from the system.

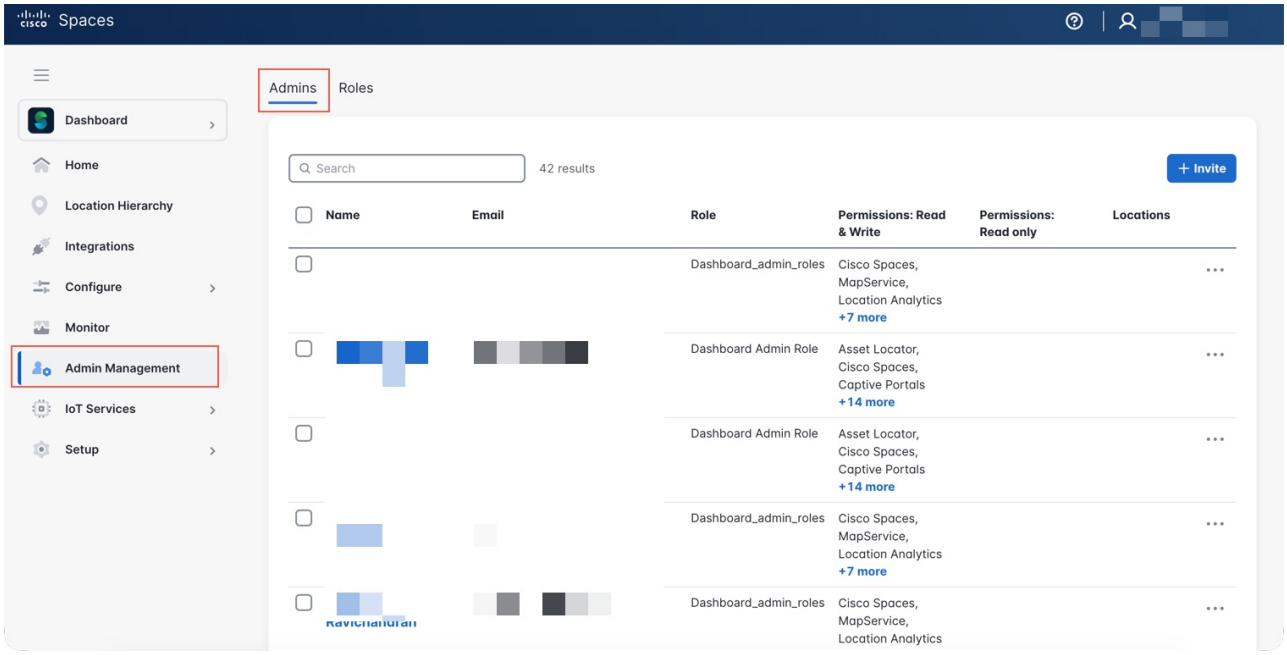
Follow these steps to remove an admin user's access:

### Procedure

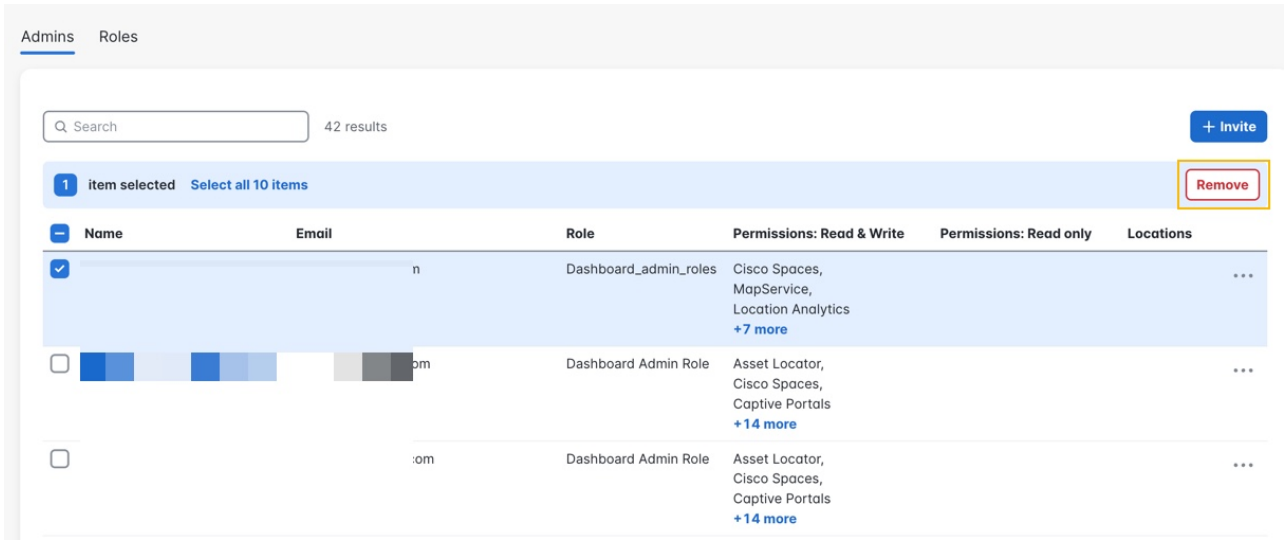
**Step 1** From the left pane, click **Admin Management**.

The **Admin Management** window is displayed.

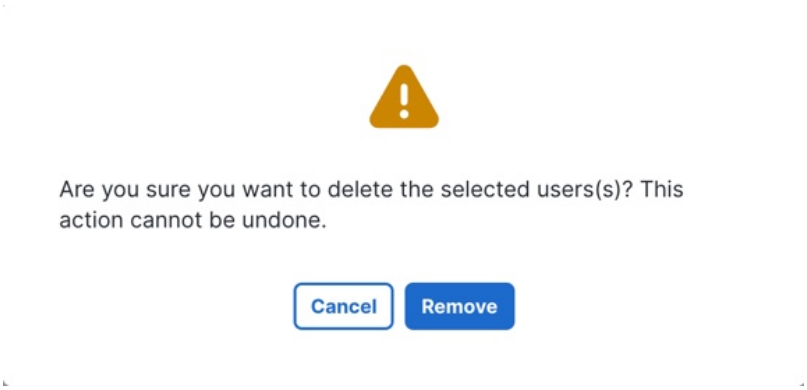
**Step 2** Click the **Admins** tab.




**Step 3** Select the target user whose access you want to remove.




**Step 4** Click **Remove** and confirm the action.




# User Management Workflows

User Management Workflows are a set of structured processes that enable administrators to manage user access and roles within an application. These workflows encompass inviting new users, managing their activation status, resending invitations, and handling invitation expiry to maintain secure and controlled access.

The purpose of User Management Workflows is to provide administrators with clear, repeatable procedures to onboard users efficiently while ensuring appropriate permissions and security measures, such as role assignment and location restrictions, are applied. These workflows also ensure that invitations are valid for a limited time and can be refreshed as needed.

**Key attributes**

- **Invitation Process**: Administrators invite new users by specifying their email, role (e.g., Read Write User or Read Only User), and optional location restrictions.
- **Invitation Resend**: If a user does not respond to an invitation, administrators can resend it, which generates a new token and restarts the invitation validity period.
- **Invitation Expiry**: Invitations expire after a fixed period (5 days), after which the token becomes invalid unless a new invitation is sent.
- **User Status Tracking**: Users remain in an "Invited - Not yet responded" state until they accept the invitation, ensuring clear visibility of pending user activations.

User Management Workflows are critical for maintaining secure and organized access control within an application. They help administrators ensure that only authorized users gain access with the correct permissions and that expired or unaccepted invitations do not pose security risks. These workflows also facilitate operational efficiency by providing mechanisms to manage and refresh user invitations systematically.

- Inviting a new user by entering their email and selecting their role.
- Resending an invitation to a user who has not yet accepted, which invalidates the previous token and issues a new one with a fresh expiry.
- Automatically expiring invitations after 5 days to enforce timely user activation.

# Invite a New App User

To enable administrators to add new users to the application by sending them an invitation email with appropriate access roles and optional location restrictions.

Inviting new users is a fundamental part of user management, allowing controlled access to the application. This process ensures that users receive the correct permissions and any necessary location-based restrictions before they start using the system.

**Before you begin**

Before starting this task, ensure you have administrative access to the User Management section and the email address of the user you intend to invite.

Follow these steps to invite a new app user to Cisco Spaces:

**Procedure**

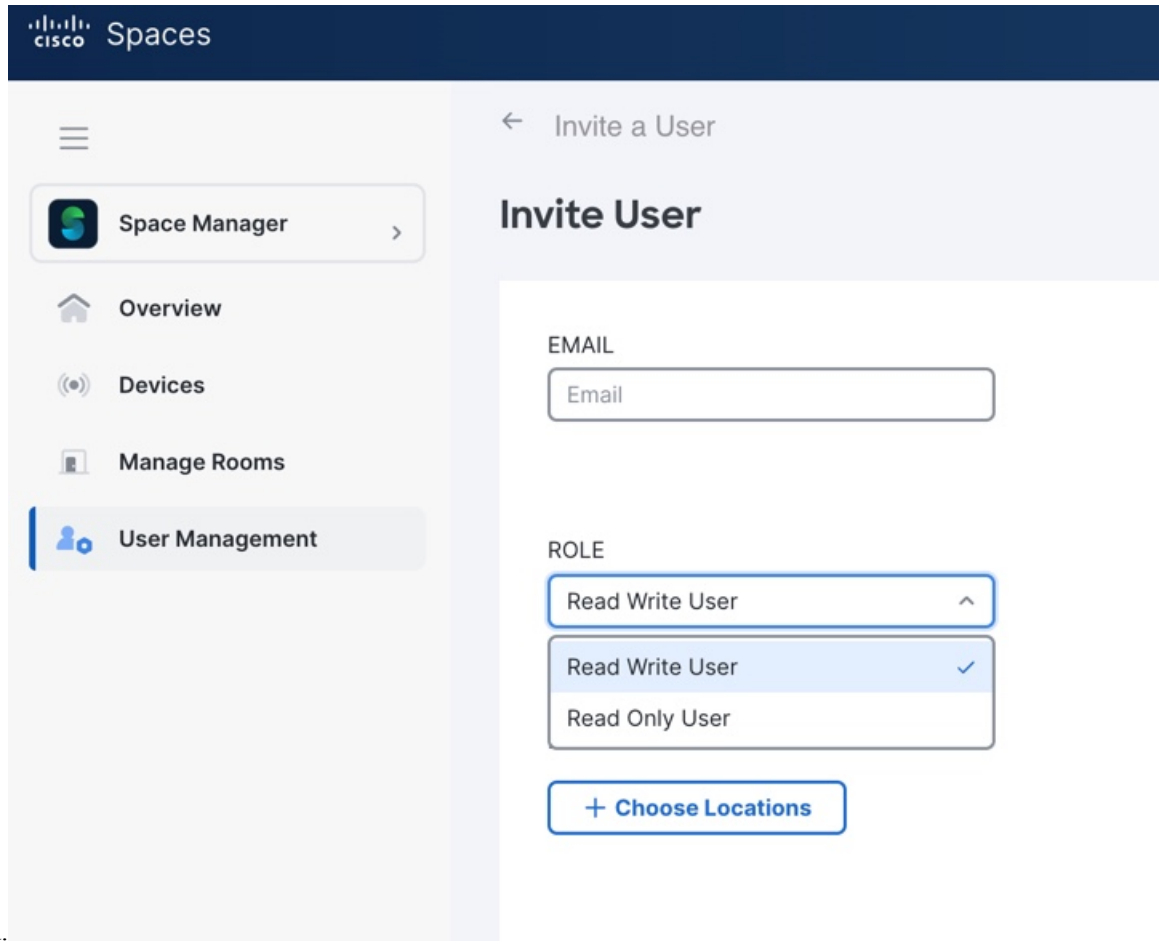
**Step 1** In the Cisco Spaces: Space Manager app, from the left pane, click **User Management**.

The **User Management** window is displayed.

**Step 2** Click the **Users** tab.

**Step 3** To invite a new app user, click **Invite User**.

The **Invite User** window is



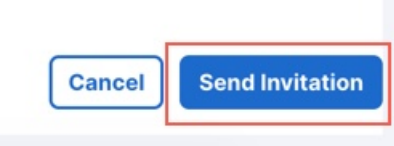

displayed.

**Step 4** In the **Email** field, enter the new app user's email address.

**Step 5** From the **Role** drop-down list, choose the role as **Read Write User** or **Read Only User**.

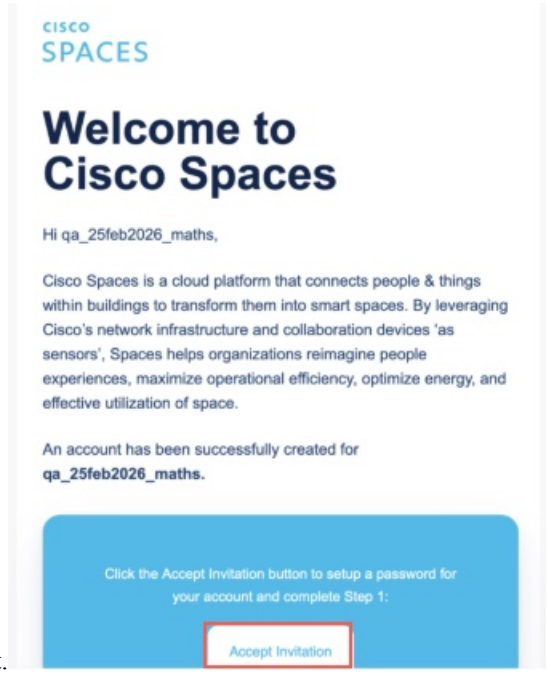
**Step 6** (Optional) Check the check box to enable location restriction and select the applicable locations.

**Step 7** Click **Send Invitation** to send the invitation.



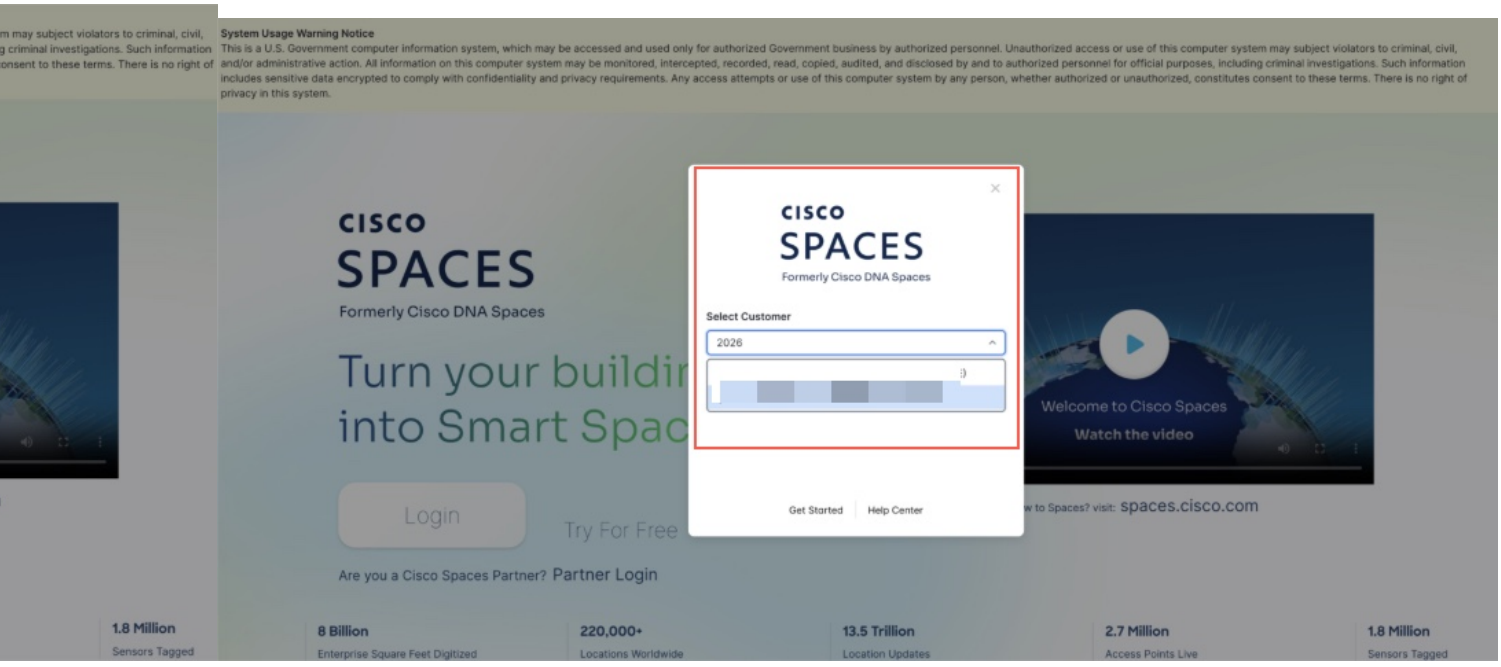

The invitation email is sent to the new user. The user status is set to "Invited - Not yet responded" until they accept.

A welcome email is sent to the user and you must click **Accept Invitation** to set up password for your account.




### What to do next

Use your email and password to login and choose the account from the **Select Customer** drop-down



# Resend Invitation

To allow administrators to resend an invitation to users who have not yet responded, ensuring they have a valid invitation token and extending the invitation validity period.

Sometimes users may not respond to the initial invitation within the validity period. Resending the invitation generates a new token and restarts the 5-day validity window, helping to maintain secure and up-to-date access control.

Before starting this task, you must have administrative access to the Dashboard, and the user's status must be "Invited - Not yet responded."

Follow these steps to resend the invitation:

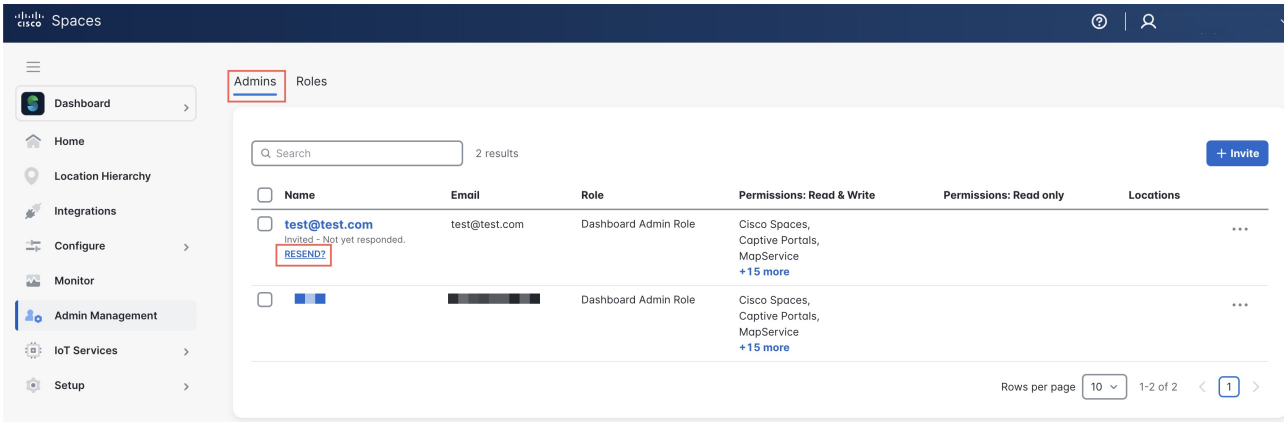
### Procedure

**Step 1** From the left pane, click **Admin Management**.

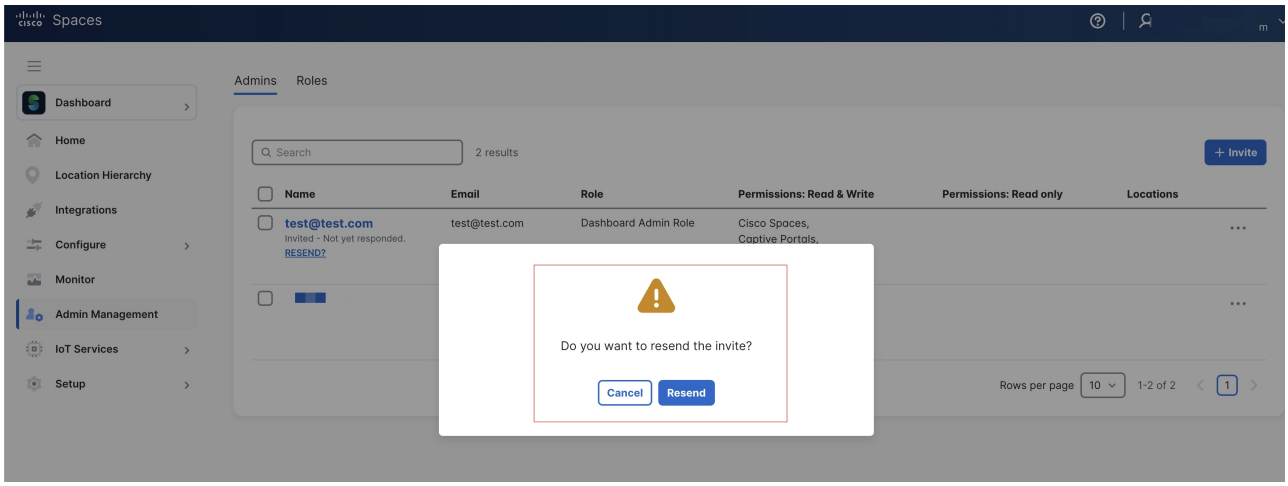
The **Admin Management** window is displayed.

**Step 2** Click the **Admins** tab.

**Step 3** Choose the user to be invited again and click **RESEND?**.




**Step 4** In the confirmation popup, click **Resend**.




When an invitation is resent, a new invitation token is generated while the old token is invalidated and becomes unusable. The invitation expiry is reset to five days from the time of the resend, and the user remains in the invited state until they accept the invitation.

### What to do next

For more information about invitation expiry rules, see Invitation Expiry Rules, on page 24.

# Invitation Expiry Rules

Understanding invitation expiry is critical for administrators to manage user access effectively, as tokens have a limited validity period to enhance security. Resending invitations refreshes this period by generating a new token, thereby maintaining control over user access and ensuring that only valid invitations are active. The purpose is to clarify the rules and behavior governing the expiration and validity of invitation tokens used in the user invitation process. Two key attributes related to the invitation tokens in the user invitation process are:

- **Token Expiry**: The invitation token has a validity period of 5 days from the time it is sent. The token is valid while the current time is less than the expiry time and becomes expired when the current time is equal to or greater than the expiry time.
- **Token Invalidation on Resend**: When an invitation is resent, a new invitation token is generated, and the old token is invalidated and no longer usable. This action resets the invitation expiry to 5 days from the resend time, while the user remains in the invited state until they accept the invitation.

### Rules

- Expiry time = invitation sent time + 5 days (432,000 seconds).
- Token is valid while current time < expiry time.
- Token is expired when current time ≥ expiry time.

### Behavior on Resend

- Resending generates a new token with a new issued-at time (iat) and expiry time (exp).
- The old token is invalidated.
- The invitation validity window restarts for 5 days from the resend time.

# Governance and Best Practices

Follow these governance guidelines and best practices to ensure secure, compliant, and uninterrupted administration of your Cisco Spaces account.

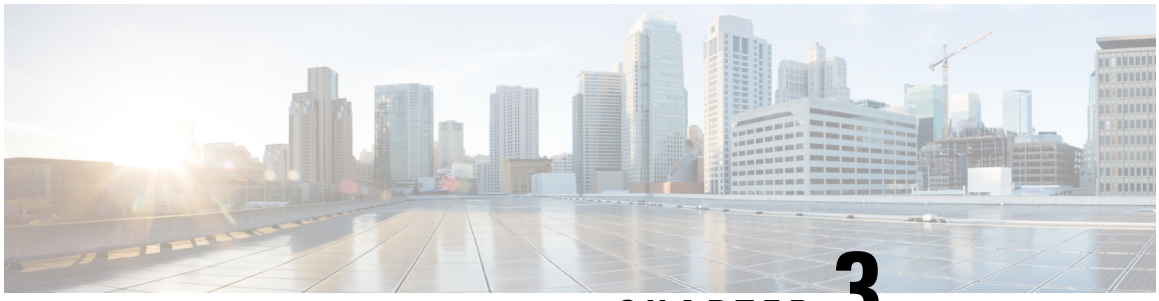
- Maintain at least two active **Default Admin** users for operational continuity.
- Apply the principle of least privilege; avoid unnecessary broad write access.
- Use least privilege by default; avoid unnecessary broad write access.
- Use location restriction where business boundaries require it.
- Perform periodic access reviews (monthly/quarterly).
- Immediately remove access during offboarding.
- Maintain audit records for role creation, assignment changes, and user removals.



PART III

# Getting Started


- Get Started with Cisco Spaces, on page 29



CHAPTER 3

# 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 29
- Log In, on page 30
- Start Working with Cisco Spaces, on page 30
- Onboard Workflow, on page 31
- Cisco Spaces: Connector 3.0, on page 31
- Idle Timeout for Cisco Spaces, on page 32
- Contact Cisco Spaces Federal Support, on page 32
- Cisco Spaces Documentation, on page 33


## Overview of Cisco Spaces

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

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

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

It covers various verticals of business such as

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

# Log In

As a Cisco Spaces user, you can log in to Cisco Spaces using the existing account login credentials. The domain specific URL to log in to Cisco Spaces is https://spaces-gov.cisco/.

# Start Working with Cisco Spaces

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



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

Follow these steps to start working with Cisco Spaces.

### Procedure

**Step 1** Log in to Cisco Spaces.

**Note**
You can enable Single Sign-On for Cisco Spaces.

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

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

- **Meraki**: For configuring a Cisco Meraki network, refer to Configuring Cisco Meraki for Cisco Spaces.
- **Cisco Unified Wireless Network with Cisco CMX**: For connecting Cisco Spaces with Cisco AireOS Controller through Cisco CMX, refer to Connecting Cisco Spaces to Cisco Wireless Controller through Cisco CMX, on page 46.
- **CiscoAireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller (without Cisco CMX )**.

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

  - **Using Cisco Wireless Controller Direct Connect**: For configuring Cisco Spaces with Cisco Wireless Controller using Wireless Controller Direct Connect, refer to the Connecting Cisco Catalyst 9800 Series Wireless Controller or Cisco Wireless Controller to Cisco Spaces Using WLC Direct Connect or Cisco Spaces: Connector, on page 47 section.

**Note**

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

**Step 3** Add your team members, and assign them roles and permissions. For more information about adding Cisco Spaces users, refer to Manage Cisco Spaces Users, on page 135.

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

**Step 5** Monitor the Cisco Spaces domain and apps using the **Monitor** section.

# Onboard Workflow

Follow these steps to log in to Cisco Spaces.

### Before you begin

We recommend that you completed FRMOD onboarding process and have the FRMOD credentials available. For a successful onboarding experience, use your organization specific Identity Provider (IDP) by configuring the domain.

### Procedure

**Step 1** Complete the FRMOD onboarding process.

**Step 2** Use your IDP and configure the domain.

For example, Cisco uses the frmod-cisco domain for Production onboarding and fedmod-cisco domain for staging environmemt.

**Step 3** Use your organization's email address to request invite for Cisco Spaces Dashboard and Administrator Management access.

**Step 4** Use the **`frmod-company.com`** email address and proceed with the activation instructions.

**Step 5** Use the same **`frmod-company.com`** credentials to log in to Cisco Spaces.

### What to do next

# Cisco Spaces: Connector 3.0

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

Connector is the next generation connector of Cisco Spaces that provides an enhanced user experience, architecture to support multiple services, simplicity, modularity, seamless upgrade and High Availability.

Connector supports an active-active High Availability setup. Unlike the earlier releases of Connector 2.x, you can specifically configure and monitor the High Availability pair. All services and device configurations are managed at the Connector level to make it easy to pair with High Availability.

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

# Idle Timeout for Cisco Spaces

A user who is logged in to the Cisco Spaces dashboard can remain idle only for a specific time period. If inactive for 15 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.

# Contact Cisco Spaces Federal Support

To contact Cisco Spaces Federal support, you need to raise a case using the Support Case Manager.

Follow these steps to raise a support case.

**Procedure**

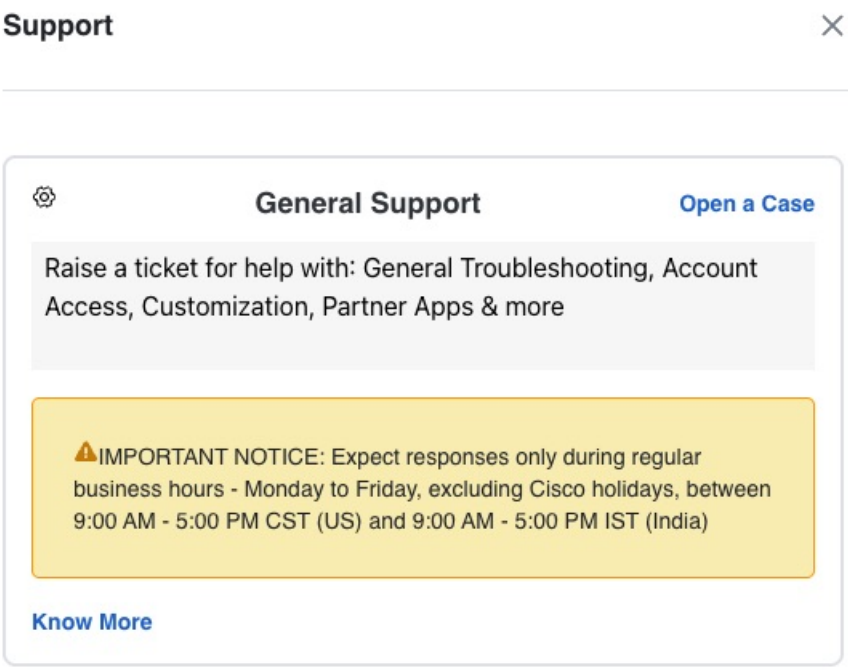
**Step 1** Log in to Cisco Spaces.

**Step 2** In the **Home** page, click the  (**Support**) icon displayed at the top-right.

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

**Step 4** In the **General Support** section, click **Open a Case** to raise a case using SCM.

*Figure 1: General Support Options*




# Cisco Spaces Documentation

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

Access these documentation support resources.

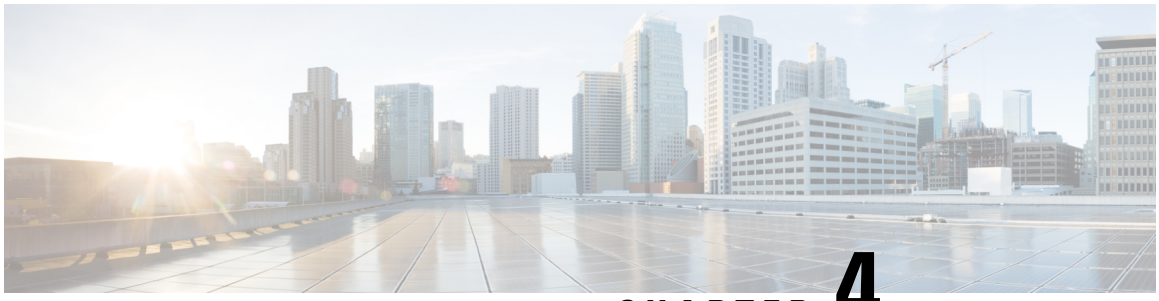
- Help Center
- Documentation
- Support
- Latest Release Notes
- Release Notes History



PART IV

# Cisco Spaces Home


- Cisco Spaces Dashboard, on page 37
- Configuring Cisco Wireless Controllers and Cisco Catalyst 9800 Series Controllers for Cisco Spaces, on page 45
- Configuring Cisco Meraki for Cisco Spaces, on page 53



CHAPTER 4

# Cisco Spaces Dashboard


- Cisco Spaces Navigation, on page 37
- Cisco Spaces Dashboard, on page 38
- Cisco Spaces Features, on page 40
- User Profile, on page 42
- Viewing Cisco Spaces Account Details, on page 42


## Cisco Spaces Navigation

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

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

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

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

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

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

The new and improved Cisco Spaces dashboard - **Home** page introduces changes to enhance user experience and navigation. The apps are categorized under **Starter Apps**, **Employee Experience**, and **Space Analytics**.

A feature to mark the apps as favorites. Click **Add to Favorites** (heart-shaped icon) displayed on the app tile to add them as favorites. A new section, **Favorite Apps**, is displayed with the apps marked as favorites.

