

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 1
- Manage the Cisco Spaces Accounts, on page 7
- Location-Based RBAC (Role-Based Access Control) in Cisco Spaces, on page 8

Manage Cisco Spaces Users

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

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

These tabs are available:

- **Admins**: Use the **Admins** tab to view Cisco Spaces users, invite new administrators, edit user roles, remove users, and resend pending invitations.

  The **Admins** table displays details such as **Name, Email, Role, Read & Write, Read only,** and **Locations**. Use the **Search** field to search for existing users. The table can also display the result count, pagination controls, row check boxes, and the row action menu.

- **Roles**: Use the **Roles** tab to search for roles, create roles, edit roles, remove roles, and manage permission templates.

  The **Roles** table displays role details such as **Role, Read & Write, Read only,** and **Locations**. The values in **Read & Write** and **Read only** summarize the apps assigned to the role.

Invite a Cisco Spaces User

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

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

By default, **Dashboard Admin Role** has read and write access rights only to the role types, **DNASpaces** (including menu items in the left pane, of the dashboard, and the apps Behavior Metrics, OpenRoaming, Location Analytics, Engagements, and Location Personas), **Captive Portals**, and **Asset Locator**.

Note

- If the **Dashboard Admin Role** requires access to any other role types (apps) such as **BLEManager**, contact the Cisco Spaces support team.
- By default, a **Dashboard Admin Role** for the **ESSENTIAL** license has access only to **Cisco Spaces**.

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

For example, you can create a user role with read-and-write permission in the **Captive Portals** app, and read-only permission in the **Asset Locator** app.

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

- **Cisco Spaces**: This role type provides access to all the menu items in the left pane of the Cisco Spaces dashboard such as Location Hierarchy, Admin Management, Monitoring and Support, Setup, and so on. In addition, this role type provides access to the apps such as Behavior Metrics, OpenRoaming, Location Analytics, Engagements, and Location Personas.
- **Captive Portals**: This role type provides access rights to the **Captive Portals** app.
- **IoT Services**: This role type provides access rights to the **IoT Services** app.
- **MapService**: This role type provides access rights to **Map Service**.
- **Location Analytics**: This role type provides access rights to the **Location Analytics** app.
- **Live Occupancy**: This role type provides access rights to the **Live Occupancy** app.
- **Behavior Metrics**: This role type provides access rights to the **Behavior Metrics** app.
- **Impact Analysis**: This role type provides access rights to the **Impact Analysis** app.
- **Camera Metrics**: This role type provides access rights to the **Camera Metrics** app.
- **Engagements**: This role type provides access rights to the **Engagements** app.
- **Location Personas**: This role type provides access rights to the **Location Personas** app.
- **OpenRoaming**: This role type provides access rights to the **OpenRoaming** app.
- **Detect and Locate**: This role type provides access rights to the **Detect and Locate** app.
- **IoT Explorer**: This role type provides access rights to the **IoT Explorer** app.
- **Space Manager**: This role type provides access rights to the **Space Manager** app.
- **Space Experience**: This role type provides access rights to the **Space Experience** app.
- **Environmental Analytics**: This role type provides access rights to the **Environmental Analytics** app.
- **Space Utilization**: This role type provides access rights to the **Space Utilization** app.
- **Energy Utilization**: This role type provides access rights to the **Energy Utilization** app.
- **Asset Locator**: This role type provides access rights to the **Asset Locator** app.
- **Proximity Reporting**: This role type provides access rights to the **Proximity Reporting** app.

- **Partner Dashboard**: This role type provides access rights to the **Partner Dashboard** app.

Note

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

Follow these steps to invite a Cisco Spaces user.

Procedure

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

Step 2 Click **Invite Admin**.

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

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

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

- The default user role and the user roles defined earlier are displayed in the drop-down list. If the required user role is not there, you can define a new user role using **Create New Role**.
- Click **Create New Role** to create a new user role. For more information on creating a new user role, refer to Create a User Role, on page 4. The user roles defined are listed on the **Roles** tab.
- After you select a role name, Cisco Spaces displays a privilege preview table with the **Apps** and **Permission Type** details for the selected role. Review the privileges before inviting the user.

Step 4 Check the **Restrict this role to specific locations** check box if you want to restrict the selected role to any particular location.

a) Click **+ Add Locations**.

b) In the **Choose Locations** window, use **Search** to find a location, or expand and collapse the location hierarchy to browse locations.

c) Check the check box for each required location. The selected locations are displayed in the **Selected Locations** pane.

d) Review the selected-location count and selected-location chips.

e) Click **Done**.

Note If a parent location is selected, access applies to the selected parent location and the child locations under it, based on the location hierarchy. License badges such as **ADVANTAGE** can appear next to locations to indicate the license level for that location.

Step 5 Click **Invite**.

