

# 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 1
- Process Flow for Cisco Spaces, on page 3
- Cisco Spaces License Packages, on page 3
- Cisco Spaces License Types and Features Compatibility, on page 6
- Log In, on page 9
- Cisco Federation Process, on page 11
- Start Working with Cisco Spaces, on page 19
- Cisco Spaces Dashboard GUI Enhancements, on page 21
- Verticals overview, on page 23
- Cisco Meraki Integration Workflow, on page 23
- Manage Networks in Cisco Meraki Dashboard, on page 24
- Cisco Magnetic Design, on page 24
- Cisco Spaces: Connector 3.0, on page 25
- Idle Timeout for Cisco Spaces, on page 25
- Migrate Data from Cisco Prime Infrastructure to Catalyst Center, on page 25
- Contact Cisco Spaces Support, on page 25
- Cisco Spaces Documentation, on page 28


# Overview of Cisco Spaces

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

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

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

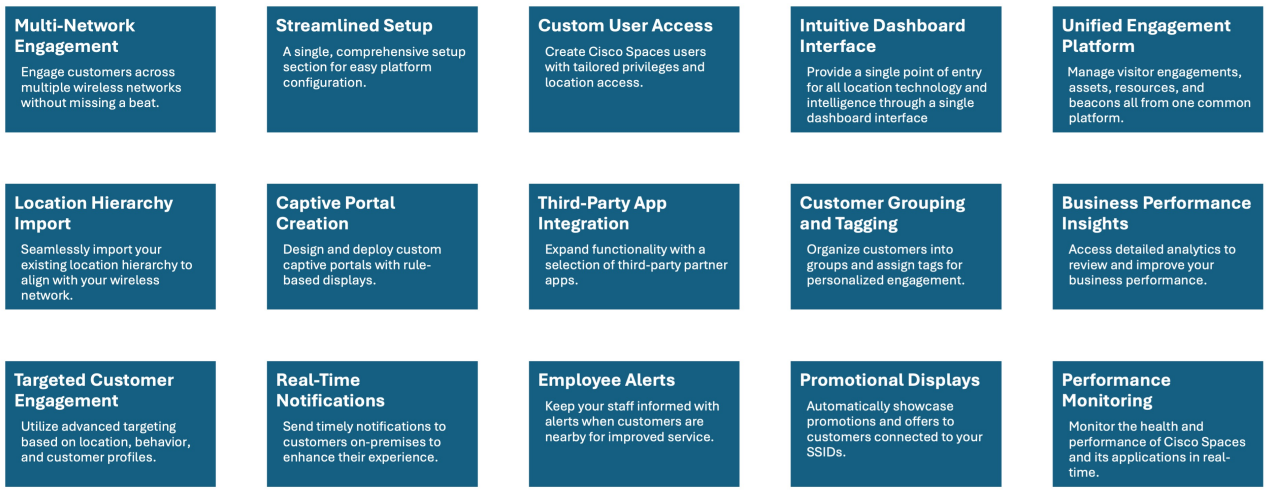
It covers various verticals of business such as

- retail

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

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

***Figure 1: Feature Highlights***




## Use Case Scenario

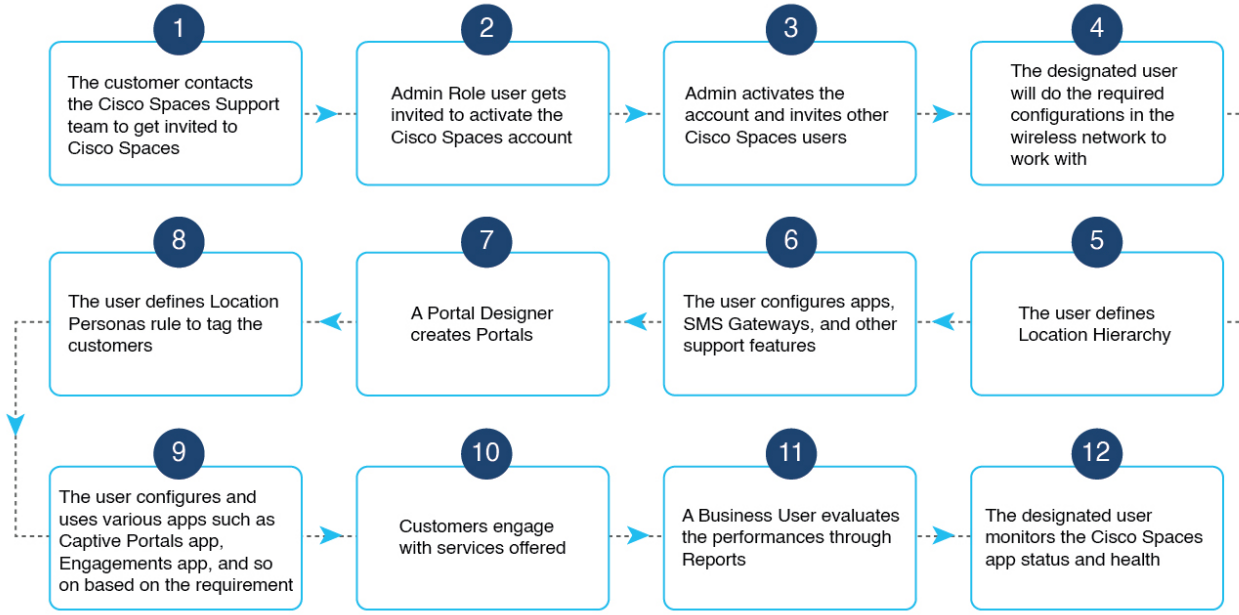
In the ABC shopping mall, to get free Wi-Fi, the customers must connect to an SSID once they enter the mall. ABC wanted to provide a personalized experience to each customer who connects to the Wi-Fi based on their purchase history and visit frequency. After installing Cisco Spaces, ABC could collect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