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

*Figure 2: Home*

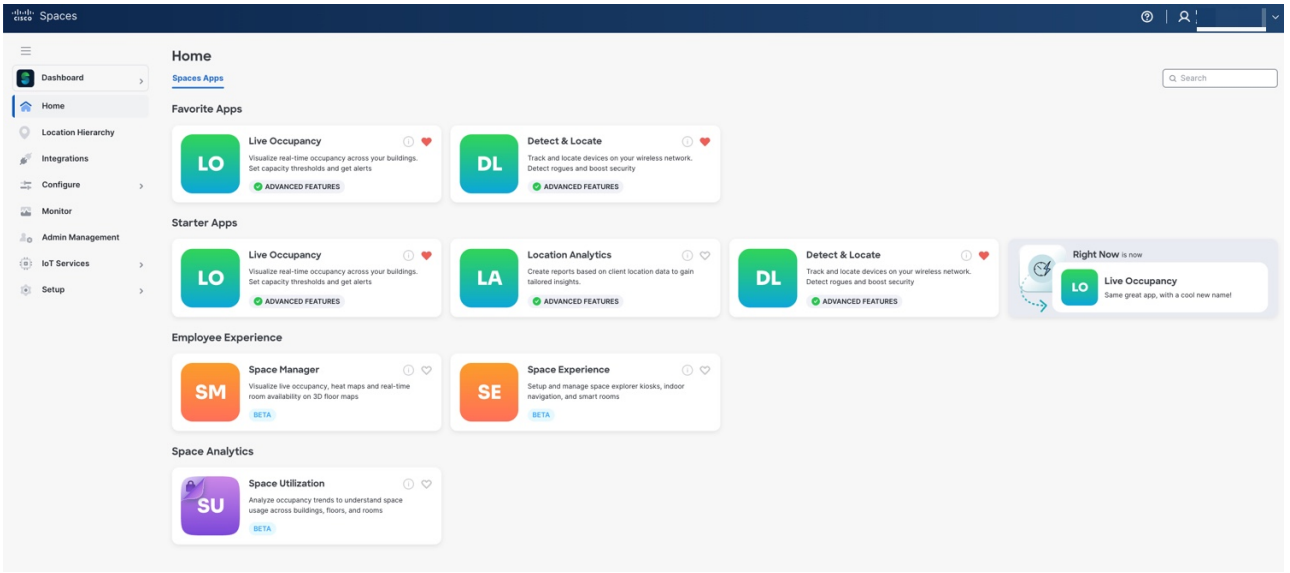
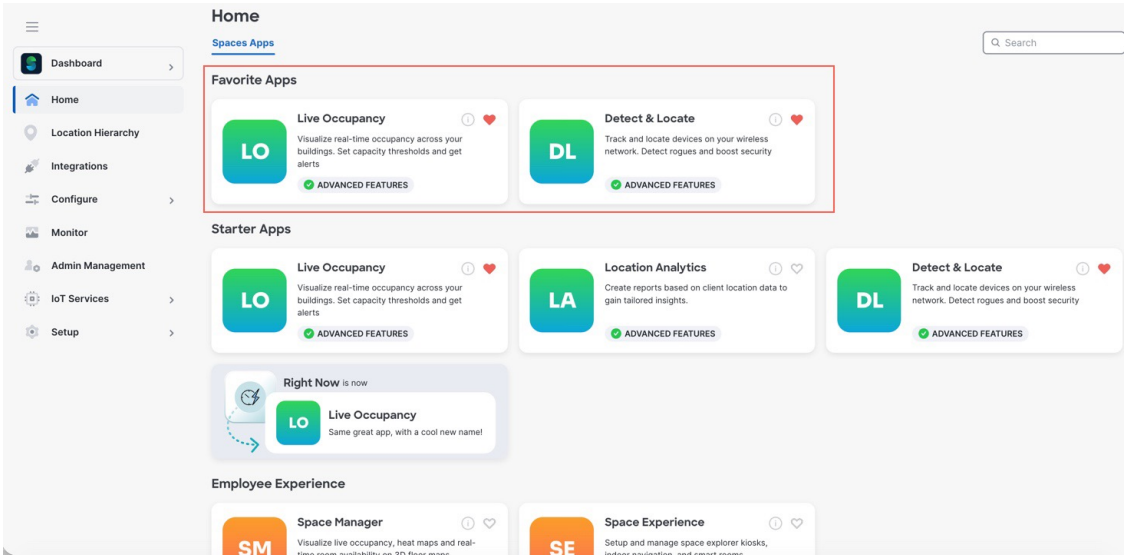



*Figure 3: Favorite Apps*

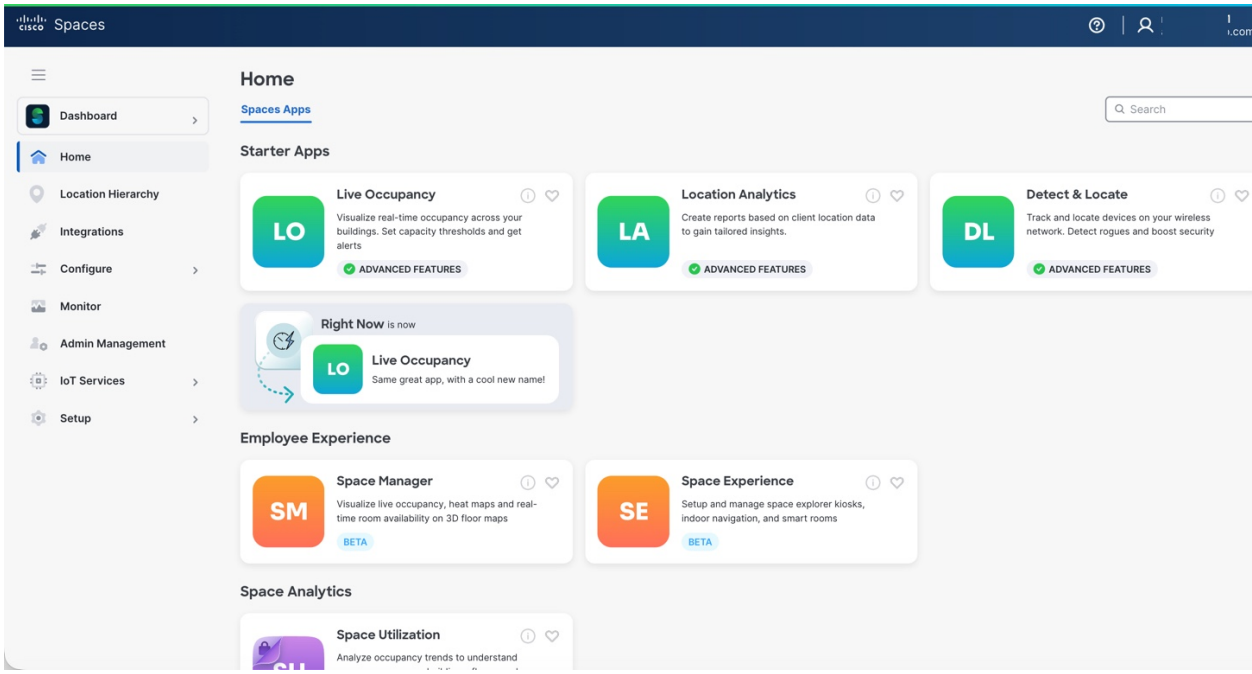



# Cisco Spaces Dashboard

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 4: Cisco Spaces Home*




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

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

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

### Left Navigation Pane

Use the left navigation pane to access these features.

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

### Icons

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

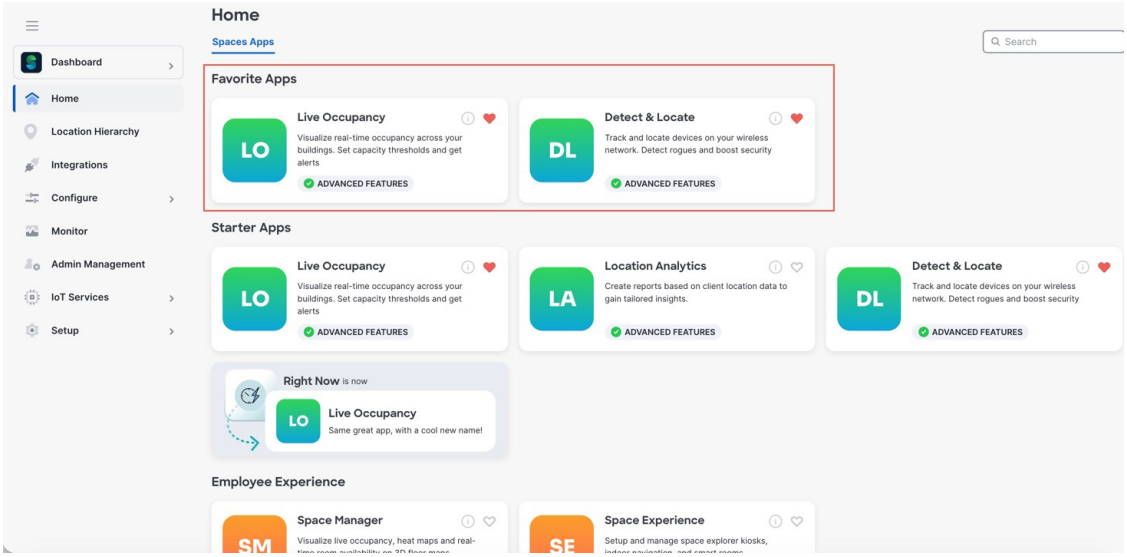
| Icon | Description |
|---|---|
| | Support: Displays help center, support and documentation links. |
| | User Profile: Displays account and logout options. The license information is available under **My Account** > **License Info** > **License Units Consumed**.<br>For more information, refer to User Profile, on page 42. |

# Cisco Spaces Features

The major features of Cisco Spaces dashboard includes:

## Cisco Spaces Apps

***Figure 5: Apps***




**Note** **Right Now** is now called **Live Occupancy** app.

## Location Hierarchy

1. Log in to Cisco Spaces.
2. In the left navigation pane, click **Location Hierarchy**.
3. Use the hierarchy tree or search option to find the required location.

4. Expand the hierarchy nodes, such as network, campus, building, floor, or zone.
5. Select the required location to view or manage its details.

# Integrations

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

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

# Configure

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

# Monitor

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

# Admin Management

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

# IoT Services

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

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

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

# Setup

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

The **Setup** menu allows you to configure and maintain your network infrastructure and confugure locations and maps.

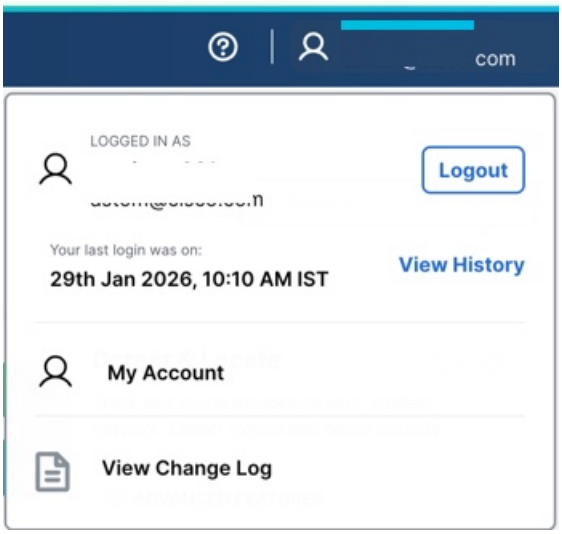
The **Setup** menu features are categorized into:

- Wireless Networks
- Locations & Maps

# User Profile

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

***Figure 6: User Profile***




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

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

- **My Account**: Click to display the **My Account** window. For more information, refer to Viewing Cisco Spaces Account Details, on page 42.
- **View Change Log**: Click to open the **Change Log** tab in the **My Account** window that displays the activity details of all the users in a particular account. For more information, refer to Viewing Cisco Spaces Account Details, on page 42.
- **Logout**: Click to log out from Cisco Spaces.

# Viewing Cisco Spaces Account Details

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

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

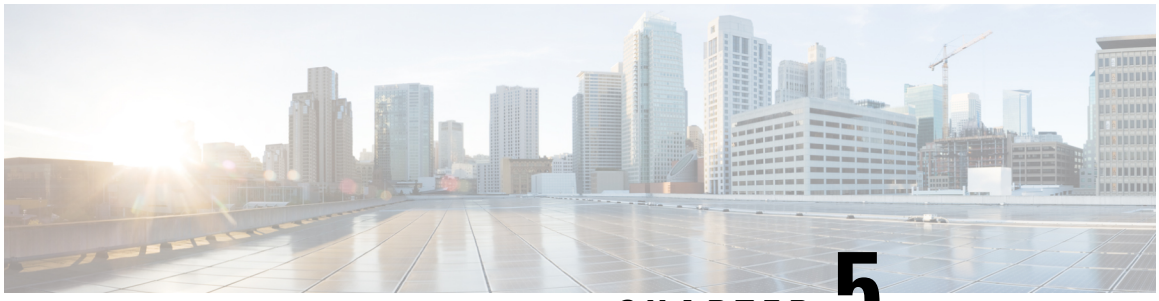


**Note**

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

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

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



CHAPTER 5

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

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

**Note**

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

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

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


- Connecting Cisco Spaces to Cisco Wireless Controller through Cisco CMX, on page 46
- Connecting Cisco Catalyst 9800 Series Wireless Controller or Cisco Wireless Controller to Cisco Spaces Using WLC Direct Connect or Cisco Spaces: Connector, on page 47

• Cisco Spaces Scale Benchmark, on page 50

# 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 Cisco Wireless Controller for Social Authentication

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

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

### Procedure

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

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

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

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

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

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

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

a) In the Cisco Wireless Controller dashboard, choose **Security** > **Access Control Lists**.

b) Click **More Actions** for the Access Control List configured for Cisco Spaces.

c) Click **Add Remove URL**.
d) Enter a social URL name, and click **Add**.
e) Repeat steps **c** and **d** for each domain.

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

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

**Facebook**

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

**LinkedIn**

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

**Twitter**

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

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

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

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

**Note**

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

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

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

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

### Before you begin

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

deployment contains Cisco Wireless Controller in Anchor Controller mode and Foreign Controller mode, you must import the certificate to the Cisco Wireless Controllers in both modes".

### Procedure

**Step 1** Import the DigiCert CA root certificate.

a) Download your root certificate from the following link:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Step 3** Check the summary using the following command:

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

The result appears.

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

**Example:**

**Sample Result**

(Cisco Controller) >show cloud-services cmx summary

CMX Service

Server ..... https://$customerpathkey.spaces-gov.cisco

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.

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

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

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

# Cisco Spaces Scale Benchmark

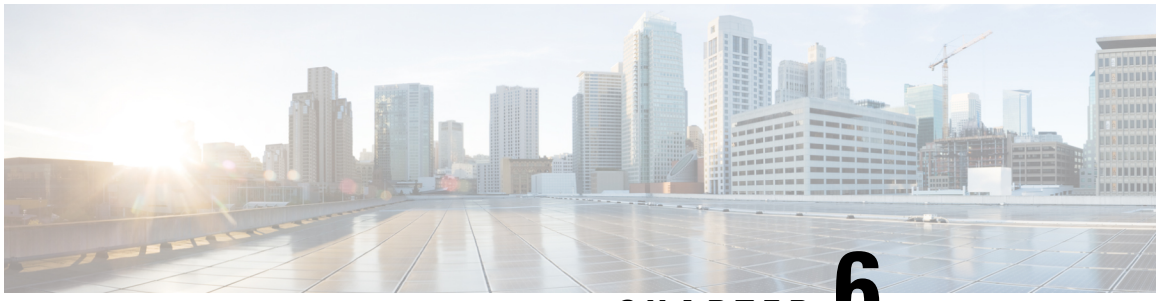
***Table 5: Scale Summary***

| SNO | Cisco Spaces: Connector | Cisco WLC Direct Connect | | CMX Tethering Connector |
|---|---|---|---|---|
| Platforms | Cisco AireOS | Cisco AireOS | Cisco Catalyst 9800 Series | Cisco AireOS |

| SNO | Cisco Spaces: Connector | Cisco WLC Direct Connect | | CMX Tethering Connector |
|---|---|---|---|---|
| Max Scale on supported appliance. | 12.5K APs, 250K clients<br>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<br>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 6

# 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 53
- Configuring Cisco Meraki for RADIUS Authentication, on page 54
- Configuring Cisco Meraki for Notifications and Reports, on page 56
- Configuring Cisco Meraki for Social Authentication, on page 57
- Manually Configuring SSIDs for Cisco Meraki, on page 57
- Configuring Scanning API in Cisco Meraki, on page 58
- Bluetooth Low Energy Device Support, on page 59


## Enabling SSIDs in Cisco Meraki

To import the SSIDs to the Cisco Spaces to configure them for the Captive Portal Rules, you must enable those SSIDs in Cisco Meraki.

**Note** As Cisco Meraki is not a part of the Cisco Spaces, the menu path and menu names are subject to change.

To enable the SSIDs in Cisco Meraki, perform the following steps:

### Procedure

**Step 1** Go to https://meraki.cisco.com.

**Step 2** Log in to the application using the login credentials for your Cisco Meraki account.

**Step 3** Click the **Cisco Merkai Organization** in which you want to enable the SSIDs, and choose the required network.

**Step 4** Choose **Wireless** > **Configure** > **SSIDs**.

The SSIDs available for the network appears.

**Step 5** Rename the SSID and enable it.

**Step 6** Click **Edit Settings**, and in the Splash page option, click the **Click-Through** radio button.

**Step 7** Click **Save Changes**.

The SSID is successfully enabled in Cisco Meraki.

# Configuring Cisco Meraki for RADIUS Authentication

To provide more security to your portals, the Cisco Spaces provides radius-authentication for the portals. Also, certain configurations are required in Cisco Meraki to manage the seamless internet provisioning that can be configured using the Captive Portal Rule.

The Radius Server Configurations required when configuring for the seamless internet provisioning is different from that of the standard radius server configuration.

## Configuring Cisco Meraki for RADIUS Authentication (Without Seamless Internet Configurations)

To configure Cisco Meraki for RADIUS authentication, perform the following steps:

### Procedure

**Step 1** Log in to Cisco Meraki with your Meraki credentials.

**Step 2** Choose **Wireless Access Control**.

**Step 3** Choose the SSID for the captive portal rule.

**Step 4** In the **Association requirements** area, choose **Open**.

**Step 5** In the **Splash page** area, choose **Sign-on with**, and from the drop-down list select **my RADIUS server**.

**Step 6** In the **Radius servers**area, click **Add a server**, and in the fields that appear mention the radius server details for authentication.

- Port:1812

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

**Step 7** From the **Radius accounting** drop-down list, choose **Radius Accounting is enabled**.

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

**Step 8** In the **Radius accounting servers** area, click **Add a server**, and in the fields that appear mention the radius server details for accounting.

- Port:1813

**Note**

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

**Step 9** Configure the Wall Garden ranges. To view the wall garden ranges, in the Cisco Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the SSIDs page.

**Step 10** Save the changes.

# Configuring Cisco Meraki for RADIUS Authentication and Seamless Internet Provisioning

To configure Cisco Meraki for RADIUS authentication and Seamless Internet Provisioning, do the following configurations in Cisco Meraki:

### Procedure

**Step 1** Log in to Cisco Meraki with your Meraki credentials.

**Step 2** Choose **Wireless** > **Access** > **Control**.

**Step 3** Choose the SSID for the captive portal rule.

**Step 4** In the Association requirements area, choose **Mac-based access control (no encryption)**.

**Step 5** In the Splash page area, choose **Click-through**.

**Step 6** In the Radius servers area, click **Add a server**, and in the fields that appear mention the radius server details for authentication.

- Port:1812

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

**Step 7** From the **Radius accounting** drop-down list, choose **Radius Accounting is enabled**.

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

**Step 8** In the **Radius accounting servers** area, click **Add a server**, and in the fields that appear mention the radius server details for accounting.

- Port :1813

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

**Step 9** From the **Radius attribute specifying group policy name** drop-down list, choose **Filter-Id**.

**Step 10** Save the changes.

**Step 11** In the Cisco Meraki dashboard, click **Network-wide Group Policies**.

**Step 12** Click **Add a Group**.

**Step 13** In the **New group** window that appears, enter a name for the group.

**Note**
You have to configure this name as the policy name in the Cisco Spaces dashboard. If you are specifying the group name as **CaptiveBypass**, this policy name will act as the default policy name for all the Captive Portal rules. That is, if you are not specifying a policy name for a Captive Portal rule for which the "Seamlessly Internet Provision" is opted, the policy name **CaptiveBypass** will be applied for that rule.

**Step 14** From the **Bandwidth** drop-down list, choose the required option, and specify the Internet bandwidth to be provisioned for the customers.

**Step 15** From the Splash drop-down list, choose **Bypass**.

**Step 16** Click **Apply**.

**Step 17** Configure the Wall Garden ranges. To view the wall garden ranges, in the Cisco Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the SSIDs page.

# Configuring Cisco Meraki for Notifications and Reports

To send notifications using the Cisco Spaces and to view the Cisco Spaces reports, you must do certain configurations in Cisco Meraki.



**Note** When you import a Meraki network location to Location Hierarchy, the Notification URL automatically gets configured in Cisco Meraki. This support is not applicable for the Meraki networks added using Meraki API Key.

To manually configure Cisco Meraki for sending notifications using the Cisco Spaces or to view the Cisco Spaces reports, perform the following steps:

**Procedure**

**Step 1** Log in to Cisco Meraki using the credentials for your Meraki account.

**Step 2** Click the organization in which you want to enable SSIDs, and choose the required network.

**Step 3** Choose **Network-wide** > **Configure** > **General**.

**Step 4** In the **CMX** area, do the following:

a) From the **Analytics** drop-down list, choose **Analytics is enabled**.

b) From the **Scanning API** drop-down list, choose **Scanning API enabled**.

c) Click **Add a Post URL**, and enter the post URL details in the respective fields.

To view the post URL details, in the Cisco Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the **SSIDs** window.

**Step 5** Click **Save Changes**.

# Configuring Cisco Meraki for Social Authentication

For social authentication with Cisco Meraki, you must do some configurations in meraki.cisco.com.

To configure Cisco Meraki for social-authentication, perform the following steps:

**Procedure**

**Step 1** In the Cisco Meraki dashboard, choose **Wireless** > **Configure** > **Access Control** .

The **Access Control**window appears.

**Step 2** From the **SSID** drop-down list, choose the SSID for which you want configure the social authentication.

**Step 3** In the **Wall Garden Ranges** field, enter the social networking domain names listed in the following table, and click **Save Changes**.

Social Authentication for Cisco Meraki is successfully configured.

***Table 6: Social Networking Domain Names***

| Facebook | Twitter | LinkedIn | |
|---|---|---|---|
| *.facebook.com<br>*.fbcdn.net<br>*.akamaihd.net<br>*.connect.facebook.net | *.twitter.com<br>*.twimg.com | *.linkedin.com<br>*.licdn.net<br>*.licdn.com | |

# Manually Configuring SSIDs for Cisco Meraki

To manually configure an SSID in Cisco Meraki, you have to initially import that SSID in the Cisco Spaces. For more information, see the "Importing the SSIDs for Cisco Meraki section .

To configure the SSID manually in Cisco Meraki, perform the following steps:

**Procedure**

**Step 1** Log in to Cisco Meraki using the credentials for your Meraki account.

**Step 2** Choose the required Cisco Meraki organization and network from the respective drop-down list.

**Step 3** Choose **Wireless** > **Access Control**.

**Step 4** From the SSID drop-down list, choose the SSID that you want to configure for the Cisco Spaces.

**Step 5** In the splash page area, choose **Click-through**.

**Step 6** From the Wall garden drop-down list, choose **Wall garden is enabled**.

**Step 7** In the **Wall garden ranges** field, enter the required wall garden ranges.

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

**Step 8** Click **Save Changes**.

**Step 9** Choose **Wireless** > **Splash page**.

**Step 10** For the previously selected SSID, in the **Custom Splash URL** area, choose **Or provide a URL where customers will be redirected**, and in the adjacent field enter the splash URL.

To generate and view the splash page URL for a Meraki SSID, follow the steps given below:

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

b) On the **SSIDs** page, click the **Configure Manually** link for the desired Meraki SSID.
The splash page URL for the selected Meraki SSID is displayed.

**Step 11** In the **Splash Behavior**area, click the **The URL they were trying to fetch** radio button under **Where should users go after the splash page**.

**Step 12** Click **Save Changes**.

**Step 13** Repeat steps 3-12 for all the SSIDS that you want to use in the Cisco Spaces.

### What to do next

# Configuring Scanning API in Cisco Meraki

For using Meraki Camera, you must configure Scanning API in Cisco Meraki.

To configure a Scanning API in Cisco Meraki, perform the following steps:

### Procedure

**Step 1** Log in to the https://meraki.cisco.com using the login credentials for your Cisco Meraki account.

**Step 2** Choose **Networkwide** > **General**.

**Step 3** In the **Location and Scanning** area, do the following:

a) From the **Analytics** drop-down list, choose **Analytics enabled**.

b) From the **Scanning API** drop-down list, choose **Scanning API enabled**.

c) Add a post URL.

- In the **Post URL** field, enter the post URL .
- In the **Secret Key** field, enter the secret key that is used by your HTTP server to validate that the JSON posts that are coming from the Cisco Meraki cloud.

**Note**
You can copy the post URL and secret key from the **Connect your Meraki Camera** window for **Setup** > **Camera** in Cisco Spaces dashboard.

- From the **API Version** drop-down list, choose the Location API version your HTTP server is prepared to receive and process.

**Step 4** Configure and host your HTTP server to receive JSON objects.

**Step 5** During the first connection, the Cisco Meraki cloud will verify the organization's identity as the Cisco Meraki customer.

The Cisco Meraki cloud will then begin performing JSON posts.

# Bluetooth Low Energy Device Support

Support for Bluetooth Low Energy (BLE) devices are available on the Cisco Meraki network, in addition to the existing support on the Cisco Catalyst Wireless network.

This enhancement allows the Cisco Spaces platform to seamlessly integrate with BLE devices using Cisco Meraki. With this enhancement, Cisco Meraki BLE devices can now be accessed in various Cisco Spaces applications, including Firehose IoT Telemetry events, IoT Explorer, Signage, and Live Occupancy.



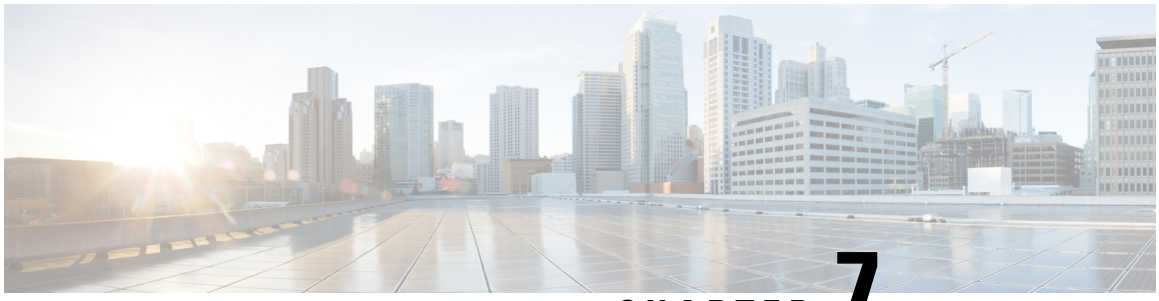
**Note** For this feature to work, you must perform specific configurations on the Cisco Meraki network to enable the data transmission to Cisco Spaces. We recommend that you contact Cisco Spaces support team for further assistance.



PART V

# Cisco Spaces: Apps


- Cisco Spaces: **Live Occupancy** App, on page 63
- Cisco Spaces: Location Analytics App, on page 69
- Cisco Spaces: Detect and Locate App, on page 83
- Cisco Spaces: Space Utilization App, on page 85
- Cisco Spaces: Smart Workspaces App, on page 87



CHAPTER 7

# Cisco Spaces: Live Occupancy App

This chapter describes about the **Live Occupancy** app.


- **Live Occupancy** Overview, on page 63
- WiFi Occupancy, on page 64
- Settings, on page 66
- Location-Based RBAC, on page 67


## Live Occupancy Overview

The **Live Occupancy** app provides you the **Live Occupancy** report that shows the details of visitors currently present at your locations.

The **Live Occupancy** app is enhanced to address issues with counts when there are any changes in the **Location Hierarchy**. Prior to this enhancement, changes in **Location Hierarchy** such as adding new locations, removing existing locations or updating vital parameters such as **TimeZone** introduced stale or incorrect counts for Wi-Fi.

With this enhancement, the **Presence** chart count gets reset (removes all existing numbers until the current time) for the present day because the counts are invalid after the **Location Hierarchy** changes.

The **Live Occupancy** app is available for these license types:

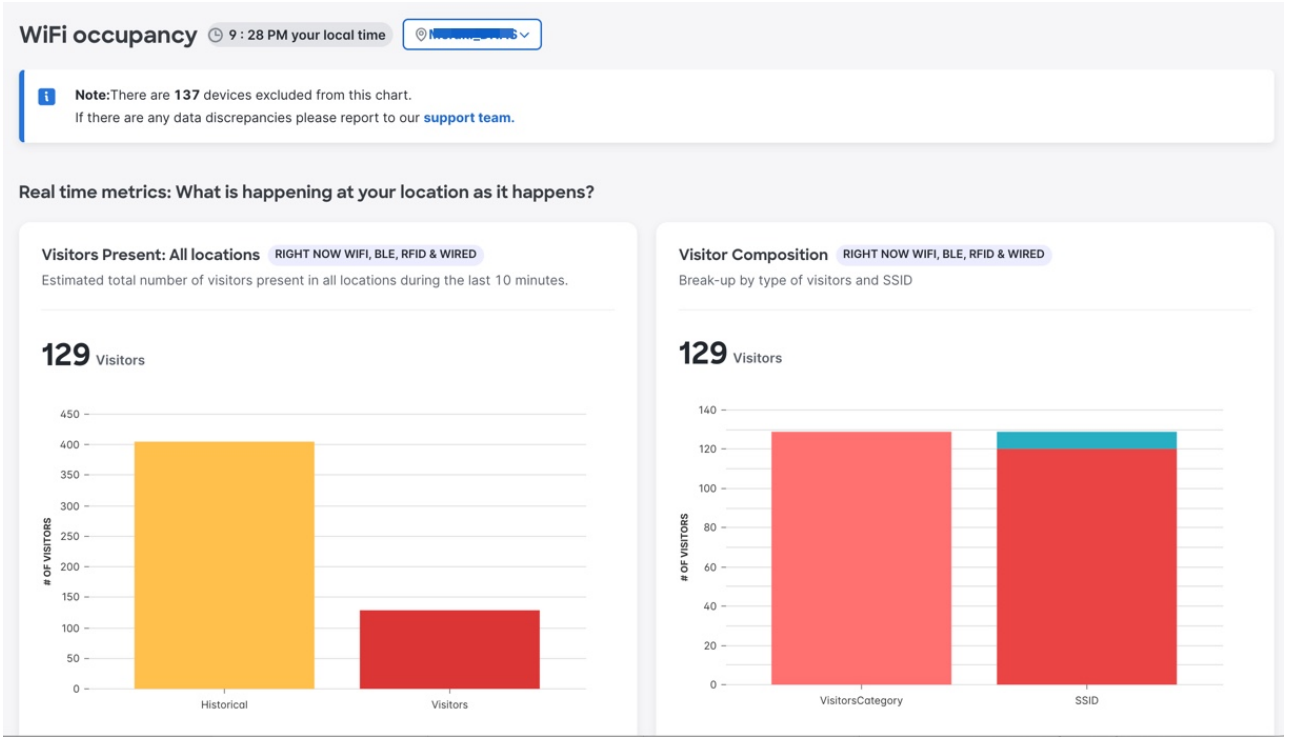
- SEE
- EXTEND
- SWITCH_EXT
- SMART_VENUES
- SMART_OPERATIONS
- SMART_OPERATIONS_BASE
- ACT (displayed in the UI as Advantage)
- UNLIMTED
- PREMIER_W
- PREMIER_CW

# WiFi Occupancy

The **WiFi occupancy** report displays the details of the visitors currently present at your locations. By default, the report shows the details of visitors currently present at all locations. You can filter upto the floor level.

The **WiFi occupancy** is enhanced to show the count of excluded devices that are not considered as visitors or filtered during data processing. The excluded device count is displayed as a message in the **Note** section of the **WiFi occupancy**.

***Figure 7: Live Occupancy App***



**Note**

- If a location is removed or modified in the location hierarchy or timezone is changed, the existing **Presence** chart count is reset.
- For BLE processing:
  - BLE group information should be received as part the IoT updates
  - RSSI value should be greater than -85
- For probing devices:
  - **Cisco Connector** and other device types: RSSI value should be greater than -70
  - **Cisco Meraki**: RSSI value should be greater than -100.

  Only those probing devices meeting the specified signal strength thresholds are allowed to share the device location update events as part of the Firehose data stream.

# Viewing the Live Occupancy Report

To view the **Live Occupancy** report, perform these steps:

**Procedure**

**Step 1** In the Cisco Spaces Dashboard, choose **Live Occupancy**.

The **Live Occupancy** app is displayed.

**Step 2** From the **Location** drop-down list, select the desired network location.

The **Live Occupancy** report for the selected network location is displayed.

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

The **Live Occupancy** report displays these charts:

- **Visitors Present: All locations**: Displays an estimated total number of visitors, during the last 10 minutes, in the filtered location including its child location.
- **Visitor Composition**: Displays the composition of active visitors, in percentage, by SSID category (employee, guest, etc.) and by SSID (top 5 SSIDs).
- **Visitors Present: All Locations**: Displays a trend of the total number of visitors during the last 10 minutes for the filtered location.
- **Visitors Present: Map View**: Displays the location-wise count of active visitors in the child locations of the filtered location.
  - **Map View**: The child locations of the filtered location are shown in the world map along with the total number of visitors in each of those child locations.
    - **Floor map view**: Select a specific floor to refer to the chosen floor map view as well.

If the selected location has a map, imported from Cisco CMX, which is uploaded to Cisco Spaces, you can view the floor and the total number of visitors on the displayed floor.

- **List View**: The child locations of the filtered location are listed, and the number of current visitors for each child location is shown against that location.

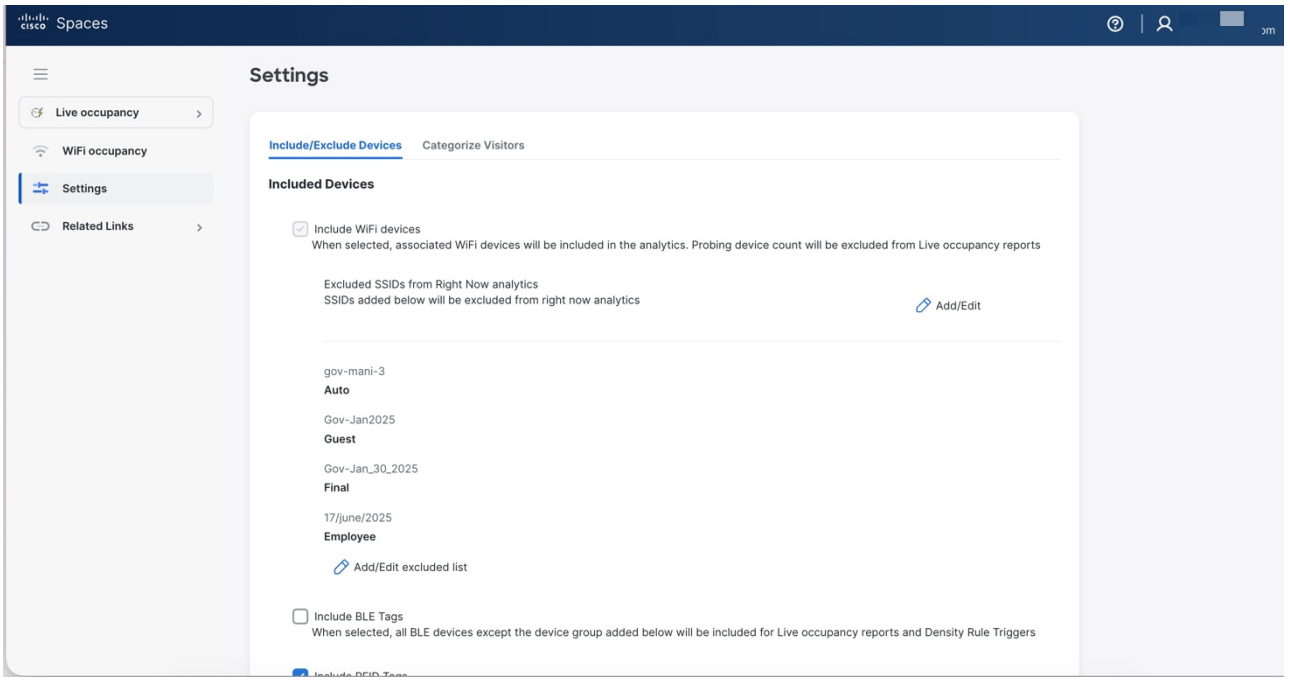
**Note**

- An "active visitor" can be any visitor who is present at the location during the last 10 minutes and is connected to the network (WLAN or SSID).
- If a device has a dwell time lesser than a minute, during the 10-minute window, it is excluded from the Live Occupancy report.
- The average value for the last 51 weeks is shown as historical data for each chart in the report.

# Settings

The **Settings** menu helps you manage devices, SSIDs, and visitors in the **Live Occupancy** app reports. The **Settings** menu includes the **Include/Exclude Devices** and **Categorize Visitors** tabs.

***Figure 8: Live Occupancy - Settings***




### Including or Excluding Devices

Use the **Include/Exclude Devices** tab to select among the following options for Wi-Fi, BLE, and RFID devices for the **Live Occupancy** reports:

- Wi-Fi devices option is included by default and you cannot deselect the same.

