Contents

Preface

Audience                          ix
Documentation Accessibility      ix
Related Documents                ix
Conventions                      ix

1 Get Started with Oracle IoT Asset Monitoring Cloud Service

Oracle IoT Asset Monitoring Cloud Service Overview                      1-1
What are the Different Assets that You Can Monitor                     1-2
Understand the Building Blocks of Oracle IoT Asset Monitoring Cloud Service 1-2
What Interfaces Can You Use to Access Oracle IoT Asset Monitoring Cloud Service 1-8
How to Access the Oracle IoT Asset Monitoring Cloud Service            1-9
The Operations Center                                                   1-9
The Design Center                                                        1-11
  Create a New Organization                                              1-12
  Change Your Current Organization                                       1-12
  Assign Users to an Organization                                        1-12
  Export and Import Organizations                                        1-13
    Export an Organization                                               1-13
    Import an Organization                                               1-13
  Create and Manage Groups                                               1-14
    Create a New Group                                                    1-14
Typical Workflow for Using Oracle IoT Asset Monitoring Cloud Service    1-15
How to Get Support                                                       1-18

2 Create and Manage Users

Understand Roles and Users                                               2-1
Create a New User                                                         2-2
Edit a User Account                                                      2-3
Search for a User Account                                                2-3
3 Work with Your Assets

What is an Asset 3-1
Create and Manage Asset Types 3-1
  Create a New Asset Type 3-2
    Add Optional Actions to the Asset Type 3-3
  About Hierarchical Asset Associations 3-4
Create Asset Associations 3-5
Edit an Asset Type 3-6
Delete an Asset Type 3-6
Create and Manage Assets 3-7
  Create an Asset 3-7
  View Asset Details 3-10
  Edit Asset Details 3-13
  Trigger Actions for Assets 3-13
  Duplicate an Asset 3-14
  Reserve an Asset 3-14
  Delete an Asset 3-14
Create and Manage Places 3-14
  Create a Place Using a Geofence 3-15
  Create a Place with a Floor Plan 3-16
  Edit a Place 3-17
  Delete a Place 3-18
Locate Your Assets in the Map View 3-18
  Use Third-Party Map Providers 3-19
Simulate Asset Sensors with the Built-In Simulator 3-20
  Define a Simulation for a Sensor Attribute 3-20
  Create Simulated Actions 3-22
  Simulate an Attribute, Action, or Alert for an Asset 3-23

4 Monitor the Health and Usage of Your Assets

Use Asset Metrics or Key Performance Indicators 4-1
  Define Your Own Metrics 4-2
Track Individual and Cumulative Asset Metrics Using Dashboards 4-4
  Create a Dashboard at the Organization Level 4-5
  Create a Dashboard at the Group Level 4-6
  Create a Dashboard at the Asset Level 4-6
  Access the Dashboard Metrics 4-7
Define an Automatic Anomaly 4-36
Create a User-Defined Anomaly 4-37
  Use Contextual Annotations in Pattern Anomalies 4-39
Edit an Anomaly 4-40
Duplicate an Anomaly 4-40
Delete an Anomaly 4-41
Use Predictions to Identify Asset Risks 4-41
  Create a Prediction 4-42
  Edit a Prediction 4-43
  Delete a Prediction 4-45

5  Set Up Your Devices in Oracle Internet of Things Cloud Service

Create Device Models in Oracle Internet of Things Cloud Service 5-1
  Create a New Device Model 5-1
  Import a Device Model 5-3
  Duplicate a Device Model 5-3
  Edit a Device Model 5-4
  View the Devices Associated with a Device Model 5-4
  Print Device Model Settings 5-4
  Export Device Model Settings 5-5
  Delete a Device Model 5-5
Assign Device Models to the Oracle IoT Asset Monitoring Cloud Service Application 5-6
  Assign a Device Model to a Cloud Service 5-6
Register and Activate Devices in Oracle Internet of Things Cloud Service 5-6
  Register a Single Device 5-7
  Register a Batch of Devices 5-7
  About CSV Batch Registration File Properties 5-9
  Activate a Device 5-10
  Activate a Batch of Registered Devices 5-11

6  Customize Your Oracle IoT Asset Monitoring Cloud Service Application

Show or Hide the Application Name 6-1
Add or Update an Application Logo 6-1
Remove an Application Logo 6-2

7  Integrate with Other Cloud and Oracle Services

Integrate Oracle Visual Builder Cloud Service with Oracle IoT Asset Monitoring Cloud Service 7-1
Download Asset Monitoring BOPs
Integrate Oracle Maintenance Cloud with Oracle IoT Asset Monitoring Cloud Service

Enable Oracle Maintenance Cloud Integration
Import Assets from Oracle Maintenance Cloud
Configure Rules to Generate Automatic Work Orders
Verify and Update the Work Orders in Oracle Maintenance Cloud
Verify Incident Status Updates in Oracle IoT Asset Monitoring Cloud Service
Automatically Update Asset Meters in Oracle Maintenance Cloud with IoT Data

Integrate Oracle Engagement Cloud with Oracle Service Monitoring for Connected Assets

Enable Oracle Engagement Cloud Integration
Import Assets from Asset Information Management
Configure Rules to Generate Automatic Service Requests
Diagnose and Troubleshoot Connected Assets from Engagement Cloud
Verify Incident and SR Status Update in Oracle Service Monitoring for Connected Assets

Integrate Oracle Service Cloud with Oracle Service Monitoring for Connected Assets
Integrate Oracle Enterprise Asset Management with Oracle IoT Asset Monitoring Cloud Service

Enable the Integration in Oracle Enterprise Asset Management
Sync Assets from Oracle Enterprise Asset Management
Configure Rules to Generate Automatic Work Orders
Verify and Update the Work Orders Created in Oracle Enterprise Asset Management
Verify Incident and Work Order Status Update in Oracle IoT Asset Monitoring Cloud Service

Integrate with Oracle Analytics Cloud
Enable Oracle Analytics Cloud Integration
Import the Sample Project in Analytics Cloud
Create a New Project in Analytics Cloud Using IoT Data
Use Asset Monitoring Widgets in Your Application
Add an Asset Monitoring Widget to Your Application or Web Page

8 Use the Oracle Internet of Things Asset Monitoring Mobile Application

How to Access the Oracle Internet of Things Asset Monitoring Mobile Application
View Asset Details in the Oracle Internet of Things Asset Monitoring Mobile Application
Edit Asset Details in the Oracle Internet of Things Asset Monitoring Mobile Application
Add a New Sensor to an Asset in the Oracle Internet of Things Asset Monitoring Mobile Application 8-3
View Asset Connectivity, Utilization, and Availability in the Oracle Internet of Things Asset Monitoring Mobile Application 8-4
View Sensor Data in the Oracle Internet of Things Asset Monitoring Mobile Application 8-4
Set the Asset Location in the Oracle Internet of Things Asset Monitoring Mobile Application 8-4
View the Asset Location History in the Oracle Internet of Things Asset Monitoring Mobile Application 8-5
View the Oracle Internet of Things Asset Monitoring Mobile Application Version Information 8-5
Log Out of the Oracle Internet of Things Asset Monitoring Mobile Application 8-5
Preface

*Using Oracle IoT Asset Monitoring Cloud Service* provides information and procedures for using Oracle IoT Asset Monitoring Cloud Service. Oracle IoT Asset Monitoring Cloud Service lets you monitor and manage the location of your assets.

**Topics:**
- Audience
- Documentation Accessibility
- Related Documents
- Conventions

**Audience**

*Using Oracle IoT Asset Monitoring Cloud Service* is intended for system administrators who are responsible for managing Oracle IoT Asset Monitoring Cloud Service.

**Documentation Accessibility**


**Access to Oracle Support**

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit [http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info](http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info) or visit [http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs](http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs) if you are hearing impaired.

**Related Documents**

For more information, see these Oracle resources:
- Oracle Cloud at [http://cloud.oracle.com](http://cloud.oracle.com)
- *Getting Started with Oracle Cloud*

**Conventions**

The following text conventions are used in this document:
<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td><strong>monospace</strong></td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
Get Started with Oracle IoT Asset Monitoring Cloud Service

Oracle IoT Asset Monitoring Cloud Service is a specialized Oracle Internet of Things Cloud Service application. Oracle IoT Asset Monitoring Cloud Service creates a digital twin version of your organization and organizational assets, and lets you monitor the location, condition, and utilization of your assets. You can also detect asset anomalies and use analytics to predict asset failures.

Topics

• Oracle IoT Asset Monitoring Cloud Service Overview
• What are the Different Assets that You Can Monitor
• Understand the Building Blocks of Oracle IoT Asset Monitoring Cloud Service
• What Interfaces Can You Use to Access Oracle IoT Asset Monitoring Cloud Service
• How to Access the Oracle IoT Asset Monitoring Cloud Service
• The Operations Center
• Create a New Organization
• Create a New Group
• Typical Workflow for Using Oracle IoT Asset Monitoring Cloud Service
• How to Get Support

Oracle IoT Asset Monitoring Cloud Service Overview

Oracle IoT Asset Monitoring Cloud Service creates a digital twin version of your organization and organizational assets, and lets you monitor the location, condition, and utilization of your assets.

Asset management traditionally employs manual techniques. Untraceable assets, asset downtimes, and asset write-offs are common problems associated with traditional asset management systems. A typical manufacturing company, for example, spends 25% of the total operating cost in asset maintenance.

Oracle IoT Asset Monitoring Cloud Service helps improve business productivity and reduce the operational costs and inefficiencies associated with asset management. With Oracle IoT Asset Monitoring Cloud Service, asset locations and asset health conditions are known at all times. Features such as anomaly detection and predictive analytics help you detect and address problem areas in time. You can proactively take asset actions and schedule maintenance and replacements.

Use Oracle IoT Asset Monitoring Cloud Service to:

• Locate Assets Instantly
What are the Different Assets that You Can Monitor

Assets are owned or leased resources of commercial value whose availability at the right place and right time can affect your business operations and profitability.

Whether your business is in the area of manufacturing, facilities management, mining, hospitals, or any other industry where assets are critical, Oracle IoT Asset Monitoring Cloud Service lets you monitor assets that are important for your business operations. You can monitor both indoor and outdoor assets.

Example 1-1   Some Examples of Assets that Can Be Monitored

Here are a few typical industries and assets that make use of asset monitoring:

- **Facilities**: HVAC systems, forklifts, office equipment such as copiers, high value machinery.
- **Manufacturing**: Lathes, boilers, extruders, milling, drilling, and shaping machines.
- **Hospitals**: Patient beds, ultrasound machines, medicine storage, blood infusion pumps.
- **Mining**: Excavators, loaders, dumpers, drag lines, shovels, rigs, generators.

Understand the Building Blocks of Oracle IoT Asset Monitoring Cloud Service

The Oracle IoT Asset Monitoring Cloud Service application includes several artifacts to help create a digital twin version of your business, and to help monitor and manage all your organizational assets.

The following sections introduce some of the key building blocks of the Oracle IoT Asset Monitoring Cloud Service application:

Organizations

Organizations are digital twin versions of your business. These are digital placeholders for the various heterogeneous entities that you have in your business, the locations where these entities operate from, and the associated users of these entities.

An organization contains digital versions of all the IoT-enabled assets that are part of your business operations. An organization is also associated with its authorized set of users. Predefined roles determine the privileges of each application user.

Your application can contain one or more organizations. For example, businesses often divide organizational operations based on geography. The following image shows a business divided into regions. Each region, Asia-Pacific, Europe, and North America has its own set of assets and users.
You may also want to have multiple organizations if you manage several clients, and you need to separate these clients into sub-tenants, so that each sub-tenant has its own set of assets and users.

The following sections include more information on organizations:

- Create a New Organization
- Create and Manage Users
- Change Your Current Organization
- The Operations Center

Groups

You can further subdivide a hierarchical organization into groups. For example, if an organization has two different set of products, you can create two distinct groups for each product with each group containing its own set of assets.

A group is a collection of similar assets under a single administration. You can group assets and authorize a single user or group of users to control the asset group. You can create asset groups based on your business needs. For example, you can create an asset group that contains all electrocardiogram (EKG) machines in a hospital. Alternatively, you may want to group the different assets present on a single floor under one group.

The following image shows some examples of hierarchical groups in an organization. The first group divides the assets by manufacturer (Asia, Japan, Manufacturer1 and Manufacturer2), the second group creates subgroups based on location (USA, West, CA, SF and LA), and the third group subdivides assets based on the product (Cars, Midsize, Brand1, Gas and Hybrid).
The assets contained in a group can be static or dynamic. You can either add assets manually to a group, or specify a filter criteria that dynamically selects the assets. For example, you can create a filter group for all assets of a particular asset type.

The following sections include more information on groups:

- **Create a New Group**
- **The Operations Center**

**Assets**

An asset is any leased or owned resource whose availability at the right time and place is important for your business operations and profitability. Use Oracle IoT Asset Monitoring Cloud Service to manage both your indoor and outdoor assets.

*Work with Your Assets* includes detailed information on working with your assets.

*Simulate Asset Sensors with the Built-In Simulator* includes information on creating asset simulations to test and understand Oracle IoT Asset Monitoring Cloud Service features without having to connect real devices.

**Asset Types**

The asset type defines the various attributes that identify an asset, and includes the sensor attributes that can be associated with the asset. A forklift asset type, for example, may include sensors for GPS coordinates, temperature, vibration, and oil viscosity.

Asset types also define asset actions and custom attributes. For example, if the asset type includes the power on/off action, you can directly power on or power off your device from the asset page. Custom attributes include attributes that vary between assets of a particular asset type, such as the asset serial number.

The following sections include more information on asset types:

- **Create and Manage Asset Types**
- **About Hierarchical Asset Associations**
- **Create Asset Associations**

**Metrics and KPIs**

Metrics or KPIs (Key Performance Indicators) help you track key metrics for your monitored assets, such as assets connected, assets available, and assets utilization.
You can also create custom KPIs to track the metrics that are relevant to your business processes. So, for example, you can create a metric to track the average hourly temperature reported by a temperature sensor. You can also aggregate the metrics for various assets in your organization or group. So, for example, you can aggregate the average fuel level across all your forklift assets.

Track your metrics using asset-level, group-level and organization-level dashboards. You can also track metrics in the map view for the assets visible in the map context.

The following sections include detailed information on working with metrics or KPIs:

- Define Your Own Metrics
- Track Individual and Cumulative Asset Metrics Using Dashboards
- Track Asset Metrics in the Map View

Places

Create places to define the storage and usage locations of your asset. You can search for your places in the map view and zoom into the available assets. If an asset moves out of its permitted place, Oracle IoT Asset Monitoring Cloud Service can generate an incident that is reported to the operations manager.

Create outdoor places by drawing a geofence on the map. For indoor places, you can additionally make use of floor plans and altitude data.

The following image shows a place created with a floor plan:

![Place with Floor Plan](image)

Create and Manage Places includes detailed information on creating and managing places.

Rules

Create rules to generate incidents, warnings, or alerts based on location, threshold, or alert conditions. So, for example you can create a location rule to generate an incident when an asset moves out of its designated location. You can create a threshold rule, say, to generate an alert when a pump device reports a blocked filter.

You can also use rules to trigger asset actions. For example, you can configure a rule to power off an overheating asset.
• **Incidents**: Use incidents to report issues and work with the maintenance staff for resolutions.

• **Alerts**: Use alerts to trigger other rules, or to pass messages to integrated enterprise applications.

• **Warnings**: Use warnings to create a log of issues that don’t require your immediate attention.

• **Actions**: Use asset actions to execute device-related actions for your asset.

*Use Rules to Monitor and Maintain Assets* includes detailed information on configuring rules.

The following sections provide more information on incidents, warnings, and actions:

• Use the Incidents Page to Manage Asset Incidents

• Use the Warnings Page to Manage Asset Warnings

• Trigger Actions for Assets

**Anomalies**

Use anomalies to detect deviations from normal asset behavior, and to flag and address device issues in time. You can create point-in-time anomalies that look for deviations in a KPI value. For example, point-in-time anomalies can help detect an HVAC device that is overheating. You can also use pattern-based anomalies to look for telltale patterns in sensor data generated by an asset. For example, you may use pattern-based anomalies to look for vibration anomalies in a forklift asset.

You can also use anomalies in rules to trigger incidents, warnings, asset actions, or alerts.

The following sections provide more information on anomalies:

• Use Anomalies to Track Deviations in Asset Behavior

• Create an Anomaly Rule

**Predictions**

Predictions use historical and transactional data to identify risks to your assets. You can either use internal Oracle Internet of Things Cloud Service data or import and use external device data to help make predictions for your asset.

Predictions help warn you of impending asset failure in advance. Preventive maintenance can help save the costs associated with asset breakdown or unavailability.

The following sections provide more information on predictions:

• Use Predictions to Identify Asset Risks

• Create a Prediction Based Rule

**Map View**

The map view lets you locate assets on the map. Assets can appear independently, or clustered together, depending on your zoom level in the map. Click a cluster on the map to display the individual assets. Click an asset to view asset details, such as the location history or the incidents associated with the asset.
A KPI ribbon appears in the lower pane of the map view. The KPI ribbon shows KPI metrics for the assets in your current view. Metrics include built-in metrics such as Asset Availability and Asset Utilization. You can also add custom KPI metrics per your business needs.

The following image shows a map view with asset clusters and the KPI ribbon:

Here are some of the built-in KPI metrics that appear in the map view:

- **Located Assets**: Shows the total number of assets located in the map.
- **Assets Connected**: Shows the percentage of assets heard from in the last one hour.
- **Assets Utilization**: Shows the percentage of assets that are currently utilized. An asset should be out of its designated storage location to be counted as utilized.
- **Asset Availability**: Shows the percentage of assets that are currently available. An available asset is one that does not have an outage incident reported against it.
- **Open Incidents**: Shows the current count of open asset incidents or issues.

The Operations Center and Locate Your Assets in the Map View includes more information on locating your assets in the map.

The following image shows the individual asset details that appear when you click an asset in the map:
Dashboards

Oracle IoT Asset Monitoring Cloud Service dashboards let you track key metrics for your monitored assets, such as assets connected, assets available, and assets utilization. You can create dashboards at the organization level, group level, or individual asset level.

If you have additionally created user-defined metrics for your assets, you can add these to your respective asset dashboards. For group and organization-level dashboards, you can display the metric values aggregated over all your assets in the group or organization. For example, you may choose to display the average fuel level across all your forklift assets.

The following section provides more information on dashboards: Track Individual and Cumulative Asset Metrics Using Dashboards

What Interfaces Can You Use to Access Oracle IoT Asset Monitoring Cloud Service

Use the browser interface from your PC, laptop, or other mobile device, such as a tablet, to access the Oracle IoT Asset Monitoring Cloud Service application URL. You can also use the Asset Monitoring mobile application on your Apple or Android phone to monitor and manage assets.

Oracle IoT Asset Monitoring Cloud Service provides the following interfaces:

• **Browser Based Application:**
  This is the primary means to access all Oracle IoT Asset Monitoring Cloud Service functionality.

• **Mobile Application:**
  The Asset Monitoring mobile application lets an operations manager access and monitor assets on the go. The application lets a technician add a sensor, for example, by scanning the device barcode with the technician's mobile. The following figure shows an operations manager monitoring an asset and using the barcode search functionality to search for a device.
Rest APIs:
You can use the set of REST APIs provided by Oracle IoT Asset Monitoring Cloud Service to build your own integrations, and to perform various asset management tasks.

How to Access the Oracle IoT Asset Monitoring Cloud Service

Log in to manage and monitor your asset monitoring application. Before you log in to Oracle IoT Asset Monitoring Cloud Service, you must have a user account. Oracle provides user account information when you subscribe to Oracle IoT Asset Monitoring Cloud Service.

1. Navigate to the following URL:
https://hostname/am
Here, hostname is the host name of your Oracle IoT Cloud Service instance.
The Oracle IoT Asset Monitoring Cloud Service login screen appears.

2. Enter your user name and password and click Sign In.
The default Oracle IoT Asset Monitoring Cloud Service view appears. You are placed in the Operations Center for your organization.

The Operations Center

The operations center is your default view for your organization. When you first log in to Oracle IoT Asset Monitoring Cloud Service, you are placed into the operations center for your organization.

You can return to the operations center from any page by clicking Menu and selecting Operations Center.
You can monitor all your digital twin assets and dashboards from within the operations center. The Map View displays your assets per their current locations on the map.

You are placed in the Map view by default. The toolbar on the left lets you access the following pages for the assets visible in the map:

- **Search** lets you search for groups, assets, locations, and places.
- **Map** displays the map view. See for more information on working with the map view.
- **Assets** displays the list of assets. If you have group subdivisions, the assets can be found under the groups and subgroups.
- **Incidents** displays the list of incidents for the assets currently visible in the map.
- **Warnings** displays the list of incidents for the assets currently visible in the map.
- **Anomalies** displays the list of anomalies for the assets currently visible in the map.
- **Predictions** displays the list of predictions for the assets currently visible in the map.
- **Trends** displays the list of trends for the assets currently visible in the map.
- **Custom Dashboards** display any custom dashboards that you have added for the organization or group.

The following image shows the Operations Center view and the various menu bar options.

![Operations Center View](image)

The breadcrumbs at the top let you filter your context. For example, in the following image, we navigate to the *Loaders* group under the *North America* organization to narrow down to the assets in the group.
By changing the context or scope using the breadcrumbs, you automatically change the context for all the options on the menu bar. So, if you change the context to the **Loaders** group, and click **Incidents**, then only the incidents for the assets in the Loaders group are displayed.

If you have created group-based dashboards, then changing the context to a group also makes the corresponding group's dashboard icons appear on the menu bar.

You can click any entity in the breadcrumbs to change your context back to that entity. For example, if you were to click **North America** in the preceding image, you would go back to the parent context.

For more information on filtering and locating your assets in the map, see [Locate Your Assets in the Map View](#).

### The Design Center

Use the design center to create and manage your organizations, groups, asset types, asset inventory, places, and all the associated entities.

Use the design center to create and manage all your asset monitoring entities. You can monitor these entities in the operations center.

When you first log in to Oracle IoT Asset Monitoring Cloud Service, you are placed into the operations center for your organization. Click **Menu** and then click **Design Center** to access the design center options.

The design center contains the following pages:

- **Organization**: Use the Organization page to create and edit organizations. You can change the list of users associated with an organization, add dashboards for the organization, and add notification subscribers for the organization. Use the Organization page to switch your current organization. The organization selected in the design center is the one that appears under the operations center.