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

# Process Flow for Cisco Spaces

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

***Figure 2: Process Flow for Cisco Spaces***




# Cisco Spaces License Packages

### Overview of Cisco Spaces License Packages

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

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

The Cisco Spaces License package supports these licenses:

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

- **PREMIER (CW)**

### License Information

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

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

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

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

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

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

### Licensing Options

The Cisco Spaces licensing options are:

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

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

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



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

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

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

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

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

For information about features included in Cisco Spaces, refer to Cisco Spaces License Types and Features Compatibility, on page 6 and the Cisco Spaces Data Sheet.

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

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

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

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

**Note** Contact Cisco Spaces support team:

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

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

***Table 1: License Consumption***

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

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

# Cisco Spaces License Types and Features Compatibility

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

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

***Table 2: Feature Compatibility***

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

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

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

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



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

# Log In

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

The new workflow is applicable to the following users:

- Cisco domain users
- Customer domain non-SSO users

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

**Note**

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

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

### Procedure

**Step 1** Go to Cisco Spaces.

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

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

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

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

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

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

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

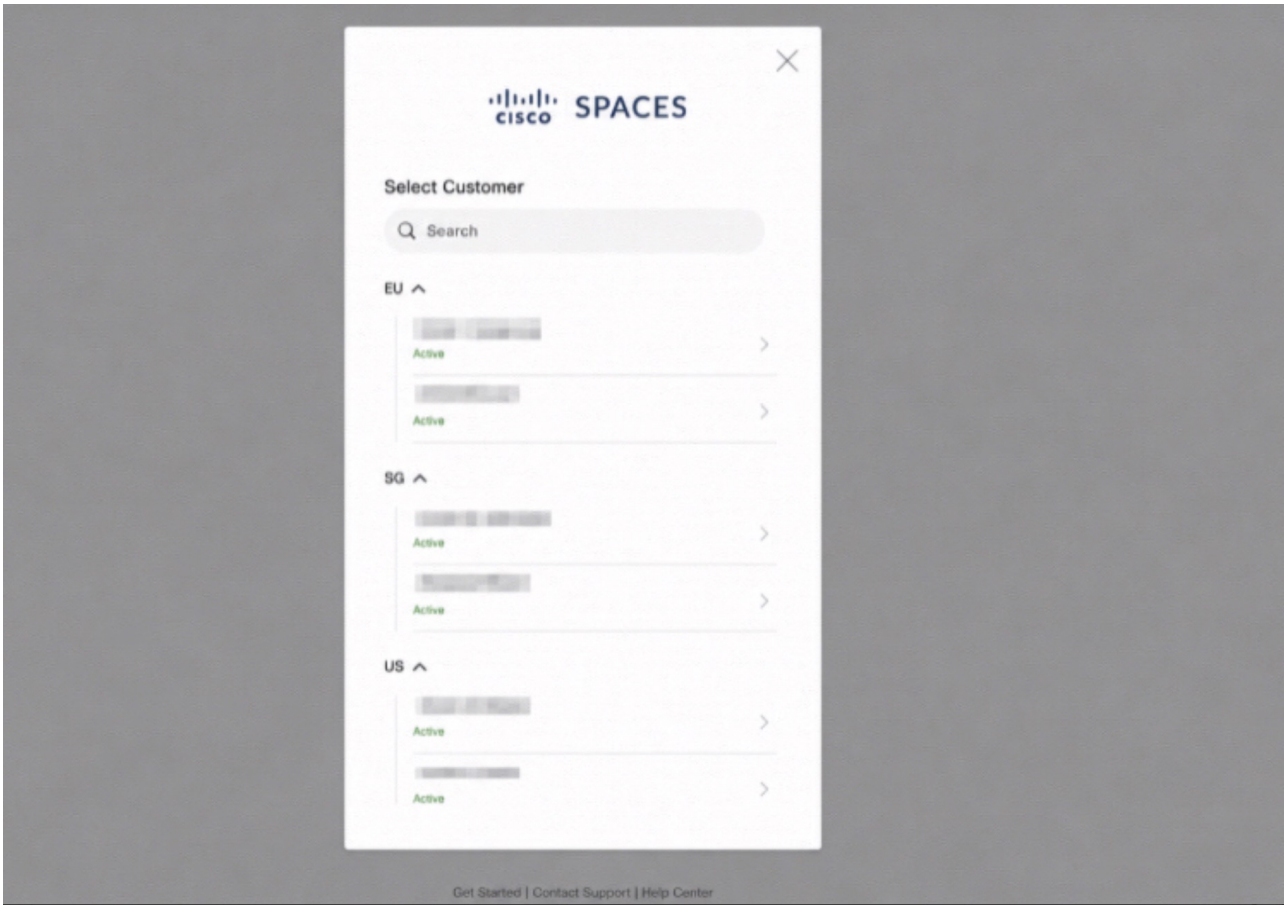
**Step 4** In the **Password** field, enter your password.

