Cisco Spaces: IoT Explorer Configuration Guide

First Published: 2022-10-28

Last Modified: 2023-08-01

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022–2023 Cisco Systems, Inc. All rights reserved.

Preface

This preface describes the audience, organization, acronyms, and conventions used in the document.

Note **Cisco DNA Spaces** is now **Cisco Spaces**. We are in the process of updating our documentation with the new name. This includes updating GUIs and the corresponding procedures, screenshots, and URLs. For the duration of this activity, you might see occurrences of both **Cisco DNA Spaces** and **Cisco Spaces**. We take this opportunity to thank you for your continued support.

This document contains the following sections:

Preface

This preface describes the audience, organization, and conventions of this document. It also provides information on how to obtain other documentation.

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Audience

This document is for Connected Mobile Experiences (CMX) network and IT administrators who deploy Cisco Beacon Point (BP) or Cisco Beacon Point Module (BPM) for high accuracy virtual beacon solution.

Conventions

This document uses the following conventions:

Table 1: Conventions

Convention	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string. Otherwise, the string will include the quotation marks.
`courier` font	Terminal sessions and information the system displays appear in `courier` font.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means the following information will help you solve a problem.

Caution Means reader be careful. In this situation, you might perform an action that could result in equipment damage or loss of data.

Related Documentation

For more information, see:

- https://support.dnaspaces.io/hc/en-us

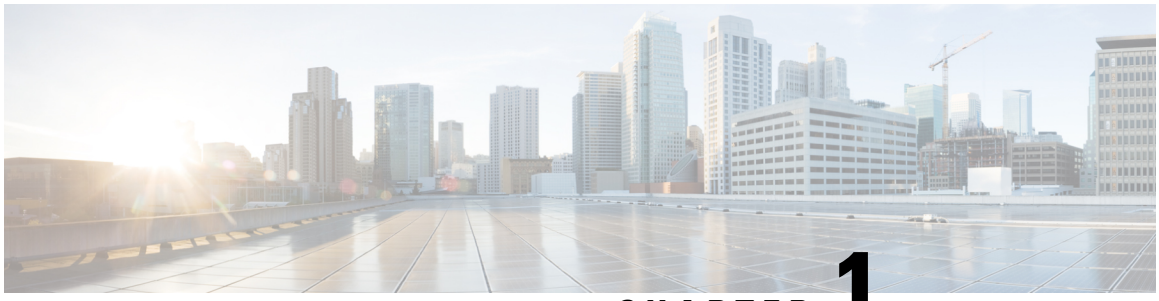
Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.



CHAPTER 1

Cisco Spaces: IoT Explorer App

Overview

The Cisco Spaces: IoT Explorer app enables you to monitor and optimize the performance of your assets, sensors, alerting system, and work flows.

Features

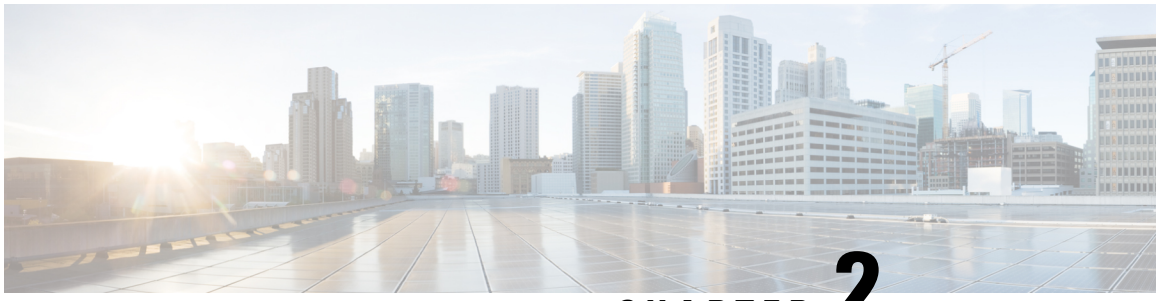
The Cisco Spaces: IoT Explorer app is a comprehensive single resource for managing, monitoring, and optimizing your assets, Internet of Things (IoT) sensors, alerting system, and operational workflows.

The Cisco Spaces: IoT Explorer app is the third generation enhanced version of Operational Insights and Cisco Asset Locator applications. The **IoT Explorer** application is designed to bring in quick value to users exploring device-driven IoT use cases in Cisco Spaces and to add value to IoT services at the ACT licensing level.