- **Asset Types**: Use the Asset Types page to create and manage your asset types. Use the Asset Types page to create any entity associated with the asset type, such as metrics, actions, rules, trends, anomalies, predictions, external data associations, and asset-level dashboards.
- **Asset Inventory**: Use the Asset Inventory page to create, view, and manage your assets. You can also reserve, edit, duplicate, or delete assets from this page.
- **Groups**: Use the Groups page to create and manage your asset groups. You can also change user-access for a group from this page.
- **Places**: Use the Places page to define and manage Geo-location boundaries and floor plans.

### Create a New Organization

Organizations are digital placeholders for the various heterogeneous entities that you have in your business, the locations where these entities operate from, and the associated users of these entities.

This operation is meant for application administrators only. Log in using the administrator account to create organizations in Oracle IoT Asset Monitoring Cloud Service.

1. Click **Menu (≡)**, and then click **Design Center**.
2. Select **Organization** from the **Design Center** sub-menu.
3. Click **Switch/Manage Organizations**.
4. Click **Create New** in the Switch/Manage Organizations page.
   
   The Create Organization dialog appears.
5. Specify a **Name** for your organization.
   
   For example, *North America Operations*.
6. Specify an optional **Description**.
7. Click **Create**.
   
   A confirmation banner appears, and the new organization is added to the list of existing organization.

### Change Your Current Organization

If you are part of more than one organization, then you can change your current organization in Oracle IoT Asset Monitoring Cloud Service.

1. Click **Menu (≡)**, and then click **Design Center**.
2. Select **Organization** from the **Design Center** sub-menu.
3. Click **Switch/Manage Organizations**.
4. Select the organization name that you wish to switch to, and click **Switch**.
   
   The current organization is changed in the design center and operations center.

### Assign Users to an Organization

Edit the organization to add or update the list of authorized users for the organization.

1. Click **Menu (≡)**, and then click **Design Center**.
2. Select **Organization** from the **Design Center** sub-menu.
3. Click **Edit** (-edit tool icon).

4. Under Users, select the users that you wish to include in the organization, and click the right-arrow icon (→).

5. Click **Save** to save the changes to the organization.

### Export and Import Organizations

You can export an organization, together with its assets, asset types, and associated artifacts from an Oracle IoT Asset Monitoring Cloud Service instance. You can then import the organization into another Oracle IoT Asset Monitoring Cloud Service instance.

When you export an organization, all assets and their associated asset types are exported. The artifacts connected with the asset types, such as metrics, rules, anomalies, predictions, and trends are also exported. Importing the organization into another instance creates the organization, together with its assets, asset types, and associated artifacts, in the importing instance.

Any groups and places that exist in the exported organization are also brought into the importing instance. Note that any devices connected to assets in the original instance are not included in the export. If you have asset types with mandatory sensor attributes, you would need to create new device links for the assets in the imported organization.

### Export an Organization

Export an organization to create an `iot` export file containing the organization along with its assets, asset types, and places.

1. Click **Menu** (ellipse), and then click **Design Center**.
2. Select **Organization** from the **Design Center** sub-menu.
3. Click **Switch/Manage Organizations**.
4. Select the organization name that you wish to export, and click **Export**.

A `.iot` archive of the organization is generated.

5. Save the generated `.iot` archive file to your hard disk or a storage location.

You will use this file when importing the organization into another instance of Oracle IoT Asset Monitoring Cloud Service.

### Import an Organization

Import an organization into an Oracle IoT Asset Monitoring Cloud Service instance to create the organizational artifacts previously exported from another instance.

1. Click **Menu** (ellipse), and then click **Design Center**.
2. Select **Organization** from the **Design Center** sub-menu.
3. Click **Switch/Manage Organizations**.
4. Click **Import**.

The Import Organization dialog appears.
5. Click **Choose File** and select a previously exported .iot archive file.

6. Click **Import**.

The organization is imported along with its containing artifacts. The organization appears in the list of existing organizations.

### Create and Manage Groups

A group is a collection of similar assets under a single administration. You can group assets and authorize a single user or group of users to control the asset group.

Create asset groups based on your business needs. For example, you can create an asset group that contains all electrocardiogram (EKG) machines in a hospital. Alternatively, you may want to group the different assets present on a single floor under one group.

You can control access to individual assets by creating asset groups, and assigning authorized users to each asset group. Let us take two examples of Forklifts and HVAC asset groups:

- **Asset Group**: Forklifts
  - **Assets**: Forklift_1, Forklift_2, Forklift_3
  - **Users**: Manager, Forklift_Operator

- **Asset Group**: HVACs
  - **Assets**: HVAC_1, HVAC_2, HVAC_3
  - **Users**: Manager, HVAC_Operator

In the preceding scenario, the Manager will be able to access all the assets. The Forklift_Operator can only see forklift assets and the HVAC_Operator can only see HVAC assets.

### Create a New Group

You can subdivide a hierarchical organization into groups. Groups can in turn contain sub-groups.

This operation is meant for application administrators only. Log in using the administrator account to create groups in Oracle IoT Asset Monitoring Cloud Service. In the Operations Center, ensure that you are in the organization for which you wish to create the groups.

1. Click **Menu (≡)**, and then click **Design Center**.
2. Select **Groups** from the **Design Center** sub-menu.
3. Click **Create Group (†)** to create a new group.
4. Specify a **Name** for your group.
   
   For example, **Forklifs**, for a group of forklift assets.

5. Specify an optional **Description**.

6. Select the **Type** of the group.
   
   The assets contained in a group can be static or dynamic. You can either add assets manually to a group, or specify a filter criteria that dynamically selects the
assets. For example, you can create a filter group for all assets of a particular asset type.

- Select **Static Group** to create a group wherein you manually select the constituent assets.
  a. Under **Parent**, select **Current Organization** to create a group directly under the current organization. Alternatively select the name of a preexisting group to create a sub-group under the existing group.
  b. (Optional) Under Selection, optionally click **Select Filter** to filter the list of assets. For example, you can filter for assets of a particular asset type.
  c. Select the assets that you wish to include in the group, and click the right-arrow icon (→) to move them into the group. Use the **Shift** and **Ctrl** keys to select multiple assets at a time.

- Select **Filter Group** to create a group wherein the constituent assets are dynamically determined using a filter criteria.
  a. Under **Parent**, select **Current Organization** to create a group directly under the current organization. Alternatively select the name of a preexisting group to create a sub-group under the existing group.
  b. Under Filter, click **Select Filter** to specify your filter criteria. For example, you can filter for assets of a particular asset type.
  c. Validate that the list of results is consistent with your filter criteria. Any new assets that satisfy your filter criteria will automatically become a part of your filter group.

7. Click the **Users** tab (👤) to assign authorized users for the group.
   a. Select an available user, and click the **Move** (→) icon to move the user to the list of authorized users.
   b. Repeat the previous step to add additional authorized users for the asset group.

8. Click **Save** to save the new group.

9. Click **Back** to return to the Groups page.

**Typical Workflow for Using Oracle IoT Asset Monitoring Cloud Service**

To implement Oracle IoT Asset Monitoring Cloud Service, start by importing or creating the assets and asset types. Once you have associated sensor devices with your assets, you can start locating and monitoring your assets.

If you are learning about Oracle IoT Asset Monitoring Cloud Service, or wish to try out its various features, use the digital twin simulator that comes along with the product. This eliminates the need to connect actual sensors, and to create assets and asset types. See [Simulate Asset Sensors with the Built-In Simulator](#) for more information.

This image represents the workflow for implementing Oracle IoT Asset Monitoring Cloud Service:
Chapter 1

Typical Workflow for Using Oracle IoT Asset Monitoring Cloud Service

1. Log in to Oracle IoT Asset Monitoring Cloud Service
2. Create Assets
   - Create Asset Types
   - Import Assets from External System such as EBS EAM
3. Create Places
   - Connect Sensors to your Assets
4. Create Metrics
   - Connect Sensors to your Assets
5. Create Rules
   - Create Asset Packages using the Asset Monitoring Simulator
6. Create Anomalies and Predictions
   - Create Asset Packages using the Asset Monitoring Simulator

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create the Device Models</td>
<td>Create device models to let data be transmitted from a device to Oracle Internet of Things Cloud Service. Perform this task in Oracle Internet of Things Cloud Service Management Console if you do not have your device models in the IoT platform already.</td>
<td>Create Device Models in Oracle Internet of Things Cloud Service</td>
</tr>
<tr>
<td>Register and Activate the Devices</td>
<td>Register the devices with the Oracle Internet of Things Cloud Service and provision the client software so that it communicates with the Oracle Internet of Things Cloud Service. Perform this task in Oracle Internet of Things Cloud Service Management Console if you do not have your devices on the IoT platform already.</td>
<td>Register and Activate Devices in Oracle Internet of Things Cloud Service</td>
</tr>
</tbody>
</table>

ORACLE
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign the Device Models to the Cloud Service</td>
<td>Assign the device models to the Oracle IoT Asset Monitoring Cloud Service, so that they can be seen and used in the Oracle IoT Asset Monitoring Cloud Service. Perform this task in Oracle Internet of Things Cloud Service Management Console.</td>
<td>Assign Device Models to the Oracle IoT Asset Monitoring Cloud Service Application</td>
</tr>
<tr>
<td>Create Assets</td>
<td>Start by creating your business assets and asset types in Oracle IoT Asset Monitoring Cloud Service. You can monitor both indoor and outdoor assets. If you are already managing your assets in an asset management system, such as Maintenance Cloud or Oracle Enterprise Asset Management, you can import your assets into Oracle IoT Asset Monitoring Cloud Service. The next step is to associate sensor devices, such as location sensors and temperature/humidity sensors, with your assets. Bluetooth and RFID devices are examples of indoor sensors. GPS devices are examples of outdoor sensors.</td>
<td>Create and Manage Asset Types Create and Manage Assets</td>
</tr>
<tr>
<td>Create Places</td>
<td>Create places to define the storage and usage locations of your asset. You can search for your places in the map view and zoom into the available assets. If an asset moves out of its permitted place, Oracle IoT Asset Monitoring Cloud Service can generate an incident that is reported to the operations manager. Create outdoor places by drawing a geofence on the map. For indoor places, you can additionally make use of floor plans and altitude data.</td>
<td>Create and Manage Places</td>
</tr>
<tr>
<td>Create Metrics/KPIs</td>
<td>KPIs or Key Performance Indicators help you track key metrics for your monitored assets, such as assets connected, assets available, and assets utilization. You can also create custom KPIs to track the metrics that are relevant to your business processes. So, for example, you could create a metric to track the average hourly temperature reported by a temperature sensor. You can track KPIs from the dashboard and the map view for the assets visible in the map. You can also track individual KPIs for an asset from the assets page.</td>
<td>Use Asset Metrics or Key Performance Indicators</td>
</tr>
<tr>
<td>Create Rules</td>
<td>Create rules to generate incidents, warnings, or alerts based on location, threshold, or alert conditions. So, for example you can create a location rule to generate an incident when an asset moves out of its designated location. You can create a threshold rule, say, to generate an alert when a pump device reports a blocked filter. You can also use rules to trigger asset actions. For example, you can configure a rule to power off an overheating asset. <strong>Incidents:</strong> Use incidents to report issues and work with the maintenance staff for resolutions. <strong>Alerts:</strong> Use alerts to trigger other rules, or to pass messages to integrated enterprise applications. <strong>Warnings:</strong> Use warnings to create a log of issues that don’t require your immediate attention. <strong>Actions:</strong> Use asset actions to execute device-related actions for your asset.</td>
<td>Use Rules to Monitor and Maintain Assets</td>
</tr>
<tr>
<td>Task</td>
<td>Description</td>
<td>More Information</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Create Anomalies and Predictions</td>
<td>Use anomalies to detect deviations from normal asset behavior, and to flag and address device issues in time. You can create point-in-time anomalies that look for deviations in a KPI value that exceed a threshold value. For example, point-in-time anomalies can help detect an HVAC device that is overheating. You can also use pattern-based anomalies to look for telltale patterns in sensor data generated by an asset. For example, you may use pattern-based anomalies to look for vibration anomalies in a forklift asset. Predictions use historical and transactional data to identify risks to your assets. You can either use internal Oracle Internet of Things Cloud Service data or import and use external device data to help make predictions for your asset. Predictions help warn you of impending asset failure in advance. Preventive maintenance can help save the costs associated with asset breakdown or unavailability.</td>
<td>Use Anomalies to Track Deviations in Asset Behavior</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use Predictions to Identify Asset Risks</td>
</tr>
</tbody>
</table>

### How to Get Support

Use these resources to resolve problems:

- If you’re an Oracle Premier Support Customer, visit [My Oracle Support](https://support.oracle.com/).
- Contact Oracle Technical Support. See Contacting Oracle Support in *Getting Started with Oracle Cloud*.
Create and Manage Users

Access to Oracle IoT Asset Monitoring Cloud Service functionality is determined by pre-defined roles.

Log in using the administrator account to create users in Oracle IoT Asset Monitoring Cloud Service and assign the required roles to them.

**Note:**

You can also use your Oracle Identity Cloud Service instance to manage users, and their assigned roles, for the registered Oracle IoT Asset Monitoring Cloud Service application.

You can access Oracle Identity Cloud Service from the My Services page of your cloud subscription.

Understand Roles and Users

Oracle IoT Asset Monitoring Cloud Service uses predefined roles for the application users. Roles are a set of privileges assigned to a user.

Oracle Identity Cloud Service provides a centralized identity store for your Asset Monitoring roles and users. When you create a user in Asset Monitoring, the user is created and stored in the identity domain associated with your IoT application in Oracle Identity Cloud Service. You can grant one or more roles to a user.

Oracle IoT Asset Monitoring Cloud Service uses the following roles:

- **Administrator (IoTAMAdministrator):** The application administrator sets up and maintains the application. The application administrator optimizes the availability of assets to meet the service levels required by the employees and users. The application administrator:
  - Sets up and configures the application by defining the organizational entities, asset types, associated device models and devices, asset creation policies, geo-fences and places.
  - Defines default KPIs or metrics, dashboard chart types and their layouts, anomalies, and predictions.

  The administrator alone has privileges to create new asset types, create and manage users, and modify application settings from the Settings page.

- **Operations Manager (IoTAMOperationsManager):** The operations manager manages and ensures the day-to-day availability of assets. The operations manager:
  - Monitors the locations, deployment status, and health (KPIs or metrics) of assets being tracked.
Assigns assets to locations and jobs that require them.
- Monitors and manages asset-related incidents.

Only the administrator or operations manager can manage asset groups, metrics or KPIs, rules, places, contextual data connections, predictions, and anomalies.

**Technician (IoTAMTechnician):** The technician performs asset registration and retirement tasks. The technician:
- Handles the IoT devices associated with the physical assets.
- Monitors and manages individual incidents. The technician carries out the directives associated with reported incidents.
- Locates assets and views their health status to perform tasks such as physical audits.

The technician can manage assets and view entities such as asset groups, metric values, rules, incidents, and warnings.

**User (IoTAMUser):** The asset user locates a required asset based on various search criteria, such as proximity, type, and utilization. The asset user puts an asset to productive use after looking at parameters, such as asset attribute details and operational health status.

Users can view asset types, assets, asset groups, and the map view.

### Create a New User

To let a user access Oracle IoT Asset Monitoring Cloud Service, create a new user in the application. Next, assign the roles appropriate for the user’s assigned tasks.

1. In the operations center, click **Menu (≡)**, and then click **Configuration**.

   If you are in the design center, you need to click **Previous (⁻)** before you see the **Configuration** option in the menu.

2. Click the **Users** tab (𓆕).

3. Click **Create User ( createUser)**.

4. Under **ROLES**, select one or more of these roles for the user:
   - **Administrator:** Select this role if the new user is an application administrator.
   - **Operations Manager:** Select this role if the new user will manage and ensure the day-to-day availability of assets.
   - **Technician:** Select this role if the new user will perform asset registration and retirement tasks.
   - **User:** Select this role if the new user needs basic access to the application.

5. Under **NAME**, enter the name for the user and the desired User ID:
   - **First Name:** Enter the first name of the user.
   - **Last Name:** Enter the last name of the user.
   - **Username:** Enter a user name for the user account.

6. Under **EMAIL**, provide the email details for the user:
   - **Work:** Enter the work email address for the user.
• **Home**: (Optional) Enter the home email address for the user.

• **Recovery**: (Optional) Enter the recovery email address for the user. This email address is used to help the user regain access to their account if they forget their password or are locked out.

• **Other**: Optionally, enter an additional email address for the user.

A primary (work) email is required. Oracle Identity Cloud Service automatically sends a mail to this address with the link for user account activation.

7. (Optional) Under **TELEPHONE**, provide the telephone details for the user.

• **Work**: Enter the work phone number for the user.

• **Home**: Enter the home phone number for the user.

• **Recovery**: Enter the recovery phone number for the user. This phone number is used to help the user regain access to their account if they forget their password or are locked out.

• **Other**: Enter an additional phone number for the user.

• **Mobile**: Enter the mobile phone number for the user.

8. Click **Save**.

9. Click **Back** to return to the **Users** page.

---

**Edit a User Account**

Edit a user account to change the user’s roles, name, e-mail, or telephone information.

1. In the operations center, click **Menu (≡)**, and then click **Configuration**.

   If you are in the design center, you need to click **Previous (⬅)** before you see the **Configuration** option in the menu.

2. Click the **Users** tab (𝑖).

3. Click **Edit (✍️)** against the appropriate user row.

4. Make the necessary changes under the **ROLES**, **NAME**, **EMAIL** and **TELEPHONE** sections.

5. Click **Save**.

6. Click **Back** to return to the **Users** page.

---

**Search for a User Account**

Use the search function to locate a specific user account or user accounts matching specific search criteria.

1. In the operations center, click **Menu (≡)**, and then click **Configuration**.

   If you are in the design center, you need to click **Previous (⬅)** before you see the **Configuration** option in the menu.

2. Click the **Users** tab (𝑖).
3. Click **Search** (🔍) to toggle the search if it is off.

4. Select one of these options in the **Show This App's Users Only** list:
   - **First Name**: Select this option to search for a user account by the user's first name.
   - **Last Name**: Select this option to search for a user account by the user's last name.
   - **Username**: Select this option to search for a user account by user name.
   - **Email**: Select this option to search for a user account by email address.
   - **Roles**: Select this option to search for a user account by role(s).

   The Users page displays Oracle IoT Asset Monitoring Cloud Service users by default.

   If you were to set **Show this App's Users Only** setting to **False** on the page, then the page also displays other users stored in the same Oracle Identity Cloud Service domain. For example, if you are also using the IoT platform and Connected Worker services in addition to Asset Monitoring, you might see additional users present in Oracle Internet of Things Cloud Service and Oracle Internet of Things (IoT) Connected Worker Cloud Service.

5. Select one of these options in the second list:
   - **starts with**: Select this option to search for a user account using a full or partial search phrase. For example, you can locate the user Tom Jones by searching for T, To, or Tom.
   - **matches**: Select this option to search for a user account using an exact match. For example, to locate the user Tom Jones, enter Tom Jones in the search field.
   - **does not match**: Select this option to search for a user account by excluding the search criteria you enter. For example, entering Tom Jones returns all users except Tom Jones.

6. Enter your search criteria in the field and then press **Enter**.

7. (Optional) Click **Add** (➕) to add additional search criteria.

8. (Optional) Click **Remove** (➖) to remove additional search criteria.

9. (Optional) Click **Clear Search** to clear your search criteria.

### Delete a User Account

Delete a user account when it is no longer needed.

1. In the operations center, click **Menu** (☰), and then click **Configuration**.

   If you are in the design center, you need to click **Previous** (➚) before you see the **Configuration** option in the menu.

2. Click the **Users** tab (👤).

3. Click **Delete** (🗑️) against the user that you wish to delete.
4. Click **Yes**.
Work with Your Assets

Asset entities in Oracle IoT Asset Monitoring Cloud Service help you monitor and manage your business assets. Associate your assets with IoT sensor devices. Assign places to assets to track their movement and utilization.

Topics:

- What is an Asset
- Create and Manage Asset Types
- Create and Manage Assets
- Create and Manage Places
- Locate Your Assets in the Map View

What is an Asset

An asset is any leased or owned resource whose availability at the right time and place is important for your business operations and profitability. Use Oracle IoT Asset Monitoring Cloud Service to manage both your indoor and outdoor assets.

Here are a few typical examples of assets used in:

- **Facilities**: HVAC systems, forklifts, office equipment such as copiers, high value machinery.
- **Manufacturing**: Lathes, boilers, extruders, milling, drilling, and shaping machines.
- **Hospitals**: Patient beds, ultrasound machines, medicine storage, blood infusion pumps.
- **Mining**: Excavators, loaders, dumpers, drag lines, shovels, rigs, generators.

You can associate multiple sensors with an asset. The sensor types or device models are defined in the asset type for the asset. An HVAC asset, for example, may include sensors for GPS coordinates, temperature, vibration, and oil viscosity.

Indoor assets typically use Bluetooth and RFID based sensors for tracking locations. Outdoor assets typically use GPS-based sensors. Additional external and internal sensors for your assets help you monitor the various asset parameters.

Create and Manage Asset Types

Each asset requires an asset type. Use asset types to categorize your assets.

The asset type defines the sensor types or devices that can be associated with the asset. A forklift asset type, for example, may include sensors for GPS coordinates, temperature, vibration, and oil viscosity. Asset types also define asset actions for assets belonging to the type. For example, if the asset type includes the power on/off action, you can directly power on or power off your device from the asset page. Asset
types also define any custom attributes for assets belonging to the type. For example, an HVAC asset type may include a model number attribute.

Let us take the example of a hospital. The hospital defines asset types for its various assets and equipment:

- **Asset Type**: HVAC
  - **Device**: HVAC Device Model (temperature and vibration sensors, alerts for door open)
  - **Custom Attribute**: Device serial number
  - **Actions**: Power On/Off
- **Asset Type**: Ultrasound Machine
  - **Device**: UM Device Model (associated location and other sensors)
- **Asset Type**: Bed
  - **Device**: Bluetooth/RFID Location Sensor
  - **Custom Attribute**: Bed Number

### Create a New Asset Type

Create an asset type, and specify common attributes applicable to all assets of the asset type. Also, create sensor attributes that will map to your device sensor attributes.