  To exclude devices connected to specific SSIDs from the **Live Occupancy** analytics, click **Add/Edit** or **Add/Edit excluded list** and select the desired SSIDs from the **Exclude SSIDs** list.

- BLE Tags: To include BLE tags in the **Live Occupancy** reports, select **Include BLE Tags**.

  To exclude specific device groups from the **Live Occupancy** analytics, click **Add/Edit** or **Add/Edit excluded list** and select the desired BLE devices from the **Exclude BLE devices** list.

- RFID Tags: To include RFID tags in the **Live Occupancy** reports, select **Include RFID Tags**.

**Note**

- If you select RFID and BLE tags, then the corresponding device count is displayed in the **Live Occupancy** report.
- If you configure an SSID to be excluded here, it not only excludes the clients connected to that SSID from **Live Occupancy** but also excludes them from other applications that receive data from **Live Occupancy** such as Partner Firehose Wifi data, Space Utilisation Floor occupancy metrics, and Signage Occupancy Count.

### Categorizing Visitors

Use the **Categorize Visitors** tab to automatically or manually classify visitors, based on the visitor type, that have joined an SSID. The options available are:

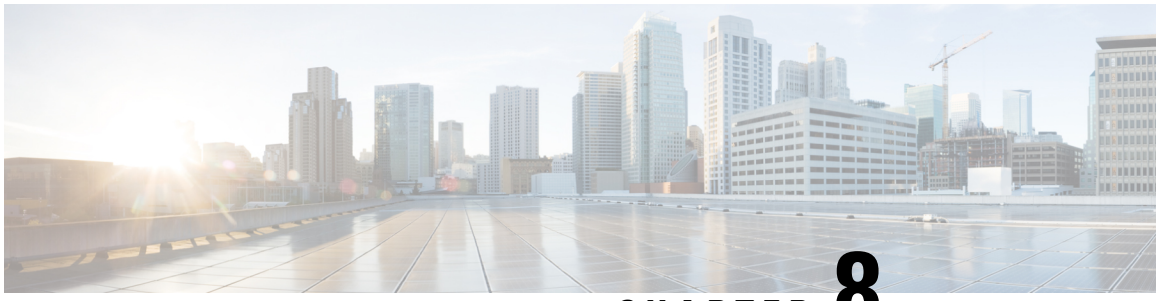
- Auto
- Guest
- Employee
- Custom

# Location-Based RBAC

A location-based RBAC role is a user access control setting that

- restricts a user's access to data and features based on assigned physical locations,
- enables administrators to specify which locations a role applies to during role creation or user invitation, and
- ensures that users can view only the data for the locations to which they are invited.

For more information, refer to Location-Based RBAC (Role-Based Access Control) in Cisco Spaces, on page 139.



CHAPTER 8

# Cisco Spaces: Location Analytics App

This chapter describes the Location Analytics Report.


- Overview of Location Analytics App, on page 69
- View Location Analytics Report, on page 71
- Compare Reports, on page 73
- Create Custom Report, on page 74
- Add Widget, on page 78
- Location-Based RBAC, on page 80


## Overview of Location Analytics App

The Location Analytics app enables you to understand and analyze footfall, visitors, visit patterns and dwell time distribution across various areas in your building, across regions and different locations. The visits of your employees are also included in the report.

Use the Location Analytics app to view the reports with visits, visitor insights and dwell time distribution data and also create custom reports as per your preferred filter criteria.

The Location Analytics app has two options on the main menu: **Reports** and **Custom Reports**.

**Reports**

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

**Custom Reports**

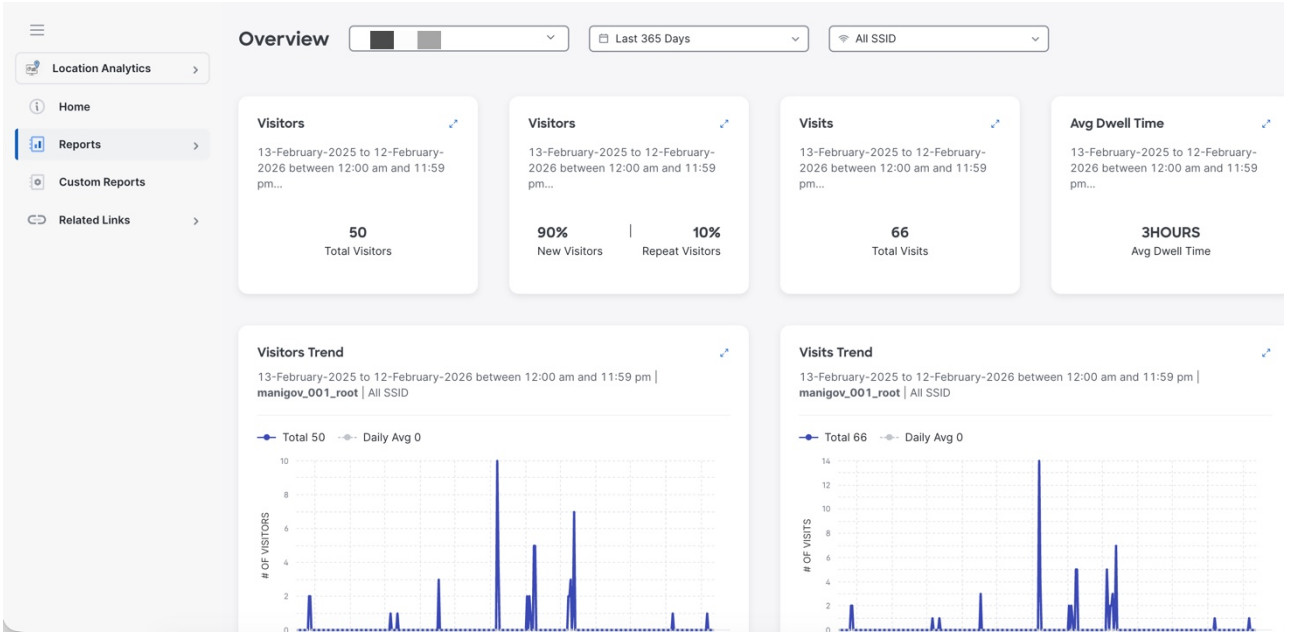
Choose **Location Analytics App** > **Custom Reports** to view and save custom reports. You can create custom reports with the available report type and also with **Path** widget included in the report.

In the Location Analytics app, choose **Reports** > **Overview** to view Location Analytics reports with visitor/visit trends/dwell time distribution in both tile and graphical format. You can also compare reports based on the available filter parameters. For more information, refer to Compare Reports, on page 73.

**Note**

- Read-only user cannot modify custom reports.

*Figure 9: Location Analytics Overview*




**Note**

- By default, a report for all locations, all SSIDs and for the last 365 days is displayed. Use the filters available on top of the window to modify the report as needed.
- If you are new to the Location Analytics app with no data, click **Location Analytics** in the left menu to view the sample reports and understand how visitor details are displayed.

The **Overview** window displays the information related to **Visitors**, **Visits**, **Daily Average Visitors** and **Daily Average Visits** as per the selected parameters.

- **Visitors** are defined as the total number of unique visitors based on the selected criteria.
- **Visits** are defined as the total number of visits for a specific location.
- **Daily Average Visitors** are defined as the daily average calculated by adding the total number of daily visitors for the selected period and then dividing that by the number of days.
- **Daily Average Visits** are defined as the daily average calculated by adding the total number of daily visits for the selected period and then dividing that by the number of days.

The **Overview** window displays the following information in tile format:

- Visitors: Daily Average Visitors
- Visitors: New vs Repeat Visitors
- Visits: Daily Average Visitors
- Visits: Average Dwell Time

The **Overview** window displays the following information in graphical format.

- Visitors Trend
- Visits Trend
- Dwell Time Distribution

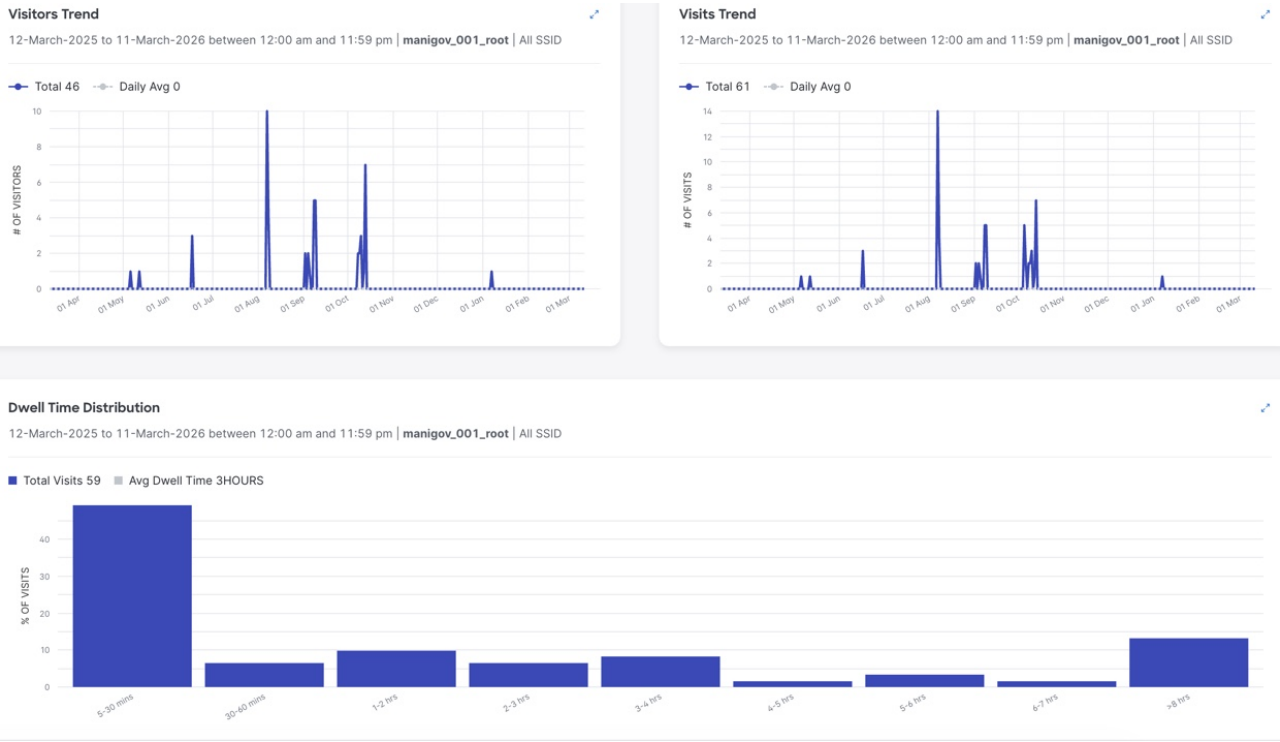
# View Location Analytics Report

### Procedure

**Step 1** In the Cisco Spaces **Home** page, click **Dashboard** and choose **Location Analytics**.
The **Location Analytics Home** page is displayed.

**Step 2** From the left panel, choose **Reports** > **Overview**.

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




**Note**

- By default, the report is displayed for the root location, all SSIDs and for the last 365 days. You can filter the report by location, date range, and SSID.
- The SSID filter option is available only to 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 7: Date Range Options***

| Date Range | Description |
|---|---|
| Today | Total number of visits every hour of the current date |
| Yesterday | Total number of visits every hour of the previous day |
| Current Week | Total number of visits on each day of the current week |
| Previous Week | Total number of visits on each day of the previous week |
| Current Month | Total number of visits on each day of the current month |
| Previous Month | Total number of visits on each day of the previous month |
| Current Year | Total number of visits on each day of the current year |
| Custom | Total number of visits on each day of the time range specified. In the **Custom Date Range** pop-up window, specify the start and end date and click **Apply**. |

**Note**
To view the visit details for a particular day, hover over that day on the graph.

**Step 5** From the **All SSID** drop-down list, select the SSID for which you want to view the report.

The **Overview** window displays the Location Analytics report as per the selected filter options.

**Step 6** View the following information in the Location Analytics report in the tile format:

***Table 8: 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 |

| Report Item | Description |
|---|---|
| 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<br>**Note**<br>• 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.<br>• Visits having a duration of more than 1440 minutes are excluded. This helps to exclude devices that are always on, and contribute to inflating the average duration metric. |
| Dwell Time Distribution | The dwell time break-up for the visits occurred in the filtered location during the period specified for selected SSIDs |
| Path widget | The visitor traverse pattern between locations and also the percentage of visits at various floors or zones within the same **Network**. In your custom report, hover the mouse over any floor or zone in the **Path widget** to view the exact visit count. You can filter using only the locations available below the **Network** to view the path analytics. The **Path widget** is available only to the ACT license users. |

**Note**
You can view the **Visitors Trend**, **Visits Trends** and **Dwell Time Ditribution** information in graphical format also.

# Compare Reports

You can compare Location Analytics reports based on various filter parameters and thereby analyze the trends and visitor pattern. To compare reports, choose **Location Analytics** > **Reports**. The Reports menu has the following three options: **Compare Locations**, **Compare Dates** and **Compare SSIDs**.

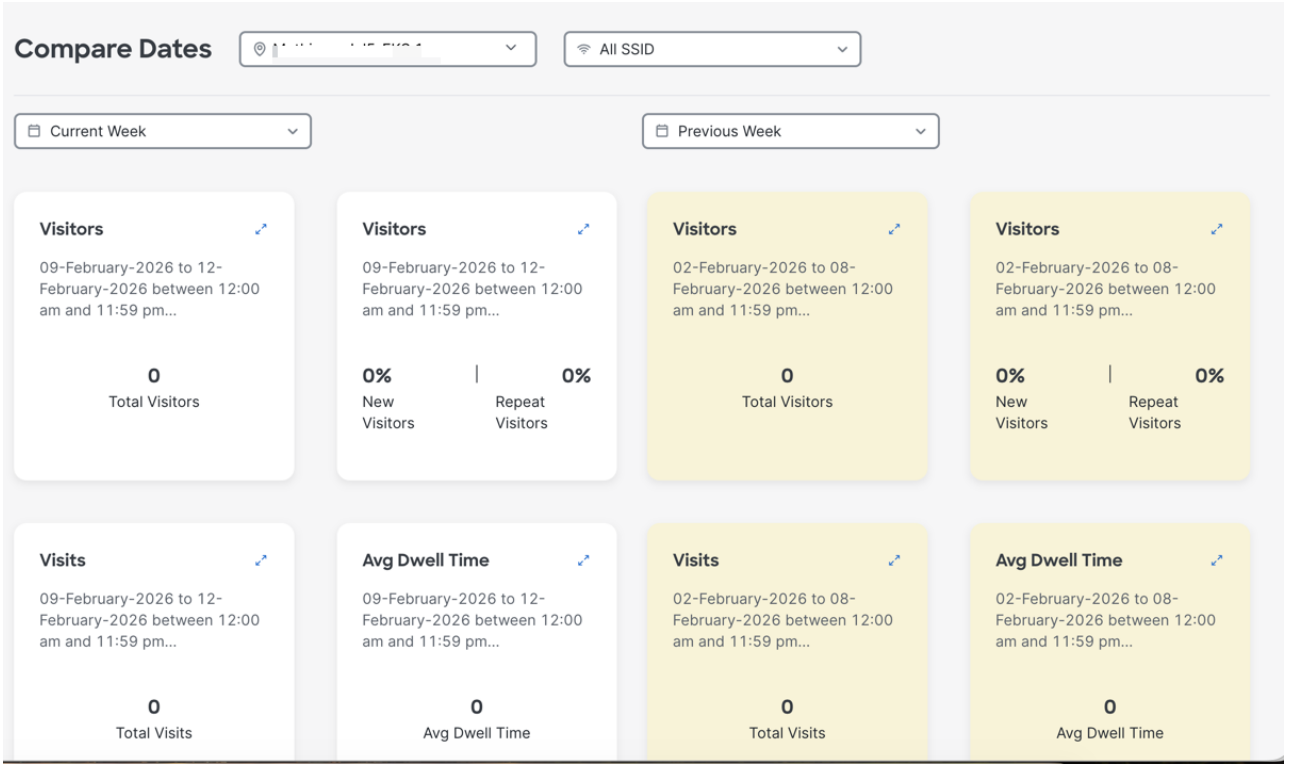
- **Compare Locations**: Use this tab to compare two location reports and view the visitors' trend. By default, two locations with most number of visitors are considered for the report. Visitor data must be available for atleast two network locations to display as charts. In the **Compare Locations** window, from the **Locations** drop-down list displayed at the top, select the locations to compare and view the reports.
- **Compare Dates**: Use this tab to choose two specific dates or date range and view the report. By default, the current week is selected as date range for the first report and previous week for the second report. In the **Compare Dates** window, from the **Date** drop-down list displayed at the top, select the required date range options to compare and view the reports.

- **Compare SSIDs**: Use this tab to compare two different SSIDs and view the visitors' trend. By default, two SSIDs with most number of visitors are considered for the report. In the **Compare SSIDs** window, from the **SSIDs** drop-down list displayed at the top, select the required SSIDs to compare and view the reports.

Depending on the selected compare options, the Location Analytics reports are displayed on the left and right side of the Location Analytics window. You can compare the Location Analytics report displayed on the left side (white background) aganist the report displayed on the right side (yellow background).

**Note** You can also use the filter parameters available on the top of the window to view the Location Analytics report.

***Figure 10: Compare Report Options***




# Create Custom Report

Use the **Custom Reports** option to create custom location analytics reports based on filters that you can apply to the default report types.

You can create custom reports based on the following default report types that are available:

The **Custom Reports** feature helps to view the default location reports and also create custom-tailored reports. The **Custom Reports** window displays all available reports, default overview reports and reports with compare options along with the number of reports in each category.

The three categories are:

- All Reports
- Overview
- Compare Reports (reports with all categories)

Use the **Custom Reports** feature in the Location Analytics app to create a report with the default filter parameters and save this as the default Location Analytics report for reference. While creating the default Location Analytics report, default filter parameters are considered such as all locations, last 365 days date range and all available SSIDs. The filter parameters at a global level are not available to filter this default Location Analytics report.

In addition to the default Location Analytics report, you can create custom reports by including any one available report type and multiple widget filters.

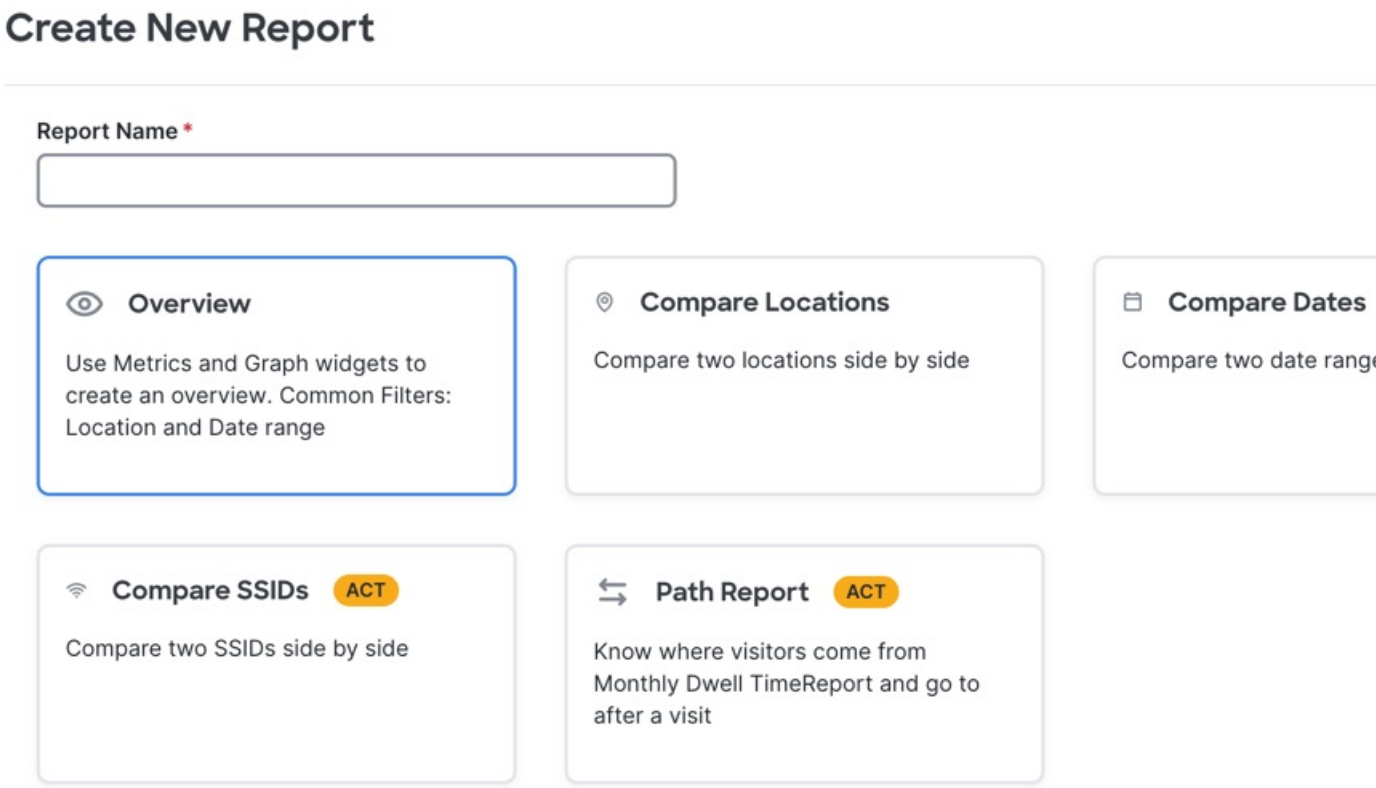
Each custom report can include multiple widgets. You can create widgets with different combinations of report types, locations, time period, SSIDs, visit ranges, and view by options. You can add more than one widget with same report type in a custom report.

### Procedure

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

**Step 2** Click **Create New Report**.

The **Create New Report** window is displayed.




**Step 3** In the **Report Name** field, enter the name for the new report.

**Step 4** Select a report type.

The available options are:

- **Overview**
- **Compare Locations**
- **Compare Dates**
- **Compare SSIDs** (Available only for 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 availble 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.

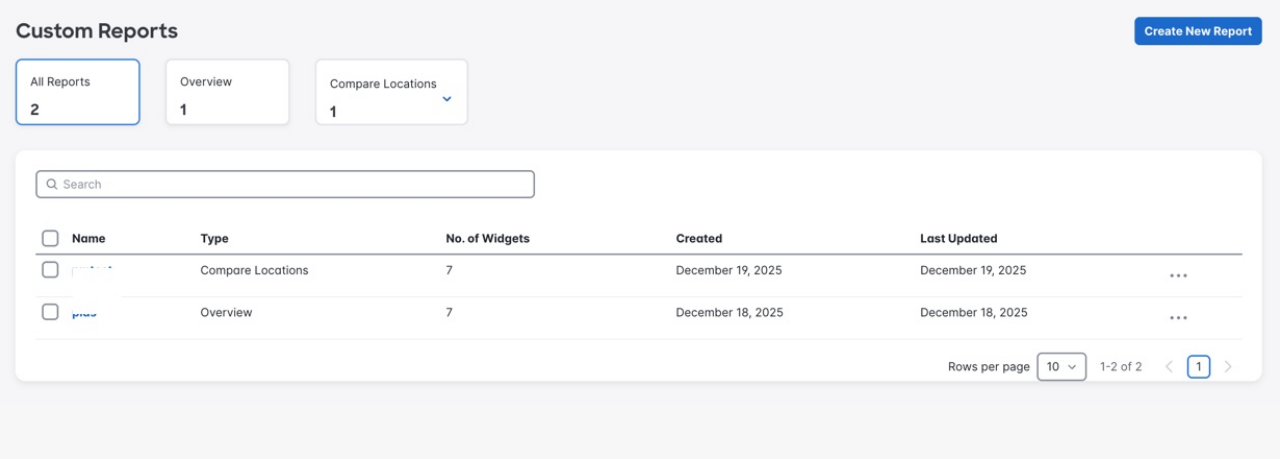
The following SSID options will be available for selection:

- **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.




**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.

# Add Widget

You can add more widgets to your custom reports while editing a report.

**Procedure**

**Step 1** In the **Location Analytics** window, click **Custom Reports** from the left panel.

**Step 2** Select the report to edit.

The selected Location Analytics report is displayed.

**Step 3** Click the three dots icon on the top-right of the window.

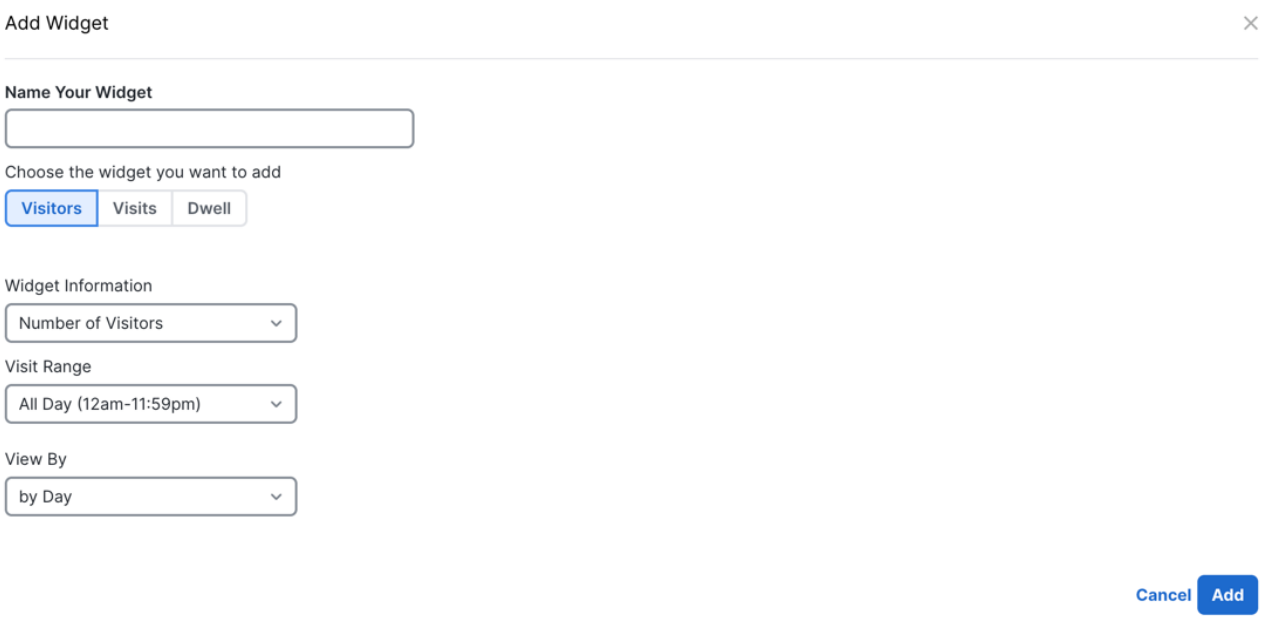
**Step 4** Click **Edit Report**.

The report is displayed in edit mode.

**Step 5** Click **Add Widget**.

The **Add Widget** pop-up window is displayed.

*Figure 11: Add Widget*




**Step 6** Enter the following information:

a) **Name Your Widget**: Enter the name for the new widget to be added.

b) **Choose the widget you want to add**: Click the widget that you wanted to add. The widget available are **Visitors**, **Visits** and **Dwell**.

c) **Widget Information**: From the **Widget Information** drop-down list, select the information that must be included in the widget. The options vary depending upon the widget selection. The options available are:

- For **Visitors** widget: **Number of Visitors** and **New vs Repeat**
- For **Visits** widget: **Number of Visits** and **New vs Repeat**
- For **Dwell** widget: **Distribution**

d) **Visit Range**: From the **Visit Range** drop-down list, select the date range for the report.

The following options are available:

- **All Day**: The visits happened during the entire day ( 12 am to 11:59 pm) are included in the report.
- **Mid Night**: Only the visits during mid night (12 am to 2:59 am) are included in the report.
- **Early Morning**: Only the visits during early morning (3 am to 4:59 am) are included in the report.
- **Morning**: Only the visits during morning (5 am to 8:59 am) are included in the report.
- **Business Hours**: Only the visits during business hours (9 am to 4.59 pm) are included in the report.
- **Evening:**: Only the visits during evening (5 pm to 8:59 pm) are included in the report.
- **Late Evening**: Only the visits during late evening (9 pm to 11:59 pm) are included in the report.
- **AM**: Only the visits during early morning (12 am to 11:59 am) are included in the report.

- **PM**: Only the visits during late evening (12 pm to 11:59 pm) are included in the report.

**Step 7** Click **Next**.

The **Add Widget** pop-up is displayed with the following tabs: **Location**, **Date Range** and **SSIDs**. You can click these tabs and choose the required options and add them.

**Step 8** Click **Locations** tab.

a) (Optional) In the **Search Location** field, enter the name and search for locations. You must enter a minimum of 3 characters to perform the location search.
b) Select the root location or click to expand and select the required zone or floor.
c) From the **View By** drop-down list, select the time duration for which you want to see the report for selected location.

- **Day**: The report displays the visit data for each day of the specified period.
- **Hour of Day**: The report displays the visit data for each hour of the day. The visit count for a particular hour will be total visits occurred during the specified period at that particular hour. For example, in the **Hour of Day** report for November 2022, the visit count displayed at 2:00 PM will be the total of number of visits occurred between 2.00 PM and 2:59 PM during the entire month of November 2022.
- **Week**: The report displays the visit data for each week in the specified period.
- **Day of Week**: The report displays the visit data for each week in the specified period with visit count for each day on that particular week.

**Step 9** Click **Date Range** tab.

a) From the **Date Range** drop-down list, select the time duration for which you want to see the report.

   If you choose **Custom** as the date range, enter the start and end dates in the **Start Date** and **End Date** fields.

b) From the **View By** drop-down list, select the time duration for which you want to see the report.

   By default, the **View By** option selected in the **Locations** tab is displayed. You can update the time duration if required and the change is reflected in the **Locations** and **SSIDs** tabs.

**Step 10** Click the **SSIDs** tab.

a) From the **SSIDs** drop-down list, select the SSID.
b) From the **View By** drop-down list, select the time duration for which you want to see the report.

   By default, the **View By** option selected in the previous tab is displayed. You can update the time duration if required and the change is reflected in the other tabs.

**Step 11** Click **Add**.

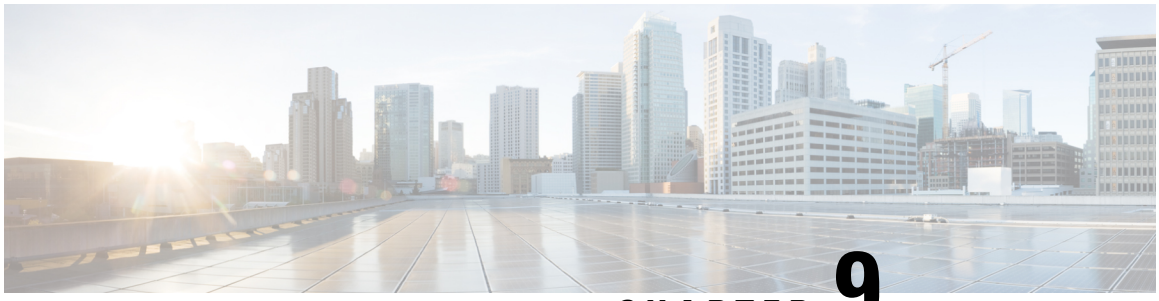
The prompt `Place Widget Here` is displayed and you can click on the blue highlighted area to insert the new widget.

# Location-Based RBAC

A location-based RBAC role is a user access control setting that

- restricts a user's access to data and features based on assigned physical locations,
- enables administrators to specify which locations a role applies to during role creation or user invitation, and
- ensures that users can view only the data for the locations to which they are invited.

For more information, refer to Location-Based RBAC (Role-Based Access Control) in Cisco Spaces, on page 139.



CHAPTER 9

# Cisco Spaces: Detect and Locate App

This chapter describes the Cisco Spaces: Detect and Locate app.

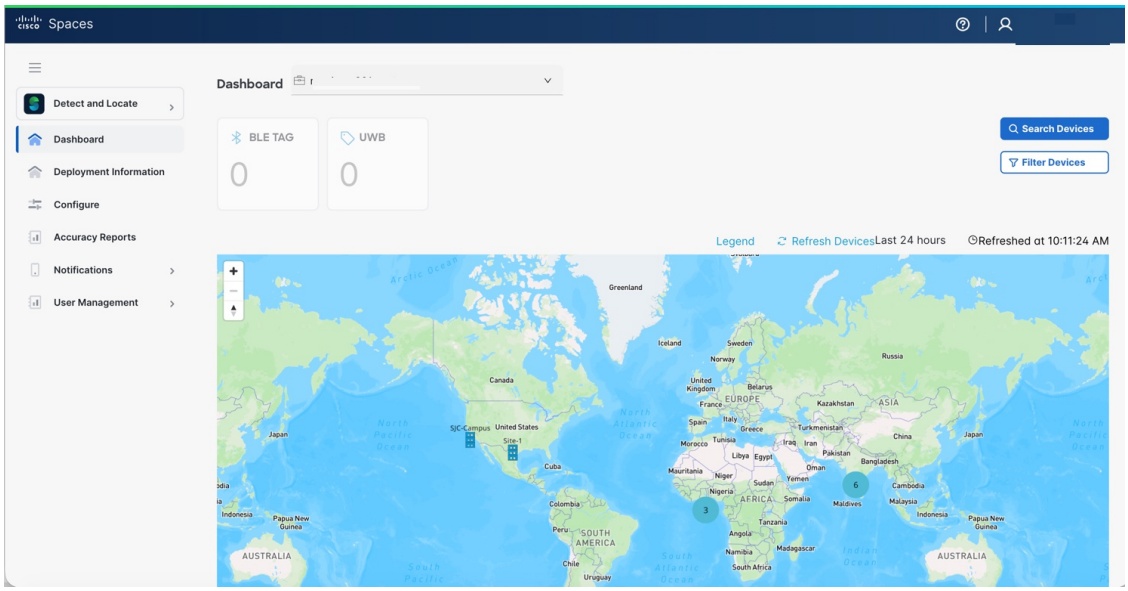

- Overview of Cisco Spaces: Detect and Locate App, on page 83


# Overview of Cisco Spaces: Detect and Locate App

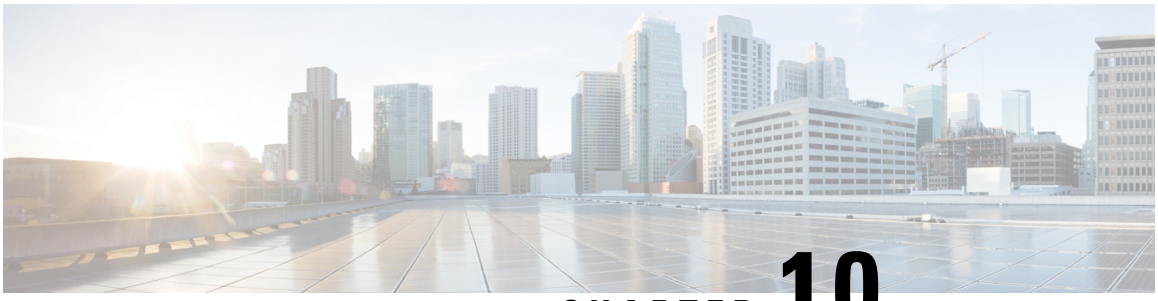
**Cisco Spaces: Detect and Locate** app enables you to view the current and historic location of Wi-Fi devices in your deployment.