This application accomplishes the three use cases listed below:

- Temperature Monitoring: Monitor spaces and receive notifications of changes in temperature
- Asset Tracking: Locate, monitor, and set up alerts to gain insight into your asset's locations
- Presence Detection: Get real time insights into how your physical spaces are occupied

Within each of these use cases, you can create rules/alerts, view data logs, view the real time location and status of the device or sensor. The **IoT Explorer** application UI is designed to set up the use case in a simplified way.



CHAPTER 2

Temperature Monitoring

Use Case Overview

Use the Temperature Monitoring use case to manage and monitor indoor environments. You can also add new temperature sensors with scalable and streamlined onboarding process and create rules to quickly notify team members when a sensor falls or rises below a certain threshold.

This use case helps to:

- Get alert when temperature is out of range
- Set up an event log to monitor temperature changes over time
- Gain insight into all the spaces temperature
- Keep assests under compliance

The following sensors are supported by this type of use case:

- BLE Tag
- CCX Tag

Configure Monitoring of Temperature of Devices

This task shows you how to monitor your spaces and receive notifications regarding changes in temperature of your devices.

Step 1 In the Cisco Spaces, click the **IoT Explorer** app tile.

Step 2 Click **Temperature Monitoring**.

Step 3 Click **Get Started**.

Step 4 In the **Use Case Name** field, enter a name for the use case.

Step 5 In the **Description** field, enter a description for the use case.

Step 6 Click **Create Use Case**.
You have created the temperature monitoring use case along with various options to set up sensors, rules, and users.

Step 7 From the IoT Explorer: **Active Use Cases**, choose the newly created temperature use case.

Step 8 Add sensors that are available on your devices to the use case. You can add sensors individually, or in bulk, or from sensors onboarded onto Cisco Spaces. See Sensors, on page 15.

Step 9 Add users that can access this use case, and if needed, add custom user roles. See What are Users and User Roles, on page 11

Step 10 Configure **Rules** that can quickly notify your team when one of the following occurs:

- **Temperature Rise**: Monitor sensors and trigger an event when a temperature rises.
- **Temperature Drop**: Monitor sensors and trigger an event when a temperature drops.
- **Temperature in Range**: Monitor sensors and trigger an event when the temperature is between a range that you can configure.
- **Temperature outside Range**: Monitor sensors and trigger an event when the temperature is outside a range that you can configure.
- **Sensor Not Heard**: Triggers an event when a sensor has been silent for the specified interval.

Step 11 Configure conditions that trigger events. See Create Rules to Your Use Case, on page 12

When the temperature rules you configured trigger events, you can see them on the **Events** tab.

View Temperature History Graphically

This task allows you to observe the temperature variations of your device visually on a graphic. You can also customize this graph.

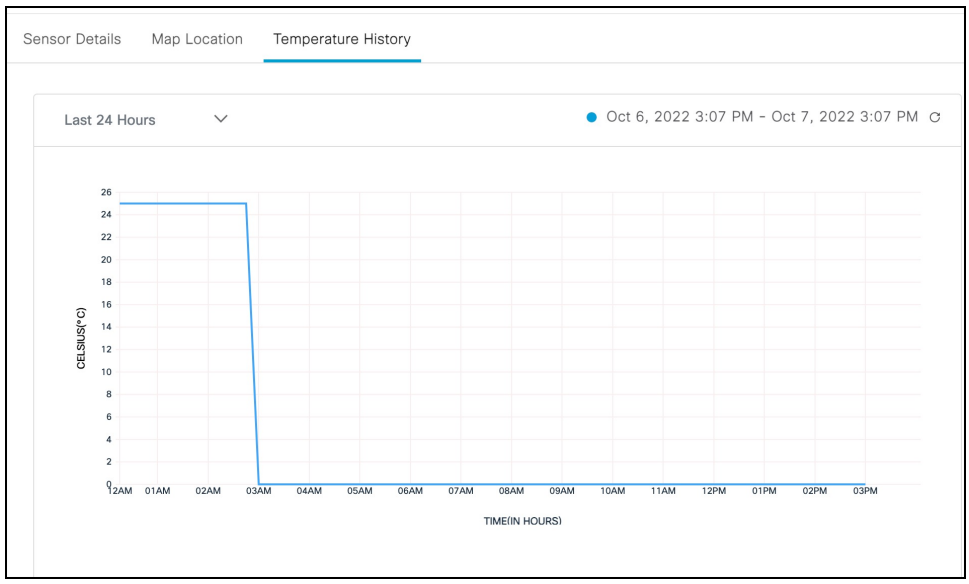
Step 1 From the Cisco Spaces: IoT Explorer: **Active Use Cases**, choose the newly created temperature monitoring use case.