1. Click **Menu (≡)**, and then click **Design Center**.
2. Select **Asset Types** from the **Design Center** sub-menu.
3. Click **Create Asset Type (+)**.
4. Enter a **Name** and an optional **Description** for the asset type under **Asset Type Details**.
   
   Do not use spaces or special characters in the **Name** field. If you add spaces or special characters, an error message appears.
5. Click **Upload Image** to upload an image for the asset type.
6. Click **Upload Icon** to upload an icon for the asset type.
   
   An icon makes it easier to quickly identify the asset type in the map view.
7. Add any required and optional attributes for the asset type:

   a. Click the **Attributes (≡)** tab.
   b. Click **Add Attribute (+)** to add a new attribute.
   c. Select the attribute type.
      
      - **Custom Attribute**: A custom attribute is specific to the asset type, such as a **model number** for a **vehicle**. Custom attributes are not associated with asset sensors.
      - **Sensor Attribute**: A sensor attribute corresponds to a device sensor value. For example, an HVAC device might support temperature and vibration sensors. Note that the actual linking to the device happens when you create the asset.
• **Alert Attribute:** An alert attribute corresponds to a device alert supported by your asset. For example, your cold-storage asset might support a door open alert.

d. Specify a **Name** for the attribute.

e. (Optional) Choose a **Category** if available.

By default, the UNCATEGORIZED category is used. You can choose to rename the category from the Attributes page.

f. (Optional) Specify any instructions related to the attribute.

g. Select whether the attribute is **Required** or optional.

You must specify a value for a required attribute when instantiating an asset type to create an asset.

h. Choose a data **Type** for the attribute.

This field is only applicable to custom and sensor attributes. You can select between text, number, date, boolean, and image data types.

i. (Optional) Specify a **Default** value of the attribute.

This field is only applicable to custom attributes. If you do not specify an attribute value when creating an asset, the default value is used.

j. (Optional) If you are creating a text attribute, you can specify a list of **Allowed Values** for your attribute.

This field is only applicable to custom attributes. Press **Enter** after entering each value.

k. Click **OK**.

l. Repeat the above steps to create additional attributes.

8. Click **Save**.

9. Click **Back** to return to the **Asset Types** list.

### Add Optional Actions to the Asset Type

If your device model supports actions, you can include these actions in your asset type. This lets you invoke the device action from an asset page or rule. For example, you can create a rule to power off an overheating device.

1. Click **Menu (≡)**, and then click **Design Center**.

2. Select **Asset Types** from the **Design Center** sub-menu.

3. Select an asset type from the **Asset Types** list.

   You can also search for an asset type.

4. Click **Actions**.

5. Click **Create Action (✚)**.

6. Specify a **Name** for the action.

7. Select **Sequential** under **Execution Order** if you want to process the action items sequentially. Alternatively, select **Parallel** if you want to process the action items in parallel.

8. Select an option for the **Action Item**.
You can set an available attribute, log the current value of an attribute, or define a function to bind to a device action later.

9. If you selected **Function** in the preceding step, specify a name for the function. You can use this name when later binding to a device action. If you selected **Log Attribute** or **Set Attribute**, you can select the name, and value, of an available attribute.

10. If you are configuring a function, specify the (data) **Type** and **Value** to be passed to the device action.

11. If you are configuring a function, optionally set the **Required** flag. A required function must be bound to a device action when you create a new asset of the corresponding asset type.

12. Repeat steps 8 to 11 to create more action items.

13. Optionally change the order of your action items by using the arrow keys under the **Order** column.

14. Click **Save** to save the action created for the asset type.

### About Hierarchical Asset Associations

Hierarchical asset associations let you link connected assets making it easier to visualize the hierarchy. You can create associated assets in one step, and view and edit associated asset types from a single interface.

For example, a truck asset may include associated assets like wheels, engine, and fuel tank. When creating the truck asset type, you can choose to define these associated assets along with their custom and sensor attributes.

The asset types may look like the following:

- **Truck**
  - Custom Attributes: Model, Color
  - **Wheels**
When you create an actual truck asset, all the required sub-assets are created automatically. You specify the mandatory and optional attributes to complete creating a truck asset. For sensor attributes, you need to associate the attributes to their respective device attributes added in Oracle Internet of Things Cloud Service.

Create Asset Associations

You can create asset associations when creating or editing an asset. You can add existing sub-assets, or create new ones.

1. From the Create Asset Type or Edit Asset Type page, click **Link to Other Asset Type**.
2. Select one of the following:
   - **Create New**: Creates and adds a new sub-asset type for the asset type.
   - **Use Existing**: Adds an existing sub-asset type for the asset type.
3. Enter or select an **Asset Type** name.
4. Enter a **Reference** name for the asset association.
   Each asset association created for the parent asset should have a unique reference name.
   For example, if you are creating the Engine sub-asset for the Truck asset type, you may want to call the reference **TruckEngine**.
5. Select **Required** if each parent asset must contain this sub-asset.
   For example, if you are creating the Engine sub-asset for a Truck asset, then you may want to set the **Required** flag, as each Truck will need to have an Engine.
   If you set the **Required** flag, then for each new instance of the parent asset that you create, the sub-asset is created automatically. You would need to specify any mandatory attributes.
6. Click **OK** to add the sub-asset.
7. To edit the just added sub-asset, or to add or remove attributes for the sub-asset, click the sub-asset icon within the parent asset, and click **Go to: SubAsset**.
8. After editing the sub-asset, you can click **Go back to Asset Type: Parent Asset Name** to go back to the parent asset type page.
9. Click **Save** to save the asset hierarchy. All changes made to the parent and sub-assets are saved.

   A dialog displays the progress of each save operation.

10. Click **OK**.

### Edit an Asset Type

Edit an asset type to edit, add, duplicate, or remove asset type settings including the asset type name, description, icon, attributes, device reference and sensor attributes.

1. Click **Menu (≡)**, and then click **Design Center**.
2. Select **Asset Types** from the **Design Center** sub-menu.
3. Select an asset type from the **Asset Types** list.
   
   You can also search for an asset type.

4. Click the **Edit (📝)** icon.
5. Edit the **Name** or **Description** fields.
6. (Optional) Click **Upload Image** to add a new image for the asset type.
7. (Optional) Click **Upload Icon** to add a new icon for the asset type, or click **Delete** to delete the existing icon.

8. Click the **Attributes (📝)** tab to add, remove, or edit asset attributes.
9. (Optional) To change the name of the attribute category, click **Edit Category (📝)**.
10. (Optional) To add a new attribute, click **Add Attribute (➕)**.

   Note that you cannot add a **Required** attribute to an asset type that has existing assets, as this will invalidate the existing assets. You get an error when trying to save the asset type with a new **Required** attribute. However, you can add optional attributes to an asset type with existing assets.

11. To edit, duplicate, or delete an existing attribute, select the attribute and use the appropriate option.
12. Click **Save**.
13. Click **Back** to return to the **Asset Types** list.

### Delete an Asset Type

Delete an asset type when it is no longer required.

**Note:**

Delete all associated KPIs, predictions, and anomalies before deleting an asset type.

1. Click **Menu (≡)**, and then click **Design Center**.
2. Select **Asset Types** from the **Design Center** sub-menu.
3. Select an asset type from the **Asset Types** list.
   You can also search for an asset type.

4. Click the **Delete** ([Trash Can icon]) icon against the asset type name.
5. Click **Delete** in the confirmation dialog.

**Create and Manage Assets**

Creating asset entities for your business assets in Oracle IoT Asset Monitoring Cloud Service lets you track, monitor, maintain, and troubleshoot your assets.

When creating a new asset, you must assign an asset type to the asset. You can then associate the asset with sensor devices allowed by your asset type. Specifying an assigned place for your asset lets you trigger rules in case the asset leaves its assigned place. You can also specify a storage location for the asset, so that you can track whether or not the asset is not being utilized.

**Create an Asset**

Create asset entities in Oracle IoT Asset Monitoring Cloud Service to monitor and manage your business assets.

1. Click **Menu (≡)**, and then click **Design Center**.
2. Select **Asset Inventory** from the **Design Center** sub-menu.
3. Click **Create New Asset** ([Plus icon]).
4. Select the **Asset Type** for the asset.
   The **Asset Type** must already exist in the application.
5. Enter a **Name** for the asset.
6. Select **Create all Optional Assets**, if the asset type has sub-assets that are optional, but you want all optional sub-assets to be created along with the asset.
   All required sub-assets are automatically created. You may need to specify any mandatory attributes that do not have default values.
7. Click **Continue** to continue creating the asset and any specified sub-assets.
   The asset along with any mandatory and specified sub-assets is created. A progress bar indicates the mandatory items that were completed, and the ones that you must complete.

   In the following example, a Truck asset is created. The truck has the following associations:
   - TruckFrontWheels
   - TruckFuelTank
   - TruckEngine
   - TruckRearWheels

   You can navigate into the individual sub-assets by clicking the respective associations. The engine sub-asset has some remaining mandatory items that you must complete before you can save the asset.
8. Specify the **Standard Attributes** for the asset, and also for any associated sub-assets.

   - **Name**: Enter a name for the asset or sub-asset.
   - **Description**: Enter an optional description for the asset or sub-asset.
   - **Tags**: Enter optional tags for the asset. Sub-assets don't require this, as the tags are specified for the parent asset.
   - **Assigned Place**: Select an optional assigned location for the asset. Sub-assets don't require this, as the value is specified for the parent asset.
   - **Storage Place**: Select an optional assigned storage location for the asset. Sub-assets don't require this, as the value is specified for the parent asset.
   - **Latitude/Longitude**: (Optional) Enter latitude and longitude values for the asset, say for a fixed asset. Use the tab key to switch from the **Latitude** to the **Longitude** field. Sub-assets don't take these values, as the co-ordinates are specified for the parent asset.

   You can alternatively click **Asset Location** to select the location in the map. Selecting a location automatically populates the latitude and longitude values.

9. Link **Sensor Attributes** for the asset, and for any associated sub-assets, to their respective IoT sensor device attributes.

   A sensor attribute lets you link to an IoT device sensor. For successful linking, the IoT device should be already present in Oracle Internet of Things Cloud Service, and the corresponding device model should have been selected for the Oracle IoT Asset Monitoring Cloud Service application.

   a. Click **Link to Device** ( ![Link to Device](image)) against a sensor attribute.
   b. Select from the list of available devices.

   For successful linking, the IoT device should be already present in Oracle Internet of Things Cloud Service, and the corresponding device model should
have been selected for the Oracle IoT Asset Monitoring Cloud Service application.

You can use Select Filter to filter the available devices, say by device name or serial number.

c. Under Sensor Attribute Binding, confirm that the correct Device Model/URN is displayed.

d. Select the Device Attribute that corresponds to the sensor attribute.

e. Click Select.

The sensor attribute is now linked to your IoT device attribute.

10. If your asset type contains actions, then link the Actions for the asset, and for any associated sub-assets, to their respective IoT sensor device actions.

An asset action lets you trigger device actions from within Oracle IoT Asset Monitoring Cloud Service. For successful linking, the IoT device should be already present in Oracle Internet of Things Cloud Service, and the corresponding device model should have been selected for the Oracle IoT Asset Monitoring Cloud Service application.

a. Click Link to Device (🔗) against an action name.

b. Select from the list of available devices.

For successful linking, the IoT device should be already present in Oracle Internet of Things Cloud Service, and the corresponding device model should have been selected for the Oracle IoT Asset Monitoring Cloud Service application.

You can use Select Filter to filter the available devices, say by device name or serial number.

c. Under Sensor Attribute Binding, confirm that the correct Device Model/URN is displayed.

d. Select the Device Action that corresponds to the asset action.

e. Click Select.

The asset action is now linked to your IoT device action.

11. Specify any custom attributes for the asset, and also for any associated sub-assets.

The custom attributes appear under the CategoryName section. The default category is Uncategorized.

For example, an HVAC asset may include the serial number attribute.

12. Click Save to save the asset along with any associated sub-assets.

A Save Progress displays the status of the asset creation.

13. Click OK after the asset is successfully created.

The status for the newly-created asset changes to Active.

14. Click Back to return to the Assets list.
View Asset Details

View details about an asset, including its state, metadata, images, actions, any current incidents, sensor behavior, and location history.

1. In the Operations Center for your organization, click **Assets**.

2. Use the breadcrumbs to navigate to the appropriate group if your asset appears in a group.

   You can use the **Filter** to search for individual assets based on asset attributes such as name, description, location, and type.

   You can also filter the assets in your view based on custom asset attributes set by your organization. For example, if your assets use attributes such as manufacturer name, model number, and warranty status, you can look for assets using the manufacturer, model, or warranty status value.

3. Click **Show Details** against the appropriate asset row.

   The Digital Twin view for the asset appears. If the asset has sensor attributes, the values of those sensor attributes are displayed. If the asset has associated assets, the sensor values from associated assets also appears.

   The following image shows the digital twin version of a gas compressor asset along with its sensor attributes:

   ![Digital Twin of Gas Compressor Asset](image1)

   The following image shows a truck asset with associated sub-assets, namely, fuel tank, engine, and wheel:

   ![Digital Twin of Truck Asset with Sub-assets](image2)
4. Click a sensor attribute to show the data plot for the sensor attribute.
   You can choose to view live sensor data or select a different time period. The following options are available:
   - Live
   - Last 1 Hour
   - Last 24 Hours
   - Last 7 Days
   - Last 30 Days
   - Custom: Lets you select a custom time period from the calendar.

   The following image shows the live sensor plot for coolant flow data from a gas compressor asset:
If you have defined high and low threshold values for your sensor attribute, you can choose to display these bars against the plot, so that you can examine threshold violations, if any.

You can choose to re-size and drag the highlighter on the timeline to examine a specific portion of the plot more closely.

The following image shows a sensor attribute with upper threshold values and time line highlight:

5. Use the menu bar on the left to navigate to various views:
   - **Search**: Lets you search for other assets, groups, locations and places.
   - **Digital Twin**: Shows the digital twin version of the asset along with its current sensor attribute values along with the sensor attribute values of all associated sub-assets.
   - **Info**: Shows all standard attribute information and actions available for the asset. You can also use the **Info** page to trigger actions for the asset device.
   - **Hierarchy**: Shows the asset hierarchy diagram with the asset and its sub-assets (if any).
   - **Asset Images**: Shows the images associated with the asset.
   - **Location History**: Shows the location of the asset over the past few hours or days. You can choose the time period for which you wish to see the location history.
   - **Incidents**: Shows the list of incident reports generated for the asset. Open incidents are flagged separately. You must have previously configured rules to generate incidents.
   - **Warnings**: Shows the list of warning logs generated for the asset. You must have previously configured rules to generate warnings.
   - **Anomalies**: Shows the anomalies detected for the asset. You must have previously configured anomalies for the asset type.
   - **Predictions**: Shows the predictions for the asset. You must have previously configured predictions for the asset type.
• **Trends**: Shows the trends for the asset sensor attributes and metrics. You must have previously configured trends for the asset type.

• **Any Custom Dashboards**: Dashboards created for an asset type are available for each asset of the corresponding type. The icon shown depends on the icon you chose for the dashboard.

6. Use the breadcrumbs to navigate back to the Operations Center view for the organization or group.

### Edit Asset Details

Edit an asset to modify the asset details and to replace or remove sensor devices.

1. Click **Menu (≡)**, and then click **Design Center**.
2. Select **Asset Inventory** from the **Design Center** sub-menu.
3. Select an asset in the **Assets** list.

   You can use the **Filter** to search for individual assets based on asset attributes such as name, description, location, and type. You can also filter the assets in your view based on custom asset attributes set by your organization. For example, if your assets use attributes such as manufacturer name, model number, and warranty status, you can look for assets using the manufacturer, model, or warranty status value.

4. Click the **Edit (📝)** icon for the asset row.
5. Edit the standard attributes, any sensor attribute associations, any action associations, and any custom attributes, as required.

   For hierarchical assets, you can edit associated sub-assets along with the parent asset after selecting them in the hierarchy.

6. Click **Save**.
7. Click **Back** to return to the **Assets** list.

### Trigger Actions for Assets

Use the asset details page to trigger actions for an asset. You can trigger actions for assets where the asset type includes actions.

1. In the Operations Center for your organization, click **Assets (🔍)**.
2. Use the breadcrumbs to navigate to the appropriate group if your asset appears in a group.
3. Click **Show Details (🔍)** against the appropriate asset row.
4. Click **Info (ⓘ)** on the asset menu bar.
5. In the Actions area, click the desired action.
6. Select or specify values for any action options that appear, and click **OK**.

A notification message appears indicating that the action request is sent.
Duplicate an Asset

Duplicate an asset to quickly copy the settings of an existing asset, such as asset type, assigned place, and asset group, to a new asset.

1. Click Menu (≡), and then click Design Center.
2. Select Asset Inventory from the Design Center sub-menu.
3. Click Duplicate (_duplicate) against the appropriate asset row.
4. Enter a Name for the duplicate asset and click Continue.
5. Modify any standard attributes and custom attributes for the asset, and any associated subassets that are created.
6. Create any required sensor attribute links and action links.
7. Click Save.
8. Click Back to return to the Assets list.

Reserve an Asset

Reserve an asset to flag the asset as being reserved for use.

1. Click Menu (≡), and then click Design Center.
2. Select Asset Inventory from the Design Center sub-menu.
3. Select an asset in the Assets list.
4. Select Reserved.
   A message appears confirming that the asset was successfully checked out.
5. Clear the Reserved check box when you no longer need exclusive use of the asset.
   An application user with privileges, such as the IoT Administrator, can also release an asset reserved by another application user.

Delete an Asset

Delete an asset when it is decommissioned or no longer required.

1. Click Menu (≡), and then click Design Center.
2. Select Asset Inventory from the Design Center sub-menu.
3. Select an asset in the Assets list.
4. Click the Delete (_delete) icon.
5. Click Yes to confirm.

Create and Manage Places

Create places to define the storage and usage locations of your asset.
You can search for your places in the map view and zoom into the available assets. If an asset moves out of its permitted place, Oracle IoT Asset Monitoring Cloud Service can generate an incident that is reported to the operations manager.

For example, an electrocardiogram (EKG) machine is a critical diagnostic tool used by a hospital cardiac unit. The cardiac unit wants to make sure the EKG machine does not move outside of their unit. When an assigned location is defined for the EKG machine, cardiac staff can be alerted when the machine moves outside of the unit.

Create outdoor places by drawing a geofence on the map. For indoor places, you can additionally make use of floor plans and altitude data.

Create a Place Using a Geofence

Create a place by drawing a geofence boundary on the map. Use the place to define the storage or usage location of your asset.

1. Click Menu (≡), and then click Design Center.
2. Select Places from the Design Center sub-menu.
3. Click the Add icon (+) to add a new place.
4. Complete these fields in the Details area:
   - **Name**: Enter a name for the place.
   - **Parent**: If you have an existing place that will contain this new place, select the existing place as the parent.
   - **Description**: Enter an optional description for the place.
   - **Tags**: Enter optional tags for the place. Press the Enter key after entering each tag name.
   - **Minimum Altitude (meters)**: To use an altitude or floor delimiter for the place, specify the minimum altitude in meters.
   - **Maximum Altitude (meters)**: To use an altitude or floor delimiter for the place, specify the maximum altitude in meters.
5. Navigate to the region that you wish to choose on the map.
   - Click the Zoom in (🔍) icon to zoom in to a map location, or click the Zoom out (🔍) icon to zoom out from a map location. Click and hold the left mouse button to drag the map.
   - You can also use the location search icon (🔍) to look for a city, state, zip code, or an existing place name.
6. Click the Draw (✍) icon to draw the geofence for the asset.
7. Click the map area to start drawing a polygon.
8. Drag the mouse to a new location on the map and click to complete the first side of your polygon.
9. Repeat the preceding step to complete the other sides of the polygon. You can draw a polygon with three, four, or more sides.
10. Click on the starting point to complete the polygon.
    Your geofence is now complete.
11. (Optional) Drag the white circles on the edges of the polygon to adjust or fine-tune your geofence.

12. Click Save.

13. Click Back to return to the Places list.

Create a Place with a Floor Plan

For indoor assets, you can choose to add your floor plans on top of the map before you create your geofence boundaries. You can also use the altitude parameter to distinguish between assets on various floors.

1. Click Menu (≡), and then click Design Center.

2. Select Places from the Design Center sub-menu.

3. Click the Add icon (✚) to add a new place.

4. Complete these fields in the Details area:
   - **Name**: Enter a name for the place.
   - **Parent**: If you have an existing place that will contain this new place, select the existing place as the parent.
   - **Description**: Enter an optional description for the place.
   - **Tags**: Enter optional tags for the place. Press the Enter key after entering each tag name.
   - **Minimum Altitude (meters)**: To use an altitude or floor delimiter for the place, specify the minimum altitude in meters.
   - **Maximum Altitude (meters)**: To use an altitude or floor delimiter for the place, specify the maximum altitude in meters.

5. To add a new floor plan:
   a. Click Add Floor Plan.
   b. Browse to the location of the floor plan image and select the image file.
   c. Click Open, and then click Continue.
   d. Drag the two marker icons (📍) to two different locations on the plan and enter the respective Latitude and Longitude values.
   e. Click Show Floor Plan on Map to view the floor plan superimposed on the map.
      Alternatively, click Use Parent Floor Plan if you wish to use the floor plan of the parent place.

6. To draw the geofence for the asset on the map:
   a. Navigate to the floor plan image on the map.
Click the **Zoom in** (↑) icon to zoom in to a map location, or click the **Zoom out** (↓) icon to zoom out from a map location. Click and hold the left mouse button to move the map.

b. Click the **Draw** (▏) icon to draw the geofence in or around the floor plan on the map.

c. Click the map area to start drawing a polygon.

d. Drag the mouse to a new location on the map and click to complete the first side of your polygon.

e. Repeat the preceding step to complete the other sides of the polygon. You can draw a polygon with three, four, or more sides.

f. Click on the starting point to complete the polygon.

Your geofence is now complete.

---

**Note:**

If you wish to redraw the polygon, click the polygon and select **Delete Polygon**.

g. (Optional) Drag the white circles on the edges of the polygon to adjust or fine-tune your geofence.

7. Click **Save**.

8. Click **Back** to return to the **Places** list.

---

**Edit a Place**

Edit a place to edit, add, duplicate, or remove place settings including the place name, description, altitude minimum and maximums, floor plan graphics, or geo-boundaries.