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

***Figure 12: Detect and Locate App***




For more information on the **Detect and Locate** app, see Cisco Spaces Detect and Locate Configuration Guide.



CHAPTER 10

# Cisco Spaces: Space Utilization App


- Work with Space Utilization App, on page 85


## Work with Space Utilization App

The Cisco Spaces: Space Utilization App offers historical insights into how your physical spaces are used, aiding in space optimization. These insights are gathered from data collected via sensors embedded within your space's networking and collaboration infrastructure.

This app allows you to view the occupancy and utilization for any physical space within a campus, building, or floor. This information includes data such as people count, peak utilization metrics, room utilization metrics and time spent by people in that physical space.

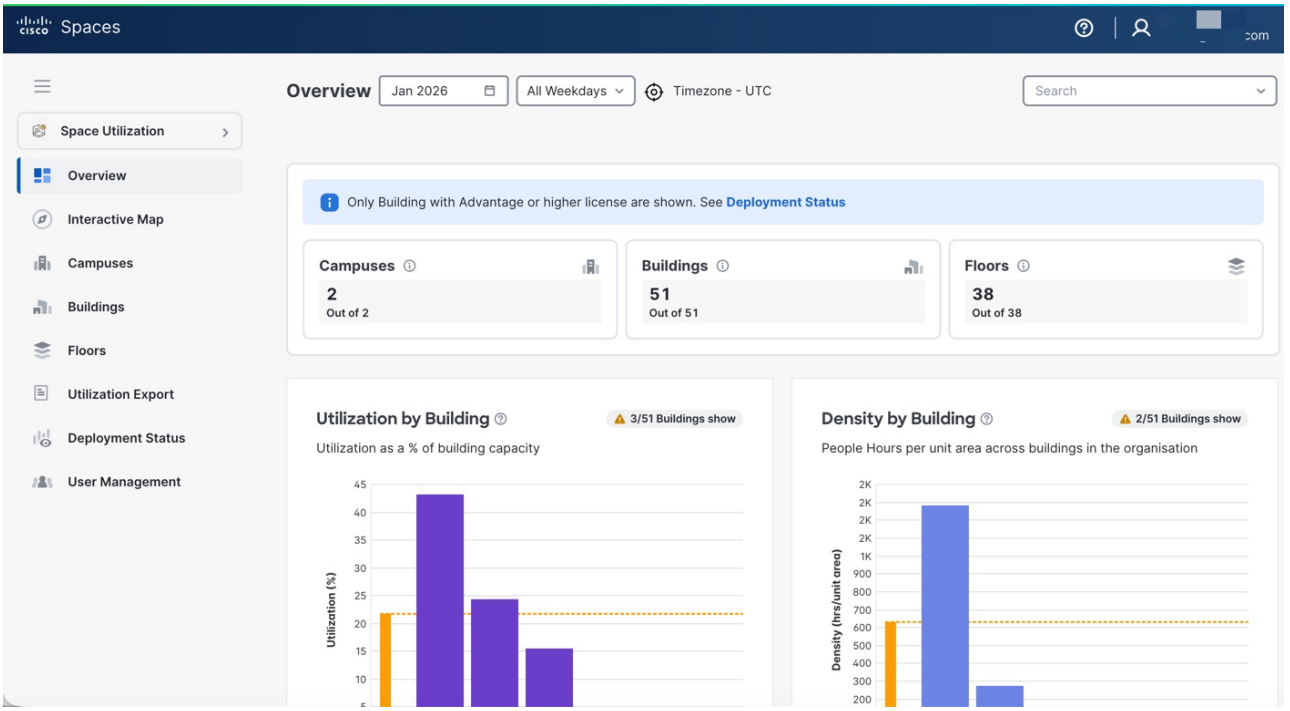
For Cisco Spaces accounts in the Workspace and Education verticals, both Floor Occupancy and Room Occupancy metrics are displayed. By default, for accounts in all other verticals, the following message is displayed: *Occupancy charts are only available to Workspaces / Education vertical*.

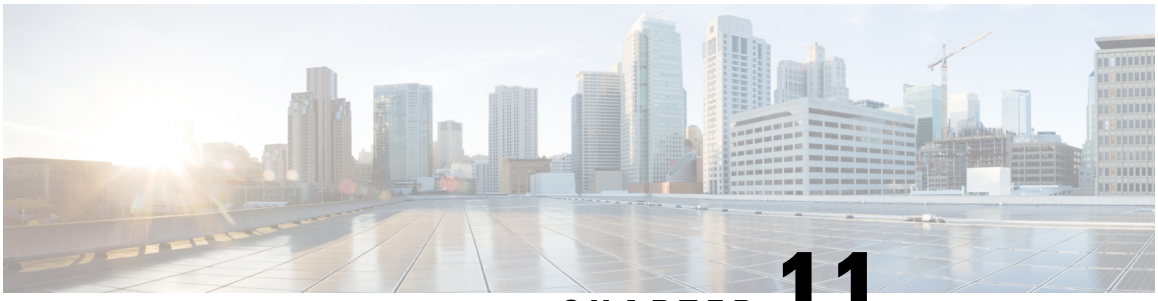
Use **Room Occupancy Reports** feature to generate an occupancy report with the data including the number of people present in the room that is aggregated in a window of every 15 minutes. This feature provides the flexibility to download and categorize the people count data based on their preferred reporting time intervals, such as 15, 30, or 60 minutes.

The Glossary enhancements in the **Space Utilization** app provide a consolidated and comprehensive set of definitions for the various metrics and charts available across all views within the **Space Utilization** application. These definitions enhance user understanding and provide clarity on how data is presented and calculated.

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

*Figure 13: Space Utilization App*





CHAPTER 11

# Cisco Spaces: Smart Workspaces App

The Cisco Spaces: **Cisco Smart Workspaces** app offers applications like **Space Manager** and **Space Experience** for your wireless deployments that are used to make your workspace hybrid-work-ready. These applications enhance and provide seamless digital experiences for your visitors through metrics such as occupancy, noise & air quality, and meeting room capacity and availability.

The **Space Manager** app allows you to have a view of real-time occupancy and environment updates like humidity, air quality, and noise levels across buildings, floors, and meeting rooms. Meanwhile, the **Space Experience** app enables signage management through Cisco Spaces.

**Note** These applications are associated with these types of licenses:

- ACT (displayed in the UI as Advantage)
- UNLIMITED
- PREMIER_W
- PREMIER_CW

• Working with Cisco Spaces: Smart Workspaces, on page 87

# Working with Cisco Spaces: Smart Workspaces

To support **Cisco Smart Workspaces** solution, two new apps are available:

- **Space Manager**: Use this app to configure various devices and sensors, to provide access to real-time occupancy data and environment telemetry (heat map, indoor air quality, temperature, humidity, and noise levels) rendered on digital maps for a specific building, floor, or meeting room.
  - In the **Devices** section, you can view the configured devices and their telemetry details on digital maps.
  - The **Manage Rooms** section displays the configured meeting room and allows you to view, add, or remove devices and sensors to and from the selected meeting room.
- **Space Experience**: Use this app to perform these:
  - Create and manage signage for **Cisco Smart Workspaces**

- Onboard new signage for a non-Webex device.
- Configure the telemetry parameters and publish the signage.
- Configuration updates are auto-notified to the corresponding signage devices.

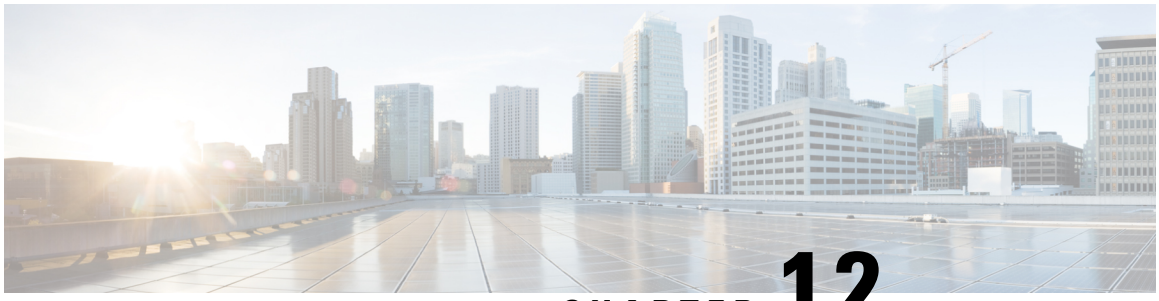
For more information, refer to Cisco Spaces: Smart Workspaces Solution Federal Support Guide.



# PART VI

# Location Hierarchy


- Location Hierarchy (Earlier Version), on page 91



CHAPTER 12

# Location Hierarchy (Earlier Version)

This chapter provides information on how to set up the earlier version of Location Hierarchy.

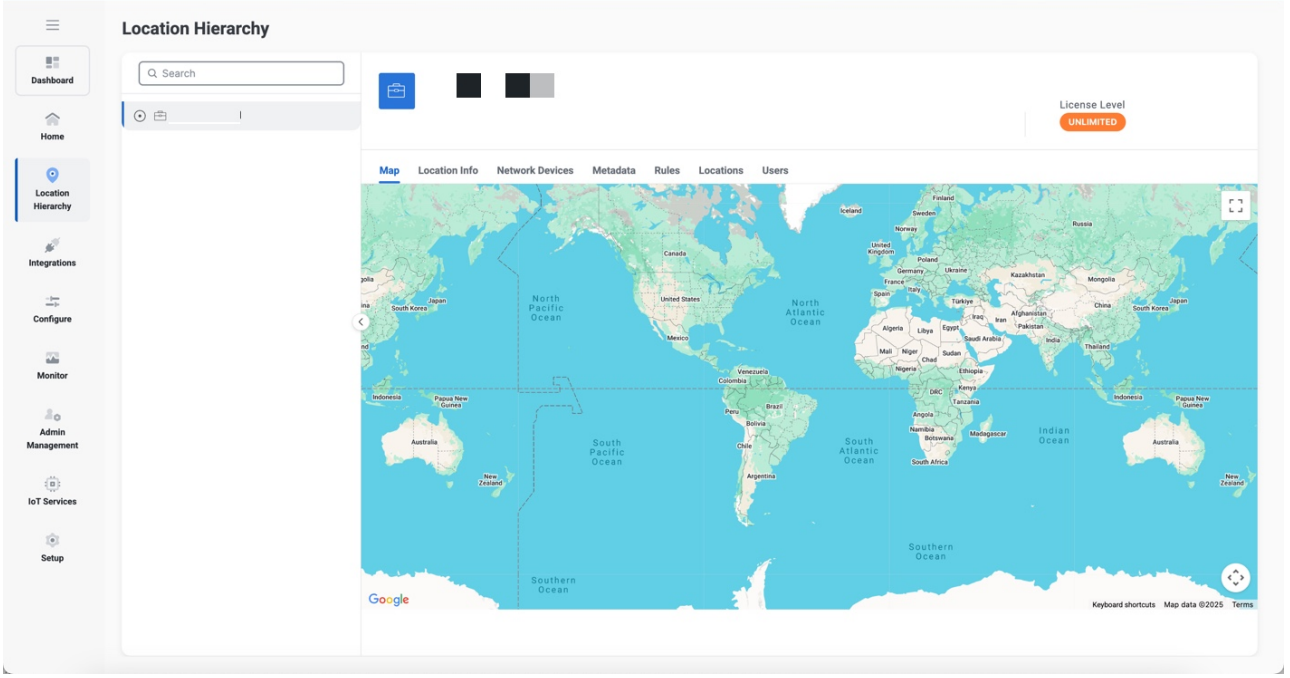

- Location Hierarchy, on page 91
- Manage Locations in Map view, on page 93
- Update Location Information, on page 96
- View the Network Devices, on page 98
- Configure Metadata, on page 98
- View Locations, on page 99
- View Users, on page 103


## Location Hierarchy

The **Location Hierarchy** feature simplifies importing locations in the same structure that you define 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 in Location Hierarchy.

In **Location Hierarchy** window, the default customer name (root location) is automatically selected, and the **Map** tab displays the location on the map.




The left pane of the **Location Hierarchy** window displays the imported root locations with the default customer name (root name). You can click the plus sign to expand and view the hierarchy. You can view the buildings and the associated floors in the root location.

If you select a root location from the left pane, you can also view additional information related to the number of organizations, campuses, wireless controller, buildings, groups, floors and zones.

For a selected location, building or floor, additional information is displayed in the following tabs:

- **Map**: Displays the selected location on the map
- **Location Info**: Displays the location data information
- **Network Devices**: Displays all the connected network devices and running devices and view the count of these devices
- **Metadata**: Displays the configured metadata information
- **Locations**: Displays the location nodes
- **Users**: Displays the users

You can perform the following additional tasks in the **Location Hierarchy** window:

- **Rename**: Click the three dots next to the location and click **Rename Location** to edit the location name.
  - For the root location, only the option to rename the location is displayed.
  - For all other locations except the root, both the options to rename and delete the location is displayed.
- **Delete**: Click the three dots next to the location and click **Delete Location** to delete the location from **Location Hierarchy**.

**Location Hierarchy** shows rich maps, if they are available for a particular floor. The option to upload rich maps is currently available under **Setup** > **Locations & Maps**. Click the **3D** toggle button to switch between 2D and 3D floor maps.

In **Location Hierarchy**, only those locations that a Cisco Spaces user can access are displayed. The accessibility to these locations are defined when you create or edit roles or invite or edit the Cisco Spaces user in **Admin Management**.

# Manage Locations in Map view

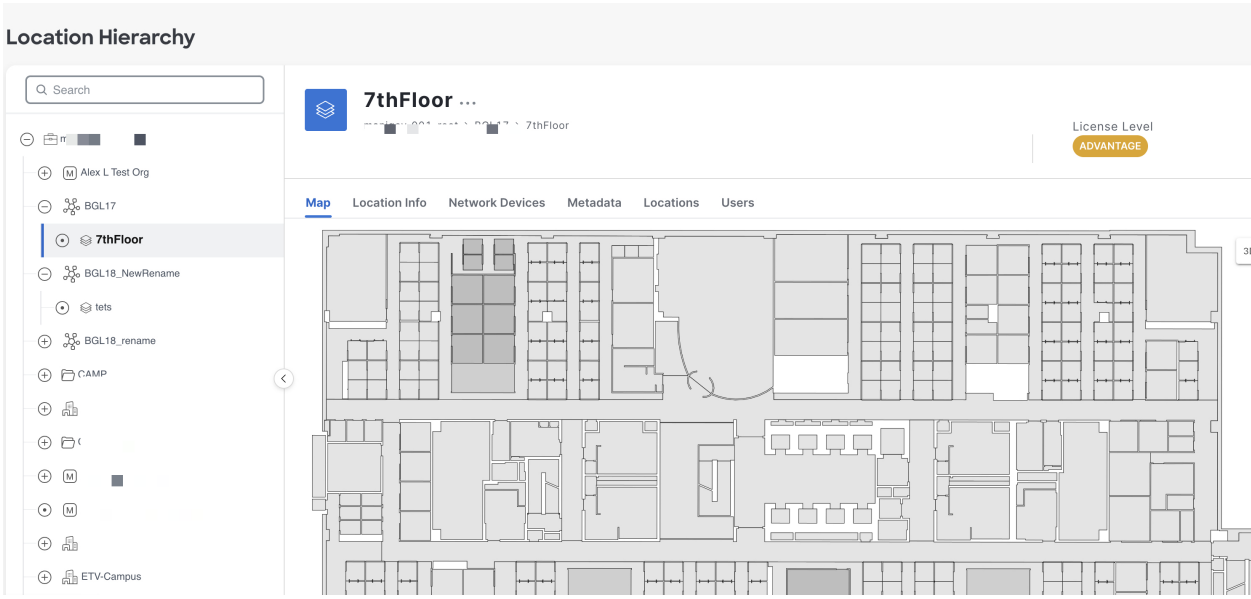
Use the **Map** tab (**Cisco Spaces dashboard** > **Menu icon ( )** > **Location Hierarchy** > **Root Location**) to view the selected location, campus, building and floor information on the map.

The **Map** tab displaies differnet map types such as default world map, latitude and longitude based maps, and 2D or 3D floor maps.

If you select the root location, the default world map is displayed.

However, in some instances, the map automatically zooms into the precise location on the map and is displayed with a 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 14: Map Tab***




If you select a building, the default world map is displayed.

If you select a floor, the exact floor map image is displayed. Use the Polygon tool ( ) to create zones. For more information, refer to Create a Zone for a Floor Location, on page 94.

Depending on the location you select, view these information:

- Organization

- Campus
- Building
- Floor
- Zone

# Create a Zone for a Floor Location

Use the **Map** tab to create Cisco CMX zones in **Location Hierarchy**.

The current implementation creates and updates polygon zones from the floor map for supported floor maps. Zone creation is available only when the selected floor has Full access and a 2D floor map is available.

**Note** Currently, Cisco Meraki zone-based reports are only supported in the **Live Occupancy** application and **Firehose** device location update events.

In Location Hierarchy, 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 Location Hierarchy.

### Procedure

**Step 1** Log in to Cisco Spaces.

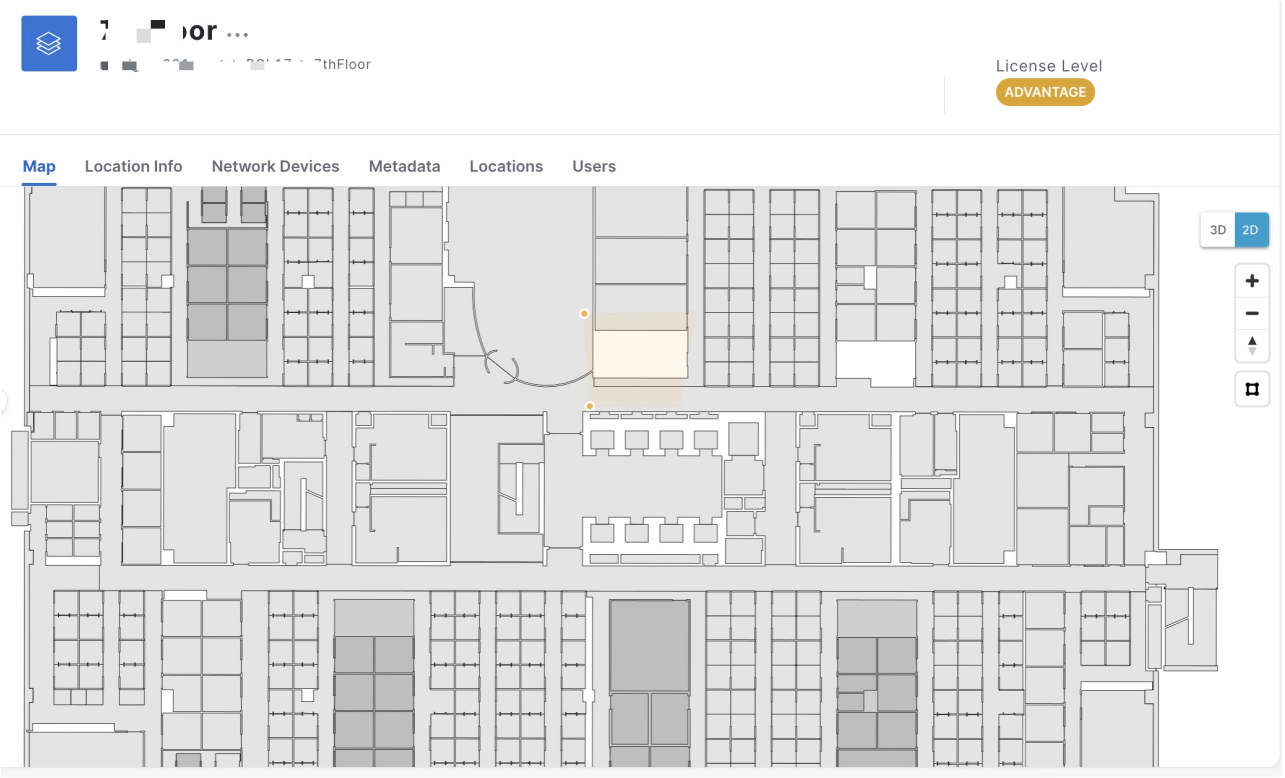
**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Location Hierarchy**.

The **Location Hierarchy** window is displayed.

**Step 3** In the left pane, navigate to the required floor location.

The floor map is displayed.

*Figure 15: Map Tab*




**Step 4** Click the Polygon tool ( ⌗ ) on the map.

The cursor changes to a plus icon.

**Step 5** Click the required map area and move the cursor to draw a polygonal zone of your choice.

**Step 6** Double-click to complete the zone creation.

A pop-up window is displayed on the right pane.

**Step 7** In the **Zone Name** field, enter the new zone name.

**Step 8** Select the overlay color to distinguish the zone.

**Step 9** Click **Save**.

- The new zone is created, and the **Location Hierarchy** window is refreshed to display the root location.
- In the left pane, navigate to the floor where you created the new zone and the zone is now listed as a new item under the floor hierarchy.

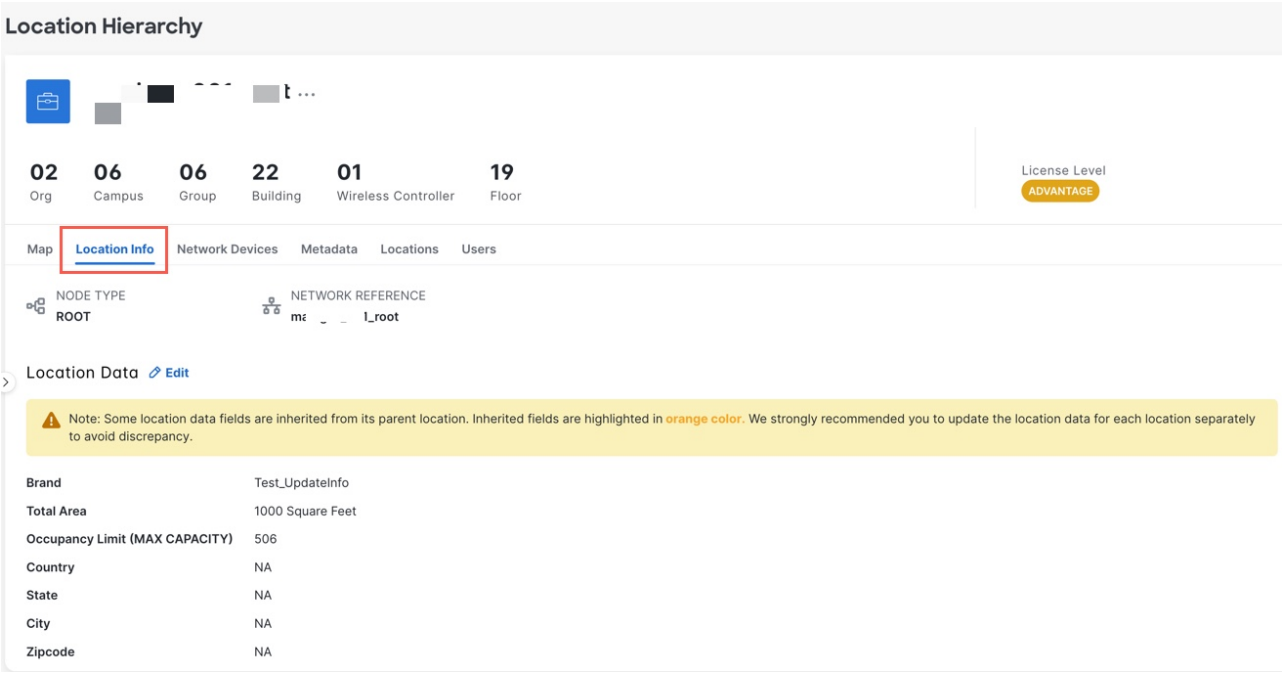
**Step 10** (Optional) Click the Polygon tool ( ⌗ ) on the map to update the zone details.

# Update Location Information

Use the **Location Info** tab (**Cisco Spaces dashboard** > **Menu icon (☰)** > **Location Hierarchy** > **Root Location**) to view and edit the location information.

For the selected location, the **Node Type** and **Network Reference** details are displayed.

***Figure 16: Location Info Tab***




Click **Edit** to update location information. For more information, refer to Edit Location Info, on page 96.

**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

**Procedure**

**Step 1** Log in to Cisco Spaces.

**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon (☰) and choose **Location Hierarchy**.

The **Location Hierarchy** window is displayed.

**Step 3** In the left pane, navigate to the required location.

**Step 4** Click the **Location Info** tab.

**Step 5** Click **Edit** next to **Location Data**.

The slide-in window is displayed.

**Step 6** Update the following location information as required:

a) **Location Name**: Edit the name of the location.
b) **Brand**: Edit the name of the brand.
c) **Total Area**: Edit the total area details. The value must be numeric and cannot include commas.
d) **Unit**: Select the unit for the total area entered. The options are **Square Feet** and **Square Meter**.
e) **Occupancy Limit (Max Capacity)**: Enter a positive integer.
f) **Address**: Enter the address details and select from the displayed options. The selected address is plotted on the map displayed on the right side.
g) **Latitude and Longitude**: Edit decimal coordinates directly or drag the marker on the map. Values can be positive or negative decimal numbers and cannot include commas.
h) **Time Zone**: Select a valid -time zone from the searchable **Time Zone** list.

**Step 7** Click **Save**.

# Edit Access Point Prefix

You can add APs of multiple prefixes to a network. For example, if you have APs with prefixes, AB, BC, and CA, and if you want to group the APs with AB and BC under one wireless network, you can do so.

The **Access Points Prefix Used** option will be available in the **Location Info** tab only for the network locations. However, the Access Points Prefix Used option will not be available for the **Unconfigured** network.

To add APs of multiple prefixes to a network of a Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller, follow these steps:

### Procedure

**Step 1** Log in to Cisco Spaces.

**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Location Hierarchy**.

The **Location Hierarchy** window is displayed.

**Step 3** In the left pane, navigate to the required network.

**Step 4** Click the **Location Info** tab.

**Step 5** Click **Add/Edit** next to **Access Point Prefix Used**.

**Step 6** In the **Add/Edit Prefix** window, in the **Prefix** field, enter the prefix.

The access points with the prefix entered get listed.

**Step 7** Click **Add Prefix**.

The newly added prefix gets listed under **Added Prefixes** in the right pane of the window. **Add Prefix** is enabled only if the APs with prefix entered are available.

**Step 8** Click **Save**.

After adding the prefix, the APs under the **unconfigured** network with this prefix is moved to this network.

# View the Network Devices

Use the **Network Devices** tab (**Cisco Spaces dashboard** > **Menu icon (☰)** > **Location Hierarchy** > **Root Location**) to view all the network devices under the selected node. The root location displays all the connected devices available within the location hierarchy.

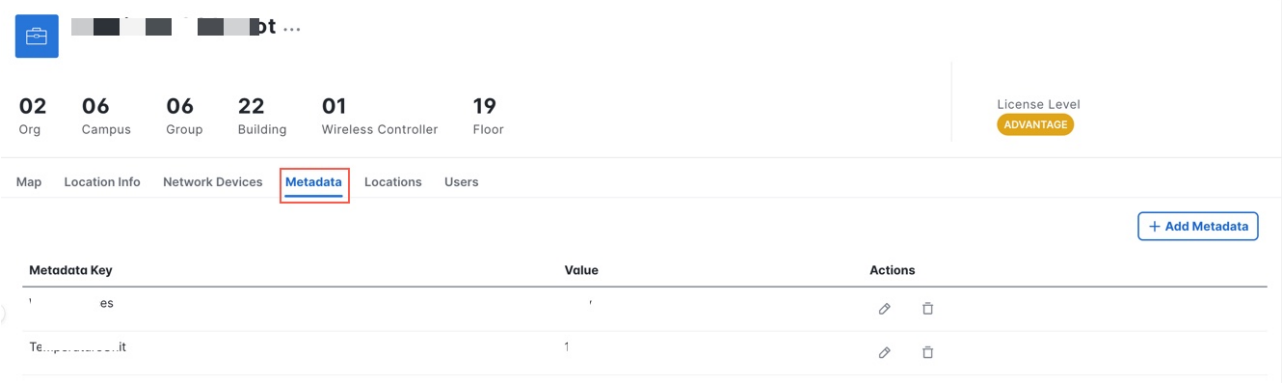
Depending on the selected location, you can view the following information:

- **Access Points**: Displays the name of the AP, MAC address and the location hierarchy path. Use the **Search Table** field to search for a specific AP. Click the copy icon next to the **Location** field to copy the hierarchy path. Navigate to the **Setup** window to configure the AP.
- **Cameras**: Displays the connected camera details such as camera name, serial number, MAC address and status of the trip-wire as a set or not. Use the **Search Table** field to search for a specific camera. Navigate to the **Connect your Meraki Camera** window to connect additional devices.
- **Security Appliances**: Displays the detailed list of security appliance devices for the respective locations.
- **Webex Devices**: Displays the connected Cisco Webex devices.
- **Linked Devices**: Displays the linked devices configured for this location. You can link IoT Devices, Non Webex Signages and Smart PUDs.

# Configure Metadata

Use the **Metadata** tab (**Cisco Spaces dashboard** > **Menu icon (☰)** > **Location Hierarchy** > **Root Location**) to view the metadata information. If metadata is not configured yet, click **Add Metadata** to add metadata. For more information, refer to Add Metadata, on page 99.

***Figure 17: Metadata Tab***



Depending on the selected location, you can view the following information:

- **Metadata Key**: Displays the metadata key.
- **Value**: Displays the value for the metadata key. The value can be alphanumeric and accepts special characters also, for example, xyz123@.

# Add Metadata

**Procedure**

**Step 1** Log in to Cisco Spaces.

**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Location Hierarchy**.

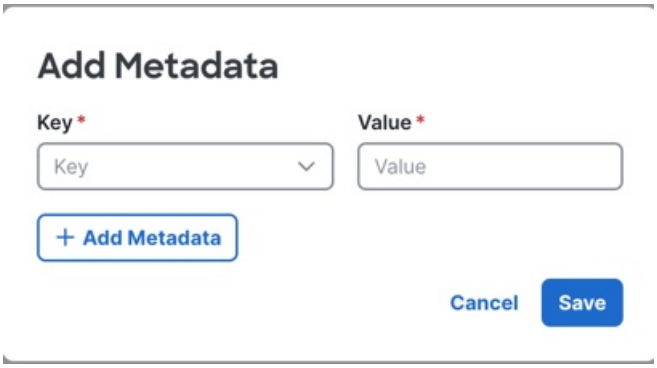
The **Location Hierarchy** window is displayed.

**Step 3** In the left pane, navigate to the required location.

**Step 4** Click the **Metadata** tab.

**Step 5** Click **Add Metadata**.

***Figure 18: 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**.

# View Locations

Use the **Locations** tab (**Cisco Spaces Dashboard** > **Menu icon ( )** > **Location Hierarchy** > **Root Location**) to view the location information such as **Location Type** and **Level**.

Use the **Location Type** and **Level** drop-down options to select the location preferences. The location types are:

- Network/Building
- Campus
- Group
- Organization
- Wireless Controller
- CMX

View these details for the selected location:

- Locations
- APs
- Camera
- Max Capacity
- Total Area (sqft)
- Time Zone

Select the required check box next to the location and click **Create Group** to add location to create your own group.

# Create a Group

Use this procedure to organize multiple child locations by creating a group.

**Before you begin**

- Verify that the parent building and the child location that you want to group already exist.
- Verify that your account has permission to update the location hierarchy.
- All selected locations must have the same parent node. If the selected locations belong to different parents, Cisco Spaces displays an error and does not create the group.

**Procedure**

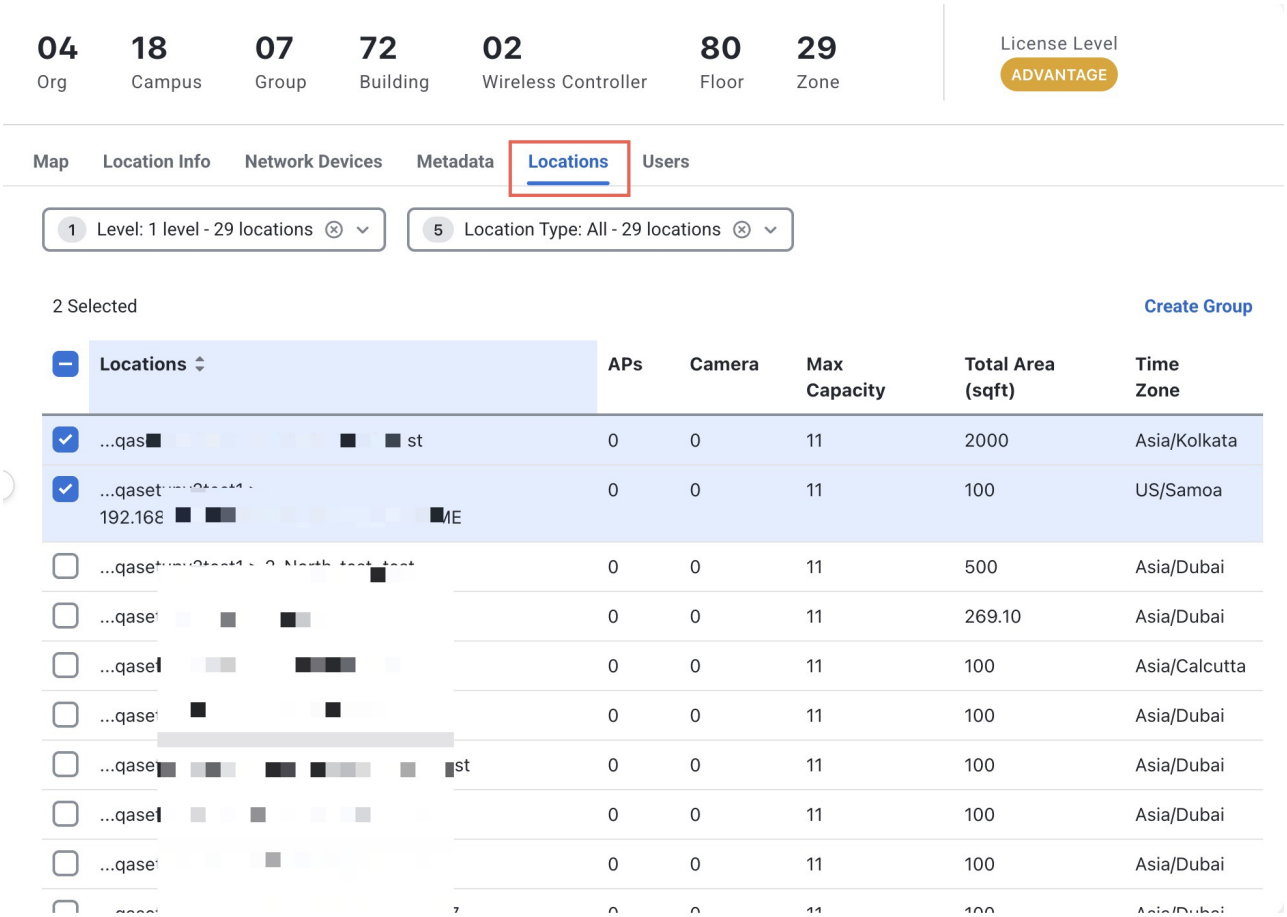
**Step 1** In the left navigation pane, click **Location Hierarchy**.

