



Users and User Roles

- [What are Users and User Roles, on page 1](#)

What are Users and User Roles

The Cisco Spaces: IoT Explorer users are provided with Role-based access control (RBAC), where users or groups of users are provided with various user roles.

A user role is a collection of controls and restrictions which can be then assigned to a user.

Some user roles and the corresponding users are inherited from Cisco Spaces, and are automatically added to all IoT Explorer use cases by default.

Cisco Spaces: IoT Explorer user roles can be defined in many ways.

User roles can be defined by the following permissions:

- **Full Access:** allows the user administrative access to all aspects of a usecase, including configuring and viewing sensors, rules, users, user roles, sensor table, events, work items, and notifications.
- **Read Only:** allows the user read-only access to aspects of a usecase such as sensor table, rules, users, events, work items, and notifications.
- **Notifications Only:** when a usecase event is generated by the Cisco Spaces: IoT Explorer rule engine, this user received a notification.

You can also have user roles that are location enabled. For instance, you can give floor staff access rights to viewing and searching for assets on the floor they work on.

Adding A User to Your Use Case

In this task, you can provide an individual user with access to your use case.

- Step 1** From the Cisco Spaces: IoT Explorer: **Active Use Cases**, choose the newly created use case.
- Step 2** Do one of the following:
- Navigate to **Users and Roles > Users** click **Add Users**.
 - Navigate to **Configure**, and from the **Users** area, click **Add User**.
- Step 3** Enter the email address of the user and click **Look Up**.

If the email address is valid and the email address is not found in the database, a **Basic Details** area is displayed.

- Step 4** In the **Basic Details** area, do the following:
- Provide name and phone number of the user.
 - Choose a role to assign the user. (image 10)
 - If you assign the user a location-enabled role, you can assign locations to the user.
 - Even if the role is not location-enabled, you can select the **Detect User Presence**, and then provide the MAC Address or user name. This is then used to send alerts to the user based on their location.
 - Click **Save**.
If all the fields are added accurately, the user details is saved.
- Step 5** You can add another user to this use case using the **Add Another User** button.
- Step 6** Click **Done** to add the user(s).

Importing or Exporting Bulk Users to your Use Case

You can also import users in bulk. Navigate to **Users and Roles > Import Users > Import a list of Users**. Download the template provided and fill the details.

You can also export users defined for your usecase using the **Export Users**. You can import users to other use cases by using the generated Microsoft Excel spreadsheet.

Import Users from an Existing Use case

This task shows you how you can import users from an existing use case.

- Step 1** From the Cisco Spaces: IoT Explorer: **Active Use Cases**, choose the newly created use case.
- Step 2** Navigate to **Users and Roles > Users** and click **Import Users** and then **Import Users from Another Use Case** and then **Next**.
- Step 3** In the **Import Users to this Use Case** window that is displayed, choose the use case from which you want to import users.
- Step 4** In the window that is displayed, you see a table that allows you to map the user role of the chosen use case (use case A), to the user role of the new use case (use case B). You can use this table to import users from the first use case and assign them to the user role of your choice. Do the following:
- From the first column, choose the user role of use case A.
 - From the second column of the same row, choose the user role of use case B to which you want to map the users.
 - From the third column of the same row, you can observe the number of users that will be imported and assigned to this new user role.
 - To skip importing users from any user role of use case A, select the corresponding **Don't import these rows** option in the fourth column.
 - Click **Next**.

You see the newly added roles and users in the **Users & Roles** tab of the new use case.

Create Custom Roles for A Use Case

You can create custom roles that are applicable only to your use case.

This feature allows you to import users to your use case from another use case. In such a scenario, you can map the roles of two use cases, and import users into a custom role.

Step 1 From the Cisco Spaces: IoT Explorer: **Active Use Cases**, choose the newly created use case.

Step 2 Do one of the following:

- Navigate to **Users and Roles > Roles** click **Add Role**.
- Navigate to **Users and Roles > Configure**, and from the **Users** area, click **Add Role**.