Note
- The **Invite Admin** option is only available for Cisco Spaces administrators with read and write permissions.
- Certain apps such as Captive Portals have provisions to manage the users for that particular app. For example, a Captive Portals app user with read and write permission can invite users with user roles **Creative User** or **Access Code Manger** from the **User Management** option in the Captive Portals app. Admin Management users are displayed in the **User Management** window. However, from the **User Management** option in the Captive Portals app, you cannot modify a user account created through **Admin Management**.
- If an invited user has not accepted the invitation, the user status is displayed as **Invited - Not yet responded**. To send the invitation again, click **RESEND** for the pending user.

Create a User Role

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

Procedure

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

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

Step 2 Click **Create New Role**.

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

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

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

For more information on role types (apps), refer to the role types described in Invite a Cisco Spaces User, on page 1.

c) From the drop-down list that displays for each role type, choose the access right to be provided for this particular user role.

You can set the access right as **Read Only** or **Read/Write**.

For example, if you want to create a user role that has complete access to Dashboard menu items, and read-only access to the captive portal app, check the **Cisco Spaces** check box, and from the corresponding drop-down list choose **Read/Write**. Then check the **Captive Portal** check box, and from the corresponding drop-down list choose **Read only**.

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

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

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

a) In the **Choose Locations** slide-in window, use **Search** to find a location, or expand and collapse the location hierarchy to browse locations.
b) Select the check box for each required location. The selected locations are displayed in the **Selected Locations** pane.
c) Review the selected-location count and selected-location chips.
d) Click **Done**.

Step 6 Click **Create Role**.

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

Edit a User Role

As a Dashboard Admin user with read and write permissions, you can change the role of a Cisco Spaces user.

Note Users from external partner organizations are automatically listed in the **Admin Management** tab after they sign in through Cisco Federation. The identity provider (IdP) of the partner organization assigns their roles. Only the **Delete** option is available for these users; the **Edit** option is not available. To change a user's role, update the role assignment in the partner organization's identity provider (IdP).

Procedure

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

Step 2 Click the row action menu for the role that you want to edit, and choose **Edit Role**.

The **Edit Role** slide-in window is displayed.

Step 3 Update the role name, app permissions, or location restrictions as required.

Step 4 Click **Update**.

Remove a User Role

Use this task to remove a user role that is no longer required.

Procedure

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

Step 2 Click the row action menu for the role that you want to remove, and choose **Remove Role**.

Step 3 Review the confirmation message and click **Remove**.

Note A role cannot be removed if it is assigned to one or more users. Before removing the role, assign those users to another role.

Edit Cisco Spaces User

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

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

Procedure

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

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

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

Step 3 Click the **Edit User**.

The **Edit User** page displays the user email address as a read-only field.

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

The default user roles and the user roles defined earlier are available in the drop-down list for selection. If the required user role is not there, you can define a user role using **Create New Role**. For more information on creating a new user role, refer to Create a User Role, on page 4.

After you select a role, Cisco Spaces displays a privilege preview table with the **Apps** and **Permission Type** details for the selected role.

Step 5 Click **Update**.

Delete a Cisco Spaces User

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

Any user with admin privileges can delete other users.

Follow these steps to delete an existing Cisco Spaces user.

Procedure

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

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

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

Step 3 Click **Remove**.

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

A confirmation message is displayed before the user is removed. Removing a user revokes the user's access to Cisco Spaces. Pending invited users can also be removed from the **Admins** table. Some protected users, such as the account owner or the currently signed-in administrator, may not be available for removal.

Manage the Cisco Spaces Accounts

This section describes how to manage the Cisco Spaces accounts.

Change the Cisco Spaces Password

We recommend that you change the Cisco Spaces password at frequent intervals to ensure more security for your application.

Follow these steps to change the password of your Cisco Spaces account.

Procedure

Step 1 In the **Cisco Spaces Home** page, click the **User Account** icon that is displayed at the far right of the dashboard.

Step 2 Click **Change Password**.

Step 3 In the window that displays, do the following:

a) In the **Current Password** field, enter the current password for your Cisco Spaces account.
b) In the **New Password** field, enter the new password that you want for your Cisco Spaces account.
c) In the **Confirm Password** field, reenter the new password for confirmation.
d) Click **Change Password**.

Password Strength

The Cisco Spaces password requires the following parameters:

- At least 8 characters
- At least 1 upper case letter (A-Z)
- At least 1 lower case letter (a-z)
- At least 1 special character
- At least 1 numeric character(0-9)

Signing Out of Cisco Spaces

To sign out of Cisco Spaces, follow these steps:

Procedure

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

Step 2 Click **Logout**.

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

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

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

When location restriction is enabled, Cisco Spaces displays the **Choose Locations** window. Use this window to search the location hierarchy, expand or collapse location levels, select locations, review selected-location chips, and confirm the selection. The selected locations are displayed in the user or role details and in the **Locations** column of the **Admins** or **Roles table**.