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

**Step 5** Click **Log In**.

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

*Figure 3:*




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

**Step 7** Click the required customer account.

Cisco Spaces dashboard Home page is displayed.

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

# Cisco Federation Process

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

Key benefits

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

### Cisco Customer Identity integration

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

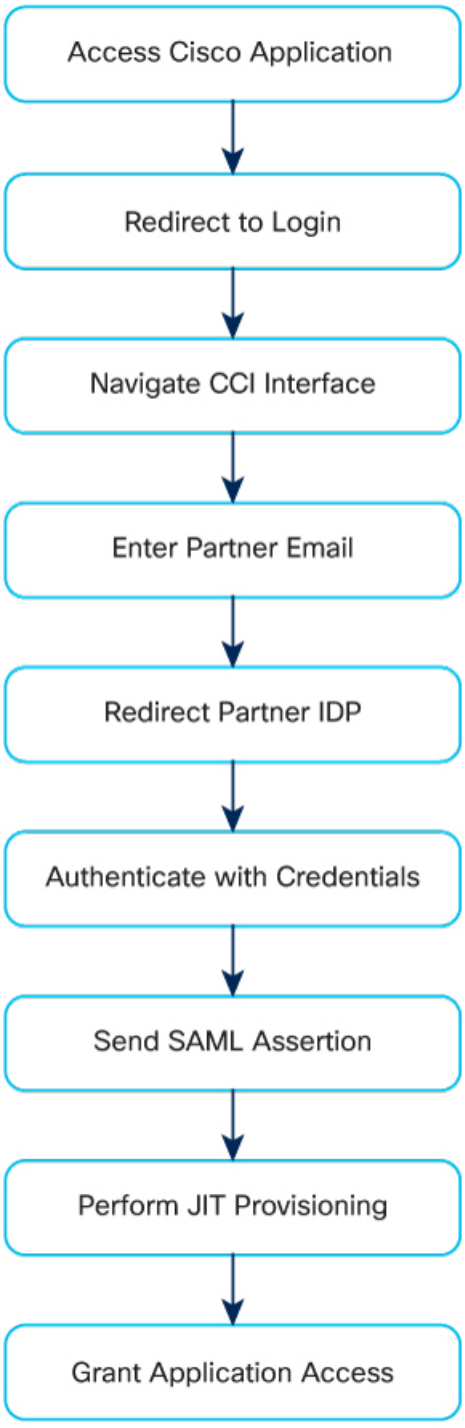
Legacy onboarding used separate IDPs for Cisco Spaces, which created challenges when enabling other applications. Cisco Customer Identity (CCI) provides a common authentication interface that prevents future integration issues for non-CCI customers. To ensure compatibility with the evolving Cisco product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

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

Key attributes:

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

*Figure 4: Authentication workflow*



# Set Up SSO for Cisco Spaces with Cisco Customer Identity

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

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

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

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

**Before you begin**

Ensure that these requirements are met:

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

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

***Table 3: Metadata***

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

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

Your SAML assertion must include these mandatory user attributes:

- `firstName`

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

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

Follow these steps to configure SSO.