1. Click **Menu** (☰), and then click **Design Center**.

2. Select **Places** from the **Design Center** sub-menu.

3. Select a place in the **Places** list.

4. Click the **Edit** (🛠) icon.

5. Edit the **Name**, **Description** or **Tags** fields.

6. Select one of these options to edit a geo-boundary:

   • Click **Add Floor Plan** to add a new floor plan.

   • Edit the **Min** and **Max** altitude numbers of the **Plan Altitude Range** to edit altitude settings.

   • Click the **Edit** (🛠) icon in the map to add an additional geo-boundary.

   • Click and drag a large circle to move a control point of an existing geo-boundary.

   • Click a small circle to add a new control point between two large circles in an existing geo-boundary.
7. Click **Save**.

## Delete a Place

Delete a place when it is no longer needed.

1. Click **Menu (≡)**, and then click **Design Center**.
2. Select **Places** from the **Design Center** sub-menu.
3. Select a place in the **Places** list.
4. Click the **Delete (🗑)** icon.
5. Click **Yes**.

## Locate Your Assets in the Map View

Use the map view to quickly locate the physical locations of your assets. Your assets can appear independently, or clustered together, depending on your zoom level in the map.

1. Click the **Menu (≡)** icon, and then click **Map**.
2. Use the zoom buttons (+ and -) to zoom in or out in the map view.
3. Click an asset cluster to view the individual assets. Alternatively, zoom in further to separate the clustered assets.

   The following image shows how clicking a cluster with two assets separates the assets:
4. Click an individual asset to view the asset details.

5. (Optional) Click the Filter (🔎) icon to search for individual assets based on asset attributes such as name, description, location, and type.
   
   You can also filter the assets in your view based on custom asset attributes set by your organization. For example, if your assets use attributes such as manufacturer name, model number, and warranty status, you can look for assets using the manufacturer, model, or warranty status value.

6. Click the GeoFences (🌲) icon to show geofences on the map.

Use Third-Party Map Providers

Oracle IoT Asset Monitoring Cloud Service lets you integrate with third-party map providers. You can customize your Map page to use the maps and search facility included by your map provider. When you select a third-party map provider, the built-in maps get replaced with the maps provided by your map provider.

To use a third-party map provider:

1. Click the Menu Icon (☰) and choose Configuration.

2. Select the Settings (⚙️) tab.

3. Under Map Provider, click Use Map Provider and select a map provider.
   
   We currently support HERE Maps, as a third-party map provider.

4. Specify information related to your map provider account.
   
   HERE Maps, for example, requires the user’s Application ID and Application Code.

5. Click Save.

The Map page now starts using maps from your specified map provider in place of the built-in maps. With HERE Maps, you can choose to display the satellite or terrain view as well. Choose from amongst the following options on the map:

- Classic
- Satellite
• Terrain
• Traffic

If you wish to revert to using the built-in Oracle maps, you can choose Oracle Maps from the Configuration page.

Simulate Asset Sensors with the Built-In Simulator

Use simulations to test Oracle IoT Asset Monitoring Cloud Service or to demonstrate its features.

Create asset sensor simulations using the built-in digital twin simulator. Use the simulator to create data patterns for sensors associated with an asset. You can also simulate anomalous data patterns.

The simulator can also simulate device alerts and actions. You can choose to invoke these device actions from an asset page or rule.

Using the simulator, you can test and demonstrate features such as metrics, rules, incidents, and analytics.

Define a Simulation for a Sensor Attribute

Define wave pattern or formula-based sensor values for an asset sensor attribute.

Make sure you have created the asset type and added the sensor attribute that you wish to simulate.

1. From the Create Asset Type or Edit Asset Type page, click the Attributes tab to edit your sensor attribute.
2. Under the Simulation column for your sensor attribute, click Edit Simulation.
3. Choose the simulation Type.
   - You can choose between predefined wave patterns, such as sine curves or square waves, and formula-based simulation values.
4. Specify a Message Interval.
   - The message interval is the frequency with which the simulated sensor sends messages.
5. If you chose Pattern Based for the simulation Type, then select a wave pattern under Pattern.
   - Depending on the wave pattern you select, you need to specify the required parameters for pattern generation.
     • For most wave patterns, you need to specify a maximum (Max) and minimum (Min) value.
     • For regular wave patterns, such as sine waves and square waves, you need to additionally specify the desired Wavelength of the patterns.
     • For a constant wave pattern, specify the constant Value.
6. If you chose Formula for the simulation Type, then use the formula editor to enter a formula.
The formula can use available functions, such as aggregation functions, trigonometric functions, mathematical, string, and time functions. You can also use other sensor attribute values as properties, use various operators such as logical and arithmetic operators, and use constants.

The following example makes use of a logarithmic function to plot the number of parts produced. Note that the function can optionally make use of another sensor attribute in the formula.

If you wish to introduce periodic anomalies in the simulated data, select **Include Anomalies**.

- **Anomaly Frequency**: The periodic time period with which the anomaly occurs. For example, a value of 5 minutes will mean that the anomaly would be attempted every 5 minutes.

- **Likelihood**: You can make the anomaly more random by specifying a likelihood percentage for the anomaly to occur. For example, a value of 80% means that there is an 80% chance of the anomaly occurring every time the periodic time period is reached. If you specify a value of 100%, then the anomaly occurs every time per the anomaly frequency.

- **Type**: Choose the anomaly **Type**. You can choose between predefined wave patterns, such as sine curves or square waves, and formula-based simulation values, as described before.

The following example shows a simulated electric current sensor attribute with simulated anomalies. We have simulated a sinusoidal simulation pattern for the electric current sensor. Every 5 minutes, there is an 80% likelihood of an anomaly occurring that results in the current dropping to 0 for 10 seconds.
The output sensor attribute simulation can be viewed from the asset page of an asset belonging to the same asset type.

The following image shows the resultant output simulation pattern for the electric current sensor attribute. Notice that the Sine waves oscillate between 8 and 12 amperes, as designed. Any two consecutive crests or troughs are 2 minutes apart, as determined by the wavelength. The anomalies occur at 2:42, 2:47, 2:57, and 3:02 pm. An anomaly does not occur at 2:52 pm, as the likelihood of the anomaly occurring is not 100%.

Create Simulated Actions

Define simulated actions to simulate sensor patterns and values when an action is invoked.

1. Click Menu (≡), and then click Design Center.
2. Select Asset Types from the Design Center sub-menu.
3. Select an asset type from the Asset Types list.
   You can also search for an asset type.
4. Click **Actions**.

5. Click **Create Action** (↑).

6. Specify a **Name** for the action.

7. Under Simulations, click **Add** (↑) to add a simulation.

8. Select the **Sensor Attribute** to simulate.

9. Select the **Duration** for which the action simulation lasts.

10. Choose the simulation **Type**.

    You can choose between predefined wave patterns, such as sine curves or square waves, and formula-based simulation values.

11. If you chose **Pattern Based** for the simulation **Type**, then select a wave pattern under **Pattern**.

    Depending on the wave pattern you select, you need to specify the required parameters for pattern generation.

    • For most wave patterns, you need to specify a maximum (**Max**) and minimum (**Min**) value.
    
    • For regular wave patterns, such as sine waves and square waves, you need to additionally specify the desired **Wavelength** of the patterns.
    
    • For a constant wave pattern, specify the constant **Value**.

12. If you chose **Formula** for the simulation **Type**, then use the formula editor to enter a formula.

    The formula can use available functions, such as aggregation functions, trigonometric functions, mathematical, string, and time functions. You can also use other sensor attribute values as properties, use various operators such as logical and arithmetic operators, and use constants.

13. Click **Add** (↑) to add any additional simulations.

    Provide the simulation settings.

14. Select **Execute Items Sequentially** if you want to process the action items sequentially. Alternatively, select **Execute Items in Parallel** if you want to process the action items in parallel.

15. Click **Save** to save the action.

### Simulate an Attribute, Action, or Alert for an Asset

To simulate alerts, sensor attribute patterns, and actions for an asset, make sure that the corresponding alerts, simulated sensor attributes, and simulated actions are defined for the asset type.

- To simulate a sensor attribute for an asset, set the **Data Source** for the sensor attribute to **Simulated** in the Create New Asset or Edit Asset page.

- To enable a predefined simulated action, set the **Data Source** for the sensor attribute to **Simulated** in the Create New Asset or Edit Asset page.

Once enabled, you can trigger the action from the Asset (Digital Twin) page in Operations Center. Click **Asset Controls** to see the actions that you can trigger.
To enable simulated alerts for an asset, set the **Data Source** for the sensor attribute to **Simulated** in the Create New Asset or Edit Asset page.

Once enabled, you can trigger the alert from the Asset (Digital Twin) page in Operations Center. Click **Asset Controls** to see the actions that you can trigger. The following image shows the Actions and Alerts sections on the Assets (Digital Twin) page.
Monitor the Health and Usage of Your Assets

Monitor the health and usage of your assets using metrics or Key Performance Indicators (KPIs), rules, incidents, warnings, alerts, predictions, and anomalies.

Topics:

• Use Asset Metrics or Key Performance Indicators
• Use Rules to Monitor and Maintain Assets
• Use the Incidents Page to Manage Asset Incidents
• Use the Warnings Page to Manage Asset Warnings
• Use Contextual Data Connections
• Use Anomalies to Track Deviations in Asset Behavior
• Use Predictions to Identify Asset Risks

Use Asset Metrics or Key Performance Indicators

Metrics or Key Performance Indicators (KPIs) help you track key asset data for your monitored assets, such as assets connected, assets available, and assets utilization.

The Map view includes default system metrics for your assets. The Map page displays aggregate data for assets currently appearing in the map. You can also create dashboards for individual assets or the organization. Use dashboards to put your most relevant metrics in a single view. See Track Individual and Cumulative Asset Metrics Using Dashboards and Track Asset Metrics in the Map View for details on the metrics that appear on the Dashboard and Map.

You can also create user-defined metrics to track asset data that is relevant to your business processes. So, for example, you can create a metric to track the average hourly temperature reported by a temperature sensor. You can then aggregate this data across your assets on a dashboard or the Map.

User-defined metrics can use sensor values or computed values. For example, you can create a computed metric to show you the average fuel level value across your forklifts. Or you can create a metric to track the count of forklifts that have their fuel levels below a certain threshold. You can create the following user-defined metric types:

• Sensor-Value Based Metric: Directly display an attribute value from one of your sensors.
• Computed Metric: Calculated and aggregated based on the formula that you specify. See Define Your Own Metrics for more information on creating sensor value based and computed metrics.
Define Your Own Metrics

Create a user-defined metric or Key Performance Indicator (KPI) to display asset data that is specific to your operating environment. Metrics are created on asset types.

1. Click Menu (≡), and then click Design Center.
2. Select Asset Types from the Design Center sub-menu.
3. Select an asset type from the Asset Types list.
   You can also search for an asset type.
4. Click Metrics.
5. Click Create Metric +:
6. Enter a Name to identify the new metric.
   The Entity Type is already populated with your chosen asset type. The metric is available for each asset of the chosen asset type. The metric can be aggregated across assets on the Dashboard or the Map view.
7. Specify the calculation details:
   a. Choose an available option under Calculate.
      Metrics can be calculated per entity (asset), or can be calculated globally for an entity type (asset type).
   a. Specify a Calculation Schedule:
      • Live calculates the metric every two minutes.
      • Hourly aggregates the metric for every hour.
      • Daily aggregates the metric for every day.
      • Weekly aggregates the metric for every week.
8. Using the Formula editor, define an expression to calculate the new metric.
   You can build your operation using the elements in the Formula editor, or click Advanced to directly edit the SQL-like expression.
   Start by choosing your aggregation. For example, select Average if you wish to, say, calculate the average hourly temperature for a sensor.

   The following aggregation functions are available:
   • Count
   • Sum
   • Average
   • Min (Minimum)
   • Max (Maximum)

   Next, build your formula by selecting properties, operators, and other functions.
   Sensor attributes are examples of properties that are often used in metrics. For example, an HVAC asset may use various sensor attributes, such as oil viscosity and output temperature.

   The following are some examples of formulae:
• **AVG (FuelLevel):** Returns the average *FuelLevel* over the specified time period.

• **MIN(MaxPressure/2 + MinPressure/2):** First uses the *MaxPressure* and *MinPressure* sensor values to compute the average pressure, and then returns the minimum of this average pressure over the specified time period.

Your expression can contain the following elements:

- Parenthesis: Use parenthesis to group operations and indicate precedence.
- Symbols: You can use arithmetic (+, -, *, /), relational (=, <, >, <=, >=, !=), and logic (AND, OR, LIKE) operators. When you click the Symbol button, the add operator appears in our formula. If you want to select another operator, click the Add icon and select a different operator from the list.
- Numbers, text, and boolean values.
- Properties: A list of system attributes and sensor attributes that you can use to build your own metrics. This list is based on the asset type and function that you selected.

The description for the metric is automatically created based on the properties and operators that you select.

The following example of the **Create Metric** editor shows a computed metric that returns the maximum value of the sum of two sensor attributes every hour.

9. Click **Save** to save the metric.

10. Click **Publish** in the status banner message that appears.

As publishing rebuilds all the existing KPI metrics and publishes them, you may see the existing KPI values disappear momentarily during the republish operation. Oracle recommends that you republish after adding a set of metrics, as opposed to republishing after adding each individual metric.

You can also republish the metrics from the Settings page using the **Republish** button in the Analytics Controls area.

You can now add the metric to a dashboard or to the **Map**.
Track Individual and Cumulative Asset Metrics Using Dashboards

Use dashboards to track individual and cumulative metrics or key performance indicators (KPIs) for your assets. You can create dashboards at the asset level, group level, or the organization level.

Oracle IoT Asset Monitoring Cloud Service dashboards let you track key metrics for your monitored assets, such as assets connected, assets available, and assets utilization.

The following are some examples of system metrics (KPIs) that are available to be added to a dashboard:

- **Assets Connected**: Shows the percentage of assets that are currently connected. An asset counts as connected if the application has heard from the asset sensors in the last one hour.

  For an individual asset dashboard, this means

- **Asset Connectivity**: Used for asset-level dashboards, the metric shows whether the asset is currently connected. An asset counts as connected if the application has heard from the associated sensor in the last one hour.

  You can select a time period to search for the percentage connectivity. For example, you can search for the percentage connectivity in the last 24 hours.

- **Asset Utilization**: When used for group-level or organization-level dashboards, shows the percentage of assets that are currently utilized. An asset counts as utilized if the asset is not present in its assigned storage place.

- **Asset Utilization**: When used for asset-level dashboards, the metric shows whether the asset is currently utilized. An asset counts as utilized if the asset is not present in its assigned storage place.

  You can select a time period to search for the percentage utilization. For example, you can search for the percentage utilization in the last 24 hours.

- **Asset Availability**: When used for group-level or organization-level dashboards, shows the percentage of assets that are currently available. An asset counts as available if there are no open outage incidents reported for the asset.

- **Asset Availability**: When used for asset-level dashboards, the metric shows whether the asset is currently available. An asset counts as available if there are no open outage incidents reported for the asset.

  You can select a time period to search for the percentage availability. For example, you can search for the percentage availability in the last 24 hours.

The system metrics are based on live data. A live metric value is refreshed every two minutes.

Some other examples of system metrics are **Open Maintenances**, **Open Incidents**, **Open Routines**, **Open Outages**, **Open Warnings**, and **Located Assets**.

If you have created user-defined metrics for your environment, you can add these to a dashboard to display the metric values aggregated over all your assets. See **Define Your Own Metrics** for more information on creating user-defined metrics to track asset data relevant to your business processes.
Adding a metric to a dashboard aggregates the metric over all assets of the asset type. For example, you may choose to display the average fuel level across your forklift assets.

The following image displays a custom dashboard in the Operations Center view:

Create a Dashboard at the Organization Level

When you create a dashboard at the organization level, you can add metrics from across your organizational assets to the dashboard. The dashboard appears in your Operations Center menu bar.

To create a dashboard at the organization level:

1. Click Menu (≡), and then click Design Center.
2. Select Organization from the Design Center sub-menu.
3. Click Dashboards.
4. Click Create Dashboard (➕).
5. Select one of the available template or layout.
   You can choose to modify the layout by resizing and repositioning your tiles later, or by adding new tiles.
6. Click Create.
7. Select a Name and Icon for your dashboard.
   Once the dashboard is created, the chosen icon will appear on the Operations Center menu bar.
8. Proceed to adding metrics to the dashboard.
   You can click Preview to preview the dashboard at any time. Click Edit to go back to editing the dashboard.
9. Click Save to save the dashboard.
Create a Dashboard at the Group Level

Create a dashboard at the group level to add metrics relevant to your group assets. The dashboard appears in your Operations Center menu bar when you change the context to the group using the breadcrumbs.

To create a dashboard at the group level:

1. Click Menu (≡), and then click Design Center.
2. Select Groups from the Design Center sub-menu.
3. Select a group from your list of groups.
   
   You can also search for a group.
4. Click Dashboards.
5. Click Create Dashboard (+).
6. Select one of the available template or layout.
   
   You can choose to modify the layout by resizing and repositioning your tiles later, or by adding new tiles.
7. Click Create.
8. Select a Name and Icon for your dashboard.
   
   Once the dashboard is created, the chosen icon will appear on the Operations Center menu bar.
9. Proceed to adding metrics to the dashboard.
   
   You can click Preview to preview the dashboard at any time. Click Edit to go back to editing the dashboard.
10. Click Save to save the dashboard.

Create a Dashboard at the Asset Level

When you create a dashboard at the asset level, you can add metrics relevant to the asset type to the dashboard. The dashboard appears in your Asset Details page menu bar.

To create a dashboard for an asset type:

1. Click Menu (≡), and then click Design Center.
2. Select Asset Types from the Design Center sub-menu.
3. Select the correct asset type and click Dashboards.
4. Click Create Dashboard (+).
5. Select one of the available template or layout.
   
   You can choose to modify the layout by resizing and repositioning your tiles later, or by adding new tiles.
6. Click Create.
7. Select a Name and Icon for your dashboard.
Once the dashboard is created, the chosen icon will appear on the asset view menu bar.

8. Proceed to adding metrics to the dashboard.
   You can click Preview to preview the dashboard at any time. Click Edit to go back to editing the dashboard.

9. Click Save to save the dashboard.

Access the Dashboard Metrics

Switch to a previously-created dashboard for an asset, group, or organization to track the cumulative metrics or key performance indicators (KPIs) for your assets.

- To access a dashboard previously created for the organization, click your dashboard icon on the menu bar in the Operations Center organization view. You can change your view context using the navigation breadcrumbs in the Operation Center.

- To access a dashboard previously created for the group, click your dashboard icon on the menu bar in the Operations Center group view. You can change your view context using the navigation breadcrumbs in the Operation Center.

- To access a dashboard previously created for an asset type, click your dashboard icon on the menu bar in the Asset Details page.

Add a Metric to a Dashboard

Add a metric or Key Performance Indicator (KPI) to your dashboard to display aggregated metric data across applicable assets.

You can add a sensor attribute, system metric, or user-defined metric to your dashboard. Adding a metric to your dashboard aggregates the metric over all assets of the asset type. For example, you may choose to display the average number of open incidents across your assets.

1. Access your organization dashboard, group dashboard, or asset dashboard from the Organization page, Groups page, or Asset Details page respectively.

2. Click Edit (📝) against your dashboard row.

3. (Optional) Click Add Group (+) to add a new group of gadgets.

4. Click Add New Gadget (+) to add a new metric.

5. Under Type, select Metrics or Sensor Attributes.
   If you are adding a user-defined metric, you must have created the metric before adding it to the Dashboard. See Define Your Own Metrics for more information on creating user-defined metrics.

6. Select the corresponding Metric or Sensor Attribute.

7. Select the Aggregation for your metric.
   This field is not available for asset dashboards, as these display data for individual assets.
   The aggregation is performed across all assets of the metric asset type.
For example, you may want to calculate the average of the temperature metric across your temperature sensors. Alternatively, you may want to display the maximum temperature amongst all your temperature sensors.

8. Select a **Label** for your Dashboard metric. The default label uses the name of the metric that you selected.

   The **Label** can be different from the metric name. For example, if you are aggregating the maximum temperature across assets, you may use *Maximum Temperature* to highlight this fact.

9. Select an **Icon** for your dashboard metric.

   The dashboard icon you select is used on the menu bar in the Operations Center or Asset Details page.

10. (Optional) Specify an optional **Unit** to display against the metric value.

   For example, if the metric measures the pressure in pounds per square inch, you may want to use *psi*.

11. Select a **Color** for your Dashboard metric.

12. Select an appropriate display type for your metric.

13. Click **OK** to add the metric to the dashboard.

14. Click **Preview** to preview your dashboard.

15. Click **Save** to save the dashboard changes.

Edit a Metric on the Dashboard

Edit a metric on the dashboard to change its aggregation settings, label, or appearance.

1. Access your organization dashboard, group dashboard, or asset dashboard from the Organization page, Groups page, or Asset Details page respectively.

2. Click **Edit** against your dashboard row.

3. Click the **Edit** icon for the metric you want to edit.

4. Edit the metric settings like aggregation, label, unit, color, and appearance.

   Aggregation is not available for asset dashboards, as these display data for individual assets.

   The aggregation is performed across all assets of the metric asset type.

   For example, you may want to calculate the average of the temperature metric across your temperature sensors. Alternatively, you may want to display the maximum temperature amongst all your temperature sensors.

   The **Label** can be different from the metric name. For example, if you are aggregating the maximum temperature across assets, you may use *Maximum Temperature* to highlight this fact.

5. Click **OK**.

6. Click **Save** to save your dashboard changes.
Change the Location of a Metric on a Dashboard

Change the location of a metric, so that the metrics appear in the order you require.

1. Access your organization dashboard, group dashboard, or asset dashboard from the Organization page, Groups page, or Asset Details page respectively.

2. Click **Edit (-pencil)** against your dashboard row.

3. Click and drag a metric, or metric group, using the Handle (arrow), to a new location on the dashboard.

4. Click **Save** to save your dashboard changes.

Remove a Metric from the Dashboard

Remove a metric from the dashboard when it is no longer required.

1. Access your organization dashboard, group dashboard, or asset dashboard from the Organization page, Groups page, or Asset Details page respectively.

2. Click **Edit (-pencil)** against your dashboard row.

3. Click the **Delete (trash can)** icon for the metric or metric group that you want to remove from your dashboard.

4. Click **Save** to save your dashboard changes.

Track Asset Metrics in the Map View

Use the KPI ribbon to track cumulative metrics or key performance indicators (KPIs) for assets appearing in the Map view. You can search for a place or zoom into a location in the map to see cumulative statistics for the location.