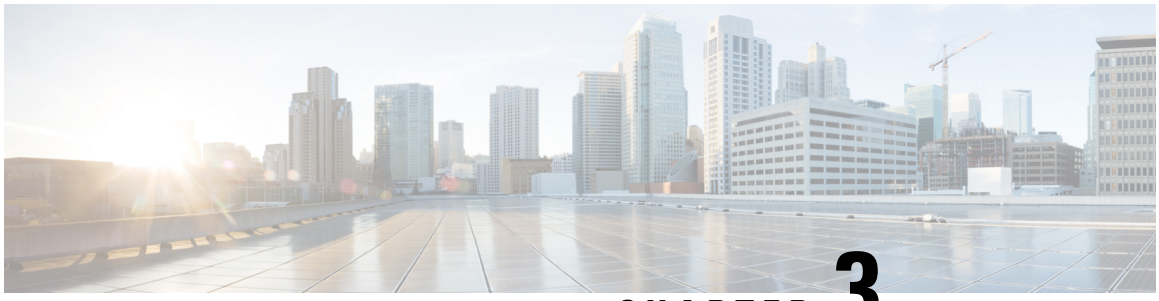
Step 2 Do one of the following:

- Navigate to the **Sensors** tab.
- In the **Configure** tab **Manage Sensors** area, click **View Sensors**.

Step 3 Click a sensor to see the temperature variations experienced by your device. In the **Temperature History** tab, a supported sensor can display graphically, the temperature of your device over a period of time. You can also modify the displayed period here.

Figure 1: View Temperature History Graphically





CHAPTER 3

Asset Tracking

Use Case Overview

Use the Asset Tracking use case to add asset tags to help manage and monitor the location of important objects and search for assets on a map. You can also add new asset tags with scalable and streamlined on-board processes and create rules to quickly notify team members when an item leaves a specific zone. The Cisco Spaces: IoT Explorer application retains asset location history for at least one year.

This type of use case helps to:

- Configure notifications when an asset leaves a zone, floor, or building
- Locate an asset in real time.
- Gain insight into how often a device is utilized
- Set up alerts when an asset tag's battery needs to be replaced

The following sensors are supported by this type of use case:

- BLE tag
- CCX tag
- BLE device
- Wi-Fi device

Configure Tracking and Monitoring of Asset Location

This task shows you how to view, monitor, and set up alerts that give insights to your assets and their locations.

Step 1 From the Cisco Spaces window, click the **IoT Explorer** app tile.

Step 2 Click **Asset Tracking**.

Step 3 Click **Get Started**.

Step 4 In the **Use Case Name** field, enter a name for the use case.

Step 5 In the **Description** field, enter a description for the use case.

Step 6 Click **Create Use Case**.
You have created the asset tracking use case, along with various options to manage your assets, set up rules, and add users.

Step 7 From the IoT Explorer: **Active Use Cases**, choose the newly created asset tracking use case.

Step 8 Add asset tags that are available on your assets to this use case. You can import assets individually, or in bulk, or from existing use case. You can also see details of each asset, and view the asset on the map location. See Assets, on page 19.

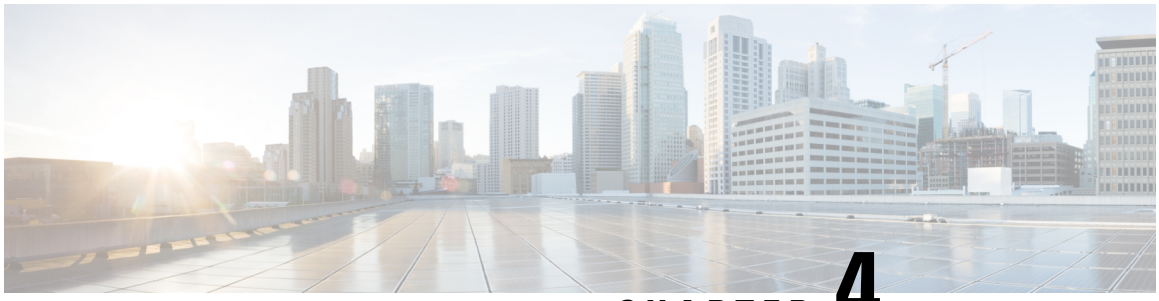
Step 9 Add users that can access this use case, and if needed, add custom user roles. See What are Users and User Roles, on page 11.