### Procedure

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

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

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

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

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

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

#### Standard Federation User Journey

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

1. Log in to Cisco Spaces.

   Cisco Spaces redirects you to the CCI login page.

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



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

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



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

# Enable Authentication and Authorization

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

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

To enable Authentication and Authorization:

### Procedure

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

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

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

**Step 4** Create corresponding roles in the Cisco Spaces dashboard.

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

The role attribute must use this format:

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

For example,

```
dnaspaces:507829691528:Dashboard_Admin
```

Where:

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

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

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

### What to do next

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

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

# Single Sign-On for Cisco Spaces

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

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

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

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

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

**Note**

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

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

    The Cisco Spaces dashboard default roles are:

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

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

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

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

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

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

The following information from the metadata.xml file:

- SSO Details
- Entity

- Entry point

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

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

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

For example,

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

# Start Working with Cisco Spaces

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

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

For more information, refer to Activation requests reminder emails, on page 21.

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

### Procedure

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

**Note** You can enable Single Sign-On for Cisco Spaces. For more information, refer to Single Sign-On for Cisco Spaces, on page 17.

**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.
- **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: Connectorsection.
- **Using Cisco Spaces Connector**: For configuring a Cisco Spaces with Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller using Cisco Spaces: Connector, refer to Connecting Cisco Spaces to Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller using Cisco Spaces: Connector.
- **Using Cisco Embedded Wireless Controller**: For configuring a Cisco Unified Wireless Network using Cisco Embedded Wireless Controller, refer to Configuring Mobility Express to work with Cisco Spaces.



**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.

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

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

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

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

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

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

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

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

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

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

**Profile Information**

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

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

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

# Activation requests reminder emails

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

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

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

# Cisco Spaces Dashboard GUI Enhancements

Cisco Spaces has introduced a new Beta version of the existing dashboard. The new beta dashboard exclusively offers all new features and enhancements, retaining the functionalities of the current one while providing an

improved experience. We encourage you to try the beta version for an enhanced experience and better performance.

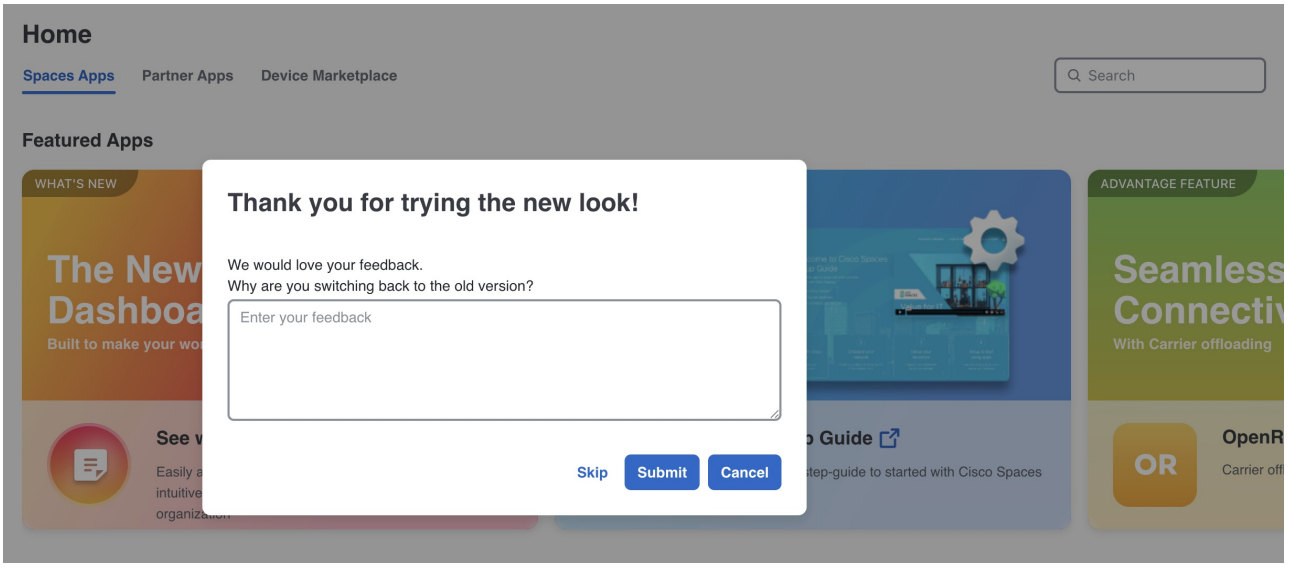
To highlight few updates in the new beta version:

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

To access the new beta Cisco Spaces dashboard, click the **Try new version (Beta)** (Try new version Beta) toggle option that is available on the top-right corner of the Cisco Spaces dashboard window.