The KPI ribbon in the Oracle IoT Asset Monitoring Cloud Service Map lets you track key metrics for your monitored assets, such as located assets, assets connected, assets available, assets utilization, and open incidents.

The following system metrics or KPIs appear in the KPI ribbon, by default:

- **Located Assets**: Shows the number of assets located in the current view. This number may increase, as you zoom out to include more places. The number may decrease, as you zoom into the assets belonging to a specific place.

- **Assets Connected**: Shows the percentage of connected assets in the current view. An asset counts as connected if the application has heard from the asset sensors in the last one hour.

- **Asset Utilization**: Shows the percentage of utilized assets in the current view. An asset counts as utilized if the asset is not present in its assigned storage place.

- **Asset Availability**: Shows the percentage of available assets in the current view. An asset counts as available if there are no open outage incidents reported for the asset.

- **Open Incidents**: Shows the number of open, or unresolved, incidents for assets in the current view. Incidents help flag issues, such as outages, for the maintenance staff to work on.
The system metrics are based on live data. A live metric value is refreshed every two minutes.

If you have created user-defined metrics for your environment, you can add these to the KPI ribbon to display the metric values aggregated over the assets that appear in the map. See Define Your Own Metrics for more information on creating user-defined metrics to track asset data relevant to your business processes.

The KPI ribbon in the map view can show a maximum of five metrics. If you wish to add a user-defined metric, you will need to remove a pre-existing metric and add the new metric.

Access the Map View Metrics

Switch to the Map view to track the metrics or key performance indicators (KPIs) for the assets located in the map.

In the Operations Center, click Map in the menu bar. The system metrics, and any added user-defined metrics, appear in the KPI ribbon below the map.

Add a Metric to the Map View

Add a metric or Key Performance Indicator (KPI) to the Dashboard to display aggregated metric data across applicable assets.

1. Click the Menu icon, and then click Map.
2. Click the Configure Metrics icon in the KPI ribbon below the map.
3. Click the Add Metric icon.
   If you already have five KPIs in the KPI ribbon, you would need to remove a KPI before you can add a new one on the KPI ribbon.
4. Under Type, select Metrics or Sensor Attributes.
   If you are adding a user-defined metric, you must have created the metric before adding it to the Dashboard. See Define Your Own Metrics for more information on creating user-defined metrics.
5. Select the corresponding Metric or Sensor Attribute.
6. Select the Aggregation for your metric.
   The aggregation is performed across all assets of the metric asset type.
   For example, you may want to calculate the average of the temperature metric across your temperature sensors. Alternatively, you may want to display the maximum temperature amongst all your temperature sensors.
7. Select a Label for your KPI ribbon metric. The default label uses the name of the metric that you selected.
   The Label can be different from the metric name. For example, if you are aggregating the maximum temperature across assets, you may use Maximum Temperature to highlight this fact.
8. (Optional) Specify an optional Unit to display against the metric value.
For example, if the metric measures the pressure in pounds per square inch, you may want to use psi.

9. Select a Color for your KPI ribbon metric.
10. Select an appropriate display type for your metric.
11. Click OK to add the metric to the KPI ribbon.
12. Click Save to save the KPI ribbon changes.

Edit a Metric in the Map View

Edit a metric that appears in the KPI ribbon to change its aggregation settings, label, or appearance.

1. Click the Menu (☰) icon, and then click Map.
2. Click the Configure Metrics (✎) icon.
3. Click the Edit (✍) icon for the metric you want to edit.
4. Edit the available metric settings like aggregation, label, unit, color, and appearance.

The aggregation is performed across all visible assets of the metric asset type. For example, you may want to calculate the average of the temperature metric across temperature sensors visible in the map. Alternatively, you may want to display the maximum temperature amongst the temperature sensors visible in the map.

The Label can be different from the metric name. For example, if you are aggregating the maximum temperature across assets, you may use Maximum Temperature to highlight this fact.
5. Click OK.
6. Click Save to save your KPI ribbon changes.

Change the Location of a Metric in the KPI Ribbon

Change the location of a metric or Key Performance Indicator (KPI) in the KPI ribbon, so the metrics appear in the order you require.

1. Click the Menu (☰) icon, and then click Map.
2. Click the Configure Metrics (✎) icon in the KPI ribbon below the map.
3. Click and drag a KPI, using the Handle ( $$$ ), to a new location on the ribbon.
4. Click Save.

Remove a Metric from the Map View

Remove a metric or Key Performance Indicator (KPI) from the map view when it is no longer required, or when you want to make space for a new metric.

1. Click the Menu (☰) icon, and then click Map.
2. Click the Configure Metrics (✎) icon in the KPI ribbon below the map.
3. Click the **Delete** (🗑️) icon for the metric that you want to remove from the map view.

4. Click **Save** to save your KPI ribbon changes.

---

**Use Statistical Trends for Your Asset Sensor Attributes and Metrics**

You can study statistical trends for your asset sensor attributes and metrics using one or more Nelson Rules. These may help you analyze the consistency and predictability of your attribute values.

Trends use a set of Nelson Rules on your sensor attribute or metric values to be analyzed. For example, you may wish to analyze the trends for the pressure, temperature, or vibration sensor values of your asset. You can choose one or more of the following Nelson Rules that are relevant for your sensor attribute or metric:

- Nelson Rule 1: One point is more than three standard deviations from the mean.
- Nelson Rule 2: Nine, or more, points in a row are on the same side of the mean.
- Nelson Rule 3: Six, or more, points in a row are continuously increasing or decreasing.
- Nelson Rule 4: Fourteen or more points in a row alternate in direction, increasing then decreasing.
- Nelson Rule 5: Two or three points in a row are more than two standard deviations from the mean in the same direction.
- Nelson Rule 6: Four, or five, out of five points in a row are more than one standard deviation from the mean in the same direction.
- Nelson Rule 7: Fifteen points in a row are all within one standard deviation of the mean on either side of the mean.
- Nelson Rule 8: Eight points in a row exist, but none within one standard deviation of the mean, and the points are in both directions from the mean.

---

**Define a Trend**

You need to define a trend before the trend model can be created for the sensor attribute or metric that you wish to monitor.

1. Click **Menu (≡)**, and then click **Design Center**.
2. Select **Asset Types** from the **Design Center** sub-menu.
3. Select an asset type from the **Asset Types** list.
   - You can also search for an asset type.
4. Click **Trends**.
5. Click the **Create Trend** (➕) icon.
6. Enter a name for the trend in the **Name** field.
7. (Optional) Specify an optional description text for the trend.
8. Under Data Analysis, verify that the correct **Asset Type** appears.
This is the asset type that you previously selected.

9. Select the **Attribute** to monitor.

Select from the list of asset sensor attributes and any metrics that you have defined for the asset type.

10. Select a value for **Detection**:  
    - **Automatic**: Automatically chooses trends corresponding to all available Nelson Rules.  
    - **Select Specific Trends**: Lets you select one or more individual Nelson Rules that are relevant for your machine attribute.

11. If you chose **Select Specific Trends** in the previous step, then select one or more Nelson Rules for your Trends.

The description and graphical depiction of each rule are shown for you.

12. Click **Save** to save the trend.

You may need to **Publish** the trend if prompted. The system now starts building a trend model for the new trend. Trends are shown in the Operations Center and Asset pages after the trend model is ready.

**View Trends**

Trends are available from the Operations Center and Asset Details page. You must have previously defined trends for your asset type.

Click **Trends** in the **Operations Center** toolbar. Use the breadcrumbs to navigate to a group, subgroup, or asset. You can choose between the following time periods:

- Last 1 Hour  
- Last 24 Hours  
- Last 7 Days
• Last 30 Days

To view trends for a single asset, click **Trends** in the Asset Details page toolbar.

### Use Rules to Monitor and Maintain Assets

Use rules to monitor and maintain your assets. Rules set conditions on asset sensor or KPI values. When a rule condition is met, the associated alert, warning, or incident is triggered. You can also use rules to trigger asset actions.

You can apply the rule to specific assets, or to all assets of an asset type. The default scope of the rule is all assets of the asset type in the organization, but you can selectively apply the rule to select asset group hierarchies.

Asset monitoring rules can be broadly categorized into the following categories:

- **Location-Based Rules**: Location rules are based on location conditions. Use location rules to track when an asset enters or leaves a place. For example, you can track when an asset leaves its assigned place, and use the rule to generate an incident.

- **Threshold-Based Rules**: Threshold rules are based on sensor or KPI (key performance indicator) values. Use threshold rules to track sensor values, such as fuel levels and temperature values. For example, you can configure a threshold rule to raise a warning when the fuel levels of an asset go below a threshold value.

  You can configure a threshold rule to trigger an asset action based on the sensor value. For example, you may want to power off an overheating device automatically.

  Threshold rules also let you track KPI values, such as the number of open incidents. For example, you may want to trigger a warning if the number of open outage incidents cross a threshold number.

- **Alert Rules**: Use alert rules to respond to device alert conditions. If your sensor device supports alerts, then you can use alert rules to configure alert responses. For example, an alert rule can trigger a device action based on an alert.

Use rules to trigger the following:

- **Incidents**: Use incidents to report issues and work with the maintenance staff for resolutions.

  The number of open incidents prominently appears on the KPI ribbon in the Map view. Open incidents against an asset are also flagged under the Asset Details page for an asset. You can access all reported incidents from the Incidents page.

  Note that the Asset Availability KPI number goes down when there are assets with open outage incidents against them.

- **Warnings**: Use warnings to create a log of issues that don't require your immediate attention.

  You can access all reported warnings from the Warnings page. Warnings against individual assets can be accessed in the Asset Details page.

- **Alerts**: Use alerts to pass device-related alerts to Oracle Internet of Things Cloud Service. These alerts can in turn be passed on to integrated applications.
Alerts generated by Oracle IoT Asset Monitoring Cloud Service appear in the Oracle Internet of Things Cloud Service management console.

- **Asset Actions**: If your asset type includes asset actions supported by your device model, then you can use to trigger these asset actions. For example, you may choose to trigger the *Power Off* action for a device if the device is overheating.

## Create a Location Rule

Create a location rule to generate an incident, alert, action, or warning when an asset enters or exits a location.

1. Click **Menu (≡)**, and then click **Design Center**.
2. Select **Asset Types** from the **Design Center** sub-menu.
3. Select an asset type from the **Asset Types** list.
   You can also search for an asset type.
4. Click **Rules**.
5. Click the **Create New Rule (➕)** icon.
6. Enter a name for the rule in the **Name** field.
7. Select an option in the **Apply To** list:
   - To assign the rule to the selected asset type, leave the default option set to **All Assets of Type: AssetType**.
   - To assign the rule to specific assets, select **Specific Assets of Type: AssetType** and then select one or more assets.
8. If you selected **All Assets of Type: AssetType** in the preceding step, then you can optionally choose to change the **Scope** of the rule to a specific asset group or asset group hierarchy.
   a. Under **Scope**, select **Specific Groups**, and then select the asset group to which you wish to apply the rule.
   b. If the group also has subgroups, and you wish to apply the rule to the whole group hierarchy, then select **Include Subgroups**.
9. In the **Condition** area, define the location condition:
   a. Select **Location** from the drop-down list.
      A second drop-down list appears.
   b. Select **Entered** or **Exited** in the second drop-down list:
      - If you want to generate an incident, alert, action, or warning when an asset enters a geo-boundary, select **Entered**.
      - If you want to generate an incident, alert, action, or warning when an asset exits a geo-boundary, select **Exited**.
      A third drop-down list appears.
   c. Select the location in the third list.
10. (Optional) Add additional location conditions.
11. (Optional) Add additional alert conditions.
See Create an Alert Rule for more information on alert conditions.

12. (Optional) Add additional threshold conditions for asset attribute values.

See Create a Threshold Rule for more information on creating threshold conditions.

13. In the Fulfillment section, select an option for the Fulfill when field:

- **All Conditions Apply**: Select this option to generate an incident, alert, action, or warning when all the conditions are met.
- **Any Conditions Apply**: Select this option to generate an incident, alert, action, or warning when any of the conditions are met.

14. In the Fulfillment section, select an option for the Generate field:

- **Incident**: Select to receive an incident notification when the rule conditions are met.
  
  Use incidents to report issues and work with the maintenance staff for resolutions.

- **Alert**: Select to generate an alert message when the rule conditions are met.
  
  Use alerts to pass device-related alerts to Oracle Internet of Things Cloud Service. These alerts can in turn be passed on to integrated applications.

- **Warning**: Select to generate a warning message when the rule conditions are met.
  
  Use warnings to create a log of issues that don’t require your immediate attention.

- **Action**: Select to trigger an asset action when the rule conditions are met.
  
  If your asset type includes asset actions, then you can use rules to trigger these asset actions.

15. Complete the mandatory and optional fields that appear, depending on your choice in the preceding step:

- **Summary**: Enter a summary of the incident, alert, or warning.

- **Type**: Specify the incident or warning type. For incidents, you can select between Outage, Maintenance, and Routine.

- **Priority**: (Optional) Select an incident priority.

- **Tags**: (Optional) Specify string tags that you can use to search the logs.

- **Description**: (Optional) Enter a detailed description of the incident or warning.

- **Severity**: (Optional) Select the severity of the alert message.

- **Suppression**: (Optional) Specify a wait time, in minutes, after which a fresh alert or warning is generated for an unresolved issue.

- **Level**: (Optional) Select the severity of the warning.

- **Action**: Select the asset action to trigger. Also specify or select the values for any action attributes that appear.

- **Subscribers**: Under Notification Subscription, you can add one or more subscriber groups to receive notifications when alerts or warnings are triggered by the rule. See Use SMS Notifications for Asset Incidents and Warnings for more information on configuring notifications.
16. Click **Save**.

17. Click **Back** to return to the **Rules** list.

**Create a Threshold Rule**

Create a threshold rule to generate an incident, alert, action, or warning when an asset type or a specific asset meets or exceeds a set threshold.

1. Click **Menu (☰)**, and then click **Design Center**.

2. Select **Asset Types** from the **Design Center** sub-menu.

3. Select an asset type from the **Asset Types** list.

   You can also search for an asset type.

4. Click **Rules**.

5. Click the **Create New Rule (✚)** icon.

6. Enter a name for the rule in the **Name** field.

7. Select an option in the **Apply To** list:

   - To assign the rule to the selected asset type, leave the default option set to **All Assets of Type: AssetType**.
   - To assign the rule to specific assets, select **Specific Assets of Type: AssetType** and then select one or more assets.

8. If you selected **All Assets of Type: AssetType** in the preceding step, then you can optionally choose to change the **Scope** of the rule to a specific asset group or asset group hierarchy.

   a. Under **Scope**, select **Specific Groups**, and then select the asset group to which you wish to apply the rule.

   b. If the group also has subgroups, and you wish to apply the rule to the whole group hierarchy, then select **Include Subgroups**.

9. In the **Condition** section, define the threshold condition:

   a. Select an asset attribute in the drop-down list.

      For example, a temperature sensor asset specifies attributes like **maxTemp** and **minTemp**.

      You can also select Key Performance Indicator (KPI) attributes for your conditions. These attribute names start with **metric/**. For example, the **metric/sys_openIncidents** KPI attribute keeps track of the number of open incidents.

      A second drop-down list appears.

   b. Select a threshold condition for the attribute in the second drop-down list.

      For example, a numeric attribute specifies conditions like **Greater Than** and **Less Than**.

      A third field appears.

   c. Specify an attribute value in the third field.

      For example, a complete condition may look like: **maxTemp Greater Than 50**.
A complete condition that uses a KPI metric may look like:\n\texttt{metric/sys\_openIncidents\ Greater\ Than\ 5}.

10. (Optional) Add additional threshold conditions for attribute values.

11. (Optional) Add additional alert and location conditions.

   See \textit{Create an Alert Rule} for more information on alert conditions.

   See \textit{Create a Location Rule} for more information on location conditions.

12. In the Fulfillment section, select an option for the \textbf{Fulfill when} field:

   - \textbf{All Conditions Apply}: Select this option to generate an incident, alert, action, or warning when all the conditions are met.

   - \textbf{Any Conditions Apply}: Select this option to generate an incident, alert, action, or warning when any of the conditions are met.

13. In the Fulfillment section, select an option for the \textbf{Generate} field:

   - \textbf{Incident}: Select to receive an incident notification when the rule conditions are met.

     Use incidents to report issues and work with the maintenance staff for resolutions.

   - \textbf{Alert}: Select to generate an alert message when the rule conditions are met.

     Use alerts to pass device-related alerts to Oracle Internet of Things Cloud Service. These alerts can in turn be passed on to integrated applications.

   - \textbf{Warning}: Select to generate a warning message when the rule conditions are met.

     Use warnings to create a log of issues that don't require your immediate attention.

   - \textbf{Action}: Select to trigger an asset action when the rule conditions are met.

     If your asset type includes asset actions supported by your device model, then you can use rules to trigger these asset actions.

14. Complete the mandatory and optional fields that appear, depending on your choice in the preceding step:

   - \textbf{Summary}: Enter a summary of the incident, alert, or warning.

   - \textbf{Type}: Specify the incident or warning type. For incidents, you can select between \textit{Outage, Maintenance,} and \textit{Routine}.

   - \textbf{Priority}: (Optional) Select an incident priority.

   - \textbf{Tags}: (Optional) Specify string tags that you can use to search the logs.

   - \textbf{Description}: (Optional) Enter a detailed description of the incident or warning.

   - \textbf{Severity}: (Optional) Select the severity of the alert message.

   - \textbf{Suppression}: (Optional) Specify a wait time, in minutes, after which a fresh alert or warning is generated for an unresolved issue.

   - \textbf{Level}: (Optional) Select the severity of the warning.

   - \textbf{Action}: Select the asset action to trigger. Also specify or select the values for any action attributes that appear.
Subscribers: Under Notification Subscription, you can add one or more subscriber groups to receive notifications when alerts or warnings are triggered by the rule. See Use SMS Notifications for Asset Incidents and Warnings for more information on configuring notifications.

15. Click Save.
16. Click Back to return to the Rules list.

Create an Anomaly Rule

Create an anomaly rule to generate an incident, alert, action, or warning when an anomaly occurs for an asset.

To create anomaly rules, you must have the anomalies defined. See Use Anomalies to Track Deviations in Asset Behavior for more information on anomalies.

1. Click Menu (≡), and then click Design Center.
2. Select Asset Types from the Design Center sub-menu.
3. Select an asset type from the Asset Types list.
   You can also search for an asset type.
4. Click Rules.
5. Click the Create New Rule (➕) icon.
6. Enter a name for the rule in the Name field.
7. Select an option in the Apply To list:
   • To assign the rule to the selected asset type, leave the default option set to All Assets of Type: AssetType.
   • To assign the rule to specific assets, select Specific Assets of Type: AssetType and then select one or more assets.
8. If you selected All Assets of Type: AssetType in the preceding step, then you can optionally choose to change the Scope of the rule to a specific asset group or asset group hierarchy.
   a. Under Scope, select Specific Groups, and then select the asset group to which you wish to apply the rule.
   b. If the group also has subgroups, and you wish to apply the rule to the whole group hierarchy, then select Include Subgroups.
9. In the Condition section, select the anomaly condition:
   a. Select the anomaly name from the list.
      A second drop-down list appears.
   b. Select one of the following:
      • Select Occurred to trigger the rule when the anomaly occurs.
      • Select Occurred in Last to specify a time duration. The rule gets triggered if the anomaly occurred in the specified time duration.
      Enter the number of seconds, minutes, hours, days, months, or years, and choose the appropriate time unit in the drop-down list that appears.
10. (Optional) Add additional anomaly or alert conditions.
See Create an Alert Rule for more information on alert conditions.

11. (Optional) Add additional location conditions.
    See Create a Location Rule for more information on location conditions.

12. (Optional) Add additional threshold conditions for asset attribute values.
    See Create a Threshold Rule for more information on creating threshold conditions.

13. In the Fulfillment section, select an option for the Fulfill when field:
    • All Conditions Apply: Select this option to generate an incident, alert, action, or warning when all the conditions are met.
    • Any Conditions Apply: Select this option to generate an incident, alert, action, or warning when any of the conditions are met.

14. In the Fulfillment section, select an option for the Generate field:
    • Incident: Select to receive an incident notification when the rule conditions are met.
      Use incidents to report issues and work with the maintenance staff for resolutions.
    • Alert: Select to generate an alert message when the rule conditions are met.
      Use alerts to pass device-related alerts to Oracle Internet of Things Cloud Service. These alerts can in turn be passed on to integrated applications.
    • Warning: Select to generate a warning message when the rule conditions are met.
      Use warnings to create a log of issues that don’t require your immediate attention.
    • Action: Select to trigger an asset action when the rule conditions are met.
      If your asset type includes asset actions supported by your device model, then you can use rules to trigger these asset actions.

15. Complete the mandatory and optional fields that appear, depending on your choice in the preceding step:
    • Summary: Enter a summary of the incident, alert, or warning.
    • Type: Specify the incident or warning type. For incidents, you can select between Outage, Maintenance, and Routine.
    • Priority: (Optional) Select an incident priority.
    • Tags: (Optional) Specify string tags that you can use to search the logs.
    • Description: (Optional) Enter a detailed description of the incident or warning.
    • Severity: (Optional) Select the severity of the alert message.
    • Suppression: (Optional) Specify a wait time, in minutes, after which a fresh alert or warning is generated for an unresolved issue.
    • Level: (Optional) Select the severity of the warning.
    • Action: Select the asset action to trigger. Also specify or select the values for any action attributes that appear.
    • Subscribers: Under Notification Subscription, you can add one or more subscriber groups to receive notifications when alerts or warnings are
triggered by the rule. See Use SMS Notifications for Asset Incidents and Warnings for more information on configuring notifications.

16. Click Save.
17. Click Back to return to the Rules list.

Create a Prediction Based Rule

Create a prediction based rule to generate an incident, alert, action, or warning based on the prediction value.

To create a prediction based rule, you must have the prediction defined. See Use Predictions to Identify Asset Risks for more information on predictions.