**Step 2** In the left pane, navigate to the location where you want to create a group.

**Step 3** Click the **Locations** tab.

**Step 4** Check the check box for each location that you want to add to the group.

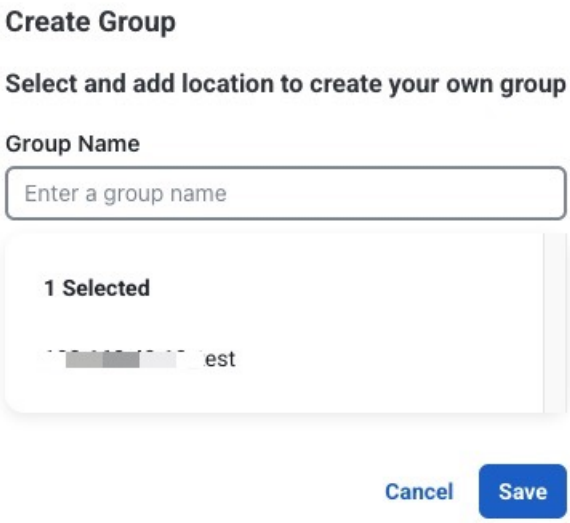
*Figure 19: Locations Tab*




**Step 5** Click **Create Group**.
The **Create Group** pop-up window is displayed.

**Step 6** In the **Create Group** pop-up window, enter a name in the **Group Name** field.

*Figure 20: Create Group*



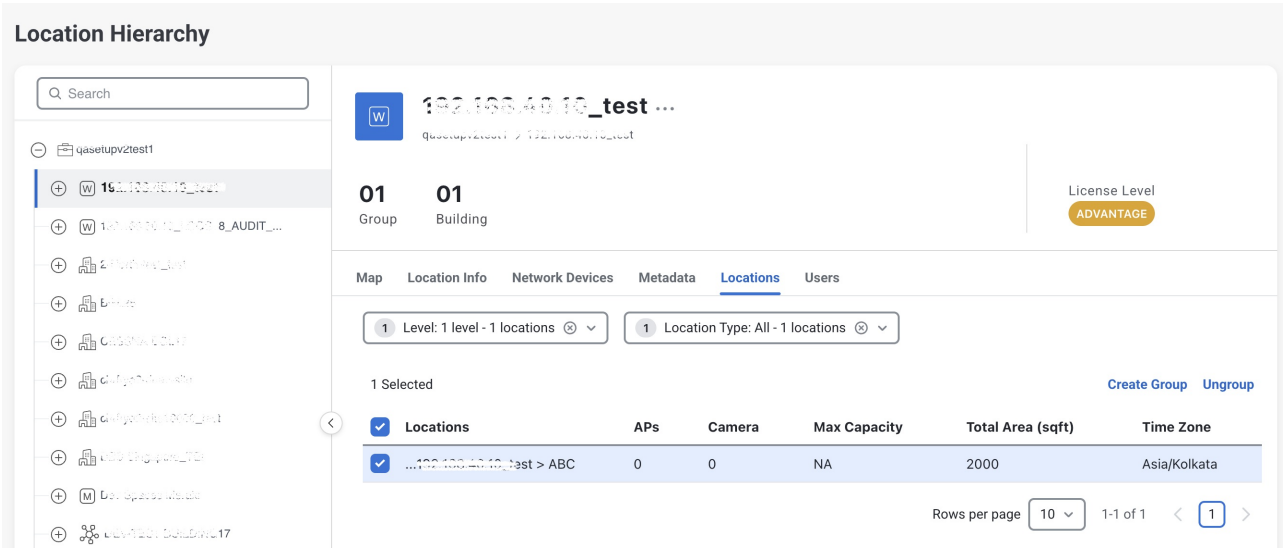

**Step 7** Review the selected locations, and then click **Save**.

**Step 8** Verify that the new group appears in the hierarchy under the selected building.
The new group is created under the selected building and moves the selected locations under that group. The building summary also updates to show the new group count.

**Step 9** (Optional) Perform these steps if required.

a) To ungroup the location, select a group row that has child locations and click **Ungroup**.

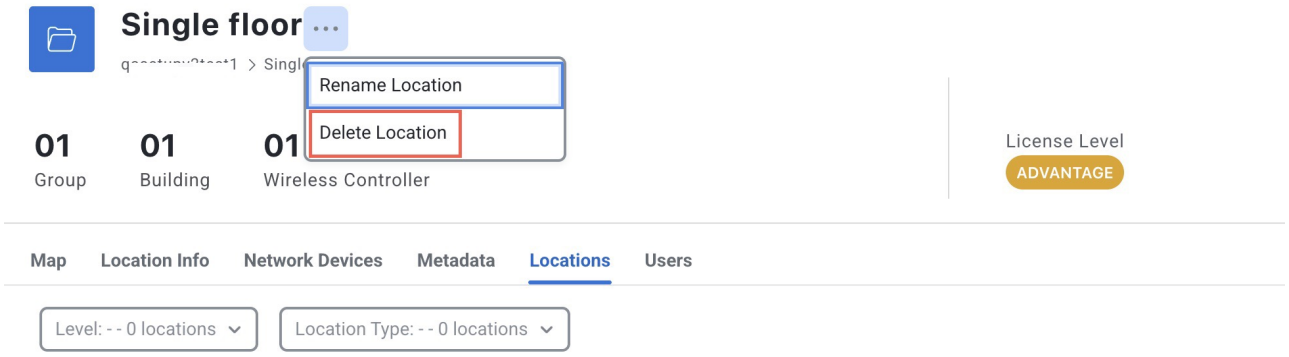
*Figure 21: Ungroup*




b) In the warning dialog, click **Yes** to confirm the ungroup action.

c) To delete a group or another non-root location, open the location action menu and click **Delete Location**.

*Figure 22: Delete Location*




# View Users

Use the **Users** tab (**Cisco Spaces Dashboard** > **Menu icon (** **)** > **Location Hierarchy** > **Root Location**) to view the users and their role permissions.

View these details:

- User
- Role
- Permissions: Read & Write
- Permissions: Read only
- Locations

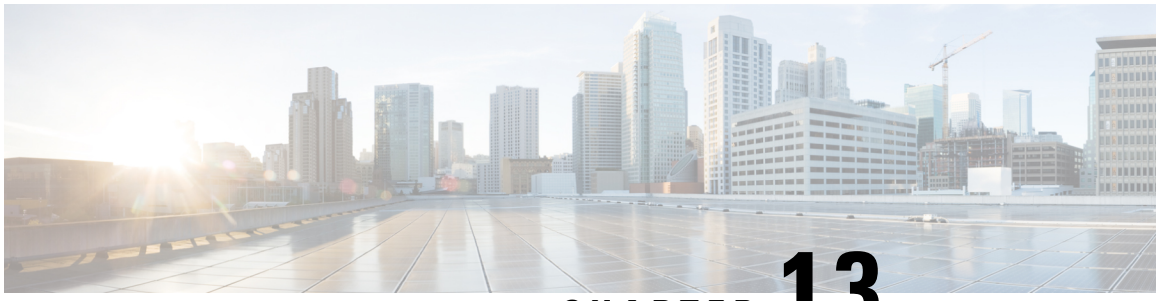
Use the **Search** option to search for users. You can click a user to edit the permission setting in the **Admin Management** > **Edit User** window.



# PART VII

# Integrations


- Cisco Catalyst Center (formerly known as Cisco DNA Center) Integration, on page 107
- Calendar Integrations, on page 111



CHAPTER 13

# 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 107
- Integrate Cisco Spaces with Catalyst Center, on page 108


## Overview

Cisco Spaces enables you to integrate with Cisco Catalyst Center (formerly known as Cisco DNA Center) so that you can monitor the Catalyst Center sites using Cisco Spaces.

**Note** The Catalyst Center and Cisco Spaces integration is currently limited to only automatic map exports and synchronization for the location hierarchy. The integration does not support captive portal-based authentication features.

For more information, refer to "About Cisco Spaces Integration" in the *Catalyst Center User Guide* at:

https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html

**Prerequisites**

- Catalyst Center, Release **2.1.2.3 or higher**.
- Catalyst Center must be able to connect to https://spaces-gov.cisco/ for the initial activation.
- You must connect your wireless network to Cisco Spaces using Cisco Spaces: Connector. To connect, log in to the Cisco Spaces dashboard and choose **Setup** > **Wireless Networks**.
- Catalyst Center checks SSL/TLS certificate revocation status using OCSP/CRL. TCP 80 is port used by Catalyst Center for outbound communication to device and other systems. To successfully verify the certificate revocation status, these URLs must be reachable both directly and through the proxy server that's configured for Catalyst Center. Otherwise, certificate revocation check will be skipped when Catalyst Center connects to cisco.com.

  http://validation.identrust.com

  http://commercial.ocsp.identrust.com

For more information, refer to "Communication ports" in the Cisco Catalyst Center Security Best Practices Guide.

# Integrate Cisco Spaces with Catalyst Center

To integrate Cisco Spaces with Catalyst Center, perform the following steps:

### Procedure

**Step 1** Log in to Cisco Spaces.

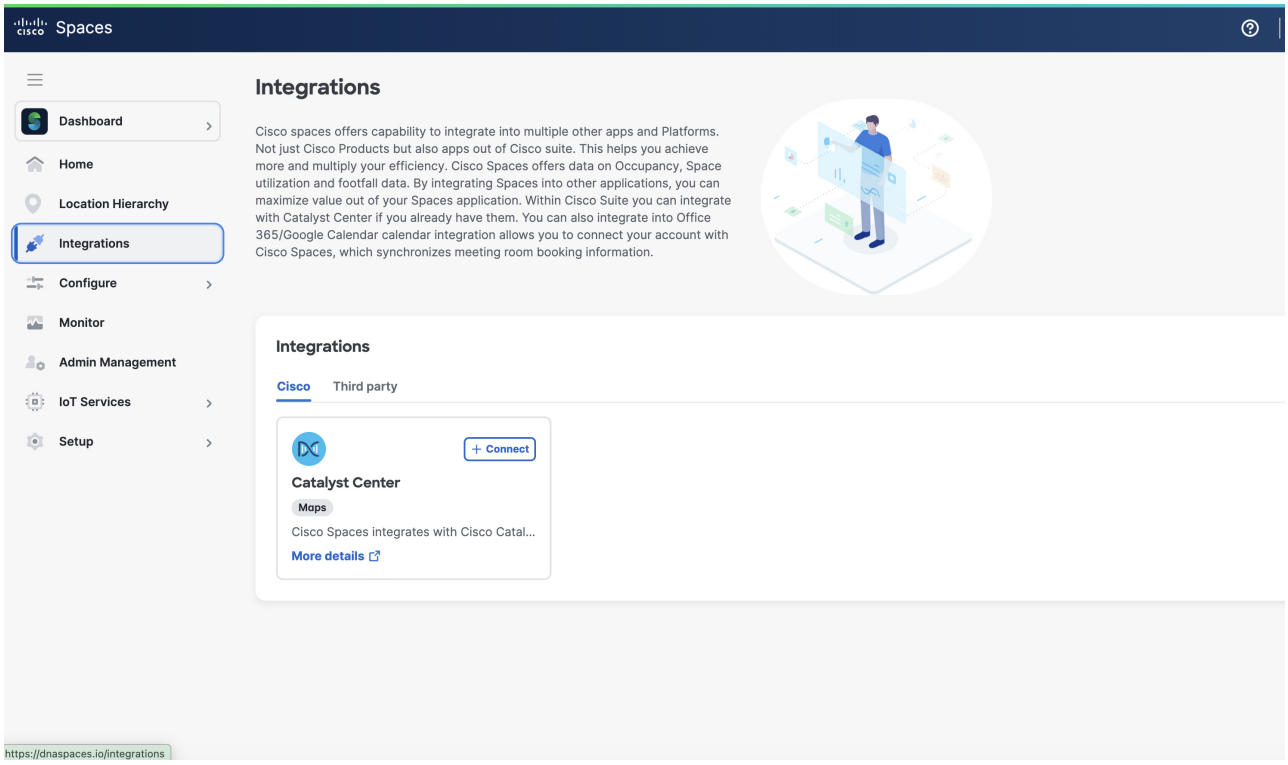
**Step 2** In the left navigation panel, choose **Integrations**.
The **Integrations** window is displayed

**Step 3** Under **Integrations**.

In the **Cisco** tab, **Catalyst Center** is displayed.

In the **Third party** tab, **Google Calendar**, **Office 365**, and **Hamina** are displayed.

***Figure 23: Integrations***




**Step 4** In the **Catalyst Center**, click **Connect**.
The **Cisco Catalyst Center Integration** window is displayed.

**Step 5** Click **Add Instance**.

**Step 6** In the **Create new token** pop-up window, enter the Catalyst Center instance name and click **Generate**.

A success message confirms that the new token is created and displays the token in the window. Copy the token.

**Note**
The new token remains valid for five minutes (5 min). If it expires, you can regenerate another token.

**Step 7** Click **Done**.

**Step 8** (Optional) In the **Token** column, click **View token** and use this tenant token in Catalyst Center.

A success message confirms that the new token is created and displays the token in the window. Copy the token.

**Note**
The new token remains valid for five minutes (5 min). If it expires, you can regenerate another token.

**Step 9** (Optional) Click **Done**.

**Step 10** Log in to Catalyst Center.

**Step 11** Click the **Menu** icon ( ) and choose **System** > **Settings**.

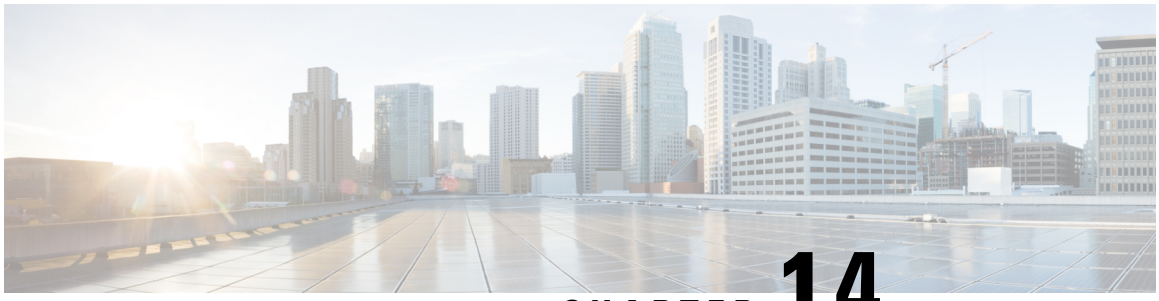
**Step 12** Click **CMX Servers/Cisco Spaces**.

**Step 13** In the **CMX Servers/Cisco Spaces** window, under the Cisco Spaces section, click **Activate**.

**Step 14** In the **Integrate Cisco Spaces** pop-up window, paste the tenant token and click **Connect**.

After the integration is complete with Cisco Spaces, the following success message is displayed: *This cluster is integrated with Cisco Spaces successfully*. The status is displayed as **Activated**.

After activating the Cisco Spaces token, you can assign Cisco Spaces to Catalyst Center sites and begin to monitor those sites. For more information, refer to the Catalyst Center User Guide.



CHAPTER 14

# Calendar Integrations

This chapter provides information on third-party integrations.

**Google Calendar Integration**

The Google Calendar integration enables you to connect your Google account with Cisco Spaces. This synchronizes meeting room booking information. The Cisco Spaces digital signage, with Google Calendar booking information, allows you to view available rooms in an intuitive, map-based approach instead of traditional lists of rooms that provide little context.

**Office 365 Calendar Integration**

The Office 365 calendar integration enables you to connect your Microsoft account with Cisco Spaces, which synchronizes meeting room booking information. The Cisco Spaces digital signage, equipped with Office 365 calendar booking information, enables you to easily access and visualize available rooms using an intuitive, map-based interface. This approach offers a more contextual and user-friendly experience compared to the traditional room lists.


- Calendar GUI Integrations, on page 111
- Integrate Google Calendar, on page 111
- Integrate Office 365 Calendar, on page 113


# Calendar GUI Integrations

The Microsoft 365 calendar integration feature is introduced in Cisco Spaces. Use this feature to connect your Microsoft 365 calendar account with the Cisco Spaces application and view the integrated calendar details in the Cisco Spaces dashboard **Menu** > **Integrations**.

The imported calendars are displayed in the Cisco Spaces: Space Manager application.

# Integrate Google Calendar

The Google Calendar integration enables you to connect your Google account with Cisco Spaces, which synchronizes meeting room booking information. With the Cisco Spaces digital signage, you can easily view available rooms in an intuitive, map-based approach instead of traditional lists that lack context. This integration brings your meeting rooms to life by displaying dynamic calendar data on a user-friendly digital signage application.

### Procedure

**Step 1** Log in to Cisco Spaces.

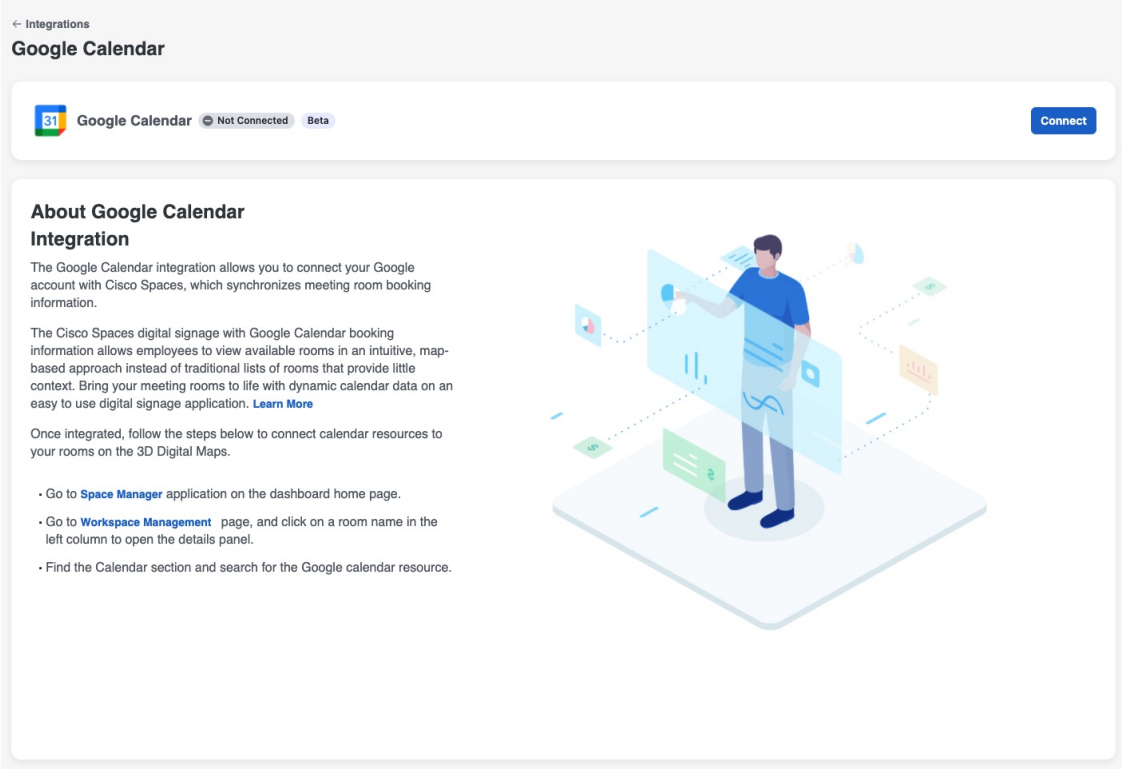
The Cisco Spaces **Home** window is displayed.

**Step 2** From the top-left corner, click the **Menu** icon ( ) and choose **Integrations** > **Third party** > **Google Calendar Integrations**.

**Step 3** Click **Connect**.

The **Google Calendar Integrations** window is displayed.

***Figure 24: Google Calendar Integrations***




**Step 4** Click **Connect**.

**Step 5** In the **Sign in - Google Accounts** pop-up window, enter your Google account credentials.

Verfiy that you select a valid google account where the calendar bookings are available from the listed **Sign in - Google Accounts** pop-up window.

**Step 6** After the account is verified, click **Proceed**.

**Step 7** Click **Go to dnaspaces.io** > **Continue** to integrate the Google account with Cisco Spaces.

A success message `Calendar integration is successfull` is displayed.

**Step 8** View the integrated Google calendar details in the **My Integrations** area along with the number of connected resources. A green tick mark indicates that the integration is successful.

The integrated calendars are available in the Cisco Spaces: Smart Workspaces app for use.

- To remove the Google Calendar Integrations, click **Remove** in the tile view.
- To disconnect the current account integration, click **Disconnect** and follow the instructions.

### What to do next

To successfully connect calendar resources to your rooms on the 3D Digital Maps:

1. Navigate to **Cisco Smart Workspaces** application.
2. Proceed to the **Workspace Management** window and select a room name from the left column to access the **Details** panel.
3. From the **Details** panel, locate the **Calendar** area and search for the Google calendar resource.

# Integrate Office 365 Calendar

The Office 365 calendar integration enables you to seamlessly connect your Microsoft account with Cisco Spaces, resulting in the synchronization of meeting room booking information. The Cisco Spaces digital signage, combined with Office 365 calendar booking information, provides you with a user-friendly and intuitive map-based approach to view available rooms. This approach is far more effective than traditional lists of rooms, which often lack context. By utilizing this easy-to-use digital signage application, you can bring your meeting rooms to life with dynamic calendar data.

### Procedure

**Step 1** Log in to Cisco Spaces.

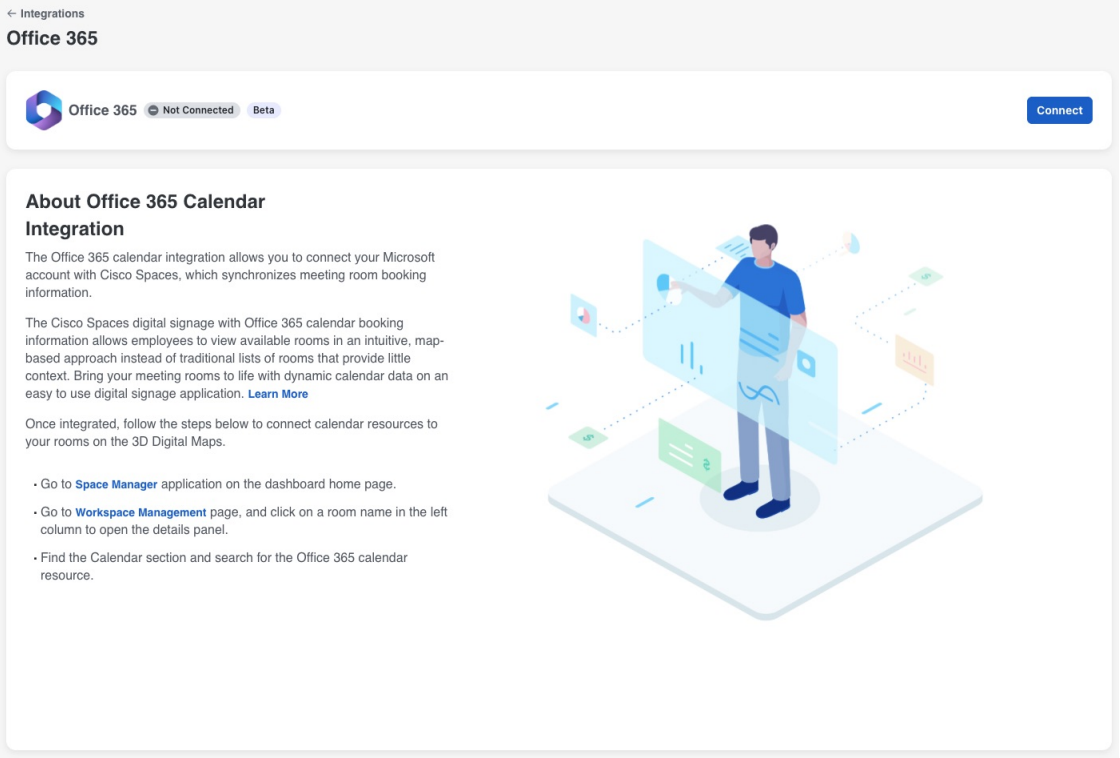
The Cisco Spaces **Home** window is displayed.

**Step 2** From the top-left corner, click the **Menu** icon ( ) and choose **Integrations** > **Third party > Office 365**.

**Step 3** Click **Connect**.

The **Integrations Office 365** window is displayed.

*Figure 25: Office 365 Integrations*




**Step 4** Click **Connect**.

**Step 5** Follow the on-screen instructions and enter your Office 365 account credentials to integrate Office 365 calendar.

**Step 6** After the account is validated, click **Proceed**.

**Step 7** Click **Go to dnaspaces.io** > **Continue** to integrate the Office 365 account with Cisco Spaces.

A success message `Calendar integration is successfull` is displayed.

**Step 8** View the integrated Office 365 calendar details in the **My Integrations** area along with the number of connected resources. A green tick mark indicates that the integration is successful.

The integrated calendars are available in the Cisco Spaces: Smart Workspaces app for use.

- To remove the Office 365 calendar, click **Remove** in the tile view.
- To disconnect the current account integration, click **Disconnect** and follow the instructions.

### What to do next

To successfully connect calendar resources to your rooms on the 3D Digital Maps:

1. Navigate to **Cisco Smart Workspaces** application.
2. Proceed to the **Workspace Management** window and select a room name from the left column to access the **Details** panel.

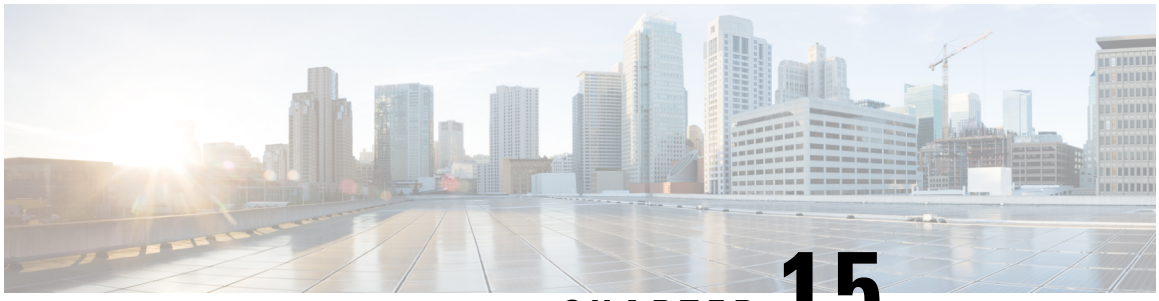
3. From the **Details** panel, locate the **Calendar** area and search for the Google calendar resource.



# PART VIII

# Configure


- Notifications, on page 119
- Location Compute, on page 125



CHAPTER 15

# Notifications


- Configure notifications overview, on page 119
- Manage categories, on page 120
- Manage subscribers, on page 121


## Configure notifications overview

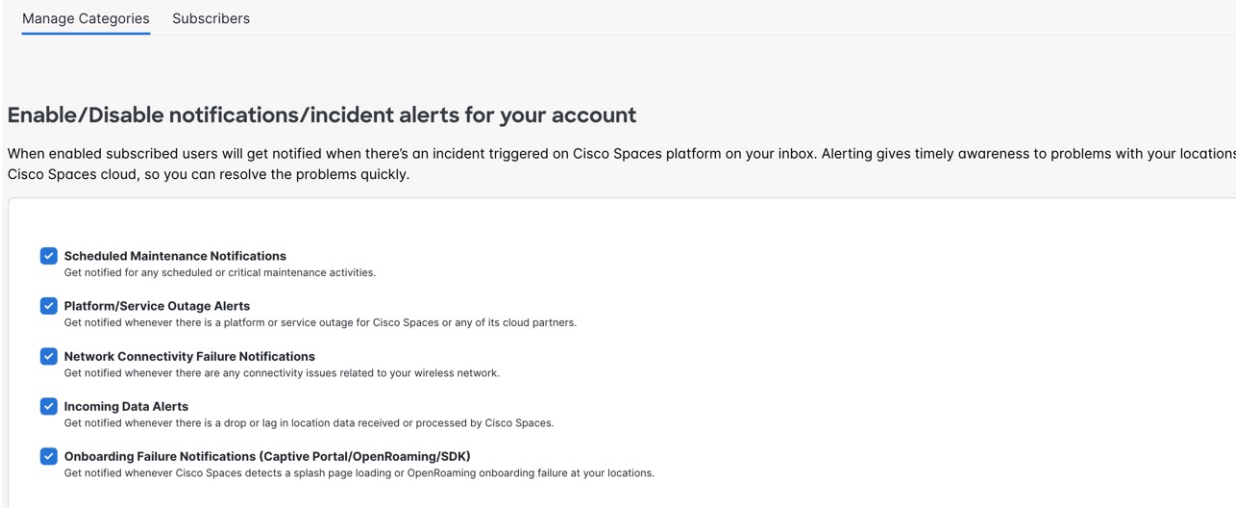
The **Notifications** feature in Cisco Spaces allows you to configure subscriber notifications (**Configure** > **Notifications**) and receive notifications on critical incidents. Enable this feature to receive email notifications when an incident occurs on the Cisco Spaces platform.

Subscriber notification provides updates about issues with Cisco Spaces cloud or locations and help you address them on a timely manner.

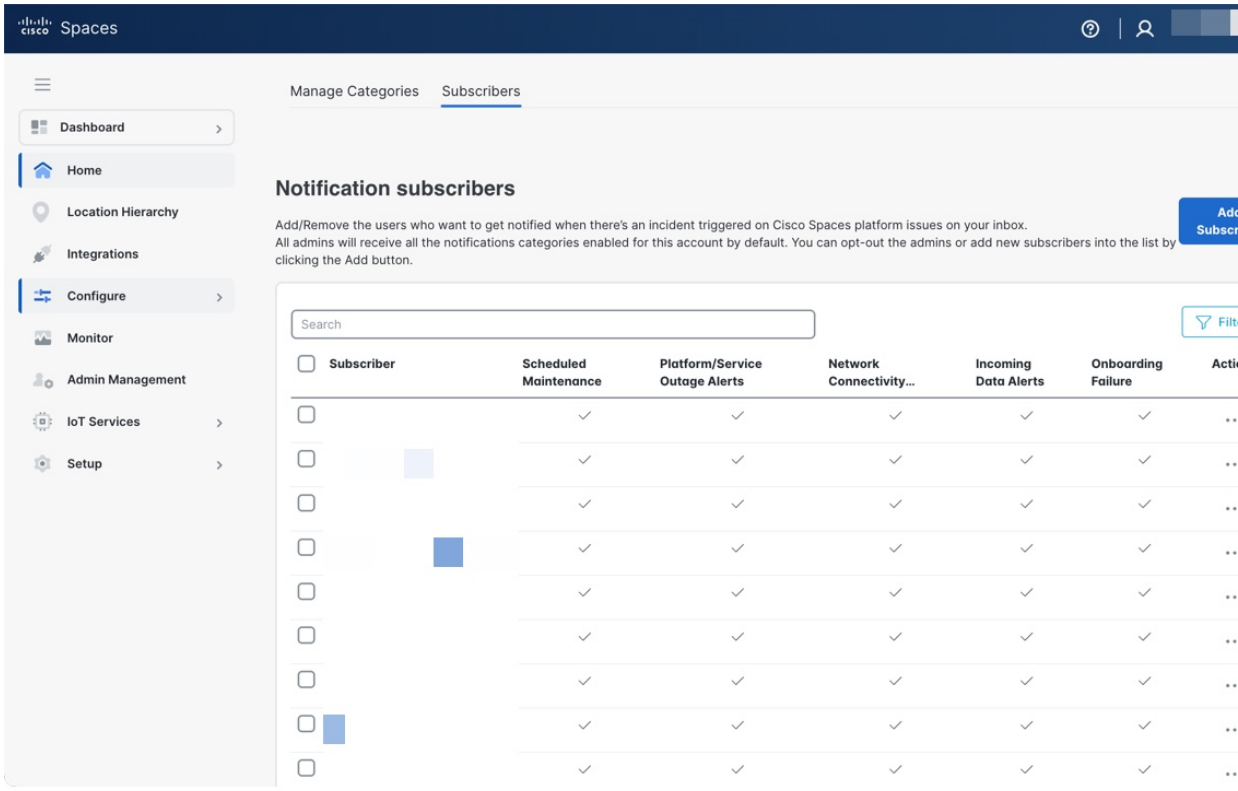
**Note** This feature is available for all users with administrator access (Read-only and Read-Write).

Use these tabs:

- **Manage Categories**: If you are an administrator with Read-Write access, configure subscriber notifications for your account by navigating to **Configure** > **Notifications** > **Manage Categories**.




- **Subscribers**: To manage subscribers, navigate to the **Subscribers** tab (**Configure** > **Notifications** > **Subscribers**).




All administrators and subscribers receive the notifications based on the categories enabled for the account.

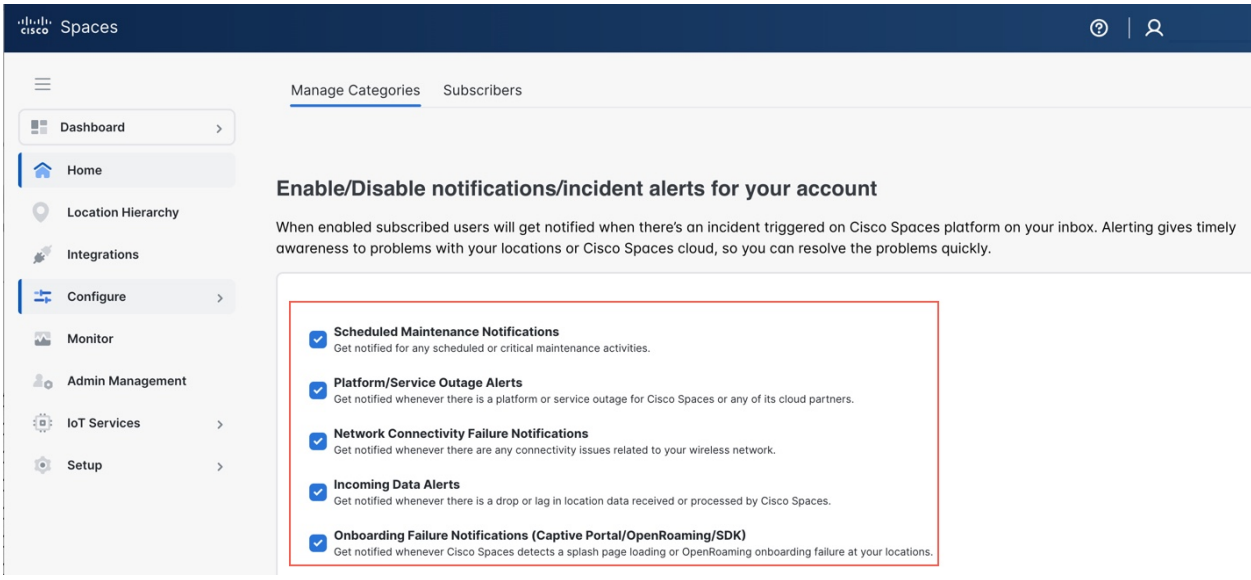
# Manage categories

The **Manage Categories** tab allows you to select the categories available for enabling the notifications. Use the categories available to enable or disable notifications and incident alerts for your account.