Step 10 Configure **Rules** that can quickly notify your team when one of the following occurs:

- **Asset Changes Location**: Monitor asset movement across building, floors, and zones.
- **Asset Not Heard**: Triggers an event when a sensor has been silent for the specified interval..

Step 11 Configure conditions that trigger events. See Create Rules to Your Use Case, on page 12.

You can now monitor and manage assets by navigating to the floor map on the **Locator** tab. From the **Assets** tab, you can also search for an asset using a name or location. When the rules you configured trigger events, you can see them on the **Events** tab.



CHAPTER 4

Presence Detection

Use Case Overview

Presence Detection is a type of use case that you can use to manage and monitor live occupancy data for desks, rooms, and offices. You can also add new occupancy sensors with scalable and streamlined onboarding process and create rules to quickly notify team members when a space is occupied for a period of time. You can also manually place the sensors on their imported map.

This use case helps to:

- Gain insight into space utilization by creating a data log rule
- Utilize the map to quickly see live occupancy status of spaces
- Share historical occupancy data with facilities team members
- Set up a rule to be alerted when a space becomes available

The following sensors are supported by this type of use case:

- Passive Infrared Sensor (PIR)
- Meraki Camera

Configure Presence Detection

This task shows you how to configure the presence detection use case. The configurations allow you to gain real-time insight into the status of your physical spaces (for example, occupied).

Step 1 In the Cisco Spaces, click the **IoT Explorer** app tile.

Step 2 Click **Presence Detection**.

Step 3 Click **Get Started**.

Step 4 In the **Use Case Name** field, enter a name for the use case.

Step 5 In the **Description** field, enter a description for the use case.

Step 6 Click **Create Use Case**.
You have now created the Presence Detection use case along with various options to manage your assets, set up rules, and add users.

Step 7 From the IoT Explorer: **Active Use Cases**, choose the newly created presence use case.

Step 8 Add occupancy sensors (that are available at the physical location) to this use case. You can add sensors individually, or in bulk, or from sensors onboarded onto Cisco Spaces. See Sensors, on page 15.

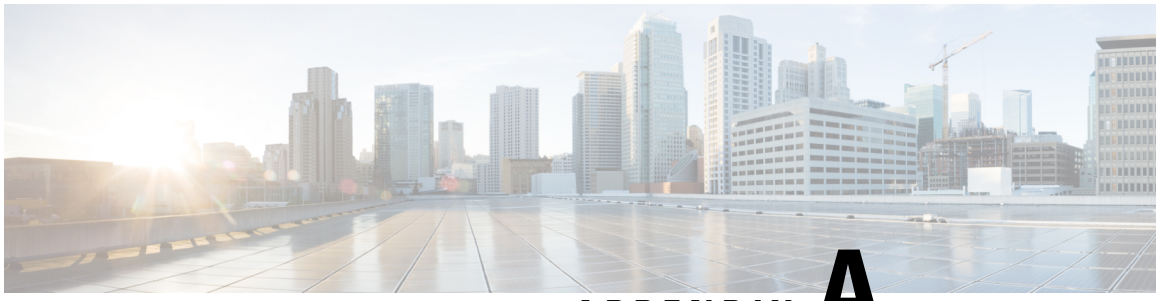
Step 9 Add users that can access this use case, and if needed, add custom user roles. See What are Users and User Roles, on page 11

Step 10 Configure **Rules** that can quickly notify your team when one of the following occurs:

- **Presence Detected**: Monitor spaces and trigger an event when someone occupies a space.
- **Presence Not Detected**: Monitor spaces and trigger an event when someone frees a space.
- **Sensor Not Heard**: Triggers an event when a sensor has been silent for the specified interval.

Step 11 Configure conditions that trigger events. See Create Rules to Your Use Case, on page 12

You can now track occupied and unoccupied spaces from the floor map image from the **Occupancy View** tab. From the **Sensors** tab, you can also search for spaces using the name or location of the associated sensor. When the rules you configured trigger events, you can see them in the **Events** tab.