1. Click Menu (≡), and then click Design Center.
2. Select Asset Types from the Design Center sub-menu.
3. Select an asset type from the Asset Types list.
   You can also search for an asset type.
4. Click Rules.
5. Click the Create New Rule (✚) icon.
6. Enter a name for the rule in the Name field.
7. Select an option in the Apply To list:
   • To assign the rule to the selected asset type, leave the default option set to All Assets of Type: AssetType.
   • To assign the rule to specific assets, select Specific Assets of Type: AssetType and then select one or more assets.
8. If you selected All Assets of Type: AssetType in the preceding step, then you can optionally choose to change the Scope of the rule to a specific asset group or asset group hierarchy.
   a. Under Scope, select Specific Groups, and then select the asset group to which you wish to apply the rule.
   b. If the group also has subgroups, and you wish to apply the rule to the whole group hierarchy, then select Include Subgroups.
9. In the Condition section, select the prediction condition:
   a. Select the prediction name from the list.
   b. Select a condition and specify the values.
      You can select an exact value (Equals) or specify a range of values (Range). You can also choose to specify just the minimum (Start) or maximum (End) value of the prediction.
   c. Optionally specify an accuracy percentage for the prediction value.
10. (Optional) Add additional prediction or alert conditions.
    See Create an Alert Rule for more information on alert conditions.
11. (Optional) Add additional location conditions.
    See Create a Location Rule for more information on location conditions.
12. (Optional) Add additional threshold conditions for asset attribute values.

See Create a Threshold Rule for more information on creating threshold conditions.

13. In the Fulfillment section, select an option for the Fulfill when field:

- **All Conditions Apply**: Select this option to generate an incident, alert, action, or warning when all the conditions are met.
- **Any Conditions Apply**: Select this option to generate an incident, alert, action, or warning when any of the conditions are met.

14. In the Fulfillment section, select an option for the Generate field:

- **Incident**: Select to receive an incident notification when the rule conditions are met.
  
  Use incidents to report issues and work with the maintenance staff for resolutions.
- **Alert**: Select to generate an alert message when the rule conditions are met.
  
  Use alerts to pass device-related alerts to Oracle Internet of Things Cloud Service. These alerts can in turn be passed on to integrated applications.
- **Warning**: Select to generate a warning message when the rule conditions are met.
  
  Use warnings to create a log of issues that don't require your immediate attention.
- **Action**: Select to trigger an asset action when the rule conditions are met.
  
  If your asset type includes asset actions supported by your device model, then you can use rules to trigger these asset actions.

15. Complete the mandatory and optional fields that appear, depending on your choice in the preceding step:

- **Summary**: Enter a summary of the incident, alert, or warning.
- **Type**: Specify the incident or warning type. For incidents, you can select between Outage, Maintenance, and Routine.
- **Priority**: (Optional) Select an incident priority.
- **Tags**: (Optional) Specify string tags that you can use to search the logs.
- **Description**: (Optional) Enter a detailed description of the incident or warning.
- **Severity**: (Optional) Select the severity of the alert message.
- **Suppression**: (Optional) Specify a wait time, in minutes, after which a fresh alert or warning is generated for an unresolved issue.
- **Level**: (Optional) Select the severity of the warning.
- **Action**: Select the asset action to trigger. Also specify or select the values for any action attributes that appear.
- **Subscribers**: Under Notification Subscription, you can add one or more subscriber groups to receive notifications when alerts or warnings are triggered by the rule. See Use SMS Notifications for Asset Incidents and Warnings for more information on configuring notifications.

16. Click Save.
17. Click Back to return to the Rules list.

Create an Alert Rule

Create an alert rule to generate an incident, alert, action, or warning when an asset type or a specific asset meets or exceeds the requirements set for an alert condition.

1. Click Menu (≡), and then click Design Center.
2. Select Asset Types from the Design Center sub-menu.
3. Select an asset type from the Asset Types list.
   You can also search for an asset type.
4. Click Rules.
5. Click the Create New Rule (➕) icon.
6. Enter a name for the rule in the Name field.
7. Select an option in the Apply To list:
   • To assign the rule to the selected asset type, leave the default option set to All Assets of Type: AssetType.
   • To assign the rule to specific assets, select Specific Assets of Type: AssetType and then select one or more assets.
8. If you selected All Assets of Type: AssetType in the preceding step, then you can optionally choose to change the Scope of the rule to a specific asset group or asset group hierarchy.
   a. Under Scope, select Specific Groups, and then select the asset group to which you wish to apply the rule.
   b. If the group also has subgroups, and you wish to apply the rule to the whole group hierarchy, then select Include Subgroups.
9. In the Condition section, define the alert condition:
   a. Select Alert from the drop-down list.
      Your asset device model determines the alerts and message formats that are available.
      A second drop-down list appears.
   b. Select the message format in the second list.
      For example, a temperature sensor asset may define the following alert message format: tooColdAlert - urn:com:oracle:iot:device:temperature_sensor:too_cold.
10. (Optional) Add additional alert conditions.
11. (Optional) Add additional location conditions.
    See Create a Location Rule for more information on location conditions.
12. (Optional) Add additional threshold conditions for asset attribute values.
    See Create a Threshold Rule for more information on creating threshold conditions.
13. In the Fulfillment section, select an option for the Fulfill when field:
- **All Conditions Apply**: Select this option to generate an incident, alert, action, or warning when all the conditions are met.
- **Any Conditions Apply**: Select this option to generate an incident, alert, action, or warning when any of the conditions are met.

14. In the Fulfillment section, select an option for the **Generate** field:
- **Incident**: Select to receive an incident notification when the rule conditions are met.
  Use incidents to report issues and work with the maintenance staff for resolutions.
- **Alert**: Select to generate an alert message when the rule conditions are met.
  Use alerts to pass device-related alerts to Oracle Internet of Things Cloud Service. These alerts can in turn be passed on to integrated applications.
- **Warning**: Select to generate a warning message when the rule conditions are met.
  Use warnings to create a log of issues that don't require your immediate attention.
- **Action**: Select to trigger an asset action when the rule conditions are met.
  If your asset type includes asset actions supported by your device model, then you can use rules to trigger these asset actions.

15. Complete the mandatory and optional fields that appear, depending on your choice in the preceding step:
- **Summary**: Enter a summary of the incident, alert, or warning.
- **Type**: Specify the incident or warning type. For incidents, you can select between **Outage**, **Maintenance**, and **Routine**.
- **Priority**: (Optional) Select an incident priority.
- **Tags**: (Optional) Specify string tags that you can use to search the logs.
- **Description**: (Optional) Enter a detailed description of the incident or warning.
- **Severity**: (Optional) Select the severity of the alert message.
- **Suppression**: (Optional) Specify a wait time, in minutes, after which a fresh alert or warning is generated for an unresolved issue.
- **Level**: (Optional) Select the severity of the warning.
- **Action**: Select the asset action to trigger. Also specify or select the values for any action attributes that appear.
- **Subscribers**: Under Notification Subscription, you can add one or more subscriber groups to receive notifications when alerts or warnings are triggered by the rule. See **Use SMS Notifications for Asset Incidents and Warnings** for more information on configuring notifications.

16. Click **Save**.

17. Click **Back** to return to the **Rules** list.
Edit a Rule

Edit a rule to change the assets the rule applies to and the rules for generating the incident or alert report.

1. Click Menu (Ξ), and then click Design Center.
2. Select Asset Types from the Design Center sub-menu.
3. Select an asset type from the Asset Types list.
   You can also search for an asset type.
4. Click Rules.
5. Select a rule in the Rules list.
6. Click the Edit (✏) icon.
7. Edit the rule name.
8. Edit the options in the Apply To area.
9. Edit the settings in the Condition area.
10. Edit the settings in the Fulfillment area.
11. Click Save.
12. Click Back to return to the Rules list.

Duplicate a Rule

Duplicate a rule to quickly copy the settings of an existing rule to a new rule.

1. Click Menu (Ξ), and then click Design Center.
2. Select Asset Types from the Design Center sub-menu.
3. Select an asset type from the Asset Types list.
   You can also search for an asset type.
4. Click Rules.
5. Select a rule in the Rules list.
6. Click the Duplicate (▶) icon.
7. Enter a name for the rule in the Name field and then modify the other rule settings including the apply to, condition, type, create incident, and create alert values.
8. Click Save.

Activate or Deactivate a Rule

Activate an existing rule to generate an incident or alert report when the incident rule criteria are met. Deactivate a rule to stop incident or alert report generation.

1. Click Menu (Ξ), and then click Design Center.
2. Select Asset Types from the Design Center sub-menu.
3. Select an asset type from the Asset Types list.
You can also search for an asset type.

4. Click **Rules**.

5. Select a rule in the **Rules** list.

6. Select one of these options:
   a. To deactivate a rule, clear the **Enabled** checkbox.
   b. To enable a rule, select the **Enabled** checkbox.

Delete a Rule

Delete a rule when it is no longer required.

1. Click **Menu** (≡), and then click **Design Center**.

2. Select **Asset Types** from the **Design Center** sub-menu.

3. Select an asset type from the **Asset Types** list.
   You can also search for an asset type.

4. Click **Rules**.

5. Select a rule in the **Rules** list.

6. Click the **Delete** (-trash) icon.

7. Click **Yes**.

Use the Incidents Page to Manage Asset Incidents

View and manage incidents from the Incidents page. You can also change the status of an incident from this page.

Incident reports identify asset issues that require your attention. For example, a hospital cardiac unit defined a permitted location for an electrocardiogram (EKG) machine. An incident is reported when the EKG machine moves outside the permitted location.

To open the Incidents page, click **Incidents** ( ≡ ) in the Operations Center menu bar. The incidents applicable for your current context appear. You can change your context from the breadcrumbs to navigate to a different group, subgroup, or asset.

**Note:** You can also view the warnings for an individual asset from its Asset Details page.

The following image shows the Incidents page for the forklifts in the oil and gas division of a company.
On the Incidents page title row, you get tools that let you export, print, or search incidents. Pie charts help categorize the incidents by status, priority, and category. A detailed table of all incidents appears below the pie charts. You can sort the table by columns, such as status and priority.

Search for Incidents Using Filters

Locate specific incidents by using the incident filters.

1. To open the Incidents page, click Incidents ( расположен в меню Operations Center) bar.

   The incidents applicable for your current context appear. You can change your context from the breadcrumbs to navigate to a different group, subgroup, or asset.

2. Click the Search ( ) icon.

3. Select your filter criteria from the options that appear, and press the Enter key.
   - Select a priority from the Priority list. For example, you can filter for high priority incidents.
   - Select a time range under Reported Time. For example, you can search for all incidents reported in the last hour.
   - Select the Last Edited time for the incident. For example, you can search for incidents edited in the last two days.
   - Select a status from the Status list. For example, you can search for open incidents.
   - Select an incident type from the Type list. For example, you can filter for outage incidents.
   - Specify a search string for the incident Summary field. For example, you can search for incident summaries that start with the string, "High Temperature".

4. Click the Add Icon (+) to add additional criteria. Click the Subtract Icon (-) to remove a criterion.

5. Click Clear Search to clear your search filters.
Sort an Incident List

Sort an incident list to view incidents by priority, reported time, status, type, or summary.

1. To open the Incidents page, click **Incidents** in the Operations Center menu bar.
   
   The incidents applicable for your current context appear. You can change your context from the breadcrumbs to navigate to a different group, subgroup, or asset.

2. To sort the list by priority, reported time, status, type, or summary use one of these options:
   
   - Right-click in a column and click **Sort** and then **Sort Ascending** or **Sort Descending**.
   
   - Click the **Up** icon or the **Down** icon in the column header to sort the column in ascending or descending order.

Edit an Incident Report

Modify the summary, description, type, tags, priority, or comments of a reported incident.

1. To open the Incidents page, click **Incidents** in the Operations Center menu bar.
   
   The incidents applicable for your current context appear. You can change your context from the breadcrumbs to navigate to a different group, subgroup, or asset.

2. Click an incident in the **Incidents** list.

3. Modify the incident report in the lower pane:
   
   a. Click the **Edit** icon to add, remove, or edit summary text.
   
   b. Add, remove, or edit a description in the **Description** field.
   
   c. Add, remove, or edit tags in the **Tags** field.
   
   d. Select a priority for the incident in the **Priority** list.
   
   e. Click the **Add** icon to add a comment.
   
   f. Select a new status in the **Status** list.

4. Click **Save**.

Print an Incident List

Print an incident list to review incidents when a computer is unavailable.

1. To open the Incidents page, click **Incidents** in the Operations Center menu bar.
   
   The incidents applicable for your current context appear. You can change your context from the breadcrumbs to navigate to a different group, subgroup, or asset.
2. Click **Print**.

3. Select a printer and then click **OK**.

### Export an Incident List

Export an incident list to a comma-separated value (CSV) file.

1. To open the Incidents page, click **Incidents** in the Operations Center menu bar.
   
The incidents applicable for your current context appear. You can change your context from the breadcrumbs to navigate to a different group, subgroup, or asset.

2. Click **Export**.

3. Select **Save File** and then click **OK**.

4. Browse to a location to save the file and then click **Save**.

### Use the Warnings Page to Manage Asset Warnings

View and manage warnings from the Warnings page. You can also delete warnings from this page.

Warnings create a log of issues that do not require your immediate attention. Your rules can generate warnings based on location, threshold, or alert conditions.

To open the Warnings page, click **Warnings** in the Operations Center menu bar.
The warnings applicable for your current context appear. You can change your context from the breadcrumbs to navigate to a different group, subgroup, or asset.

**Note:** You can also view the warnings for an individual asset from its Asset Details page.

The following image shows the Warnings page for the forklifts in the oil and gas division of a company.

On the Warnings page title row, you get the **Search** icon that lets you search for warnings using filters. Use the following steps to search for warnings:
1. Click the **Search** (🔍) icon.

2. Select your filter criteria from the options that appear, and press the **Enter** key.
   - Select a level from the **Level** list. For example, you can filter to exclude Low level warnings.
   - Select a time range under **Created Time**. For example, you can search for all warnings created in the last hour.
   - Select a time range under **Last Occurred Time**. For example, you can search for all warnings that occurred in the last five minutes.
   - Select a status from the **Status** list. For example, you can search for active warnings.
   - Select a time range under **Duration**. For example, you can search for all warnings that are active for less than one day.

3. Click the **Add Icon** (+) to add additional criteria. Click the **Minus Icon** (-) to remove a criterion.

4. Click **Clear Search** to clear your search filters.

Below the Warnings page title, a pie chart appears summarizing the total number of active and resolved warnings. Warnings resolve automatically once the warning condition is no longer applicable.

A list of all warnings appears below the pie chart. You can sort the list by the desired column, such as **Status** or **Created Time**.

Click the **Show Details** (🔍) icon against a Warning row to see the warning details, such as the asset against which the warning was raised.

Click the **Delete** (🗑️) icon against a Warning row to delete the warning.

---

**Use SMS Notifications for Asset Incidents and Warnings**

Oracle IoT Asset Monitoring Cloud Service integrates with the Twilio SMS service to help provide seamless SMS notifications.

You can configure Oracle IoT Asset Monitoring Cloud Service to send SMS notifications for asset incidents and warnings. When a rule triggers an asset incident or warning, SMS notifications are sent to all configured subscribers on their mobile devices.

SMS notifications eliminate the need to monitor the Oracle IoT Asset Monitoring Cloud Service application continuously. All subscribers are actively informed about asset incidents and warnings that need attention. You can then use the Oracle IoT Asset Monitoring Cloud Service mobile application or Web interface to look at, and address, the issues.

You must have a Twilio account subscription to use the SMS notification service. Add your Twilio account information to Oracle IoT Asset Monitoring Cloud Service to start using the notification service. After adding your account, you can add subscribers that need to receive these notifications, and select the rules that should send the notifications.
Add Your Notification Account Details

To start using the notification feature, add your notification account details in Oracle IoT Asset Monitoring Cloud Service. For SMS notifications, add your Twilio account details.

Make sure that the IoT administrator has already added the Twilio domain as a trusted CN in the Oracle Internet of Things Cloud Service management console. To do this, the administrator adds *.twilio.com under Trusted CN in the Settings page.

To add the notification account details in Oracle IoT Asset Monitoring Cloud Service:

1. In the operations center, click **Menu (≡)**, and then click **Configuration**.
   - If you are in the design center, you need to click **Previous (👈)** before you see the **Configuration** option in the menu.

2. Click the **Settings** tab (**⚙️**).

3. Under Notifications, click **Add (➕)**.

4. Enter a **Name** for your notification account.
   - For example, *My Twilio Account*.

5. Select your **Provider**.
   - Oracle integrates with Twilio, as the third-party notification service provider.

6. Enter the **SID** for your Twilio account.
   - This is your Twilio account SID that you can get from your Twilio console.

7. Enter the **Authorization Token** associated with your Twilio account.
   - You can get the authorization token from your Twilio console.

8. Enter the **Sender Phone No** for notification messages.
   - The sender phone number is provided by Twilio, and can be generated in your Twilio account.

9. Click **OK** to add the notification account.

You can next add subscribers or recipients for the SMS notifications.

Add Subscribers for the Notifications

You can add one or more subscribers for a notification. You can also create different subscriber groups and add them to rules, as desired.

1. Click **Menu (≡)**, and then click **Design Center**.

2. Select **Organization** from the **Design Center** sub-menu.

3. Click **Subscribers**.

4. Click **Create Subscriber (➕)** to add a new subscriber or group or subscribers.

5. Enter a **Name** for the subscriber or group of subscribers that you are creating.
   - For example, *Water Utility Team*
You may want to create different subscriber groups based on the assets managed by each group.

   See Add Your Notification Account Details for more information about adding a notification account.

7. (Optional) Select pre-existing Rules to subscribe to events from the selected rules.
   Note that you can also add notification subscribers to a rule by editing the rule, or when creating a rule.

8. (Optional) Select existing Users to add them as subscribers.

9. Enter the subscriber Phone Numbers.
   Precede the phone numbers with the country codes. Press enter after entering each phone number.

10. Click OK to finish creating the subscriber group.

Use Contextual Data Connections

Contextual data connections, also known as external data connections, let you access asset-related data from database tables. You can store your data in the Oracle NoSQL Database Cloud Service instance associated with Asset Monitoring. You can also use a Database Cloud Service instance. Contextual data connections, also known as external data connections, let you access asset-related data from database tables. You can store your data in the Oracle NoSQL Database Cloud Service instance associated with Asset Monitoring. You can also use a Database Cloud Service instance. Contextual data can be used in custom KPI computations. For example, if you have a common asset type for forklifts, but different forklifts have different fuel capacities based on their model numbers, then you can store the fuel capacity data for your assets in a Database Cloud Service table. If you now need to compute a KPI such as the average percentage fuel level for your forklifts, you can use a formula such as the following:

\[
\text{Average}(\text{FuelLevel} * 100 / \text{FuelCapacity})
\]

Here, \text{FuelLevel} is a sensor value, and the \text{FuelCapacity} for the asset is retrieved from the contextual data table.

Contextual data can also be used for predictive analytics. For example, you can configure an Oracle NoSQL Database Cloud Service table to store historical sensor data for training the prediction model.

Create a Contextual Data Connection to the Autonomous NoSQL Database Cloud Service (ANDC) Instance

Create a contextual data connection to link to an Autonomous NoSQL Database Cloud Service (ANDC) table. You can use the data in the table for KPI computations and predictive analytics.

1. In the operations center, click **Menu** (☰), and then click **Configuration**.
   If you are in the design center, you need to click **Previous** (⮯) before you see the **Configuration** option in the menu.
2. Click the **External Data** tab.

3. Click the **Create New** icon.

4. Enter a **Name** and an optional **Description** for the external data connection.

5. Select **NoSQL** in the **Type** list.

6. Enter the name of a table in the **Table Name** field.
   - Select **Table already exists** if the table is already present in the NoSQL database.

7. If you are creating a new table, then under the **Fields** section, click **Create New** to add a table column.
   - Specify a **Name** and **Type** (data type) for each table column that you add. Select **Primary Key** when adding the primary key column.

8. Under **Associations**, you can associate the NoSQL table fields with their corresponding sensor attributes.
   - Click **Add** and select a **Name** for the association.
   - Under **From**, select an asset type.
   - Select a sensor attribute from the list of sensor attributes available for the asset type.
   - Under **To**, select the corresponding NoSQL table column.
   - Add additional sensor attributes to column associations, as required.

9. Click **Save** to create the external data connection.

### Create a Contextual Data Connection to a Database Cloud Service Instance

Create a contextual data connection to link to a Database Cloud Service table. You can use the data in the table for KPI computations and predictive analytics.

1. In the operations center, click **Menu (☰)**, and then click **Configuration**.
   - If you are in the design center, you need to click **Previous (↩)** before you see the **Configuration** option in the menu.

2. Click the **External Data** tab.

3. Click the **Create New** icon.

4. Enter a **Name** and an optional **Description** for the external data connection.

5. Select **DBaaS** in the **Type** list.

6. Enter the name of a table in the **Table Name** field.
   - Select **Table already exists** if the table is already present in the DBaaS database.

7. Enter the URL for the Database Cloud Service instance in the **Connection String** field.
8. Enter the user name for the Database Cloud Service instance in the **User Name** field.

9. Enter the password for the Database Cloud Service instance in the **Password** field.

10. If you are creating a new table, then under the **Fields** section, click **Create New** to add a table column.

    Specify a **Name** and **Type** (data type) for each table column that you add. Select **Primary Key** when adding the primary key column.

11. Under **Associations**, you can associate the DBaaS table fields with their corresponding sensor attributes.

    a. Click **Add** and select a **Name** for the association.

    b. Under **From**, select an asset type.

    c. Select a sensor attribute from the list of sensor attributes available for the asset type.

    d. Under **To**, select the corresponding DBaaS table column.

    e. Add additional sensor attributes to column associations, as required.

12. Click **Save** to create the external data connection.

### Edit a Contextual Data Connection

Edit a contextual data connection to change the data connection settings.

1. In the operations center, click **Menu (≡)**, and then click **Configuration**.

   If you are in the design center, you need to click **Previous (↵)** before you see the **Configuration** option in the menu.

2. Click the **External Data** tab.

3. Select an external data connection in the **External Data** list.

4. Click the **Edit (✎)** icon.

5. Edit the external data connection settings.

6. Click **Save**.

### Duplicate a Contextual Data Connection

Duplicate a contextual data connection to quickly copy the settings of an existing contextual data connection to a new contextual data connection.