These are the categories in the **Manage Categories** tab.

- **Scheduled Maintenance Notifications**: Select **Scheduled Maintenance Notifications** check box to get notified in case of any scheduled or critical maintenance activities.
- **Platform/Service Outage Alerts**: Select **Platform/Service Outage Alerts** check box to get notified whenever there is a Cisco Spaces platform or service outage or any of its cloud partners.
- **Network Connectivity Failure Notifications**: Select **Network Connectivity Failure Notifications** check box to get notified whenever there are any connectivity issues related to your wireless network.
- **Incoming Data Alerts**: Select **Incoming Data Alerts** check box to get notified whenever there is a drop or lag in location data received or processed by Cisco Spaces.

***Figure 26: Notification Categories***




When you enable the notifications, subscribers receive notifications in their mailbox whenever an incident is triggered on the Cisco Spaces platform. Alerts provide timely awareness of issues with your locations or the Cisco Spaces cloud, allowing you to resolve problems quickly.

# Manage subscribers

The **Subscribers** tab allows you to add or edit subscribers. You can add or remove subscribers who want to receive notifications in their mailbox whenever an incident is triggered on the Cisco Spaces platform.

By default, all Cisco Spaces administrators receive notifications for all enabled categories under the account. You can opt-out specific administrators or add new subscribers to the list by clicking the **Add Subscriber** button.

Use the **Search** field in the **Notification subscribers** window to search for subscribers.

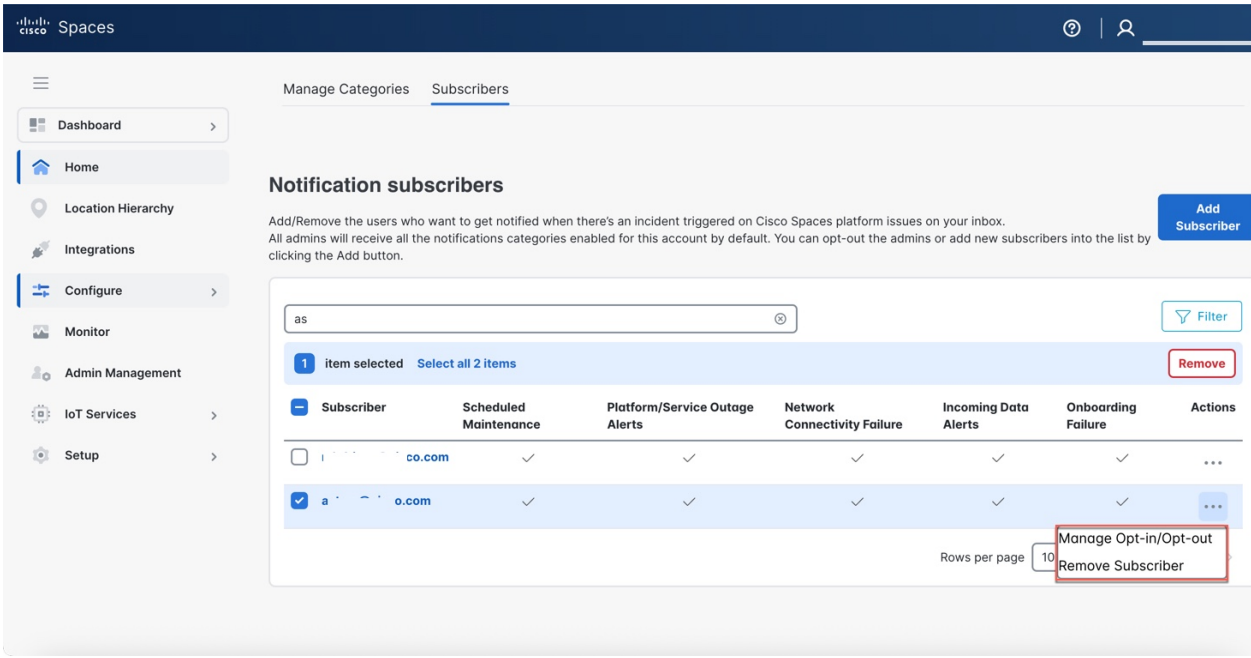
### Subscriber details

The table provides detailed information about the subscribers.

*Table 9: Subscriber details*

| Field | Description |
|---|---|
| Subscriber | Email address of the subscriber. |
| Scheduled Maintenance | A tick mark indicates that this notification category is enabled for the subscriber. |
| Platform/Service Outage Alerts | A tick mark indicates that this notification category is enabled for the subscriber. |
| Network Connectivity Failure | A tick mark indicates that this notification category is enabled for the subscriber. |
| Incoming Data Alerts | A tick mark indicates that this notification category is enabled for the subscriber. |
| Onboarding Failure | A tick mark indicates that this notification category is enabled for the subscriber. |
| Actions | Click the three dots under the **Action** column either to<br>• manage **Opt-in** or **Opt-out** the notifications categories, and<br>• remove the subscribers.<br>**Note**<br>An administrator with Read-Write access only can **Opt-in** or **Opt-out** the notifications categories and remove the subscribers. |

*Figure 27: Notification Subscribers*




# Add subscribers

You need to add subscribers to the alert list. Only the subscribed users get notified when there's an incident triggered on Cisco Spaces platform.

Complete these steps to add new subscribers.

### Procedure

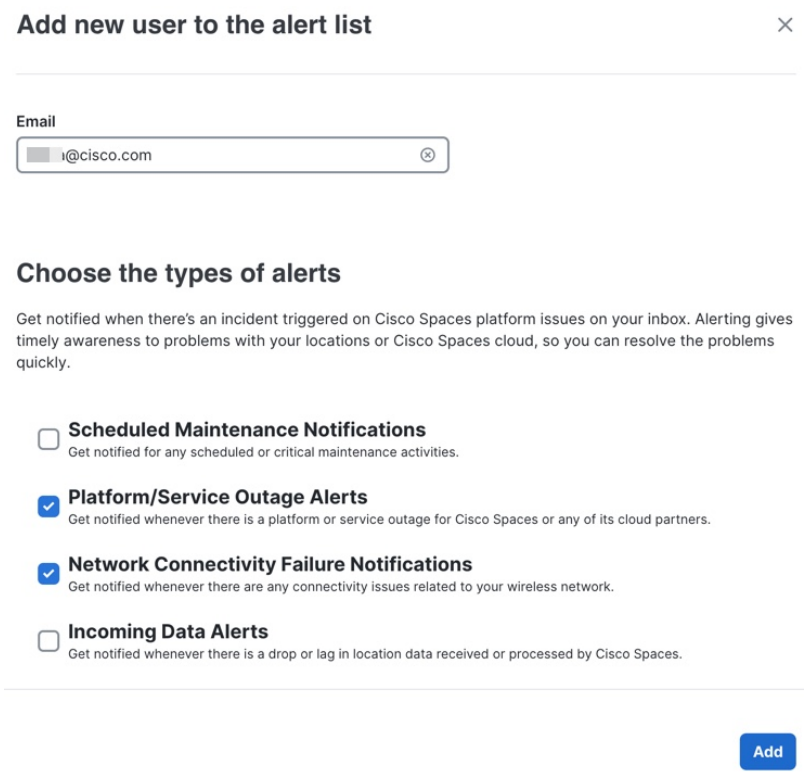
**Step 1** Log in to Cisco Spaces.

The Cisco Spaces **Home** window is displayed.

**Step 2** From the top-left corner, click the **Menu** icon ( ) and choose **Configure** > **Notifications** > **Subscribers**.

**Step 3** Click **Add Subscriber**.

*Figure 28: Add Subscriber*




The **Add new user to the alert list** slide-in window is displayed.

**Step 4** In the **Email** field, enter the email address of the new subscriber.

**Step 5** Check the required **Notification Categories** check box.

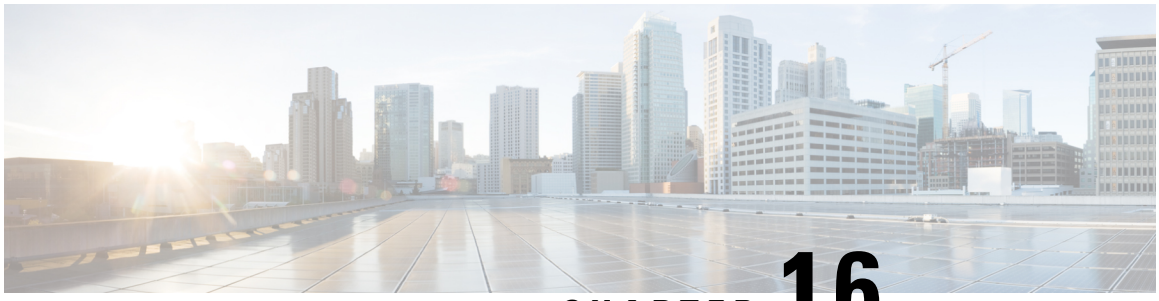
You can opt in for receiving notifications and incident alerts for five notification categories. You can select more than one category.

**Step 6** Click **Add**.

The new user is added to the notification subscriber list.

### What to do next

The **Notification subscribers** window displays the new subscriber details. Use the **Actions** column to manage subscription.



CHAPTER 16

# Location Compute

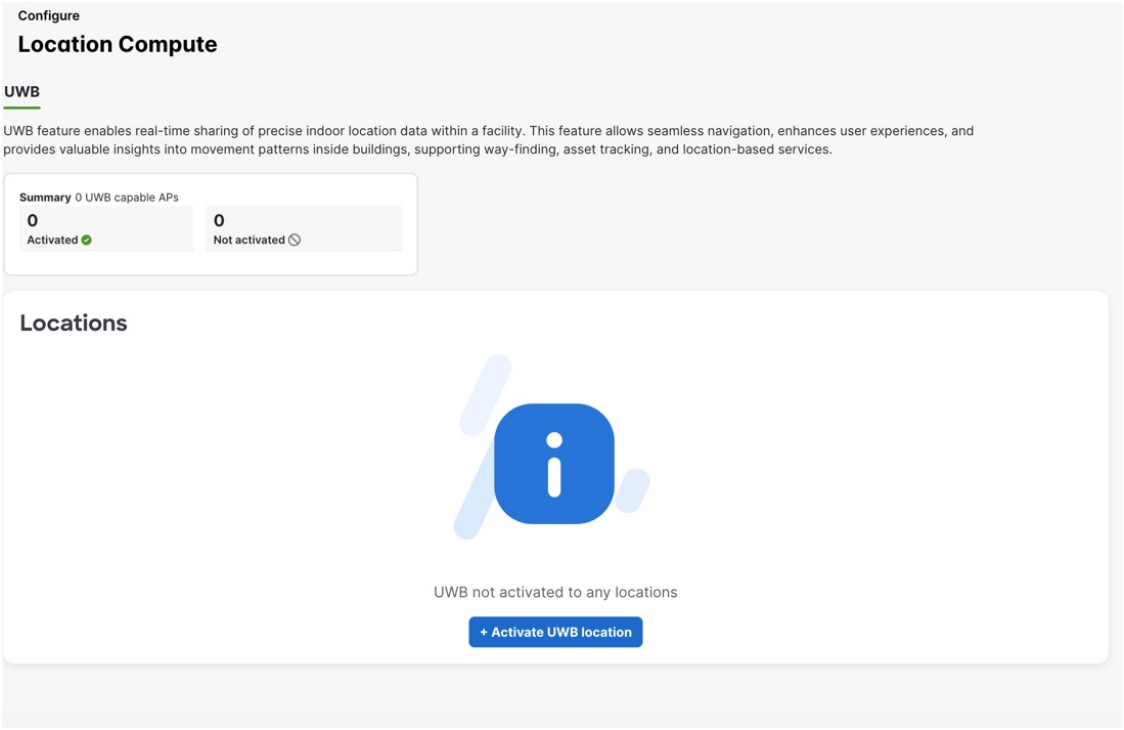

- Location Compute, on page 125
- Activate UWB Location, on page 126


## Location Compute

The UWB feature is designed to provide high-precision indoor positioning within a facility. The primary functions and benefits include:

- **Real-time Data**: Enables the sharing of precise indoor location data in real-time.
- **Navigation & Way-finding:** Supports seamless navigation and way-finding for users inside buildings.
- **Asset Tracking:** Allows for the monitoring and tracking of physical assets within the facility.
- **Operational Insights:** Provides valuable data on movement patterns to enhance user experiences and location-based services.

*Figure 29: Location compute*




# Activate UWB Location

Enable UWB on supported access points in a specific building to allow advanced location and ranging capabilities.

Use this task when you want to activate Ultra-Wideband technology in a building. Activation will start several non-disruptive processes on your controller and access points.

**Before you begin**

- Ensure you have administrator access to the controller's management interface.
- Verify that the building contains UWB-capable access points.

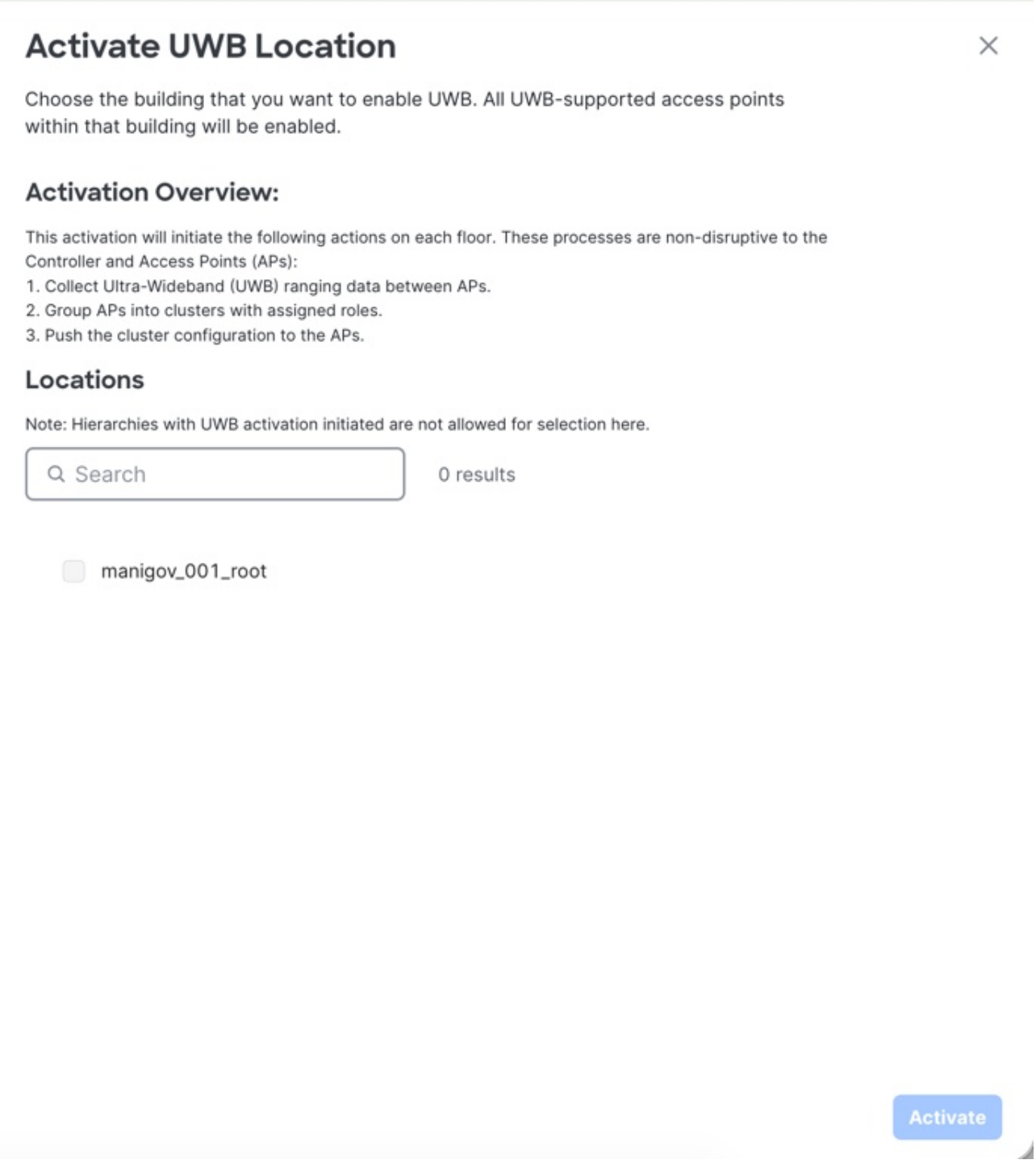
Follow these steps to activate UWB location:

## Procedure

**Step 1** In the **Location Compute** window, click **+ Activate UWB Location**.

The **Activate UWB Location** slide-in window is displayed.

*Figure 30: Activate UWB Location*




**Step 2** In the **Search** field, enter the building name.

**Step 3** Check the check box for the building where you want to enable UWB.

You cannot select hierarchies that already have UWB activation in progress.

**Step 4** Click **Activate**.

The UWB activation process is initiated.

- The following actions occur automatically for each floor:
  - The system collects Ultra-Wideband (UWB) ranging data between access points.
  - Access points are grouped into clusters with assigned roles.
  - Cluster configurations are pushed to all APs in the building.
- Monitor the activation status to ensure all access points are successfully enabled.

---

All UWB-capable access points within the selected building are enabled for Ultra-Wideband services, allowing advanced location and ranging functionality.

Initiate the UWB activation process.

### What to do next

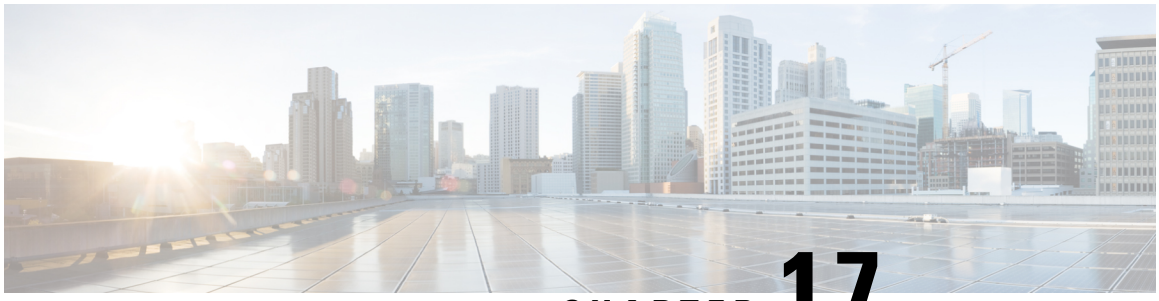
Optionally, verify UWB functionality by checking device location accuracy or reviewing status reports in the platform's dashboard.



# PART IX

# Monitor


- Monitoring and Support, on page 131



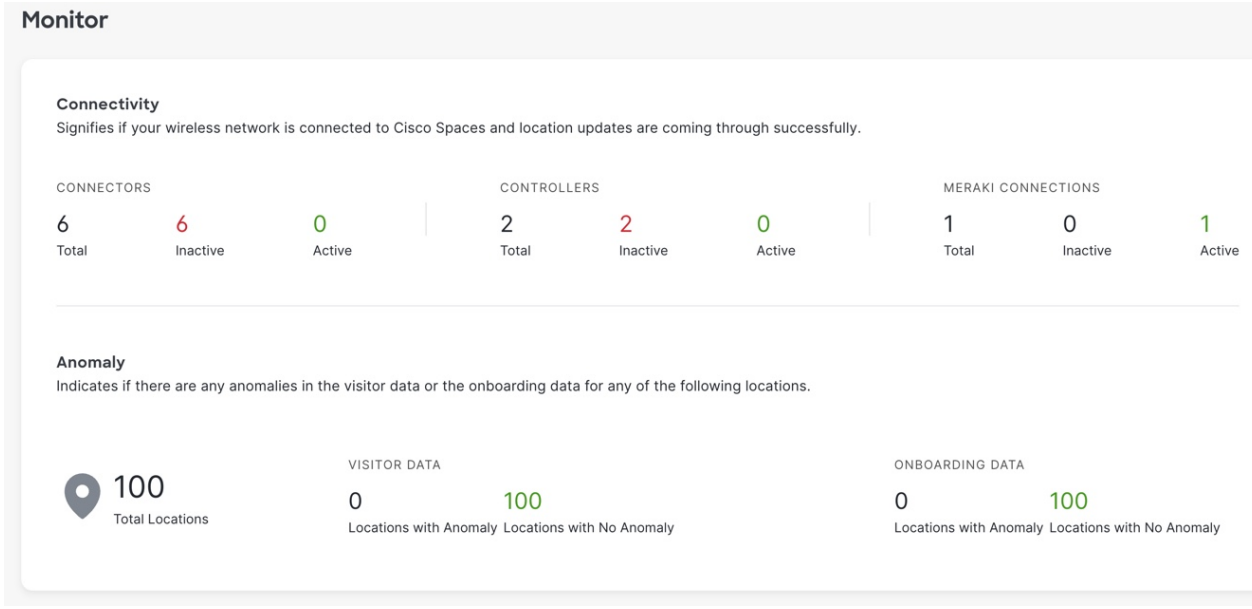
CHAPTER 17

# Monitoring and Support

This chapter describes the monitoring details that are displayed in Cisco Spaces.

To access the **Monitor** window, in the **Cisco Spaces** dashboard, click the three-line menu icon at the top-left, and choose **Monitor**.

***Figure 31: Monitor***





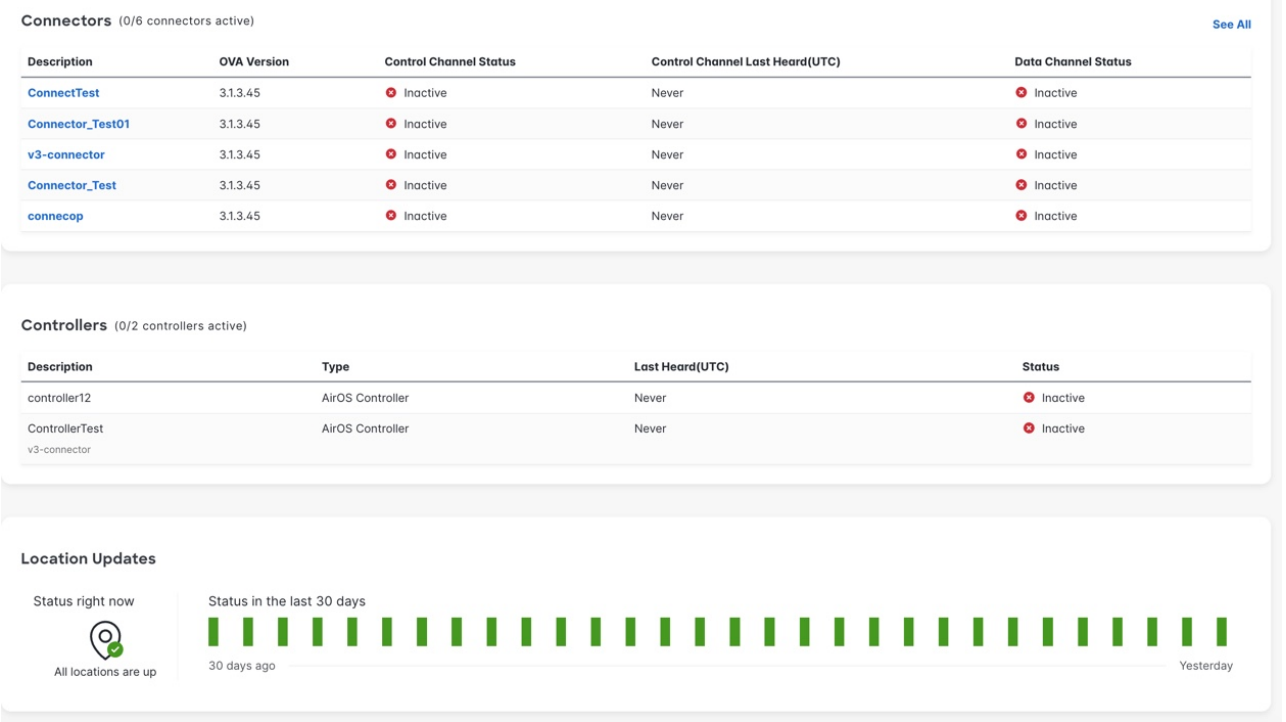
- Monitor, on page 131


# Monitor

The **Monitor** window serves as the centralized health and diagnostic hub for your Cisco Spaces environment. Use the **Monitor** feature to monitor the health details and performance metrics of Cisco Spaces.

By using this feature, administrators can quickly identify connectivity gaps, address data anomalies, and ensure that location services are functioning optimally.

*Figure 32: Monitor*




View these details:

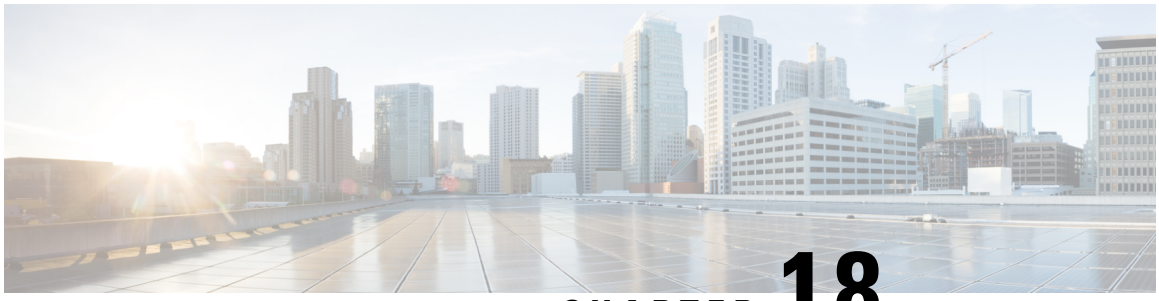
- **Connectivity**: Signifies if your wireless network is connected to Cisco Spaces and location updates are coming through successfully. View the details for connectors, controllers and Meraki connections.
- **Anomaly**: Displays the current status of location updates and internet provisioning (this is applicable only of you have configured customer acquisition through captive portals) in the locations. This section is marked as up if location updates and internet provisioning are happening for all the locations without any issues. If any of them is not happening for any location, the status will be down. If both location update and internet provisioning are not happening for a location, such locations will be listed out.
- **Connectors**: Displays the active connectors. Click a controller to view the descriptions, OVA version, control channel status, control channel last heard (UTC) and data channel status for active connectors.
- **Controllers**: Displays the active controllers. View the description, type, last geard (UTC) and status for active controllers. You can monitor the status of your wireless controllers. This provides insight into whether your hardware is successfully transmitting data to the platform.
- **Location Updates**: Displays the current location update status for the locations to which you have access. This section will be marked as up if location updates are received from all the locations, and the status will be **All Locations Connected**. If there is any location update issue, this section will be marked as down, and the total number of locations that have location update issue will be displayed.



PART X

# Admin Management


- Managing Cisco Spaces Users and Accounts, on page 135



CHAPTER 18

# Managing Cisco Spaces Users and Accounts

This chapter explains how to invite and manage Cisco Spaces users and accounts.


- Manage Cisco Spaces Users, on page 135
- Manage the Cisco Spaces Accounts, on page 138
- Location-Based RBAC (Role-Based Access Control) in Cisco Spaces, on page 139


## Manage Cisco Spaces Users

Cisco Spaces provides users with different rights and privileges based on the role they perform.

After you log in to the Cisco Spaces **Home** page, click **Admin Management** from the left navigation.

These tabs are available:

- **Admins**: Use the **Admins** tab to view the Cisco Spaces users and invite new administrators.

  Use the **Search** the field to search for existing users.

- **Roles**: Use the **Roles** tab to search for roles, create new roles and manage them.

### Invite a Cisco Spaces User

When a Cisco Spaces account is created, a **Dashboard Admin Role** user is created for the account with the email ID provided. This **Dashboard Admin** can invite other users to Cisco Spaces.

Cisco Spaces provides only one default user role, **Dashboard Admin Role**.

Cisco Spaces allows you to define user roles with different access rights to different apps.

You can include the following role types (apps) in a user role if that particular service is enabled for your account.

- **Cisco Spaces**: This role type provides access rights to the **Cisco Spaces** app.
- **Location Analytics**: This role type provides access rights to the **Location Analytics** app.
- **Live Occupancy**: This role type provides access rights to the **Live Occupancy** app.
- **Detect and Locate**: This role type provides access rights to the **Detect and Locate** app.
- **IoT Services**: This role type provides access rights to the **IoT Services** 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.
- **Space Utilization**: This role type provides access rights to the **Space Utilization** app.

**Note**

- Import of duplicate payload from Catalyst Center to Cisco Spaces is restricted. In the **Import History** section, the following error message is displayed: `Warning: Import ignored due to no changes in request payload`.
- For the Dashboard Admin role, access to **Location Analytics** is provided by default. For other roles, you must assign access separately. However, you can assign **Location Analytics** to a role only along with the **Cisco Spaces** service. For example, you can create a role with read and write access to **Location Analytics** and Read Only access to **Cisco Spaces**. The Location Analytics tile is disabled for Cisco Spaces user accounts that do not have access to **Location Analytics**.

Follow these steps to invite a Cisco Spaces user.

### Procedure

**Step 1** From the left navigation menu, choose **Admin Management** > **Admins**.

**Step 2** Click **Invite Admin**.

**Step 3** In the **Invite Admin** window, enter the following details:

a) In the **Email** field, enter the email address of the user to add.

b) From the **Role Name** drop-down list, select the user role that you want to provide to this user.

- The default user role and the user roles defined earlier are displayed in the drop-down list. If the required user role is not there, you can define a new user role using **Create New Role**.
- Click **Create New Role** to create a new user role. For more information on creating a new user role, see Create a User Role, on page 137. 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**.

The **Invite Admin** option is only available for Cisco Spaces administrators with read and write permissions.

# Create a User Role

To create a Cisco Spaces user role, follow these steps:

### Procedure

**Step 1** From the left navigation menu, choose **Admin Management** > **Roles** tab.

**Note**
You can also click **Create New Role** in the **Role Name** drop-down list in the **Invite Admin** window.

**Step 2** Click **Create Role**.

**Step 3** In the **Create New Role** slide-in window, enter the following details:

a) In the **ROLE NAME** field, enter a name for the user role.

b) In the **APPS** area, check the check boxes for the role types that you want to provide to this user role.

For more information on role types (apps), refer to the role types described in Invite a Cisco Spaces User, on page 135.

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**.

**Step 4** Check the **Restrict this role to specific locations** check box to restrict role access to specific locations.

The **+ Add Locations** option is displayed.

**Step 5** Click **+ Add Locations** to select locations.

a) In the **Choose Locations** slide-in window, select the check box aganist the locations. The selected locations are displayed in the **Selected Locations** pane.

b) Click **Update**.

**Step 6** Click **Create Role**.

The user role is available in the **Role Name** drop-down list of the **Invite Admin** window.

# Edit Cisco Spaces User

As a Dashboard Admin user with read and write permission, you can change the user role of a user. For example, a Dashboard Admin Read can be promoted to a Dashboard Admin Read and Write user.

Follow these steps to edit the user privileges of a Cisco Spaces user.

### Procedure

**Step 1** From the left navigation menu, click **Admin Management**.

The **Admin** page is displayed with the list of e-mail IDs of the Cisco Spaces users.

**Step 2** Click the three dots next to the user (at the far right) you want to edit.

**Step 3** Click the **Edit User**.

The **Edit User** page is displayed.

**Step 4** From the **Role Name** drop-down list, choose the type of access that you want to provide to the user.

The default user roles and the user roles defined earlier are available in the drop-down list for selection. If the required user role is not there, you can define a user role using **Create New Role**. For more information on creating a new user role, refer to Create a User Role, on page 137.

**Step 5** Click **Update**.

## Delete a Cisco Spaces User

If a user no more needs access to Cisco Spaces, we recommend that you delete such users from the Cisco Spaces user list.

Any user with admin privileges can delete other users.

Follow these steps to delete an existing Cisco Spaces user.

### Procedure

**Step 1** From the left navigation menu, click **Admin Management**.

The **Admins** page is displayed with the list of the Cisco Spaces users.

**Step 2** Click the three dots next to the user (at the far right) you want to edit.

**Step 3** Click **Remove**.

To delete multiple users, select the check box for the corresponding e-mail IDs, and click **Remove** option which displays on the top right of the window.

# Manage the Cisco Spaces Accounts

This section describes how to manage the Cisco Spaces accounts.

## Signing Out of Cisco Spaces

To sign out of Cisco Spaces, follow these steps:

**Procedure**

**Step 1** In the **Cisco Spaces** dashboard, click the **User Account** icon () that displays in the far right of the dashboard.

**Step 2** Click **Logout**.

# Location-Based RBAC (Role-Based Access Control) in Cisco Spaces

Location-Based RBAC (Role-Based Access Control) in Cisco Spaces is an enhanced security feature that allows administrators to restrict user roles and permissions to specific physical locations within Cisco Spaces. This means when creating or assigning a user role, you can limit that role's access rights to particular locations such as campuses, buildings, floors, or zones.

Use the **Restrict this role to specific locations** option to enable this feature. This option is available during role creation (**Admin Management** > **Roles** > **Create Role**) and when inviting users (**Admin Management** > **Invite Admin**).



PART XI

# IoT Services


- IoT Services, on page 141
- Prerequisites for Cisco Spaces: IoT Service (Wireless) Deployment, on page 141
- IoT Service (Wireless) Features, on page 142


# IoT Services

Cisco Spaces: IoT Service (Wireless) is a platform within Cisco Spaces that enables the claiming, management, and monitoring of IoT devices using Cisco's wireless infrastructure. Supporting multiple vendors and protocols, it initially focuses on Bluetooth Low Energy (BLE). The service integrates hardware, software, and partner solutions—including Cisco Catalyst 9800 Series Wireless Controllers, Cisco Spaces: Connector, Cisco Wi-Fi 6 access points, and Cisco Spaces—to simplify IoT device management in complex enterprise environments.

# Prerequisites for Cisco Spaces: IoT Service (Wireless) Deployment

To successfully deploy Cisco Spaces: IoT Service (Wireless), ensure your environment meets the following prerequisites.

- **Licensing**: Ensure your account has the required Cisco Spaces licensing for IoT Services.
- **Spaces Connector**
  - Spaces Connector version 3.0 or later is required.
  - Confirm the connector is active and meets the version requirement.

- **Wireless Controllers**: Cisco Catalyst 9800 Wireless Controllers with software release 17.3.1 or later are required.
- **Access Points/Switches**
  - Compatible Cisco APs or switches must be present.
  - Activate IoT Services in Cisco Spaces to view detailed compatibility information.



**Note** Verify all components are present, active, and meet the version requirements before deploying IoT Services.

For upgrades or deployment assistance, contact: cisco-spaces-support@external.cisco.com.