APPENDIX A

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.

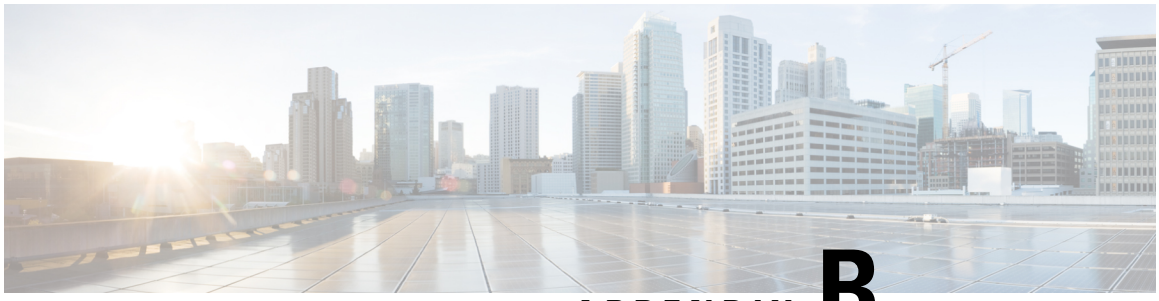
Note
- **Only when the user is present**: You can choose to customize your rules by enabling location awareness to your actions. The rule engine sends Emails and SMSs only when users are present in the business location. You can configure the business location when you configure the users and user roles.

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



APPENDIX B

Sensors

Sensors

Cisco Spaces: IoT Explorer continually monitors data from the sensors attached to your assets—including battery levels, or telemetry data such as temperature or humidity. When any measure deviates from the norm established by your workflows, policies, and business rules, the solution swings into action. It can give you an immediate alert or, if you prefer, can trigger an automated action that is predefined by your workflows and business rules.

Once you have created your use case, you can include sensors to it in multiple ways.

Importing Sensors to Your Use Case Using a Template File

This task shows you how you can import sensors in bulk using a template (XLS) file.

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

Step 2 Navigate to **Configure** and in the **Manage Sensors** area, click **Import Sensors**.

Step 3 In the **Add Sensors** page displayed, choose **Bulk Import Sensors** and click **Next**.

Step 4 In the **Add Sensors - Import Via Spreadsheet** page, click **Download Template Here** to download the template file.

Step 5 Fill the template file with the details of all the sensors that you want to import.

Step 6 In the **Add Sensors - Import Via Spreadsheet** page, click **Click here to browse or Drag a file to upload**. Upload the edited template file. Click **Import**.

You can see the imported sensors in the **Sensor** tab of this use case.

Importing Sensors to Your Use Case Using Location Hierarchy and Device Groups

This task shows you how you can import sensors from the Cisco Spaces Location Hierarchy. You can import sensors that are already on board the Cisco Spaces: IoT Service. You can also import sensors that are part of

a device group. Although, you can only select those device groups that are within the scope of your location hierarchy.

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

Step 2 Navigate to **Configure** and in the **Manage Sensors** area, click **Import Sensors**.

Step 3 In the **Add Sensors** page displayed, choose **Setup Existing Sensor Filter Criteria**.
You can see the number of supported sensors.

Step 4 Click **Next**.

Step 5 In the **Add Sensors – Set Up Filter Criteria: Select Locations** page displayed, you can select locations to include in your use case. Click one of the following:

- **Include all Locations**: You can include all current locations to your use case. Any locations added to the hierarchy in the future is automatically added.
- **Select Locations**: You can select specific locations that you can include to this use case. Once you select this option, you can navigate the displayed location hierarchy, and chose to import sensors from specific locations to your use case.

Step 6 Click **Next**.

Step 7 In the **Add Sensors – Set Up Filter Criteria: Select Device Groups** page displayed, you can import only specific groups of devices from the selected locations to your use case. Click one of the following:

- **Include all Groups**: You can include all groups to your use case, along with automatically including any device groups added to the hierarchy in the future.
- **Select Groups**: You can select specific device groups that you can include to this use case. Once you select this option, you can select from the device groups applicable to the use case locations and choose to import only those sensors to your use case. Any sensors added to the selected device groups in the future are automatically added to the use case.

Step 8 Click **Next**.

Step 9 Click **Add Sensors.**

You have imported sensors to your use case by specifying locations and device groups.