1. Click **Menu (≡)** and select **Configuration**.

2. Click **Menu (≡)**, and click the **Previous (↵)** icon to the left of your current organization name.

3. Click **Configuration**.

4. In the operations center, click **Menu (≡)**, and then click **Configuration**.

   If you are in the design center, you need to click **Previous (↵)** before you see the **Configuration** option in the menu.
5. Click the External Data tab.
6. Select an external data connection in the External Data list.
7. Click the Duplicate icon.
   A duplicate external data connection opens up for editing.
8. Enter a name for the external data connection in the Name field and then add an optional description.
9. (Optional) Edit the remaining external data connection settings.
10. Click Save.

Delete a Contextual Data Connection

Delete a contextual data connection when it is no longer required.
1. In the operations center, click Menu, and then click Configuration.
   If you are in the design center, you need to click Previous before you see the Configuration option in the menu.
2. Click the External Data tab.
3. Select an external data connection in the External Data list.
4. Click the Delete icon.
5. Click Yes to confirm.

Use Anomalies to Track Deviations in Asset Behavior

When the set parameters of an asset do not conform to a regular pattern, an anomaly occurs. An anomaly can help you identify and resolve potential problems with your assets.

Use anomalies to detect deviations from normal asset behavior, and to flag and address device issues in time. You can define the following types of asset anomalies in Oracle IoT Asset Monitoring Cloud Service:

- **Automatic Anomaly:** Use an automatic anomaly to automatically look for deviations in a sensor or metric (KPI) value. For example, automatic anomalies can help detect an HVAC device that is overheating.

- **User-Defined Anomaly:** Create a user-defined anomaly to look for telltale patterns in sensor or metric data generated by an asset. For example, you may create user-defined anomalies to look for vibration anomalies in a forklift asset. User-Defined anomalies are based on acceptable or anomalous data patterns. You train the system by providing it with samples of acceptable data or anomalous data. These samples can come from sensor data, user-defined patterns, and contextual data stored in external systems.

  For acceptable data, you specify a time window containing acceptable patterns of sensor or metric data. The time window is a period of typical operations during which your assets, and associated sensors, behaved normally. The system uses the data pattern that you select to train itself. During day-to-day operations, the
system looks out for deviations in data patterns that are beyond the specified deviation percentage, and flags these as anomalies.

For anomalous data, you can use IoT sensor or user-defined data to supply the patterns. You can also use contextual data sources. For example, if you have your breakdown event data stored in a Database Cloud Service table, you can overlay these events on the sensor data timeline to define anomalies that occur around the breakdown events.

All detected anomalies appear on the Anomalies page accessible from the Operations Center or Asset Details page of individual assets. The anomalies displayed in the Operations Center depend on your current context (organization, group, and subgroup).

The following image shows some anomalies for the organization context in the Operations Center view. Anomalies for different groups and assets are shown in the same page. You can change your context using the breadcrumbs in the Operations Center.

Use the breadcrumbs to change your context in the organization. You can filter your view for a group, subgroup, or individual asset.

Define an Automatic Anomaly

Define an automatic anomaly to automatically identify deviations from regular patterns.

Anomalies are created for asset types.

1. Click Menu, and then click Design Center.
2. Select Asset Types from the Design Center sub-menu.
3. Select an asset type from the Asset Types list.
   You can also search for an asset type.
4. Click Anomalies.
5. Click the Create New icon.
6. Enter a name for the anomaly in the Name field.
7. (Optional) Specify an optional description text for the anomaly.
8. Under Detection Target, verify the Asset Type for your anomaly. The anomaly applies to all assets of the chosen asset type.

9. Select an available Attribute to monitor. The list of attributes includes sensor attributes and query-type (computed) metrics.

10. Under Training Data, select Automatic. Use an automatic anomaly to automatically look for deviations in a sensor or metric (KPI) value. For example, automatic anomalies can help detect an HVAC device that is overheating intermittently.

11. Select a Specimen Asset that provides the training data for anomaly detection. A list of all assets with the selected asset type appears. The asset with the most data is chosen by default. You can choose a different asset if required.

12. Specify a Training Window period. This is the amount of historical data used to train the system for anomaly detection.

13. Select a Deviation Threshold. The deviation threshold is the acceptable standard deviation multiple from the mean. Attribute values exceeding this will result in anomalies.

14. Click Save.

Create a User-Defined Anomaly

Create a user-defined anomaly to look for patterns in sensor data generated by an asset.

1. Click Menu (Ξ), and then click Design Center.

2. Select Asset Types from the Design Center sub-menu.

3. Select an asset type from the Asset Types list. You can also search for an asset type.

4. Click Anomalies.

5. Click the Create New (➕) icon.

6. Enter a name for the anomaly in the Name field.

7. (Optional) Specify an optional description text for the anomaly.

8. Under Detection Target, verify the Asset Type for your anomaly. The anomaly applies to all assets of the chosen asset type.

9. Select an available Attribute to monitor. The list of attributes includes sensor attributes and query-type (computed) metrics. For example, a temperature sensor asset may include the temperature attribute.

10. Under Training Data, select User Defined Anomaly. A user-defined anomaly lets you manually specify anomalous or normal data patterns for a sensor or metric. You can select the data pattern from existing sensor, or metric, data. Alternatively, you can manually plot an anomalous data pattern that the system uses to identify anomalies.
11. Select a **Specimen Asset** that provides the data pattern for anomaly detection.

   A list of all assets with the selected asset type appears. The asset with the most data is chosen by default. You can choose a different asset if required.

12. Choose a **Selection Type**, and complete the corresponding steps.

   - Choose **Anomalous Data** to select an anomalous data pattern from existing sensor or metric data.
     a. (Optional) Change the **Data End Time** for the chart, if required. The current date and time are automatically populated.
     b. (Optional) If you wish to show contextual annotations using event data stored in a contextual data connection, then select **Show Contextual Annotation**.
        
        For example, if you have breakdown events and their timestamps stored in a Database Cloud Service table, you can overlay this data on your sensor data timeline to define pattern anomalies that occur before the breakdown events. See **Use Contextual Annotations in Pattern Anomalies** for more information.
     c. Click **Generate Chart** to display the sensor or metric data for the selected attribute and asset.
        
        The data plot for the selected asset attribute appears.
     d. Use the mouse to select the anomaly pattern in the data plot.
        
        You can zoom in and zoom out in the data plot area. You can also navigate along the time axis using the **Next** and **Previous** buttons.
        
        If you wish to change the selected pattern, you can select another pattern in the data plot and the first pattern is deselected.
     e. Click **Save** to save the anomaly.
     f. Click **Publish** to deploy the anomaly.

   - Choose **Acceptable Data** to select acceptable or non-anomalous data from existing sensor or metric data.
     a. Select a **Deviation Percentage**.
        
        This is the percentage of deviation required to trigger an anomaly.
     b. Specify a **Data Start Time** and **Data End Time** to plot the chart.
        
        This is the broad time period that contains acceptable, or non-anomalous, attribute data.
     c. Click **Generate Chart** to display the sensor or metric data for the selected attribute and time period.
        
        The data plot for the selected asset attribute appears.
d. Click within the left-half chart to select the start time.
   This marks the beginning of acceptable, or non-anomalous, data.

e. Click within the right-half chart to select the end time.
   This marks the end of the sample (acceptable) data.

f. Click **Save** to save the anomaly.

g. Click **Publish** to deploy the anomaly.

- Choose **User Defined Data** to manually plot an anomalous data pattern.
  a. Enter the **Event Frequency**.
     The event frequency specifies the time interval (in milliseconds) between any two data points.
  b. Specify the **Number of Points** that you need to plot.
  c. In the **Scale** field, enter a lower and upper limit for the sensor attribute.
  d. Click **Generate Chart**.
     An empty chart is created based on the scale, frequency, and number of data points that you specified.
  e. Create an anomaly pattern by clicking at various points in the data plot area.
  f. Click **Save** to save the anomaly.
  g. Click **Publish** to deploy the anomaly.

After creating and publishing an anomaly, you can access the anomaly data for an asset from the asset details page.

**Use Contextual Annotations in Pattern Anomalies**

When manually creating pattern-based anomalies, you can add contextual annotations to the data plot if you have contextual data stored in a data connection. This can help identify events, such as breakdowns, on the sensor data plot.

For instance, if you have breakdown events and their timestamps stored in a Database Cloud Service table, you can overlay this data on your sensor data timeline to define pattern anomalies that occur before the breakdown events.

1. Create a manual anomaly as described in **Create a User-Defined Anomaly**.
2. Select **Show Contextual Annotation** to add contextual annotations.
3. Select a **Data Source**.
The data source contextual link is the name of your Database Cloud Service or Oracle NoSQL Database Cloud Service contextual data connection.

4. Specify the contextual data table column that corresponds to **Important Event Field**.
   This column should contain information about events related to your asset.

5. Specify the contextual data table column that corresponds to the **Timestamp Field** for the events.
   This column should contain timestamp information for the stored events.

6. Click **Generate Chart** to display the sensor or metric data along with the contextual annotations.

### Edit an Anomaly

Edit an anomaly to change the anomaly settings.

1. Click **Menu (≡)**, and then click **Design Center**.
2. Select **Asset Types** from the **Design Center** sub-menu.
3. Select an asset type from the **Asset Types** list.
   You can also search for an asset type.
4. Click **Anomalies**.
5. Select an anomaly from the **Anomalies** list.
6. Click the **Edit (-pencil)** icon.
7. Edit the anomaly settings.
8. Click **Save**.

### Duplicate an Anomaly

Duplicate an anomaly to quickly copy the settings of an existing anomaly to a new anomaly.

1. Click **Menu (≡)**, and then click **Design Center**.
2. Select **Asset Types** from the **Design Center** sub-menu.
3. Select an asset type from the **Asset Types** list.
   You can also search for an asset type.
4. Click **Anomalies**.
5. Select an anomaly from the **Anomalies** list.
6. Click the **Duplicate (folders)** icon.
7. Enter a name for the anomaly in the **Anomaly Name** field.
8. (Optional) Edit the remaining anomaly settings.
9. Click **Save**.
Delete an Anomaly

Delete a anomaly when it is no longer required.

1. Click Menu (☰), and then click Design Center.
2. Select Asset Types from the Design Center sub-menu.
3. Select an asset type from the Asset Types list.
   You can also search for an asset type.
4. Click Anomalies.
5. Select an anomaly in the Anomalies list.
6. Click the Delete (🗑) icon.
7. Click Yes.

Use Predictions to Identify Asset Risks

Predictions use historical and transactional data to predict future asset parameters, and to identify potential risks to your assets.

You can either use internal Oracle Internet of Things Cloud Servicedata or import and use external device data to help make predictions for your asset.

>Note:

For predictions to work, the data source must have at least 72 hours of historical data in it. This is required for predictive analytics to train the system. You may have to wait until the system completes the training for the predictions to start showing.

Predictions help warn you of impending asset failure in advance. Preventive maintenance can help save the costs associated with asset breakdown or unavailability.

All detected predictions appear on the Predictions 📊 page accessible from the Operations Center or Asset Details page of individual assets. The predictions displayed in the Operations Center depend on your current context (organization, group, and subgroup).

The following image shows some predictions for the organization in the Operations Center view. Predictions for different assets are shown in the same page. You can change your context using the breadcrumbs in the Operations Center.
Create a Prediction

Create a prediction to identify risks to your assets.

1. Click **Menu** (≡), and then click **Design Center**.
2. Select **Asset Types** from the **Design Center** sub-menu.
3. Select an asset type from the **Asset Types** list.
   
   You can also search for an asset type.
4. Click **Predictions**.
5. Click the **Create New** (➕) icon.
6. Enter a name for the prediction in the **Name** field.
7. Enter an optional description for the prediction in the **Description** field.
8. In the **Metric** area, select one of these options for **Metric Data Type**:
   
   • **Categorical**: Select this option to select a specific category of data. This option can only be used with Query-type metrics (computed KPIs), and must return a Boolean value.
   
   • **Continuous**: Select this option to select data of any value. This option can be used with sensor attributes and Query-type metrics.
9. Verify the **Asset Type** name for which you are creating the prediction.
10. Select the **Attribute** on which to create the prediction. The list can include both sensor attributes and query-type metrics, and also depends upon the value selected for the **Metric Data Type**.
11. Under **Prediction Time Window**, select one of the options:
   
   • **Next 24 Hours**: Select this option to create a prediction for the next 24 hours.
   
   • **Next 7 Days**: Select this option to create a prediction for the next 7 days.
• **Next 30 Days**: Select this option to create a prediction for the next 30 days.

**Note**: Predictive analytics may need to collect at least 72 hours of data to train the system. Your predictions start showing after the initial training is complete.

12. (Optional) Select one or more contextual links from the **Contextual Link** list.

A contextual link is used to provide additional data to the prediction for training the system. If you have existing contextual data connections that you would like to use as additional data sources for the prediction, you can optionally add them to the prediction.

13. Click **Save** to complete configuring the prediction.

**Edit a Prediction**

Edit a prediction to change the prediction settings. You can also tweak your prediction model to add or remove features, and re-train the prediction model for your environment.

1. Click **Menu (≡)**, and then click **Design Center**.
2. Select **Asset Types** from the **Design Center** sub-menu.
3. Select an asset type from the **Asset Types** list.

You can also search for an asset type.

4. Click **Predictions**.
5. Select a prediction from the list.

If the initial training for the prediction has completed, you should see an accuracy percentage for the prediction. The accuracy percentage reflects the scoring accuracy history of your prediction model measured against actual data.

6. Click the **Edit (✎)** icon.

7. (Optional) Under Prediction Model, click **Configure Model** if you wish to re-configure the current prediction model for your prediction.
This setting is available if the training for your prediction has completed, and a scoring accuracy is available. You can add or remove features or attributes currently associated with your prediction to select a feature-set that you believe is most relevant for your environment and will result in better scoring accuracy. Your changed feature-set is then used to re-train the prediction model. You may also wish to re-train the prediction model if golden data has arrived post the initial training of the prediction.

a. Select or deselect features, or attributes, as required under the Used column.

![Edit Prediction Model](image-url)

Select the features you would like to use when calculating the prediction model. The best model column shows features included in the most accurate model trained so far.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Best Model</th>
<th>Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gas_Compressor_DM_Motor_Speed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gas_Compressor_DM_Inlet_Temperature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gas_Compressor_DM_Coolant_Temperature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gas_Compressor_DM_Motor_Temperature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gas_Compressor_DM_Suction_Pressure</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

☑ Automatically accept new model if accuracy is increased.
If an attribute shows selected under the Best Model column, it means that the attribute is part of the best prediction model to date.

b. Select **Automatically accept new model if accuracy is increased** to automatically switch the active model to your new model if the scoring accuracy is better.

If you do not select this option, then after the training is complete, you can see both the currently active model and new model scores. You can then choose to switch to the new prediction model if you wish.

c. Click **Rerun Training** to re-train the prediction with the chosen features and cumulative data.

Clicking **Cancel** discards your changes.

8. Edit other prediction settings, as required.

9. Click **Save**.

**Delete a Prediction**

Delete a prediction when it is no longer required.

1. Click **Menu (≡)**, and then click **Design Center**.

2. Select **Asset Types** from the **Design Center** sub-menu.

3. Select an asset type from the **Asset Types** list.

   You can also search for an asset type.

4. Click **Predictions**.

5. Select a prediction from the list.

6. Click the **Delete (Trash) icon**.

7. Click **Yes**.
5

Set Up Your Devices in Oracle Internet of Things Cloud Service

The device model options for asset types and device options for assets are fetched from your Oracle Internet of Things Cloud Service instance.

Topics:
- Create Device Models in Oracle Internet of Things Cloud Service
- Assign Device Models to the Oracle IoT Asset Monitoring Cloud Service Application
- Register and Activate Devices in Oracle Internet of Things Cloud Service

Create Device Models in Oracle Internet of Things Cloud Service

The device model options for asset types are fetched from your Oracle Internet of Things Cloud Service instance.

The Oracle IoT Asset Monitoring Cloud Service application relies on your platform side Oracle Internet of Things Cloud Service for its device models. If you do not already have your device models set up in Oracle Internet of Things Cloud Service, you need to add the device models for your sensor devices.

Create a New Device Model

A device model is an interface that lets any device communicate with Oracle Internet of Things Cloud Service regardless of its manufacturer or operating system.

1. Open the Oracle Internet of Things Cloud Service Management Console.
   You can access the Oracle Internet of Things Cloud Service Management Console from the following URL:
   https://hostname/ui
   Here, hostname is the host name of your Oracle Internet of Things Cloud Service instance.

2. Click the Menu (≡) icon.

3. Select Devices and then select Model.

4. Select one of these options:
   - If you have not previously created a device model, click Create Device Model.
   - If you have previously created a device model, click the Add (⊕) icon.

5. Complete these fields:
a. **Name**: Enter a name for the device model.

b. **Description**: Enter an optional description for the device model.

c. **URN**: Enter a unique identifier for the device model. Use this format:
   `urn:com:<mycompany>:<mydevice>:<what the device model does>`.

6. Select system attributes for the device model.

7. (Optional) Add custom attributes for the device model:
   a. Expand the **Custom Attributes** option list.
   b. Click the **Add** icon.
   c. Enter a name for the custom attribute in the **Name** field.
   d. Enter an optional description for the custom attribute in the **Description** field.
   e. Select a data type in the **Type** list.
   f. Select **Writable** if you want to make the custom attribute writable.
   g. Click **OK**.

8. (Optional) Define the actions that can be invoked on the device:
   a. Expand the **Actions** option list.
   b. Click the **Add** icon.
   c. Enter a name for the action in the **Name** field.
   d. Enter an optional description for the action in the **Description** field.
   e. Select the data type for the action in the **Arguments** list.
   f. Enter an optional alternate name for the action in the **Alias** field.
   g. Click **OK**.

9. (Optional) Create alerts and custom message formats for the device model:
   a. Expand the **Alerts and Custom Messages** option list.
   b. Click the **Add** icon.
   c. Enter a name for the alert or custom message in the **Name** field.
   d. Enter an optional description for the alert or custom message in the **Description** field.
   e. Enter a unique identifier for the alert or custom message in **URN** field. Use this format:
   f. Select a data type in the **Type** list.
   g. Click **OK**.
   h. Select the alert message format and then click the **Add** icon in the **Fields** column.
   i. Enter a name for the message type in the **Name** field.
   j. Select a data type in the **Type** list.
   k. Select **Optional** to indicate the field value can be missing in the device model message format.
1. Click OK.

10. Click Save.

**Import a Device Model**

If you have previously exported a device model, you can import the .json file into Oracle Internet of Things Cloud Service.

1. Open the Oracle Internet of Things Cloud Service Management Console. You can access the Oracle Internet of Things Cloud Service Management Console from the following URL:

   https://hostname/ui

   Here, hostname is the host name of your Oracle Internet of Things Cloud Service instance.

2. Click the Menu (≡) icon.

3. Select Devices and then select Model.

4. In the Device Models tab, click the Import (quivo) icon.

5. Click Choose File and select the .json file to import.

6. Click Import to import the device model.

**Duplicate a Device Model**

Duplicate a device model to quickly copy the settings of an existing device model to a new device model.

1. Open the Oracle Internet of Things Cloud Service Management Console. You can access the Oracle Internet of Things Cloud Service Management Console from the following URL:

   https://hostname/ui

   Here, hostname is the host name of your Oracle Internet of Things Cloud Service instance.

2. Click the Menu (≡) icon.

3. Select Devices and then select Model.

4. Click the Duplicate (fita) icon.

5. Complete these fields:

   a. **Name**: Enter a new name for the device model.

   b. **Description**: Enter an optional description for the device model.

   c. **URN**: Enter a new unique identifier for the device model. Use this format: .

6. Select system attributes for the device model.

7. (Optional) Add or edit the custom attributes for the device model.

8. (Optional) Add or edit the actions that can be invoked on the device.
9. (Optional) Add or edit the alerts and custom message formats for the device model:

10. Click **Save**.

### Edit a Device Model

Edit a device model to edit, add, duplicate, or remove device model settings including the device model name, description, and attributes.

1. Open the Oracle Internet of Things Cloud Service Management Console.
   
   You can access the Oracle Internet of Things Cloud Service Management Console from the following URL:
   
   https://hostname/ui
   
   Here, **hostname** is the host name of your Oracle Internet of Things Cloud Service instance.

2. Click the **Menu** (>>) icon.

3. Select **Devices** and then select **Model**.

4. Click the **Edit** (✏️) icon.

5. Edit the device model settings.

6. Click **Save**.

### View the Devices Associated with a Device Model

View the devices associated with the device model to determine how many devices are using the device model.

1. Open the Oracle Internet of Things Cloud Service Management Console.
   
   You can access the Oracle Internet of Things Cloud Service Management Console from the following URL:
   
   https://hostname/ui
   
   Here, **hostname** is the host name of your Oracle Internet of Things Cloud Service instance.

2. Click the **Menu** (>>) icon.

3. Select **Devices** and then select **Model**.

4. Click the **Device** (_WIFI) icon.

### Print Device Model Settings

Print the device model settings to view a hard copy of the device model settings.

1. Open the Oracle Internet of Things Cloud Service Management Console.
   
   You can access the Oracle Internet of Things Cloud Service Management Console from the following URL:
   
   https://hostname/ui
Here, hostname is the host name of your Oracle Internet of Things Cloud Service instance.

2. Click the Menu (Ξ) icon.
3. Select Devices and then select Model.
4. Click the Print (⎙) icon.
5. Select a printer.
6. Click OK.

Export Device Model Settings

Export the device model settings to use the device model settings in another application or to save a copy of the device model settings as a backup in case of a system failure.

1. Open the Oracle Internet of Things Cloud Service Management Console.
   You can access the Oracle Internet of Things Cloud Service Management Console from the following URL:
   https://hostname/ui
   Here, hostname is the host name of your Oracle Internet of Things Cloud Service instance.
2. Click the Menu (Ξ) icon.
3. Select Devices and then select Model.
4. Click the Export (✍) icon.
5. Click Save File.
6. Click OK.
7. Browse to a location to save the file.
8. Click Save.

Delete a Device Model

Delete a device model when it is no longer required.

1. Open the Oracle Internet of Things Cloud Service Management Console.
   You can access the Oracle Internet of Things Cloud Service Management Console from the following URL:
   https://hostname/ui
   Here, hostname is the host name of your Oracle Internet of Things Cloud Service instance.
2. Click the Menu (Ξ) icon.
3. Select Devices and then select Model.
4. Click the Delete (🗑) icon.
A warning appears if the device model is in use. If you delete the device model, the related message flows, explorations, integrations, and device message links are affected as well.

