Managing Cisco Spaces Users and Accounts

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

Managing Cisco Spaces Users

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

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

The following tabs are available:

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

Inviting a Cisco Spaces User

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

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

Note

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

Cisco Spaces allows you to define user roles with different access rights to different apps. For example, you can create a user role with read-and-write permission in the **Captive Portals** app, and read-only permission in the **Asset Locator** app.

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

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

Note

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

To invite a Cisco Spaces user, follow these steps:

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:

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

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

- The default user role and the user roles defined earlier are displayed in the drop-down list. If the required user role is not there, you can define a new user role using **Create New Role**.
- Click **Create New Role** to create a new user role. For more information on creating a new user role, see Creating a User Role, on page 4. The user roles defined are listed on the **Roles** tab.
- After you select a role name, the permission type and app details are displayed in the bottom of the **Invite Admin** window.

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

a) Click **Add Locations**.

b) In the **Choose Locations** window, check the check box against the required location from the Location Hierarchy. The selected location is displayed in the **Selected Locations** area.

c) Click **Done**.

Step 5 Click **Invite**.

Note

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

Creating a User Role

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

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 4.

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.

Changing the Cisco Spaces Password

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

To change the password of your Cisco Spaces account, follow these steps:

Procedure

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

Step 2 Click **Change Password**.

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

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 (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**).