Adding Sensor Individually to Your Use Case

This task shows you how you can add a sensor individually to your use case, one by one. You can add a sensor that is already on board the Cisco Spaces: IoT Service location hierarchy.

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

Step 2 Navigate to **Configure** and in the **Manage Sensors** area, click **Add individual Sensor**.

Step 3 In the **Add Sensors** page displayed, go to the **TAG INFORMATION** area, and select one of the tags types listed.

Step 4 Fill the **Device MAC address** text field.

Step 5 In the **Asset Name** text field, enter a preferred name for your sensor.

Step 6 Click **Save**.

Step 7 (Optional) Click **Add Another Sensor** to add more sensors to your use case.

You have added the sensor to your use case.

Viewing Sensors Added to Your Use Case

This task shows you how to view the list of sensors added to your use case. You can also view further details of the sensor such as:

- Percentage of remaining battery
- Last heard time of the sensor
- Sensor location on the floor map

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 the **Sensors** tab.
- In the **Configure** tab **Manage Sensors** area, click **View Sensors**.

In the **Sensors** Tab, you can view the following:

- **All Sensors**: List of all sensors added to your use case.
- **Heard Recently**: Lists of sensors according to when they were last heard. You can see device categories according to last-heard time as: not heard in the last hour, not heard in the last 24 hours, and Heard Recently (heard in the last hour).
- **Battery**: Displays the battery level of sensors. You can see device categories according to battery levels: less than 10%, greater than 50%, and greater than 90%.

Step 3 Click a sensor to see further details of the sensor. If the sensor is part of the Cisco Spaces location hierarchy, then the **Map Location** tab contains the floor map where the sensor is located.

Customizing Your View of Sensor List

You can customize your view of the list of sensors displayed for 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 the **Sensors** tab.
- In the **Configure** tab **Manage Sensors** area, click **View Sensors**.

Step 3 Click a sensor to see further details of the sensor. If the sensor is part of the Cisco Spaces location hierarchy, then the **Map Location** tab contains the floor map where the sensor is located.

Step 4 Click on the three dots near the title of any column to do one of the following:

- **Hide Columns**: Once hidden, a column can be made visible by the **Unhide Columns** button that is displayed.
- **Pin Column**: Move and fix the column to the start of columns.
- **Sort Ascending**: Sort the rows in ascending order of content of this column.
- **Sort Decending**: Sort the rows in descending order of content of this column.

Step 5 Once you have customized your view of the **Sensor** tab, you can save the view by clicking **Save as a new view** button that comes up.

Step 6 You can also filter the view by certain parameters.

Adding Custom Attributes to Sensors

You can add custom attributes to your sensor and monitor these attributes from a newly-added column on the **Sensor** tab.

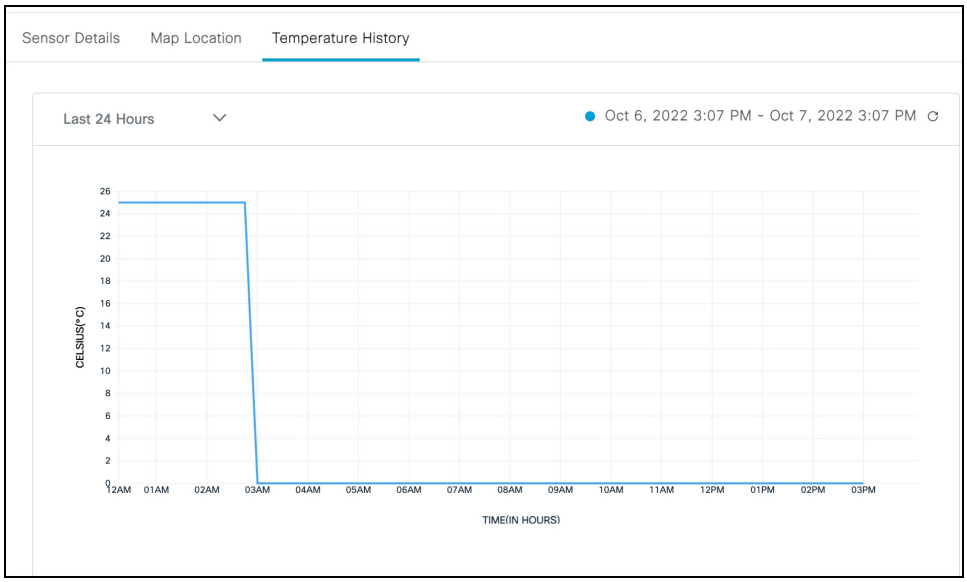
Step 1 From the Cisco Spaces: IoT Explorer: **Active Use Cases**, choose the newly created use case.

