



Managing Cisco Spaces Users and Accounts

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

- [Managing Cisco Spaces Users, on page 1](#)
- [Managing the Cisco Spaces Accounts, on page 4](#)
- [Location-Based RBAC, on page 5](#)

Managing Cisco Spaces Users

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

In the Cisco Spaces dashboard, click the **Menu** icon (☰) and choose **Admin Management** to manage admin users and create roles.

The following tabs are available:

- **Admins**: Use the **Admins** tab to view the Cisco Spaces users and invite new administrators.
- **Roles**: Use the **Roles** tab to search for roles, create new roles and manage them.

Inviting a Cisco Spaces User

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

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



Note

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

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

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

- **Right Now**: This role type provides access rights to the **Right Now** app.

- **Location Analytics:** This role type provides access rights to the **Location Analytics** app.
- **Detect and Locate:** This role type provides access rights to the **Captive Detect and Locate** app.
- **Space Manager:** This role type provides access rights to the **Space Manager** app.

**Note**

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

To invite a Cisco Spaces user, follow these steps:

Procedure

-
- Step 1** In the **Cisco Spaces** dashboard, click the Menu icon (☰) and choose a **Admin Management > Admins** tab.
- Step 2** Click **Invite Admin**.
- Step 3** In the **Invite Admin** window, enter the following details:
- In the **Email** field, enter the email address of the user to add.
 - From the **Role Name** drop-down list, select the user role that you want to provide to this user.
 - The default user role and the user roles defined earlier are displayed in the drop-down list. If the required user role is not there, you can define a new user role using **Create New Role**.
 - Click **Create New Role** to create a new user role. For more information on creating a new user role, see [Creating a User Role, on page 3](#). 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.
- Click **Add Locations**.
 - 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.
 - Click **Done**.
- Step 5** Click **Invite**.


Note

- The **Invite Admin** option is only available for Cisco Spaces administrators with read and write permissions.
- Certain apps such as Captive Portals have provisions to manage the users for that particular app. For example, a Captive Portals app user with read and write permission can invite users with user roles **Creative User** or **Access Code Manger** from the **User Management** option in the Captive Portals app. Admin Management users are displayed in the **User Management** window. However, from the **User Management** option in the Captive Portals app, you cannot modify a user account created through **Admin Management**.

Creating a User Role

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

Procedure

Step 1 In the **Cisco Spaces** dashboard, click the **Menu** icon () and choose **Admin Management > Roles > tab**.

Note

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

Step 2 Click **Create Role**.

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

- a) In the **ROLE NAME** field, enter a name for the user role.
- b) In the **APPS** area, check the check boxes for the role types that you want to provide to this user role.

For more information on role types (apps), see the role types described in [Inviting a Cisco Spaces User, on page 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 **DNA Spaces** check box, and from the corresponding drop-down list choose **Read/Write**. Then check the **CaptivePortal** check box, and from the corresponding drop-down list choose **Read only**.

- d) Click **Create**.

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

Editing Cisco Spaces User

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

To edit the user privileges of a Cisco Spaces user, follow these steps:

Procedure

-
- Step 1** In the **Cisco Spaces** dashboard, click the **Menu** icon (☰) and choose **Admin Management**.
The **Admin** window is displayed with the list of e-mail IDs of the Cisco Spaces users.
- Step 2** Click the **Edit** icon at the far right of the e-mail ID of the user whom you want to edit.
The **Invite Admin** window is displayed.
- Step 3** From the **Role Name** drop-down list, choose the type of access that you want to provide to the user.
The default user roles and the user roles defined earlier are available in the drop-down list for selection. If the required user role is not there, you can define a user role using **Create New Role**. For more information on creating a new user role, see [Creating a User Role, on page 3](#).
- Step 4** Click **Update**.
-

Deleting a Cisco Spaces User

If a user no more needs access to Cisco Spaces, we recommend that you delete such users from the Cisco Spaces user list. A **Dashboard Admin Role** user can delete other users.

To delete an existing Cisco Spaces user, follow these steps:

Procedure

-
- Step 1** In the **Cisco Spaces** dashboard, click the **Menu** icon (☰) and choose **Admin Management**.
The **Admins** window is displayed with the list of the Cisco Spaces users.
- Step 2** Click the **Delete** icon at the far right of the e-mail ID of the user whom you want to delete.
To delete multiple users, select the check box for the corresponding e-mail IDs, and click **Delete Admins** which displays on the top right of the window.
-

Managing the Cisco Spaces Accounts

This section describes how to manage the Cisco Spaces Accounts.

Signed 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 (RBAC) is now enhanced to support specific locations. Use the **Restrict this role to specific locations** option to support specific locations while creating a role (**Admin Management > Roles > Create Role**) and inviting user flows (**Admin Management > Invite Admin**).

