Rules

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.

Business Rules, Policies, or Workflows of a Use Case

Cisco Spaces: IoT Explorer allows you to define workflows, policies, and business rules. You can configure conditions that observes measurements, and when any measure deviates from the norm established by these rules, the IoT Explorer solution swings into action. It can give you an immediate alert or, if you prefer, triggers an automated action that is predefined by your workflows and business rules.

You can have different types of rules that check for conditions, and when the conditions are fulfilled, the rules trigger actions like sending SMS, Emails, or logging an event.

Create Rules to Your Use Case

This task shows you how to add rules to your use case. Rules allow you to configure conditions that trigger events and sent you important alerts regarding the status of your assets and devices.

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

Step 2 Configure rules for your newly created use case. Do one of the following:

- Navigate to **Configure**, and from the **Rules** area, click **Add Rule**.
- Navigate to the **Rules** tab and click **Add Rule**.

The displayed **Add New Rule** window is configured with the default **Rule** and **Event** for this use case. Each use case can have only one rule. However, you can provide other conditions and further customize this rule.

Step 3 (Optional) To modify the default rule, from the **Rules** tab, drag and drop a new rule over the default rule.
The new rule is now the default rule.

Step 4 (Optional) To configure a schedule for the rule, click the **Conditions** tab, and from the **Schedule** area configure any of the following:

- **Duration**: Specify a start and end date between which this rule is applicable.
- **Day of the Week**: Specify the days of the week on which the rule is applicable.
- **Time of the Day**: Configure the time of the day when the rule is applicable.

Step 5 (Optional) From the **Conditions** tab **Location** area, you can choose locations from the location hierarchy that apply to the rule.

Step 6 (Optional) From the **Conditions** tab **Location Metadata** area, you can configure location names that apply to the rule.

Step 7 (Optional) From the **Conditions** tab **Asset Metadata** area, you can configure specific asset names that apply to the rule.

Step 8 (Optional) From the **Action** tab, you can configure events. When a rule condition is satisfied, an event is triggered. The default action is **Log the Event**. You can view the logged event in the **Events** of the use case. However, you can also do the following:

- **Send Email**: Configure to send emails to the users or user roles that have 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 access to this use case. You can specify the message and choose the users and use roles that must be notified.
- **Cisco Webex**: Configure to send a message on Webex Teams to specified users or Teams Spaces whenever this event occurs. You can configure your Webex account, specify the notification message, and choose the Webex link to communicate your message.
- **Log the Event**: Modify the default log event, by giving the event a name and description. If the event occurs too frequently, you can configure to aggregate the data points that occur over a span of time and log it as a single event.

Note
- **Only when the user is present**: You can choose to customize your rules by enabling location awareness to your actions. The rule engine sends Emails and SMSs only when users are present in the business location. You can configure the business location when you configure the users and user roles.

Step 9 Click **Save and Publish**.

Step 10 In the **Rule Summary** window displayed, you can review the configurations made for this rule. You can then do one of the following:

- **Save Only**: Save this rule as a draft only. The configured actions are not triggered when the rule conditions are met.
- **Save and Publish**: Deploy the rule into action. The configured actions are triggered when the rule conditions are satisfied.

Rules