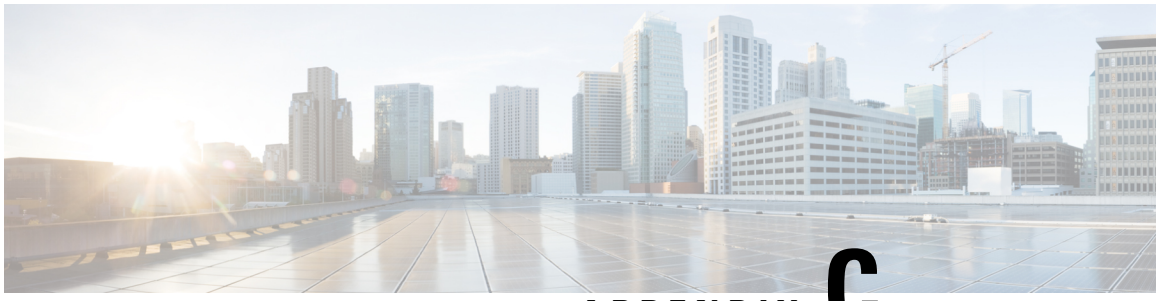
Step 2 In the **Configure** tab **Manage Sensors** area, click Sensor **Database**.

Step 3 In the **Sensor Database** page displayed, click **Add Column**. Do the following:

a) In the **Column** text field, enter a name for the custom attribute.
b) Select the **Data Type**.
c) Select the **Visibility** of the attribute.
d) Click **Save** on the new row.
e) Click **Save** to close the **Sensor Database**page.

Step 4 Now navigate to the **Sensors** tab. You can see the newly added custom attribute displayed as column.





APPENDIX C

Assets

Assets

Cisco Spaces: IoT Explorer continually monitors data from the tags attached to your assets, like the position of your assets. When any measure deviates from the norm established by your workflows, policies, and business rules, the solution swings into action. It can give you an immediate alert or, if you prefer, can trigger an automated action that is predefined by your workflows and business rules.

Once you have created your usecase, you can include assets to it in many ways.

Importing Assets to Your Use Case Using a Template File

This task shows you how you can import assets in bulk using a template (XLS) file.

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

Step 2 Navigate to **Configure** and in the **Manage Assets** area, click **Import Assets**.

Step 3 In the **Add Assets** page displayed, choose **Bulk Import Assets** and click **Next**.

Step 4 In the **Add Assets - Import Via Spreadsheet** page, click **Download Template Here** to download the template file.

Step 5 Fill the template file with the details of all the assets that you want to import.

Step 6 In the **Add Assets - Import Via Spreadsheet** page, click **Click here to browse or Drag a file to upload**. Upload the edited template file. Click **Import**.

You can see the imported assets in the **Asset** tab of this use case.

Importing Assets to Your Use Case Using Location Hierarchy

This task shows you how you can import assets from the Cisco Spaces Location Hierarchy. You can import assets that are already on board the Cisco Spaces: IoT Service.

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

Step 2 Navigate to **Configure** and in the **Manage Assets** area, click **Import Assets**.

Step 3 In the **Add Assets** page displayed, choose **Setup Existing Sensor Filter Criteria**.
You can see the number of supported assets.

Step 4 Click **Next**.

Step 5 In the **Add Assets – Set Up Filter Criteria: Select Locations** page displayed, you can select locations to include in your use case. Click one of the following:

- **Include all Locations**: You can includes all current locations to your use case, along with automatically including any locations added to the hierarchy in the future.
- **Select Locations**: You can select specific locations that you can include to this use case. Once you select this option, you can navigate the displayed location hierarchy, and chose to import assets from specific locations to your use case.

Step 6 Click **Next**.

Step 7 In the **Add Assets – Set Up Filter Criteria: Select Device Groups** page displayed, you can import only specific groups of devices from the selected locations to your use case. Click one of the following:

- **Include all Groups**: You can include all groups to your use case, along with automatically including any device groups added to the hierarchy in the future.
- **Select Groups**: You can select specific device groups that you can include to this use case. Once you select this option, you can select from the device groups applicable to the use case locations and chose to import only those assets to your use case. Any assets added to the selected device groups in the future are automatically imported to the use case.