To go back to the old version, click **Switch to old version** (Switch to old version). Use the **Feedback** pop-up window to share your feedback and valuable suggestions to improve the user experience.

***Figure 5:***




## Cisco Spaces: Licenses

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

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

# Verticals overview

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

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

These are the four verticals supported:

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

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

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

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



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

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

# Cisco Meraki Integration Workflow

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

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

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

These integrations options are available:

- **Native Integration**: Simple and seamless flow to enable Cisco Spaces integration via Cisco Meraki dashboard
- **Bundled Licensing**: Cisco Spaces Licenses are now bundled with Cisco Meraki Enterprise and Advanced licenses.
    - If you already have a Cisco Spaces account with Smart Licensing, you must create a new Cisco Spaces account when integrating Cisco Meraki Organization with Cisco Spaces. Otherwise, the

bundled Cisco Meraki licenses are not displayed in Cisco Smart Software Manager (CSSM), and the Smart Licensing dashboard displays the status as Out of Compliance.

- If you already have a Cisco Spaces account with Legacy Licensing, and the existing licensing tier matches the Cisco Meraki Organization being integrated, we recommend that you use the existing account when integrating Cisco Meraki Organization.

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

- If you already have a Cisco Spaces account with Cisco Spaces Legacy Licensing, and the existing licensing tier is higher than the Cisco Meraki Organization being integrated, we recommend that you create a new Cisco Spaces account when integrating Cisco Meraki Organization.

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

# Manage Networks in Cisco Meraki Dashboard

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

Key details include:

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

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

# Cisco Magnetic Design

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

The enhancements include:

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

# Cisco Spaces: Connector 3.0

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

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

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

# Idle Timeout for Cisco Spaces

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

# Migrate Data from Cisco Prime Infrastructure to Catalyst Center

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

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

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

# Contact Cisco Spaces Support

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

**Note** All the support contact email addresses are decommissioned.

Follow these steps to raise a support case.

### Procedure

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

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

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

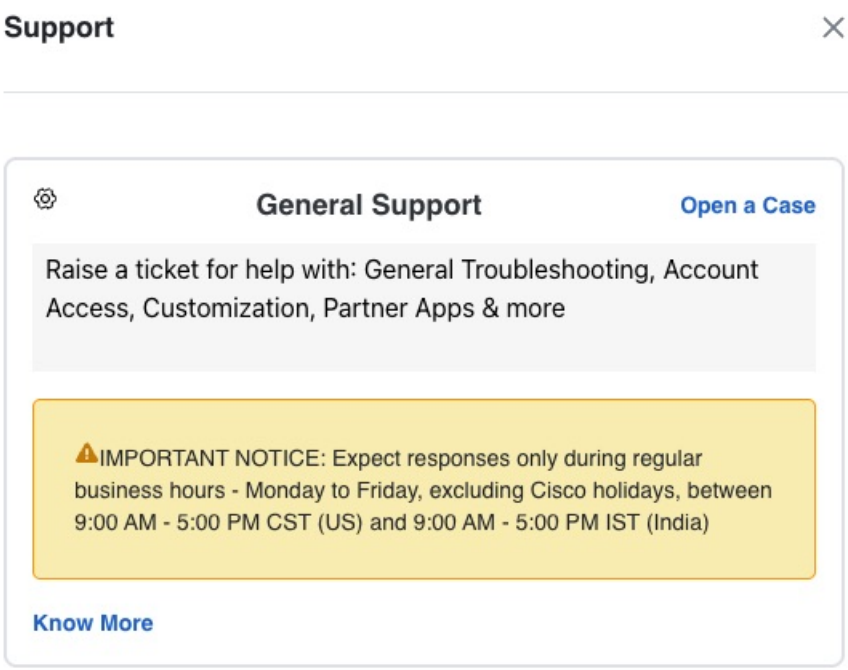
**Step 4** Depending on the account types, the following support options are available:

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

*Figure 6: Paid Account Support Options*

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

***Figure 7: Non-Paid Account Support Options***




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

# Cisco Spaces Documentation

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

Access these documentation support resources.

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