# IoT Service (Wireless) Features

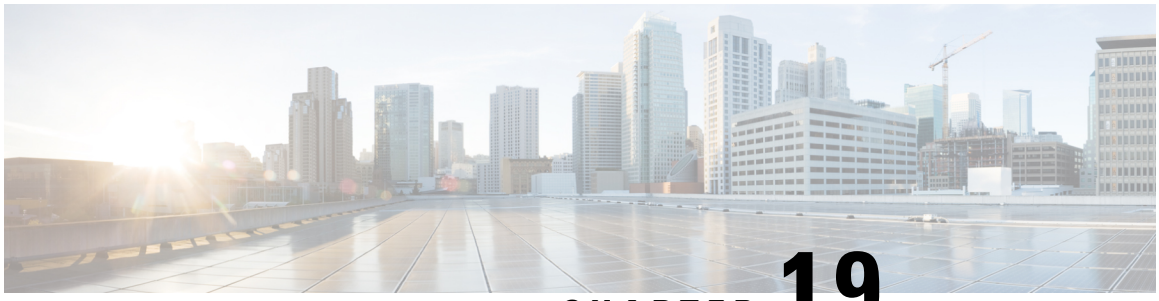
Use the **IoT Service** feature to manage IoT Gateways (AP Gateways and Wired Gateways), manage devices, and monitor them.



# PART XII

# Setup


- Set Up Wireless Network, on page 145
- Set Up Locations and Maps, on page 153
- Set Up Cisco Webex, on page 177



CHAPTER 19

# 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 145
- Wireless Network Bars, on page 147
- Set Up Meraki API Key Method, on page 150
- Wireless Network Status, on page 152


# Setting Up Cisco Spaces to Work with Various Wireless Networks

You can set up Cisco Spaces with wireless networks that are based on the following options:

- Cisco AireOS wireless controllers
- Cisco Catalyst 9800 wireless controllers
- Cisco Meraki

### Procedure

**Step 1** Log in to Cisco Spaces.

**Step 2** In the **Home** page, from the left navigation pane, choose **Setup** > **Wireless Networks**.

**Step 3** In the **Connect your wireless network** window, click **Add New**.

The **Connect your wireless network** window is displayed with the options **AireOS Controller/Catalyst 9800 Wireless Controller** and **Cisco Meraki**.

- For **AireOS Controller/Catalyst 9800 Wireless Controller**, these configurations are available:
  - **Via Spaces Connector**: To connect Cisco Spaces to Cisco Wireless Controller using Cisco Spaces: Connector.
  - **Connect Cisco Wireless Controllers directly**: To connect Cisco Spaces to Cisco Wireless Controller using a Cisco Wireless Controller Direct Connect.
  - **Connect via CMX Tethering**: To connect Cisco Spaces Cisco Wireless Controller using Cisco CMX.

- For **Cisco Meraki**, these configurations are available:
  - **Connect via API Key**: To connect Cisco Spaces to Cisco Meraki using a Cisco Meraki API Key.

    You can login to the **Meraki** dashboard, choose **Account Name** > **My Profile** > **API Access**, and click **Generate** to generate an API Key. Enter this key in the **Connect via API key** field in the Cisco Spaces dashboard to add your network to Cisco Spaces. For more information, see Set Up Meraki API Key Method, on page 150.

**Note**
For new Cisco Spaces accounts, click **Get Started**.

**Step 4** Click **Select** to choose your preferred method through which you want to connect to Cisco Spaces.

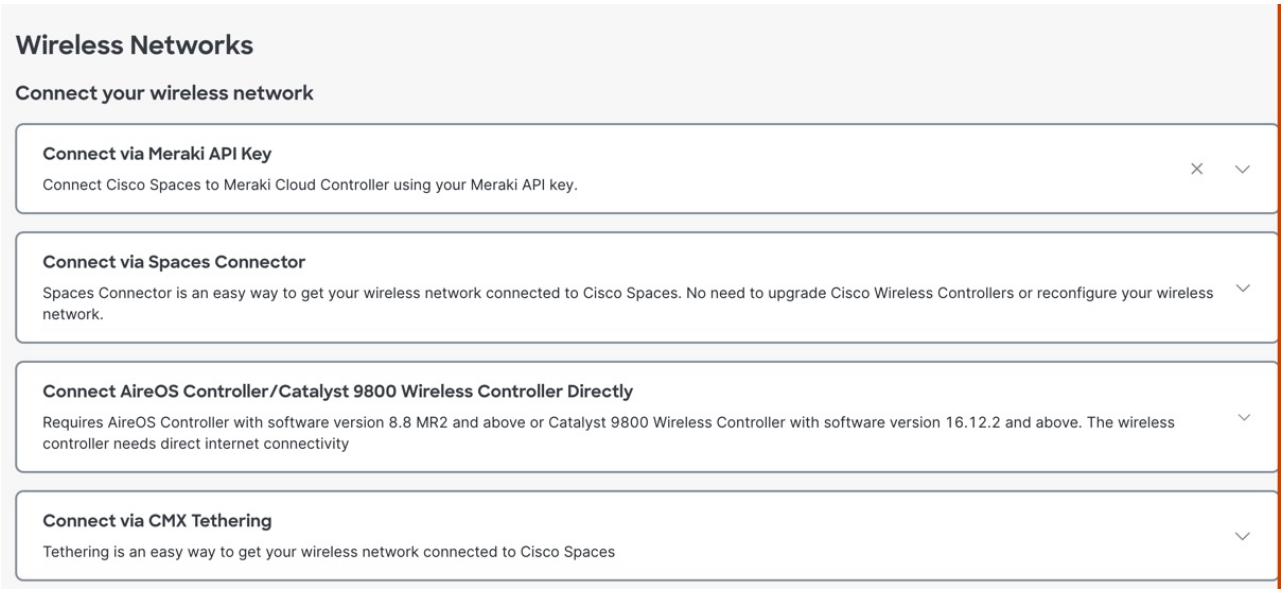
The prerequisites for connecting to the wireless network using the selected method are displayed.

**Step 5** Click **Continue Setup**.

The following message is displayed: `Successfully saved the configuration`.

**Step 6** A bar corresponding to the wireless network configuration method selected is displayed in the **Connect your wireless network** window. For example, if **Via Spaces Connector** is selected, a bar with the label **Connect via Spaces Connector** displays.

***Figure 33: Connected wireless networks***




**Step 7** To view the instructions and configure the wireless network, click the drop-down button at the far right of the bar.

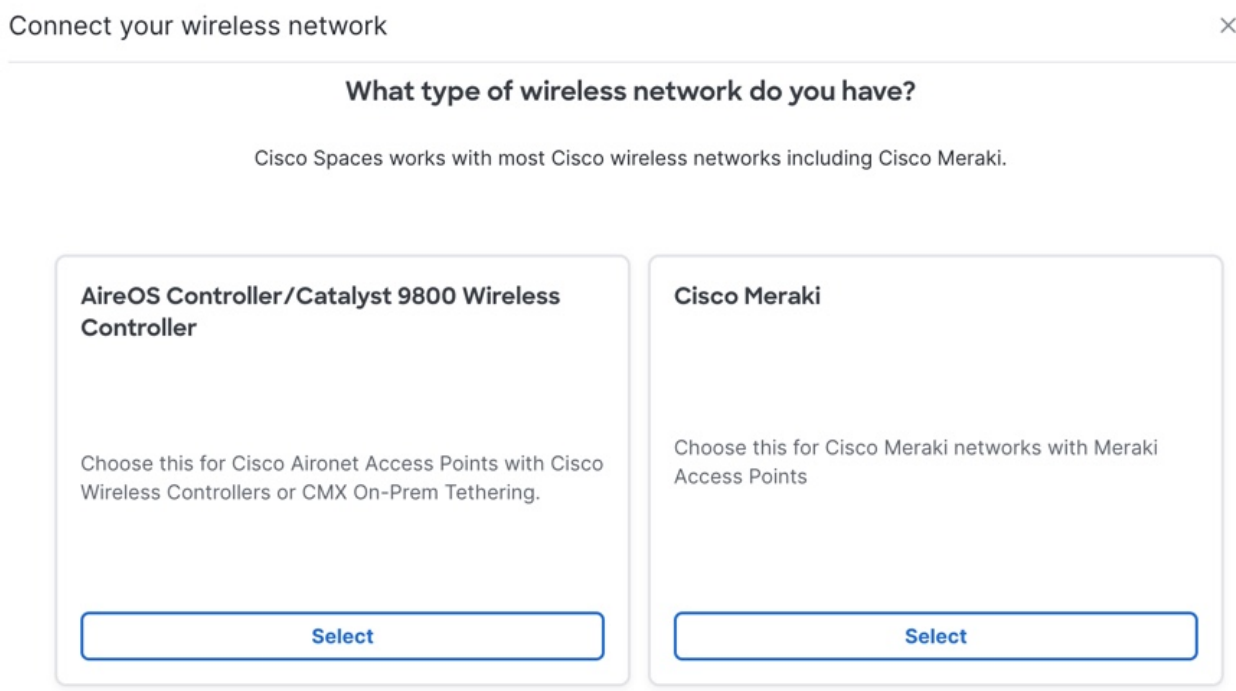
The instructions and the features to connect to preferred wireless network are displayed.

**Step 8** Follow the on-screen instructions to add the wireless network.

# Wireless Network Bars

To connect your wireless network with Cisco Spaces, use any available options in the **Setup** > **Wireless Networks** > **Connect your wireless network** window.

***Figure 34: Wireless Network***




The following tabs are displayed for Cisco Meraki based on your selection:

- **Connect via Meraki API Key**: Use this option to connect Cisco Spaces to Cisco Meraki Cloud Controller using your Cisco Meraki API key. Follow the on-screen instructions to import a Cisco Meraki organization and the related child locations to the location hierarchy using the **Import Networks** option.

**Note** We recommend using **Connect via API Key** to connect Cisco Meraki with Cisco Spaces.

Perform the following:

1. **Connect your Meraki**: Connect Cisco Meraki with Cisco Spaces using the API key.
2. **Configure Meraki scanning API**: Cisco Meraki scanning APIs are automatically configured after importing the networks into the location hierarchy.

**Note** To configure manually, use the **Post URL** with URL validator and **Secret Key** and validate manually in the Cisco Meraki dashboard to establish a connection with Cisco Spaces.

3. **Import Meraki Networks into Location Hierarchy**: Click **Import Networks** to import the Cisco Meraki networks.

**Note** The user count that is getting synchronized with Cisco Meraki is displayed under the **Connect your Meraki** option: **Connect via Meraki API Key**.

The following bars are displayed for Cisco AireOS based on the connection method selected:

- **Connect via Spaces Connector**: Use 'to connect Cisco Spaces to Cisco Wireless Controller'

**Note** You need not upgrade your Cisco Wireless Controllers or reconfigure your wireless network when you use **Connect via Spaces Connector** option.

Perform the following:

1. **Install Spaces Connector OVA**: Download and install Cisco Spaces: Connector OVA as a virtual machine.

   Click the **Download Spaces Connector** link to download the Spaces Connector.

2. **Configure Spaces Connector**: Click **Create Connector** to create a new connector. You need a token to configure Cisco Spaces: Connector. Connect to `https://<your connector IP>/` from a browser to configure the token. You can optionally configure Cisco Spaces: Connector to connect via HTTPS proxy.

   Click **View Connectors** to view the available connectors.

3. **Add Controllers**: Click **Add Controllers** to add Cisco Wireless Controllers. Click **View Controllers** to view the available controllers.

4. **Import Maps**: Click **Import/Sync Maps** to import or synchronize the maps. You must upload a Cisco Prime Infrastructure or Catalyst Center (version 1.3.1 and above) map to work with Cisco Spaces: Detect and Locate, Asset Tracker, and IoT Services.

5. **Setup location hierarchy**: Click **Add Locations** to add the imported maps to Location Hierarchy.

**Note**

- You can view the location hierarchy using the **View Location Hierarchy** option.
- For the OpenRoaming app, you can configure the hotspots through the **Add OpenRoaming Hotspot** option. You can also view the configurations for the OpenRoaming app for various controllers separately using the **OpenRoaming Controller Configuration** option.
- The Network Configuration Protocol (NETCONF) support is available from Hotspot client version v2.2.95 and on Cisco Catalyst 9800 Series Wireless Controllers version 17.12.

For more information, refer to Cisco Spaces: Connector Configuration Guide.

- **Connect AireOS Controller/Catalyst 9800 Wireless Controller Directly**: Use 'to connect Cisco Spaces to Cisco Wireless Controller (**Connect AireOS Controller/Catalyst 9800 Wireless Controller**)'.

**Note** To connect to this wireless network, you need either an AireOS Controller with software version 8.8 MR2 or later, or a Catalyst 9800 Wireless Controller with software version 16.12.2 or later. The wireless controller needs direct internet connectivity.

Perform the following:

1. **Install Root Certificate**: You can install the certificate from AireOS Controller CLI with View root certificate.
2. **Configure Token in AireOS Controller**: You can view token and contollers using the View Token and View Controllers options
3. **Import Maps**: You can now manage maps from the **Setup** window under Connect WLC/Catalyst 9800 Directly and Connect Via Spaces Connector
   - **Import/Sync Maps**: Upload a Cisco Prime Infrastructure or the Catalyst Center map in order to work with Detect & Locate, Asset Tracker, and IoT Services seamlessly.
   - **Map Upload History**: View the list of uploaded maps. You can view the filename, source type, status and other related information.
   - **Manage Maps**: Navigate to the **Map Service** application to manage maps.
4. **Setup location hierarchy**

- **Connect via CMX Tethering**: Use 'to connect Cisco Spaces to Cisco Wireless Controller'. Displays step-by-step instructions to configure location updates for a Cisco CMX node using CMX tethering with token. You can create the token using the **Create New Token** option in Step 2, and configure it in Cisco CMX.

The other options available on the **Connect your wireless network** window are:

*Table 10: Connect your wireless network Options*

| | |
|---|---|
| **Cisco AireOS Controller/Catalyst 9800 Wireless Controller** | Displays instructions to import a Cisco CMX Node (CMX On-Prem) to the **Location Hierarchy** window. |
| **Cisco Meraki** | Displays instructions to import a Meraki Organization to the **Location Hierarchy** window. |

# Set Up Meraki API Key Method

Use the **Cisco Meraki** option to integrate Cisco Spaces with Meraki. Use the Meraki account credentials to connect to Cisco Meraki cloud, import locations into Cisco Spaces and activate or synchronize the Meraki networks.

### Procedure

**Step 1** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Wireless Networks** > **Add New** > **Cisco Meraki** > **Connect via API key**.

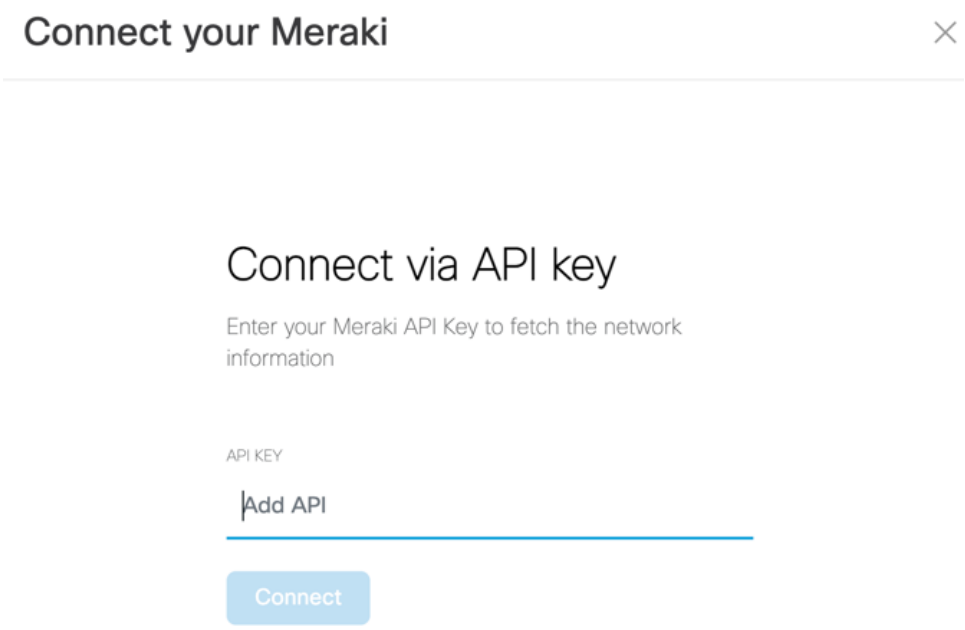
**Step 2** In the Meraki dashboard, navigate to **Organization** > **Configure** > **Settings** and enable **Dashboard API Access**.

**Step 3** In the Meraki dashboard, navigate to **Username** > **My Profile** > **API Access** and generate the API token. The generated API token is an alphanumeric value.

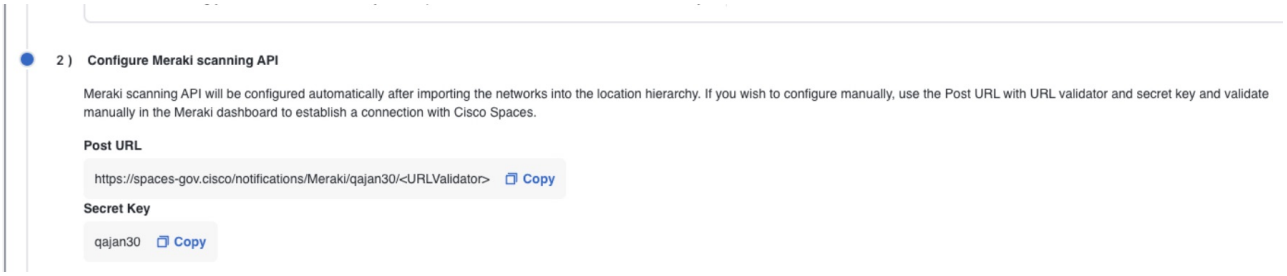
**Step 4** Copy the generated API token to enter it in the Cisco Spaces dashboard.

**Step 5** In the Cisco Spaces dashboard, perform the following:

a) In the **Connect your Meraki** pop-up window, paste the copied API token in the **API KEY** field.




b) Click **Connect**. After a successful synchronization with Meraki, the connection status displays as active.
c) From the **Configure Meraki scanning API** area, copy the values for **Post URL** and **Secret Key**.




**Step 6** In the Meraki dashboard, navigate to your specific network and choose **Network-wide** > **Configure** > **General**.

**Step 7** Scroll down to **Location and Scanning** and enable **Analytics and Scanning API**.

**Step 8** In the **Post URLs** field, paste the post URL and secret key.

**Step 9** From the **Location and Scanning** field, copy the **`validator ID`**.

**Step 10** Edit the post URL **`<URLValidator>`** with the validator.

**Step 11** Click **Validate** to validate the post URL functions.

**Step 12** The dashboard opens an Import Networks wizard, select **Meraki Organization > Next > Choose Networks > Import Locations**.

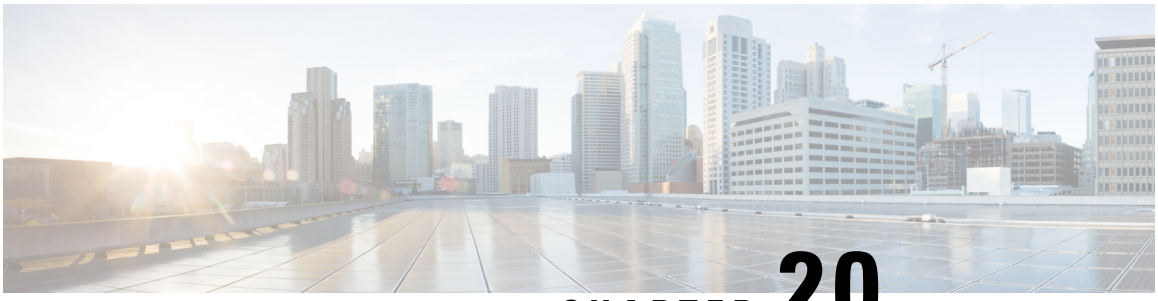
After successful synchronization, verify if the networks are displayed in the **Location Hierarchy**.

**Note**

If IP address restriction is enabled on the Cisco Meraki dashboard, reach out to Cisco Spaces support to add Cisco Spaces IP addresses to the allowed list.

# Wireless Network Status

The **Wireless Network Status** option enables you to view the synchronization status of your wireless network. You can view the time at which the last synchronization happened.



CHAPTER 20

# Set Up Locations and Maps


- Locations and Maps, on page 153
- Import Locations, on page 158
- Add Network Map, on page 169
- Add Digital Map, on page 171
- Catalyst Center Map Export, on page 173
- Setting up Map Service, on page 174


## Locations and Maps

The Locations and Maps feature in Cisco Spaces helps to import, normalize and unify network hierarchies from various sources such as Cisco Meraki, Catalyst Center, and Cisco Prime Infrastructure into a single business-orientated hierarchy. Use this feature as a platform to standardize the network hierarchy structure and provide a standardized location hierarchy view.

Apart from the traditional way of creating location hierarchy by importing/syncing from network sources, this new feature includes a new option to create a business centric hierarchy from a Microsoft Excel (.xlsx) file. The Microsoft Excel (.xlsx) file import allows to perform bulk add/update of the metadata information for multiple locations.

While Cisco Spaces creates a logical location hierarchy matching the network hierarchy, most Cisco Spaces users have one more source where the hierarchy/names differ because of the taxonomy, or because they are managed by different teams/people. With the Locations and Maps feature, you can create a business orientated hierarchy, merge/unify hierarchies from different network sources into the business hierarchy making it a clean unified hierarchy thereby helping in managing various outcomes.

You can import your business locations and organize them within Cisco Spaces based on the physical business locations and network deployments. You can also organize the hierarchy based on specific brands, regions, campuses, and other taxonomies relevant for the business.

The Locations and Maps feature in Cisco Spaces helps to translate your IT network view into a business view and present a cleaner business relevant insights report. Any changes to your network topology are automatically reflected in Cisco Spaces making it easy to manage.

The **Locations and Maps** window has these tabs:

- **Locations**: Use this tab to add or manage locations.
- **Network Maps**: Use this tab to add Network Maps.

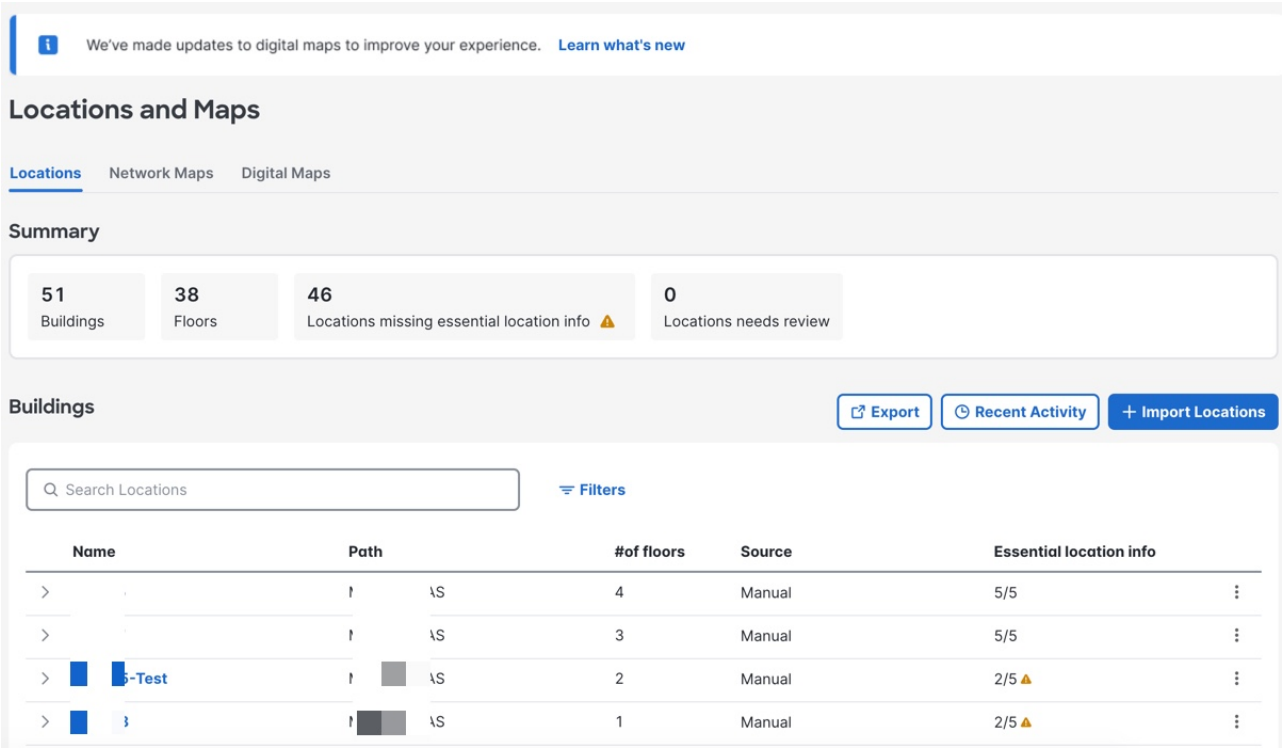
- **Digital Maps**: Use this tab to add or manage Digital Maps.

Use the **Filter** option in these tabs to open the **Filter** drawer, select your filter values, and then apply them to the list.

Each tab under **Setup** > **Locations and Maps** includes a list-level search field and a Filter drawer. You can open the Filter drawer, select one or more filter values, click **Apply**, and remove individual filters by clicking the active filter chips above the table or reset the list by clicking **Clear all**.

You can also narrow the list by selecting a location from the location hierarchy picker within the Filter drawer. This allows you to filter by campus, building, floor, network, or other supported hierarchy levels before applying filters specific to each tab.

***Figure 35: Locations and Maps***




## Locations Tab

The **Summary** section in the **Locations** tab displays the number of buildings and floors. The **Buildings** section in the **Locations** tab displays the following information related to the imported location:

- Name
- Path
- #of Floors
- Source
- Essential Location Info

Perform these tasks:

- Enter the building name in the **Search Locations** field and filter the specified building information.
- Click **Export** to export the location data. You can click **Download** to download the same.
- Click **Recent Activity** to open the **Recent Activity** window and view the recent activity details.
- Click **Import Locations** to import locations. For detailed information, see Import Locations, on page 158.

When no locations are available, the **Locations** tab shows a Day 0 onboarding view with a **Click to Get Started** call to action (CTA). To start importing locations, navigate to **Setup** > **Locations and Maps** > **Locations**, then click either **Click to Get Started** or **Add Locations**.

To filter the Locations list, go to **Setup** > **Locations and Maps** > **Locations** and select **Filter**. In the Filter drawer, you can choose a hierarchy node, one or more Sources, a Number of Floors value or a custom floor range, and Location Metadata status. Click **Apply** to refresh the list.

After applying filters, the active filter options appear above the table. You can remove filters one at a time by clicking the individual filter options or reset the list to show all locations by clicking **Clear all**.

If imported locations require review, a review banner displays the number of pending items. Click **Review** on the banner to open the review workflow, where you can complete actions such as merge, retain, create, skip, or delete as needed.

If essential location information is incomplete, you can update it from the warning message or the row action menu. Navigate to the relevant building in the **Locations** table, click the warning icon or the action menu, and select the metadata update option to complete the missing details.

### Network Maps Tab

The **Network Maps** tab also displays the imported location information. The **Buildings** section in the **Network Maps** tab displays the following information related to the imported location:

- Name
- Path
- #of Floors
- #of APs
- Source
- Network Map Status

Perform these tasks:

- Enter the building name in the **Search Locations** field and filter the specified building information.
- Click **Recent Activity** to open the **Recent Activity** window and view the recent activity details.
- Click **Add Network Map** to add network maps. For detailed information, see, Add Network Map, on page 169.

In the **Network Maps** tab, you can review two summary indicators before uploading or validating maps: the number of buildings with network maps and the number of network maps that are geolocated. These indicators help you confirm how many locations already have map coverage and how many are positioned geographically.

To filter network map results, navigate to **Setup** > **Locations and Maps** > **Network Maps**, then select **Filter**. In the Filter drawer, choose a hierarchy node, one or more Sources, a Number of APs value or custom AP range, and a Number of Floors value or custom floor range. Click **Apply** to refresh the list.

If a building does not yet have a network map, a warning tooltip appears in the building row. Open the tooltip and use the provided action to start the upload or import flow for that building.

### Digital Maps Tab

**Digital Maps** shows 3D visualizations and include all the available features of **Cisco Smart Workspaces**.

The **Digital Maps** tab also displays the imported location information.

The **Buildings** section in the **Digital Maps** tab displays the following information related to the imported location:

- Name
- Path
- #of Floors
- Digital map status
- Actions



**Note** In the **Digital Maps** tab, the **Actions** menu adapts to the building's status. These options are available based on the building state.

- **Add digital maps**
- **Add/update floors**
- **Set default map view**
- **Set address**
- **Confirm address**
- **Review**
- **Cancel**
- **View/Edit**
- **Preview**
- **Delete Digital Map**
- **View History**
- **Export to Catalyst Center**

Perform these tasks:

- Enter the building name in the **Search Locations** field and filter the specified building information.
- Click **Recent Activity** to open the **Recent Activity** window and view the recent activity details.

- Click **Add Digital Map** in the **Actions** column to add digital maps. For detailed information, see Add Digital Map, on page 171.
- You can also click **Upload CAD File** under **Actions** column to add digital maps to the selected location.

To filter digital map results, navigate to **Setup** > **Locations and Maps** > **Digital Maps**, then select **Filter**. In the Filter drawer, choose a hierarchy node, one or more Processing Status values, and a Number of Floors value or custom floor range. Click **Apply** to refresh the list.

After you apply filters, the selected values appear as filter chips above the table. You can remove a single filter from the chip row or click **Clear all** to reset the filtered list.



**Note** Locations with ACT/UNLIMITED licenses have access to digital maps, while the other license types do not support digital maps.

### Digital Maps: User Experience Enhancements

The following enhancements are made in the Cisco Spaces dashboard:

- The **Select Floor** window is redesigned to minimize user effort. The new design reduces the number of entries required from users, enabling a quicker and more efficient process by automatically generating the floor level number and short name for each floor.
- The file upload process is enhanced to improve efficiency. You can now upload files for multiple floors simultaneously, with each being processed in parallel. The full-page loader that previously displayed during single floor uploads is replaced by individual loader indicators for each floor, allowing clear visibility into the status of each upload.

  If any floor file requires additional time, you have the option to cancel that specific upload without affecting the progress of others. This enables better management of successful uploads and more effective time allocation.
- **Map Processing Status Reporting with Estimated Time and Email Notifications**: Map Processing feature is enhanced to address the issues reported with time-intensive map generation. With this enhancement, after you successfully submit the map, the window is displayed with an estimated processing time. You can also view the processing status, including a tentative ETA or error details, by hovering over the status message for each building in the Digital Maps list view. Additionally, the submitter receives email notifications regarding any changes in the map status.
- **Re-Processing Maps/Re-submission of CAD Files**: The map re-processing experience is enhanced to include a feature that allows you to specify the exact changes needed. This helps to reduce the turnaround time. You can select from a list of common reasons and provide additional comments, along with any supporting documents or images as evidence for the re-processing request.

The current processing status experience enhances user interaction by providing richer hover details. When you hover over the processing status, the interface shows floor-level grouping, the submitted date, the expected review timeline, the draft state, and detailed error information for the affected floors.

If a preview session is interrupted, you can resume your previous work or discard unpublished changes. This feature helps you return to unfinished map preparation without restarting the entire workflow.

When you try to save or publish with unsaved editor changes, the interface displays confirmation dialogs. These dialogs let you choose to save and continue or discard the pending edits based on your selected action.

### Network Map Calibration

The **Network Map Calibration** tool enables precise alignment of 2D network map images with 3D **Digital Maps**. You can access the tool from the **Digital Map Editor**, allowing you to precisely place GPS markers ensuring client and access point positions are accurately represented.

The Network Map Calibration link is enabled in the user interface only for maps that have associated network maps.

Use **Network Map Calibration** after you have a digital map preview and a related network map for the same building. Open the Digital Maps editor for that building, launch the calibration tool, and align the network map markers so that device and AP positions match the final map view more accurately. This process helps ensure better accuracy between the network map and the digital map.

# Import Locations

Use the **Locations** tab to import the business hierarchy.

After you successfully import locations, you can immediately review the imported hierarchy and update any incomplete metadata. Then, use the **Filters** option in the **Locations** tab to validate the imported data by source, floor count, or metadata completeness before proceeding to Digital Maps. This process helps ensure your data is accurate and complete before moving forward.

### Procedure

**Step 1** Log in to Cisco Spaces.

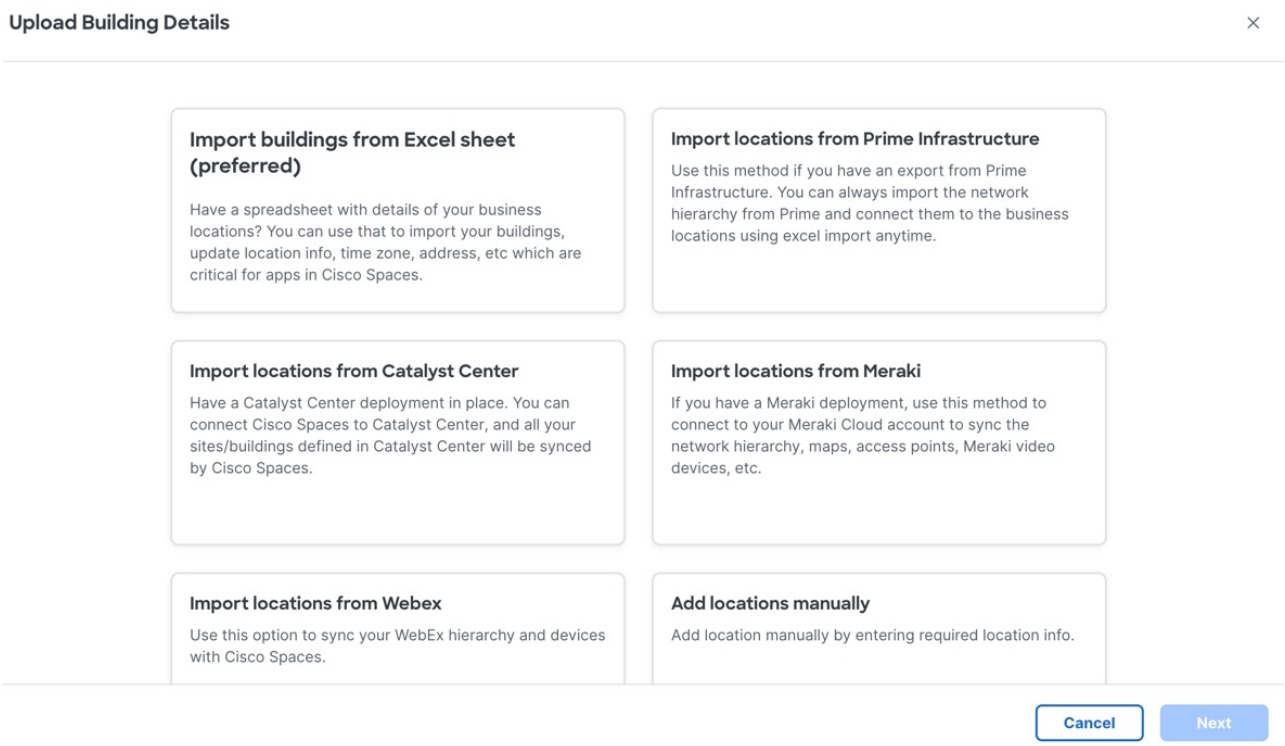
**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed with the **Locations** tab selected. The other tabs available are **Network Maps** and **Digital Maps**.