Step 8 Click **Next**.

Step 9 Click **Add Assets.**

You see the number of assets that are imported to your use case.

Adding Assets Individually to Your Use Case

This task shows you how you can add an asset individually to your use case, one by one. You can add an asset that is already on board the Cisco Spaces: IoT Service location hierarchy.

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

Step 2 Navigate to **Configure** and in the **Manage Assets** area, click **Add individual Asset**.

Step 3 In the **Add Assets** page displayed, go to the **TAG INFORMATION** area, and select one of the tags types listed.

Step 4 Fill the **Device MAC address** text field.

Step 5 In the **Asset Name** text field, enter a preferred name for your asset.

Step 6 Click **Save**.

Step 7 (Optional) Click **Add Another Asset** to add more assets to your use case.

The asset is added to your use case.

Viewing Assets Added to Your Use Case

This task shows you how to view the list of assets that are added to your use case. You can also view further details of the asset such as:

- Percentage of remaining battery
- Last heard time of the asset
- Asset location on the floor map

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 the **Assets** tab.
- In the **Configure** tab **Manage Assets** area, click **View Assets**.

In the **Assets** Tab, you can view the following:

- **All Assets**: List of all assets added to your use case.
- **Heard Recently**: Lists of assets according to when they were last heard. You can see asset categories according to last-heard time as: not heard in the last hour, not heard in the last 24 hours, and Heard Recently (heard in the last hour).
- **Battery**: Displays the battery level of assets. You can see asset categories according to battery levels: less than 10%, greater than 50%, and greater than 90%.

Step 3 Click an asset to see further details of the asset. If the asset is part of the Cisco Spaces location hierarchy, then the **Map Location** tab contains the floor map where the asset is located.

Customizing Your View of Asset List

You can customize your view of the list of assets displayed for 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 the **Assets** tab.
- In the **Configure** tab **Manage Assets** area, click **View Assets**.

Step 3 Click an asset to see further details of the asset. If the asset is part of the Cisco Spaces location hierarchy, then the **Map Location** tab contains the floor map where the asset is located.

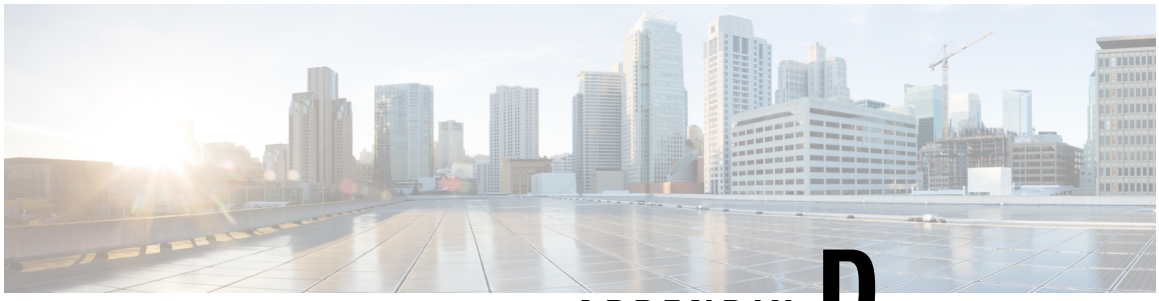
Step 4 Click on the three dots near the title of any column to do one of the following:

- **Hide Columns**: Once hidden, a column can be made visible by the **Unhide Columns** button that is displayed.
- **Pin Column**: Move and fix the column to the start of columns.
- **Sort Ascending**: Sort the rows in ascending order of content of this column.

- **Sort Descending**: Sort the rows in descending order of content of this column.

Step 5 Once you have customized your view of the **Asset** tab, you can save the view by clicking **Save as a new view** button that comes up.

Step 6 You can also filter the view by certain parameters.



APPENDIX D

Users and User Roles

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:

a) Provide name and phone number of the user.
b) Choose a role to assign the user. (image 10)
c) If you assign the user a location-enabled role, you can assign locations to the user.
d) 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.
e) 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:

a) From the first column, choose the user role of use case A.
b) From the second column of the same row, choose the user role of use case B to which you want to map the users.
c) 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.
d) 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.
e) 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.