Step 3 In the **Add New Role** displayed, do the following.

- a) Fill the **Enter the Role Name** field and also the **Enter a description for this Role** field.
- b) Choose the access type of this role.

- **Full Access**: allows the user administrative access to all aspects of a use case, including configuring and viewing sensors, rules, users, user roles, sensor table, events, work items, and notifications.

- **Read Only**: allows the user read-only access to aspects of a use case such as sensor table, rules, users, events, work items, and notifications.

- **Notifications Only**: when a use case event is generated by the Cisco Spaces: IoT Explorer rule engine, this user received a notification.

- **Custom**: you can mix and match the access levels to various features.

Step 4 (Optional) Choose to assign locations to users assigned to this role by checking the **This is a Location-Enabled Role** option.

Selecting this option also gives you further flexibility to configure location-specific event notifications. Users of this role can receive notifications based on the locations they are present in.

Note If you chose **Custom** in the previous step, you can now also configure what a user views on their respective IoT Explorer dashboard. You can allow a user to view data pertaining to their assigned locations.

Step 5 Click **Add**.

Configure Location-Enabled Rules

You can create rules that trigger location-dependent notification events like an email or an SMS. You can assign locations to users and user roles. You can then configure rules such that a user is notified of an event only if the user is at the assigned location when the event occurs.

1. Create location-enabled user roles.
2. Assign users to the location-enabled user roles.
3. Assign specific locations to each of these users.
4. Create a rule with location-enabled events, and notify only these location-enabled users or user roles.

-
- Step 1** From the IoT Explorer: **Active Use Cases**, choose a use case that requires location-enabled rules.
- Step 2** You can add a new location-enabled role or edit an existing role. Navigate to **Users and Roles > Roles** and do one of the following:
- To edit an existing role, click the three dots at the end of the role to open the role-specific menu and click **Edit Role**.
 - To add a new role, click **Add Role**.
- Step 3** In the page that opens, choose an **Access Type** and check the **This is a Location Enabled Role** option. You can add users to this user role, and assign locations for these users. The rule engine sends notifications based on these assigned locations. Further, if you choose the **Custom** access type in the preceding step, you can assign special permissions based on the locations that are assigned to the user.
- Step 4** You can add a new user to this location-enabled role. Navigate to **Users and Roles > Users** click **Add Users**.
- Step 5** Enter the email address of the user and click **Look Up**.
If the email address is valid and the email address is not found in the database, a **Basic Details** area is displayed.
- Step 6** In the **Basic Details** area, do the following:
- a) Provide name and phone number of the user.
 - b) Choose a role to assign the user.
 - c) If you assign the user a location-enabled role, you can assign locations to the user.
 - d) Click **Save**.
If you have added all the fields accurately, the user details are saved.
- Step 7** You can add another user using the **Add Another User** button.
- Step 8** Click **Done** to add the users.
- Step 9** Now let us configure location-enabled rules for this use case. Navigate to the **Rules** tab and click **Add Rule**.
- Step 10** Required: To configure this rule for specific locations from the location hierarchy, click the **Conditions** tab, and from the **Location** area choose locations from the location hierarchy.
- Step 11** Required: To configure to send notifications based on the location, click **Events**. However, you can do the following:
- **Send Email**: Configure to send emails to the users or user roles that have been given access to this use case. You can specify the message, and choose the users and use roles that must be notified.
 - **Send SMS**: Configure to send SMS to the users or user roles that have been given access to this use case. You can specify the message and choose the users and use roles that must be notified.
- Note** **Only when the user is present**: You can further customize these actions by enabling location awareness to your actions. Emails and SMSs are sent only when users are present in the business location. You can configure this business location when you configure users and user roles.
- a) Click the **Action** tab.
 - b) Drag the **Send Email** or **Send SMS** option to the rule.
 - c) Specify the message and other details.
 - d) Choose the configured location-enabled user role or location-enabled user.
-