**Step 3** In the **Locations** tab, click **Add Locations**. If locations are already imported and available, then **Import Locations** option is displayed.

The **Upload Building Details** window is displayed with the various methods to upload the locations.

*Figure 36: Upload Building Details*




**Step 4** Import the locations using the following methods:

- Import buildings from Excel sheet (preferred)
- Import locations from Cisco Prime Infrastructure
- Import locations from Catalyst Center
- Import locations from Cisco Meraki
- Add locations manually

The imported location details are displayed in the **Locations** tab.

- The **Summary** section displays the details of the buildings, floors, missing location metadata information and locations that need review.
- The **Building** section in the **Locations** tab displays the location details such as name, path, number of floors, source and so on.
- In the **Building** section, the **Essential Location Info** field displays an alert if the required location metadata is not updated.

**Step 5** In the **Essential Location Info** field, click **Alert** icon ( ) to add the missing metadata if required.

A pop-up window is displayed with the information related to missing location metadata. Click **Click Here** to update the location info.

**Step 6** Click **Review** to view and proceed with location reviews. For more information, see Review Locations.

The **Review** option is displayed when you import locations using methods other than **Import buildings from Excel sheet** method.

**Step 7** (Optional) In the **Locations** tab, use the following options as required:

- **Export**: Click to export the imported business location details into a Microsoft Excel file (.xls). You can click **Download** to download the same.
- **Recent Activity**: Click to view the recent activity details. The **Recent Activity** slide in window displays the history of activities happened in the recent past.
  - File Name
  - User
  - Type
  - Time
  - Status
- **Filter**: Click to view the filter options. In the **Filter** slide-in window that is displayed, choose the location from the **Locations** drop-down list and the required filter options and click **Apply**. The filter options are: **Source**, **# of Floors** and **Location Metadata**.

# Import Buildings from Microsoft Excel Sheet

Use the **Import buildings from Excel sheet** option to add locations by importing a Microsoft Excel (.xlsx) file. We recommend that you choose this method to import the locations with buildings, location metadata, time zone, address, and so on that are important for Cisco Spaces application.

### Procedure

**Step 1** Log in to Cisco Spaces.

**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed with the **Locations** tab selected.

**Step 3** In the **Locations** tab, click **Add Locations**. If locations are already imported and available, then **Import Locations** option is displayed.

The **Upload Building Details** window is displayed with various methods to upload the locations.

**Step 4** Click **Import buildings from Excel sheet** and click **Next**.

**Step 5** In the **Import Location Details** window, drag and drop the Microsoft Excel (.xlsx) file or click **Click here to upload** to upload the Microsoft Excel (.xlsx) file with details of the business locations to be imported.

**Note**

If you do not have the template, you can download the template from the link available in the **Import Location Details** window and upload the same with the building details in the correct format.

**Step 6** Click **Next**.

The **Import Location Details** window is displayed with location information from the Microsoft Excel (.xlsx) file in the left column and existing location level and group level information in the right column.

**Step 7** In the **Import Location Details** window, map the imported location metadata in the **Column from CSV** column with the corresponding hierarchy and group levels under the **Link to** drop-down and assign respective location metadata values accordingly.

The options available in the **Link to** drop-down are:

- **Location Info**: Use this for location metadata information such as Country, City, Occupancy, Band, Address, Time Zone and so on. You must assign a corresponding metadata value also.
- **Hierarchy Level**: Use this to map the **Level** column value from the Microsoft Excel (.xlsx) file. The Microsoft Excel (.xlsx) file can have multiple **Level** values. Level values from the Microsoft Excel (.xlsx) file are mapped as **Hierarchy Level** in the Location Hierarchy.

  For each **Hierarchy Level**, you can assign a grouping level value. The options are: **Grouping Level1**, **Grouping Level2** and **Grouping Level3**.

  In the Microsoft Excel (.xlsx) file, you can have `NYC1 Campus` as **Level1** and `NYC2 Campus` as **Level2**. In the **Import Location Details** window, you can map **Level1** and **Level2** with **Hierarchy Level** in the **Link to** drop-down list. For **Level1**, you can assign the grouping value as **Grouping Level1** and **Grouping Level2** for **Level2**.
- **Location Name**: Use this to map with the **Location** column value from the Microsoft Excel (.xlsx) file.

  **Note**
  You need not assign any value for **Location Name**. The location name is directly fetched from the Excel file and cannot be modified or mapped with any header columns.
- **Location ID**: The Location ID is auto-generated after the location import is successfully complete.

**Step 8** Click **Next**.

The **Merge Locations** window is displayed.

- A message indicating that the Location Hierarchy in Cisco Spaces is updated to include new locations discovered by importing the Microsoft Excel (.xlsx) file.
- The **Merge Locations** window displays the number of new locations and their levels imported using **Import buildings from Excel sheet** method.
- The **Merge Locations** window displays three columns: **Locations found in CSV**, **Actions** and **Existing Locations**.
- You must review the hierarchy and take necessary action using the **Action** drop-down list.
- You can use the **Search Location** field to enter search criteria and search for location name.

**Step 9** In the **Locations found in CSV**, click the plus symbol to expand the location.

**Step 10** From the **Actions** drop-down list, select the required action to merge the imported location with the existing Location Hierarchy displayed on the right side.

The options are:

- **Create New**: Select this option if you want to create the imported location as a new location into the existing Location Hierarchy.
- **Merge With**: Select this option if the imported locations from the Microsoft Excel (.xlsx) file are repeating and the location already exists in the Location Hierarchy. We recommend that you perform this action with attention as you cannot revert once you merge the locations.
- **Skip**: Select this option if you want to skip importing the locations into the Location Hierarchy. We recommend that you perform this action with attention as you cannot revert once you skip the locations.

**Note**
In the existing Location Hierarchy:

- If there are no existing campuses or buildings, the new imported locations are added as new entries.
- If there are locations with similar name, you can merge the new locations with the existing ones.

**Step 11** Click **Next**.

You need to review the merge location updates displayed in the **Merge Locations** section. You can view the number of locations that are processed.

**Step 12** Click **Submit**.

A success message is displayed indicating that the location details are uploaded.

You can click **Add Digital Maps** if you want to add digital maps or **View Locations** to view the locations.

**Step 13** Click **Close this window** to return back to **Locations** tab.
The **Building** section in the **Locations** tab displays the location details such as name, path, number of floors, source and so on. The **Summary** section displays the details of the buildings, floors, missing location metadata information and locations that need review.

# Import Locations from Cisco Prime Infrastructure

Use the **Import locations from Prime Infrastructure** option to add locations using an export file from Cisco Prime Infrastructure into Cisco Spaces. You can import the network hierarchy from Cisco Prime Infrastructure and connect them to the business locations.

### Procedure

**Step 1** Log in to Cisco Spaces.

**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed with the **Locations** tab selected.

**Step 3** In the **Locations** tab, click **Add Locations**. If imported locations are already available, then **Import Locations** option is displayed.

The **Upload Building Details** window is displayed with the various methods to upload the locations.

**Step 4** Click **Import locations from Prime Infrastructure** and click **Next**.

The **Import Location Details** window is displayed.

**Step 5** In the **Import Location Details** window, drag and drop the Cisco Prime Infrastructure map file as a .GZ file (compressed archive file) or click **Click here to upload** to upload the .GZ file with the Cisco Prime Infrastructure map information.

**Step 6** Click **Next**.

The **Import Location Details** displays a message indicating that the map data is processing. The Map Service takes some time to process the same. You can verify the map data processing status in the **Recent Activity** section.

After the map data is processed successfully, you must merge the map data with the locations.

**Step 7** Click **Close this window** to close the window.

The **Building** section in the **Locations** tab displays the newly imported location details. The same location information is also displayed in the Cisco Spaces Location Hierarchy.

An alert message indicating that the import of maps from Cisco Prime Infrastructure added new locations to the Location Hierarchy is displayed in the **Location** tab.

**Step 8** Click **Review** to review and take appropriate action.

The **Merge Locations** window is displayed.

- A message indicating that the Location Hierarchy in Cisco Spaces is updated to include new locations discovered by importing Cisco Prime Infrastructure maps.
- The **Merge Locations** window displays the number of new sites and building imported using **Import locations from Prime Infrastructure** method.
- The **Merge Locations** window displays three columns: **Locations from Prime Map**, **Actions** and **Existing Locations**.
- You must review the hierarchy and take necessary action using the **Action** drop-down list.
- You can use the **Search Location** field to enter search criteria and search for location name.

**Step 9** In the **Locations from Prime Map**, click the plus symbol to expand the location.

The location hierarchy includes campus, buildings, and floors.

**Step 10** From the **Actions** drop-down list, select the required action to merge the imported location with the existing Location Hierarchy displayed on the right side.

The options are:

- **Merge With**: Select this option if the imported locations from Cisco Prime Infrastructure are repeating and the location already exists in the Location Hierarchy. We recommend that you perform this action with attention as you cannot revert once you merge the locations.
- **Delete**: Select this option if you want to remove the imported locations from the existing Location Hierarchy. We recommend that you perform this action with attention as you cannot revert once you delete the locations.
- **Create New**: Select this option if you want to create or add a new location into the existing Location Hierarchy.
- **Accept**: Select this option if the locations imported from Cisco Prime Infrastructure are accepted as it is with the existing Location Hierarchy.

**Note**
In the existing Location Hierarchy:

- If there are no existing campuses or buildings, the new imported locations are added as new entries.
- If there are locations with similar name, you can merge the new locations with the existing ones.

**Step 11** Click **Next**.

You need to review the merge location updates displayed in the **Locations** section. You can view the number of locations that are processed.

**Step 12** Click **Submit**.

A success message is displayed indicating that the location details are uploaded.

You can click **Add Digital Maps** if you want to add digital maps or **View Locations** to view the locations.

**Step 13** Click **Close this window**.

The **Building** section in the **Locations** tab displays the location details such as name, path, number of floors, source and so on.

The **Summary** section displays the details of the buildings, floors, missing location metadata information and locations that need review.

# Import locations from Cisco Catalyst Center

Use the **Import locations from DNA Center** option to add locations from Catalyst Center. You can connect Cisco Spaces to Catalyst Center and all the sites or buildings defined in Catalyst Centeris synchronized with Cisco Spaces.

**Procedure**

**Step 1** Log in to Cisco Spaces.

**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed with the **Locations** tab selected.

**Step 3** In the **Locations** tab, click **Add Locations**. If locations are already imported and available, then **Import Locations** option is displayed.

The **Upload Building Details** window is displayed with various methods to upload the locations.

**Step 4** Click **Import locations from DNA Center** and click **Next**.

To import locations from Catalyst Center, you must integrate Catalyst Center maps with Cisco Spaces.

**Step 5** (Optional) Click **View How to Integrate DNA Center Maps**.

The **Cisco DNA Center Integration** window is displayed.

Cisco Spaces integrates with Catalyst Center for map synchronization and to provide device location updates to Catalyst Center. To integrate Cisco Spaces with Catalyst Center, click **Create Token** to create a token and configure the token in Catalyst Center.

**Note**
Cisco Spaces integration feature in Catalyst Center is available for limited users. For additional support, contact Cisco Spaces support team.

**Step 6** Click **Next**.

The **Import Location Details** window is displayed.

**Step 7** Follow the instructions to connect the Catalyst Center.

**Step 8** Click **Finish**.

The **Building** section in the **Locations** tab displays the location details. The **Summary** section displays the details of the buildings, floors, missing location metadata information, and locations that need review.

# Import locations from Cisco Meraki

Use the **Import locations from Meraki** option to add locations from Cisco Meraki. If you have a Cisco Meraki deployment, use this method to connect to your Cisco Meraki Cloud account to synchronize the network hierarchy, maps, Access Points, and Meraki video devices.

**Procedure**

**Step 1** Log in to Cisco Spaces.

**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed with the **Locations** tab selected.

**Step 3** In the **Locations** tab, click **Add Locations**. If locations are already imported and available, then **Import Locations** option is displayed.

The **Upload Building Details** window is displayed with various methods to upload the locations.

**Step 4** Click **Import locations from Meraki** and click **Next**.

The **Import Location Details** window is displayed.

To import locations from Cisco Meraki, you must connect your Cisco Meraki with Cisco Spaces.

**Step 5** (Optional) Click **View How to Integrate Meraki** to view the instructions.

**Step 6** In the **Import Location Details** window, click **Next**.

**Step 7** Read the instructions to connect Cisco Meraki and click **Next**.

The **Connect your wireless network** window is displayed. You can connect use this option to connect to Cisco Meraki.

**Step 8** If you are already connected, proceed with adding locations using the Location Hierarchy.

# Add Locations Manually

Use the **Add locations manually** option to add a standalone building directly under the root location without importing a Microsoft Excel (.xlsx) file or a network map.

## Procedure

**Step 1** Log in to Cisco Spaces.

**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

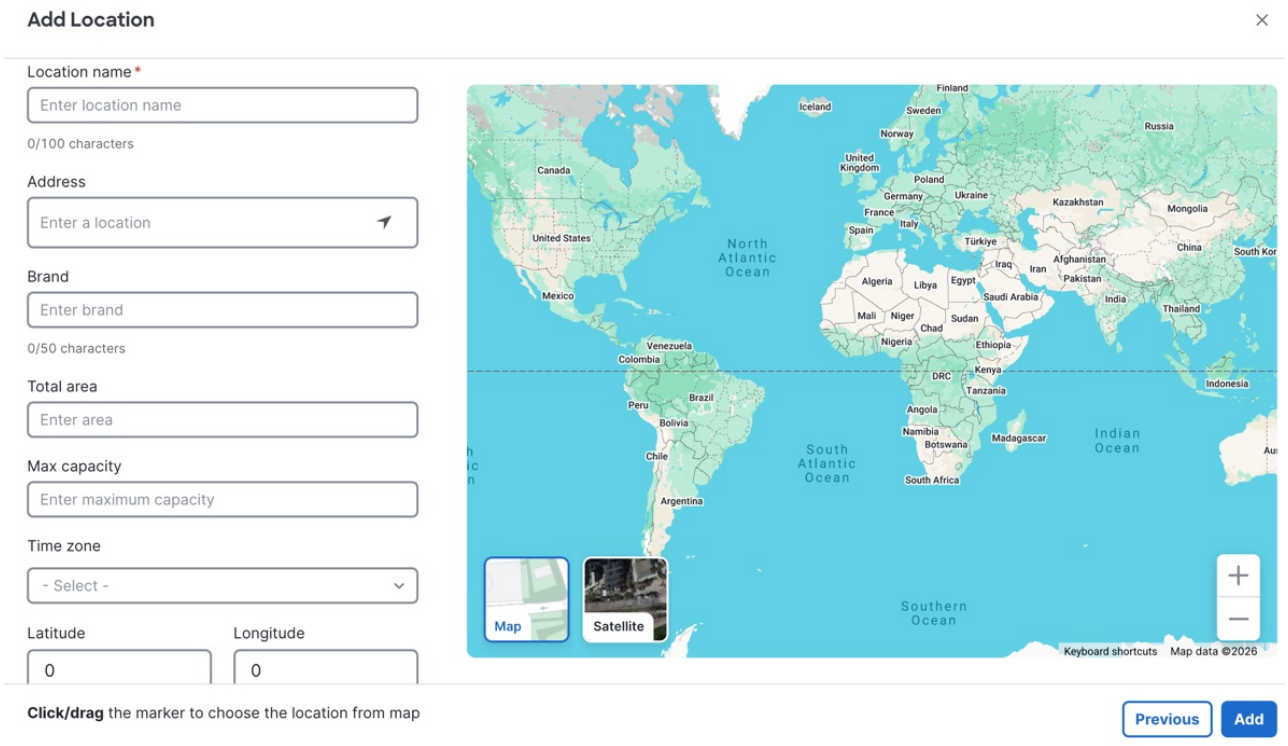
The **Locations and Maps** window is displayed with the **Locations** tab selected.

**Step 3** In the **Locations** tab, click **Add Locations**. If locations are already imported and available, then **Import Locations** option is displayed.

The **Upload Building Details** window is displayed with the various methods to upload the locations.

**Step 4** Click **Add locations manually** and click **Next**.

***Figure 37: Add Location***




**Step 5** In the **Add Location** window, enter the following location details to add a new location:

- **Location Name**: Name for the new location.
- **Brand**: Brand for the new location.

- **Total Area**: Total area details for the new location.
- **Max Capacity**: Maximum capacity information for the new location.
- **Address**: The address of the new location. You can manually enter the address or drag the marker to choose the address from map displayed on the right side.
- **Time Zone**: Select the time zone from the drop-down list.
- **Latitude**: Latitude of the new location.
- **Longitude**: Longitude of the new location.

**Step 6** Click **Add**.

A success message is displayed indicating that a new location is added. You can click **Add Another Location** if you want to add more locations manually.

**Step 7** Click **Done**.

The **Building** section in the **Locations** tab displays the location details. The Summary section displays the details of the buildings, floors, missing location metadata information and locations that need review.

# Update Location Information

The **Locations** tab displays an alert message if location metadata is missing for the imported location.

You can update location information as part of map preparation. You refine the building address, verify geo-coordinates, and save corrected metadata before proceeding to floor selection or map upload workflows.

### Procedure

**Step 1** Log in to Cisco Spaces.

**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed with the **Locations** tab selected.

**Step 3** In the **Buildings** section, next to Essential Location Info field, click the Alert icon to update the missing location metadata.

The **Update Location Info** window is displayed.

**Step 4** In the **Update Location Info** window, update the following location details as required:

- **Location Name**: Name for the new location.
- **Brand**: Brand for the new location.
- **Total Area**: Total area details for the new location.
- **Max Capacity**: Maximum capacity information for the new location.
- **Address**: The address of the new location. You can manually enter the address or drag the marker to choose the address from map displayed on the right side.

- **Time Zone**: Select the time zone from the drop-down list.
- **Latitude**: Latitude of the new location.
- **Longitude**: Longitude of the new location.

**Step 5** Click **Save**.

# Review Locations

In the **Locations and Maps** window, an alert message is displayed if the imported location hierarchies need review. You need to review the locations and need necessary actions.

During review, the system validates unsupported merge combinations and displays actionable error messages. The interface prevents unsupported merges such as Webex-to-Webex, Meraki-to-Meraki, certain same-source hierarchy merges, and floor merges that do not correspond to the correct building context.

If you must merge a floor, first complete the review and merge steps for the parent building. Then return to the floor-level review items. This process keeps the final hierarchy consistent and prevents invalid merges between floors or between floors and different buildings.

### Procedure

**Step 1** In the **Locations and Maps** window, click **Preview** to view and proceed with location reviews.

The **Review Locations** window displays all sources from which locations are imported, for example, Cisco Meraki or Catalyst Center. You can also view the number of sites, buildings and campuses imported for each location.

**Step 2** Select the source location to review and click **Next**.

The **Review Locations** window displays the imported location hierarchy levels for the selected source in the left column and existing destination location hierarchy levels in the right column. Use the **Search Locations** field to search for specific locations.

**Step 3** Use the options available in the **Action** drop-down list and select a recommended action to merge each level in the source location hierarchy with a relevant destination business hierarchy level in the right column.

By default, Cisco Spaces recommends some actions for reviewing the imported location hierarchy. The available actions are: Merge with, Accept, Create New and Delete.

- The action that you opt for the highest node in the source location hierarchy is automatically cascaded over to the subsequent nodes.
- You cannot delete a campus node from the source location hierarchy if the levels under the campus node are already merged with any relevant destination business hierarchy level.
- You cannot merge a building from the source location hierarchy to a campus in the destination business hierarchy.
- You can merge a site from the source location hierarchy to a campus in the destination business hierarchy.
- If the name of the source location hierarchy matches with any business hierarchy available in Cisco Spaces Location Hierarchy, then Cisco Spaces automatically displays the matching destination levels, and you proceed with the merge action.

- If the source location hierarchy is new, then select **Create** action to automatically create a new business hierarchy in Cisco Spaces Location Hierarchy.

**Step 4** From the **Existing Locations** drop-down list, select the relevant destination level to merge and unify the imported location hierarchies from any source location with the business hierarchy available in Cisco Spaces Location Hierarchy.

The **Existing Locations** drop-down list displays all the destination nodes available in the Cisco Spaces Location Hierarchy. You can view the source from where the business hierarchy is imported in the drop-down list.

**Step 5** Click **Next**.

The **Merge Locations** window displays the summary of the actions and its implications with respect to the associated analytics data. We recommend that you review this alert information before proceeding.

**Note**
If a location that you selected to be deleted includes rules associated with it, you cannot proceed with the delete action. You need to review the action and update your merge preferences accordingly.

If a location that you selected to be deleted includes reports associated with it, you can proceed with the delete action. The reports are generated again after the locations are merged.

**Step 6** Click **Agree and Continue**.

The selected review actions are processed, and the location is marked as reviewed. If you select to merge the source location level with a relevant destination node, all the properties of the source location levels are applied to the destination node in the business hierarchy.

# Add Network Map

Use the **Network Maps** tab to add a network map and view the locations with the network maps associated with it. You can import locations only if the source has network maps associated with it. Currently, Cisco Prime Infrastructure, Catalyst Center, Cisco Meraki and Cisco Connected Mobile Experiences includes network maps.

In addition to the basic add-network-map workflow, the current page supports filter-based validation of imported network map coverage. Use the Filter drawer to narrow the list by hierarchy, source, number of APs, and number of floors before taking action on a building.

If a location does not yet have a network map, use the row-level warning tooltip to open the upload or import path for that building.

### Procedure

**Step 1** Log in to Cisco Spaces.

**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed.

**Step 3** Click **Network Maps** tab.

**Step 4** Click **Add Network Map**.

The **Upload Building Details** window is displayed.

**Step 5** Import the locations using the following methods that include network maps:

- Import locations from Cisco Prime Infrastructure
- Import locations from Catalyst Center
- Import locations from Cisco Meraki
- Import locations from Cisco CMX
- Add locations manually

The imported location details are displayed in the **Locations and Maps** window under the **Network Maps** tab.

**Step 6** Click **Preview** to view and proceed with location reviews. For more information, see Review Locations.

**Step 7** (Optional) In the **Network Maps** tab, use the following options as required:

- **Export**: Click to export the imported business location details into a Microsoft Excel file (.xls). You can click **Download** to download the same.
- **Recent Activity**: Click to view the recent activity details. The **Recent Activity** slide-in window displays the following information:
  - File Name
  - User
  - Type
  - Time
  - Status
- **Filter**: Click to view the filter options. In the **Filter** slide-in window that is displayed, choose the location from the **Locations** drop-down list and the required filter options and click **Select** to apply.

# Import locations from Cisco CMX

Use the **Import locations from CMX** option to import locations from Cisco CMX. You must tether Cisco CMX with Cisco Spaces to import locations.

### Procedure

**Step 1** Log in to Cisco Spaces.

**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed.

**Step 3** Click **Network Maps** tab.

**Step 4** Click **Add Network Map**.

The **Upload Building Details** window is displayed with various methods to upload the locations.

**Step 5** Click **Import locations from CMX** and click **Next**.

The **Import Location Details** window is displayed.

**Step 6** (Optional) Click **Learn how to tether CMX** to view the instructions to tether Cisco CMX with Cisco Spaces. For more information, see Cisco CMX Tethering.

**Step 7** In the **Import Location Details** window, click **Next**.

**Step 8** Read the instructions to connect Cisco CMX and click **Next**.

The **Connect your wireless network** window is displayed. Use this option to connect to Cisco CMX.

**Step 9** If you are already connected, proceed with adding locations using the Location Hierarchy.

# Add Digital Map

Use the **Digital Maps** tab to add digital maps for buildings in your location hierarchy. You need to upload the Computer-aided design (CAD) file(s) for the floor to convert them into a three-dimensional floor plan.

The **Summary** area displays the number of buildings for which digital maps are imported, number of buildings for which map review is pending and number of buildings with errors.

The **Buildings** area displays the locations available.

Working with your building floor plans is more efficient than ever with the redesigned Digital Maps management. The new listing screen provides a floor-level view with contextual actions based on each floor's status—from setting the building address to adding floors, uploading CAD files, and reviewing, editing, or publishing maps.

Granular per-floor statuses replace the earlier building-level view, and each floor can be reviewed and published independently on its own schedule.

### Procedure

**Step 1** Log in to Cisco Spaces.

**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed.

**Step 3** Click **Digital Maps** tab.

**Step 4** Select the building or floor you want to add digital maps.

**Step 5** In the **Actions** column, click **Add digital maps**.

The **Add Digital Map: Support DNA** window is displayed.

a) Read through the CAD file (.dwg) or Vector PDF related information displayed.

b) Click **Proceed**.

**Step 6** To confirm the address, complete these steps and click **Confirm Address**.

a) To select the location, either enter the building name in the **Search** field or click directly on the map to place a marker.

b) Alternatively, click and drag the marker to adjust the location on the map as needed.

Verify that the building location on the map is correct.

**Note**
If you want to choose the location from the map displayed on the right panel, you need to provide permission to Cisco Spaces to use the current location to populate the geo-coordinates.

**Step 7** Upload source files to use for Digital Maps generation. You can drag and drop files to the designated upload section or click **Choose file** to browse locally and upload them.

**Note**

- Upload only one CAD file per floor. Cross references (XREFs) are not supported.
- The supported file types are ZIP, AutoCAD Drawing file (DWG), AutoCAD Drawing Interchange File (DXF), Portable Document Format (PDF).
- You can upload one file per floor or use **Bulk Upload** to upload multiple source files together. The page displays per-floor upload progress and lets you cancel or replace an upload if needed.

  If you perform a bulk upload after individual floor files are already staged, a confirmation pop-up appears. Confirm the bulk action to replace the existing staged files for that workflow.

  When you upload a file identical to a previously processed one, the interface requires you to provide a re-processing reason and additional comments. Select a reason, enter comments explaining the correction, and optionally upload supporting evidence such as reference files or explanatory documents. You can upload supporting files from the floor card when more context is needed for re-processing.

  For buildings in review or draft state, you can use **View/Edit** or **Review** from the window to reopen the editor. When a building has an in-progress PRO map workflow, the contextual menu also shows **Preview** option, allowing you to inspect the current generated state.

**Step 8** Click **Submit**.

**Step 9** Click **Review** if the map is processed and ready to review.

**Step 10** In the **Review Digital Maps** window, select the building you want to review and click **Next**.

The digitized map is displayed.

**Step 11** (Optional) Select a floor or space and click to update them if required.

A pop-up window is displayed, and you can edit the name or update the type category.

**Step 12** Click **Publish this Building**.

The digitized map is published and available for other applications to use them, for example, Cisco Smart Workspaces, Environmental Metrics app and so on.

In Cisco Spaces Location Hierarchy, for a selected location, digital maps are displayed by default if the location has digital maps.

Click **Skip this building** if you want to discard the changes.

Additionally, use the **View History** option to inspect building-level map workflow events and **Delete Digital Map** option to remove an existing digital map when you have the appropriate permissions and state conditions are met.

# Catalyst Center Map Export

In **Locations & Maps**, the **Digital Maps** feature (**Setup** > **Locations & Maps** > **Digital Maps**) lets you export building maps (published version) to Cisco Catalyst Center.

The option to export is available only for buildings with a published map.

The map export feature works only if the APs are placed under the **Setup** > **Device Placement** option.

## Export Building Maps to Catalyst Center

**Before you begin**

The **Export** option is not available in these scenarios:

- When using an older version of the Cisco Spaces dashboard UI. We recommend that you switch to the beta version of the dashboard to access this feature.

  For locations where Access Points (APs), configured via the **Device Placement** feature, are not placed using PRO maps.

  The Rich Map must not be in any of these statuses:

  - Processing
  - Error
  - Cancelled
  - Review
  - Deleted

To support network planning and monitoring, you can export the published version of a building's digital map from Cisco Spaces to Catalyst Center.

Use the **Export to Catalyst Center** feature in Cisco Spaces to seamlessly transfer building maps to Catalyst Center.

Use the **Export to Catalyst Center** to export building maps (published version) to Catalyst Center.

You start the export from the building row action menu after the building map is in a supported published state.

**Procedure**

**Step 1** Log in to Cisco Spaces.

**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Locations and Maps**.

The **Locations and Maps** window is displayed with the **Locations** tab selected.

**Step 3** Click the three dots next to a building and select **Export to Catalyst Center** to process the map.

When the export starts, the UI shows a processing state while it prepares the ZIP package. After the export completes successfully, the **Download** option is displayed.

**Note**
If the export cannot complete for the selected building, an error message is displayed indicating that the building is not currently supported for this export action.

**Step 4** Click **Download** to save the processed digital map (in ZIP format) for the selected building.

**Step 5** Follow the instructions in the pop-up window to import the map hierarchy into Catalyst Center.

# Setting up Map Service

Use **Map Service** in Cisco Spaces to import or synchronize multiple campuses with the same name under different sites into Cisco Spaces **Location Hierarchy** from Catalyst Center. You can move campuses between sites within Catalyst Center and allows to seamlessly import and synchronize these changes into the Cisco Spaces **Location Hierarchy**.

**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 is 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 **Recent Activity** section shows the entire hierarchy in the **Recent Activity** 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 recent activity 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

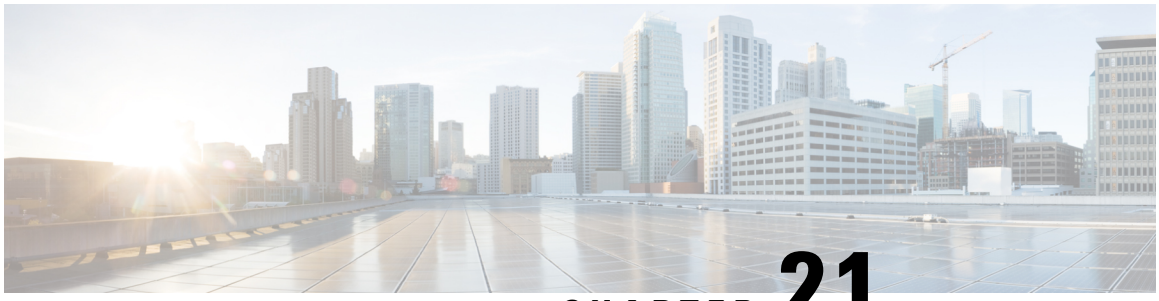
Click **Maps Upload** to upload maps from Cisco Prime Infrastructure or Catalyst Center. In the **Maps Upload** pop-up window, select the required option and click **Select File** and to upload the maps downloaded from the sources.

**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 21

# Set Up Cisco Webex

This chapter provides information on how to integrate Cisco Webex with Cisco Spaces.


- Integrate Cisco Webex, on page 177
- Set Up Cisco Webex, on page 178
- Generate an Activation Code, on page 178


## Integrate Cisco Webex

The integration of Cisco Webex with Cisco Spaces enables Cisco Webex devices in the **Webex Control Hub** account to perform a cloud-to-cloud integration between **Webex Control Hub** and Cisco Spaces.

**Note** Cisco Webex integration supports only **Cisco Smart Workspaces** users.

This integration supports:

- Synchronization of Cisco Webex entities such as Cisco Webex workspaces, devices, workspace locations, and floor details from the **Webex Control Hub**. The synchronization process is scheduled at the backend every three hours after the token is configured in the Cisco Spaces dashboard. Choose **Setup** > **Webex** to configure the tokens.
- Cisco Webex devices to send device data such as temperature, air quality, occupancy, and so on, which is then used in **Cisco Smart Workspaces**.

As part of **Cisco Webex** integration, Cisco Spaces supports integration with persistent web app for **Cisco Webex** navigators. When a customer activates the control hub integration with Cisco Spaces, the necessary configuration supporting this integration is updated in the **Cisco Webex** control hub.

**Note** Currently, this integration is only available for **Cisco Smart Workspaces** users.

# Set Up Cisco Webex

You can connect your Cisco Webex account to Cisco Spaces and then import the Cisco Webex networks into Location Hierarchy.

### Procedure

**Step 1** Log in to Cisco Spaces.

**Step 2** In the Cisco Spaces dashboard, click the **Menu** icon ( ) and choose **Setup** > **Webex**.

**Step 3** In the **Connect your Webex** window, click **Connect**.

The Webex Token slider is displayed.

**Step 4** In the **Enter or copy-paste your Webex Token** field, enter the Cisco Webex token.

You can get the token from the **Webex Control Hub**. For more information about generating an activation code, refer to Generate an Activation Code, on page 178.

**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**.

# Generate an Activation Code

Use the Cisco Webex Control Hub to generate code.

### Procedure

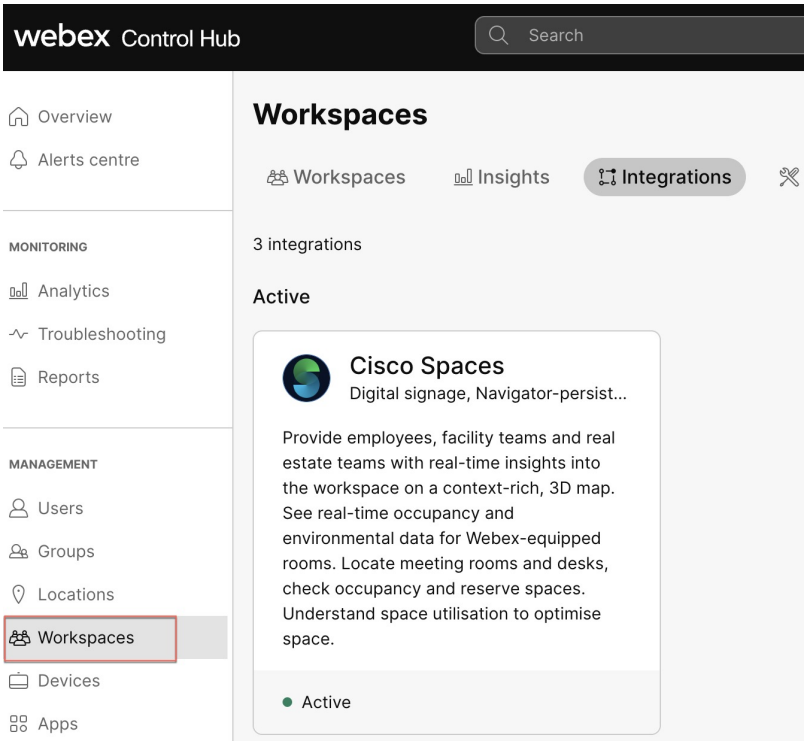
**Step 1** Log in to Cisco Webex Control Hub.

**Step 2** Enter your **Cisco Webex Control Hub** account email ID to sign in.

**Step 3** In the **Cisco Webex Control Hub** dashboard, choose **Management** > **Workspaces**.

**Step 4** Click the **Integrations** tab.

*Figure 38: 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.