5. Click Continue.

Assign Device Models to the Oracle IoT Asset Monitoring Cloud Service Application

Choose the device models in Oracle Internet of Things Cloud Service that should be associated with the Oracle IoT Asset Monitoring Cloud Service application.

When configuring asset types in Oracle IoT Asset Monitoring Cloud Service, the device model options that appear are the ones that you pre-select in Oracle Internet of Things Cloud Service.

Assign a Device Model to a Cloud Service

To use a device model in a specific cloud service, you must associate it with the cloud service.

1. Open the Oracle Internet of Things Cloud Service Management Console.
   You can access the Oracle Internet of Things Cloud Service Management Console from the following URL:
   https://hostname/ui
   Here, hostname is the host name of your Oracle Internet of Things Cloud Service instance.

2. Click the Menu (≡) icon, and then click Applications.

3. Click the entry corresponding to the Oracle IoT Asset Monitoring Cloud Service application.

4. Click Device Model.

5. Click the Choose Device Model (👍) icon.

6. Select the Add checkbox for the device model you want to assign to the cloud service.

7. Click Done.

Register and Activate Devices in Oracle Internet of Things Cloud Service

To associate device sensors with your assets, make sure that the devices are registered and activated in Oracle Internet of Things Cloud Service.

The Oracle IoT Asset Monitoring Cloud Service application relies on your platform side Oracle Internet of Things Cloud Service for its devices. If you do not already have your sensor devices set up in Oracle Internet of Things Cloud Service, you need to register and activate these devices.
Register a Single Device

To communicate with Oracle Internet of Things Cloud Service, every device that is connected to Oracle Internet of Things Cloud Service must be registered and then activated. All devices are registered as a Directly Connected Device (DCD). During activation, the device indicates support for indirect enrollment. A device indicating indirect enrollment capability is automatically changed from DCD to gateway.

1. Click the Menu icon adjacent to the Oracle Internet of Things Cloud Service title on the Management Console.
2. Click Devices.
3. Click Registration.
4. Click Register Single Device.
5. Complete the optional and mandatory fields.

Note:
If you leave the Activation Secret field blank, a value is auto-generated and displayed when the device registration is confirmed. You can enter your own Activation Secret value. Any additional information, such as Name, Description, and Metadata are optional, but can be useful as search criteria when managing your registered devices.

6. Click Register.
7. Enter a password in the File Protection Password field to encrypt the provisioning file that contains the configuration and credentials to activate your device.
8. Enter the password again in the Confirm Password field.
9. Download the provisioning file:
   a. Click Download Provisioning File.
   b. Click Save File.
   c. Click OK.
   d. Browse to a location to save the provisioning file.
   e. Click Save.
10. Click Finish.

Register a Batch of Devices

Registering a batch of devices reduces the time required to register multiple devices. You create a comma-separated values (CSV) file to define the settings for each device. You upload the CSV file to Oracle Internet of Things Cloud Service.

To view the information that you should include in the CSV file, see About CSV Batch Registration File Properties.
1. Click the **Menu** (⋮) icon adjacent to the Oracle Internet of Things Cloud Service title on the Management Console.

2. Click **Devices**.

3. Click **Registration**.

4. Select one of these options:
   - Click **Download CSV template** to download a CSV template that you can complete.

   ![Note:]
   
   The CSV file contains the mandatory and optional property values for each device. If a value is not provided for the optional properties, insert a comma to indicate that a value is not provided. In the last line of the sample CSV file, a comma indicates that property values are not provided for **ActivationId** and **Activation Secret**

   - Click **Batch Registration** to upload an existing CSV file.

5. Click **Browse** and browse to the CSV file that contains the registration information for the devices you are registering.

6. Click **Next** when the CSV registration file is successfully uploaded.

   If the Review page contains a warning (⚠️) icon, select one of these options:
   - **Update** - Choose this option if you want to update the information for an existing registered device. The registered device has the same manufacturer, model and serial number as one of the devices listed in the CSV registration file.
   - **Ignore** - Choose this option if you do not want to include the device in the current registration process.

7. Click one of these options:
   - **Next**: Click to proceed to register the items in the CSV registration file that have been identified as being viable candidates for registration.
   - **Cancel**: Click to discontinue the batch registration process.

8. Enter a password in the **File Protection Password** field to encrypt the provisioning file that contains the configuration and credentials to activate your device.

9. Enter the password again in the **Confirm Password** field.

10. Download the provisioning file:
    a. Click **Download Provisioning File**.
    b. Click **Save File**.
    c. Click **OK**.
    d. Browse to a location to save the provisioning file.
    e. Click **Save**.

11. Click **Finish**.
12. Activate the registered devices to begin a secure communication between the devices and Oracle Internet of Things Cloud Service. See Activate a Batch of Registered Devices.

About CSV Batch Registration File Properties

The following table provides descriptions of the properties that appear in the Comma Separated Values (CSV) file used to register a batch of devices with Oracle Internet of Things Cloud Service. Mandatory and optional values are described in the table and are listed in the order they are expected to appear in the CSV file.

To register a batch of devices with Oracle Internet of Things Cloud Service, see Registering a Batch of Devices.

<table>
<thead>
<tr>
<th>Property</th>
<th>Required / Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Optional</td>
<td>The String data type assigned to the registered device. This value can be modified after device registration.</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>Required</td>
<td>The manufacturer of the device.</td>
</tr>
<tr>
<td>Model Number</td>
<td>Required</td>
<td>The model number of the device</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Required</td>
<td>The serial number of the device</td>
</tr>
<tr>
<td>Activation ID</td>
<td>Optional</td>
<td>A Device Unique Identifier (UID) that is required for device activation. If a value is not specified, an auto-generated value is assigned to the device after a successful registration. The value cannot be changed after the device is successfully registered.</td>
</tr>
<tr>
<td>Activation Secret</td>
<td>Optional</td>
<td>The Activation Secret (also known as Shared Secret) value required to activate your device. If a value is not specified, an auto-generated string value is assigned to the device after a successful registration. This value is available after a successful registration. This value can be modified before you modify your device.</td>
</tr>
<tr>
<td>Latitude</td>
<td>Optional</td>
<td>The decimal notation of the latitude of the device's position. For example: -43.5723 [World Geodetic System 1984]. If you specify the latitude, then you must also specify the longitude.</td>
</tr>
<tr>
<td>Longitude</td>
<td>Optional</td>
<td>The decimal notation of the longitude of the device's position. For example: -43.5723 [World Geodetic System 1984]. If you specify the longitude, then you must also specify the latitude.</td>
</tr>
<tr>
<td>Altitude</td>
<td>Optional</td>
<td>The decimal notation of the altitude of the device's position, in meters above sea level.</td>
</tr>
</tbody>
</table>
Activate a Device

A device can be activated after it is registered and an application has been created and run on the device. During activation, the device indicates support for indirect enrollment. A device indicating indirect enrollment capability is automatically changed from DCD to Gateway.

1. Register your directly connected device. See Registering a Single Device.

2. Create an application for the device using the Oracle Internet of Things Cloud Service Client Software Library APIs. See Developing Device Software Using the Client Software Libraries.

When using the Java Client Library, for example, use the following steps to initialize and activate the device:

   a. Add this statement to the device application code to initialize the device:

      ```java
      DirectlyConnectedDevice dcd = new DirectlyConnectedDevice(configFilePath, configFilePassword);
      ```

   b. Add this statement to the device application code to activate the device:

      ```java
      if (!dcd.isActivated())
      { dcd.activate(deviceModelUrn); }
      ```

3. Verify the device has been activated:
   a. Open the Oracle Internet of Things Cloud Service Management Console.
   b. Click the Menu (≡) icon adjacent to the Oracle Internet of Things Cloud Service title on the Management Console.
   c. Click Devices.
   d. Click Management.
   e. Locate the device in the device table or use the Property and Value fields at the top of the table to search for a specific device.
   f. Verify Activated and not Registered is displayed in the State column.
Activate a Batch of Registered Devices

After you've registered a batch of devices, you need to activate the devices before they can securely communicate with Oracle Internet of Things Cloud Service.

1. Register the devices and download the provisioning file. See Registering a Batch of Devices.

2. Activate each of the registered devices. See Activate a Device.

3. Verify that each of the registered devices has been activated.
   a. Open the Oracle Internet of Things Cloud Service Management Console.
   b. Click the Menu icon adjacent to the Oracle Internet of Things Cloud Service title on the Management Console.
   c. Click Devices.
   d. Click Management.
   e. Locate the device in the device table or use the Property and Value fields at the top of the table to search for a specific device.
   f. Verify Activated and not Registered is displayed in the State column.
Customize Your Oracle IoT Asset Monitoring Cloud Service Application

Add a corporate logo or modify the application name to personalize your Oracle IoT Asset Monitoring Cloud Service application.

Topics
- Show or Hide the Application Name
- Add or Update an Application Logo
- Remove an Application Logo

Show or Hide the Application Name

Show or hide the application name when business requirements change.

1. Click Menu (≡), and click the Previous (Previous) icon to the left of your current organization name.
2. Click Configuration.
3. Click the Settings tab (Settings).
4. Select one of these options:
   a. Select Show Application Name in Title Bar to display the application name on all application pages.
   b. Clear Show Application Name in Title Bar to remove the application name from all application pages.

Add or Update an Application Logo

Add or update corporate logos when business requirements change or a new corporate logo is issued.

1. Click Menu (≡), and click the Previous (Previous) icon to the left of your current organization name.
2. Click Configuration.
3. Click the Settings tab (Settings).
4. Select Show Logo in Title Bar and then click Upload Image.
5. Browse to the location of the logo, select the logo, and then click Open.
Remove an Application Logo

Remove a logo when an application logo is no longer required.

1. Click **Menu (≡)**, and click the **Previous (↵)** icon to the left of your current organization name.
2. Click **Configuration**.
3. Click the **Settings tab (⚙️)**.
4. Clear **Show Logo in Title Bar**.
Integrate with Other Cloud and Oracle Services

Integrate Oracle Visual Builder Cloud Service with Oracle IoT Asset Monitoring Cloud Service

Oracle IoT Asset Monitoring Cloud Service can integrate with other cloud and Oracle services, such as Oracle Application Builder Cloud Service (ABCS) and Oracle Maintenance Cloud.

Topics

• Integrate Oracle Visual Builder Cloud Service with Oracle IoT Asset Monitoring Cloud Service
• Integrate Oracle Maintenance Cloud with Oracle IoT Asset Monitoring Cloud Service
• Integrate Oracle Engagement Cloud with Oracle Service Monitoring for Connected Assets
• Integrate Oracle Service Cloud with Oracle Service Monitoring for Connected Assets
• Integrate Oracle Enterprise Asset Management with Oracle IoT Asset Monitoring Cloud Service
• Use Asset Monitoring Widgets in Your Application

Integrate Oracle Visual Builder Cloud Service with Oracle IoT Asset Monitoring Cloud Service

Oracle IoT Asset Monitoring Cloud Service supports integration with Oracle Visual Builder Cloud Service applications. This enables you to create web and mobile applications that leverage data from IoT.

You can download the asset monitoring Business Object Provider (BOP), and import the BOP into Oracle Visual Builder Cloud Service to access IoT application data as business objects. Business objects can include assets, places, incidents, and other asset monitoring object types. Use these objects in Oracle Visual Builder Cloud Service to create dashboards and mashups.

Download Asset Monitoring BOPs

Use the Oracle Internet of Things Cloud Service Management Console to download asset monitoring Business Object Providers (BOPs). You can then import these BOPs into an Oracle Visual Builder Cloud Service application.

1. Click the Menu (☰) icon adjacent to the Oracle Internet of Things Cloud Service title on the Management Console.
2. Click Applications.
3. Click **Browse Applications**.

4. Click the **Settings** icon adjacent to Oracle IoT Asset Monitoring Cloud Service.

5. Select **Download ABCS BOP** in the context menu that appears.

6. Save the zip file on your disk.

You can next proceed to import the downloaded zip file into an Oracle Visual Builder Cloud Service application, as a Business Object Provider (BOP) extension. The asset monitoring data becomes available to the Oracle Visual Builder Cloud Service application as BOP objects.

## Integrate Oracle Maintenance Cloud with Oracle IoT Asset Monitoring Cloud Service

You can import assets from the SCM Maintenance Cloud into Oracle IoT Asset Monitoring Cloud Service.

When an incident is created against an imported asset in Oracle IoT Asset Monitoring Cloud Service, the incident automatically translates into a work order in the SCM Maintenance Cloud. For example, if a threshold rule triggers an incident when a device associated with an asset is overheating, a work order corresponding to the incident automatically gets created in the SCM Maintenance Cloud.

When you release, close, cancel, or modify the work order in the SCM Maintenance Cloud, the corresponding incident status in Oracle IoT Asset Monitoring Cloud Service is automatically updated. The synchronization between Oracle IoT Asset Monitoring Cloud Service and SCM Maintenance Cloud happens every five minutes.

**Note:**

If you directly modify the status of an incident in Oracle IoT Asset Monitoring Cloud Service, the change is not synchronized back with the work order in SCM Maintenance Cloud.

## Enable Oracle Maintenance Cloud Integration

Use the Settings page in Oracle Internet of Things (IoT) Asset Monitoring Cloud Service to enable integration with Oracle Maintenance Cloud.

1. In Oracle IoT Asset Monitoring Cloud Service, click **Menu** (Ξ), and click the **Previous** (Previous) icon to the left of your current organization name.

2. Click **Configuration**.

3. Click the **Settings** tab (Settings).

4. In the Integrations section, click **Oracle Maintenance Cloud Service**.

5. Select the **Maintenance Cloud Enabled** option.

6. Specify the Endpoint URL for your Oracle Maintenance Cloud instance.
7. Specify the User Name for your Oracle Maintenance Cloud instance.

8. Specify the Password for your Oracle Maintenance Cloud instance.

9. (Optional) Select the Storage Cloud Integration to use for storing external data received from Oracle Maintenance Cloud.

   External data such as asset data, work order data, and maintenance schedules from Oracle Maintenance Cloud can be stored and used to analyze asset failure patterns. Learning work-flows, and associated analytics entities, are then created to suggest optimal maintenance schedules for Oracle Maintenance Cloud.

10. If you chose a Storage Cloud Integration, then specify a corresponding Storage Cloud Container name to store the Oracle Maintenance Cloud data.

    After you specify your Oracle Maintenance Cloud integration details, you may proceed to import assets from Oracle Maintenance Cloud.

Import Assets from Oracle Maintenance Cloud

To generate work orders automatically from incidents, you must first import assets from Oracle Maintenance Cloud.

Use the Assets page to import assets from Oracle Maintenance Cloud into Oracle IoT Asset Monitoring Cloud Service

1. In Oracle IoT Asset Monitoring Cloud Service, Click Menu (≡).

2. Click Assets.

3. Click Import from Maintenance Cloud (➡️) adjacent to the Assets page title.

4. Search for Oracle Maintenance Cloud assets to import by doing one of the following:

   a. From the Search By list, select Name, Type (Item in Oracle Maintenance Cloud), or Organization Code.

   b. **Note:**
      
      The search value field is case sensitive.

      In the Search Value field, specify the corresponding Name, Type, or Organization Code value.

   c. Click Search.

5. Select the assets that you want to import from the search results.

6. Click Import.

The selected assets are imported into Oracle IoT Asset Monitoring Cloud Service. The asset types for the imported assets are derived from the asset data in Oracle Maintenance Cloud.
Configure Rules to Generate Automatic Work Orders

Configure rules to automatically create work orders in Oracle Maintenance Cloud when an incident is created in Oracle IoT Asset Monitoring Cloud Service.

When creating incident rules in Oracle IoT Asset Monitoring Cloud Service, an additional Work Order section appears for assets imported from Oracle Maintenance Cloud.

For basic information on using rules in Oracle IoT Asset Monitoring Cloud Service, refer to Use Rules to Monitor and Maintain Assets.

If you are creating a rule to generate an incident for an imported asset, click Create Work Order in Maintenance Cloud.

If you have defined condition event codes in Oracle Maintenance Cloud for your IoT assets, then you can pass the event code corresponding to the incident back to Oracle Maintenance Cloud. Select the Event Codes to pass to Oracle Maintenance Cloud when the incident rule is triggered.

You can define maintenance programs in Oracle Maintenance Cloud to act on the incident based on the event code passed back by Oracle IoT Asset Monitoring Cloud Service. The maintenance program can trigger one or more work orders in Oracle Maintenance Cloud based on the reported incident.

For example, when a low amperage condition is detected for an HVAC device in Oracle IoT Asset Monitoring Cloud Service, a maintenance program in Oracle Maintenance Cloud triggers the HVAC oil check and motor check work orders.
Verify and Update the Work Orders in Oracle Maintenance Cloud

When an incident is created for an imported asset in Oracle IoT Asset Monitoring Cloud Service, a corresponding work order is automatically created in Oracle Maintenance Cloud.

Note:

The scheduler job synchronizes Oracle Maintenance Cloud with Oracle IoT Asset Monitoring Cloud Service every 5 minutes.

1. Sign in to your Oracle Maintenance Cloud instance.
4. Click Search Filters to specify criteria, such as the asset name and work order creation time, for your search.
5. Select one or more work order rows from the search results.
   - Click Release to release the selected work orders.
   - Click Mass Action to change the status of the work orders.

When you change the status of a work order in Oracle Maintenance Cloud, the status of the incident in Oracle IoT Asset Monitoring Cloud Service is automatically updated. For example, when you release a work order in Oracle Maintenance Cloud, the status of the corresponding incident in Oracle IoT Asset Monitoring Cloud Service changes from New to Open. When you close or cancel a work order, the status for the associated incident changes to Withdrawn.
Verify Incident Status Updates in Oracle IoT Asset Monitoring Cloud Service

When you change the status of a work order in Oracle Maintenance Cloud, the associated incident status is automatically updated in Oracle Internet of Things (IoT) Asset Monitoring Cloud Service.

**Note:**
The scheduler job synchronizes Oracle Maintenance Cloud with Oracle IoT Asset Monitoring Cloud Service every 5 minutes.

1. To open the Incidents page, click **Incidents** in the Operations Center menu bar. The incidents applicable for your current context appear. You can change your context from the breadcrumbs to navigate to a different group, subgroup, or asset.
2. Use one of the following methods to verify the status of an incident:
   - In the Incidents table, view the **Status** column value that corresponds to the incident.
   - Search for the incident by using incident filters.

Automatically Update Asset Meters in Oracle Maintenance Cloud with IoT Data

Oracle Maintenance Cloud assets can use meters corresponding to asset attribute values. You can update these meter readings automatically using IoT sensor values.

IoT data coming from devices is automatically pushed to asset meters in Oracle Maintenance Cloud. The maintenance supervisor can see the data directly coming from the devices without having to physically access the asset, facilitating preventive maintenance.

For example, the following image shows sample Oracle Maintenance Cloud meter readings, which represent the odometer and fuel usage values from sensor devices of a forklift device.

If you already have assets with meters in Oracle Maintenance Cloud, these meters are imported along with the assets when you import the assets into Oracle Internet of Things (IoT) Asset Monitoring Cloud Service.
1. In Oracle Internet of Things (IoT) Asset Monitoring Cloud Service, edit the imported asset type to add sensor attributes corresponding to the Oracle Maintenance Cloud meters.

For example, if you have imported forklift assets that use meters for fuel and distance, you need to add sensor attributes corresponding to the fuel meter and odometer.

See Edit an Asset Type for more information on editing an asset type to add sensor attributes.

2. Edit the asset to link the sensor attributes to their corresponding sensor devices.
   
a. On the Edit Asset page for an imported asset, click Link to Device against your sensor attribute and associate the sensor attribute to its corresponding device.
For more information on editing assets, see Edit Asset Details.

b. Repeat the previous step for any more sensor attributes that you created.

3. Associate the sensor attributes with their corresponding Oracle Maintenance Cloud meters.
   a. Under the Maintenance Cloud Meters section on the Edit Asset page, select Linked Sensor Attribute corresponding to each Oracle Maintenance Cloud meter.

b. Click Save on the Edit Asset page.

The scheduler job sends meter readings back to Oracle Maintenance Cloud once every day.
Integrate Oracle Engagement Cloud with Oracle Service Monitoring for Connected Assets

You can integrate Oracle Engagement Cloud with Oracle Service Monitoring for Connected Assets to directly manage your IoT connected assets from Engagement Cloud. When an incident gets created for an imported asset in Oracle Service Monitoring for Connected Assets, the incident rule automatically creates a corresponding service request (SR) in Engagement Cloud.

Note:
This integration is available only for Oracle Service Monitoring for Connected Assets, it is not available in the standard version of Oracle IoT Asset Monitoring Cloud Service.

Oracle delivers the Oracle Engagement Cloud solution for businesses that want to combine Oracle's sales and service capabilities on a single platform. Engagement Cloud provides a seamless service management interface that lets organizations capture and track service requests, collaborate between sales and service, and follow up with customers efficiently.

Engagement Cloud uses a tight integration with Oracle Service Monitoring for Connected Assets. You can not only sync incidents to Engagement Cloud, but also take asset actions, and set asset attributes from Engagement Cloud. Diagnostics let you see a graphical plot of your asset sensor attributes, and the results of the actions that you execute from Engagement Cloud.

Once you change the status of the SR in Engagement Cloud, the incident status automatically gets updated in Oracle Service Monitoring for Connected Assets.

The following topics discuss integration between Oracle Service Monitoring for Connected Assets and Engagement Cloud:

- Enable Oracle Engagement Cloud Integration
- Import Assets from Asset Information Management
- Configure Rules to Generate Automatic Service Requests
- Diagnose and Troubleshoot Connected Assets from Engagement Cloud
- Verify Incident and SR Status Update in Oracle Service Monitoring for Connected Assets

Enable Oracle Engagement Cloud Integration

Use the Settings page in Oracle Service Monitoring for Connected Assets to enable integration with Engagement Cloud.

Oracle Service Monitoring for Connected Assets can import assets from the Oracle CX Cloud Suite Asset Information Management (AIM).

To export incidents, Oracle Service Monitoring for Connected Assets connects to Engagement Cloud through the Oracle Integration Cloud Service.
1. In Oracle Service Monitoring for Connected Assets, click Menu (☰), and click the Previous ( 返回) icon to the left of your current organization name.
2. Click Configuration.
3. Click the Settings tab ( ⚙).
4. In the Integrations section, select Oracle Engagement Cloud Service.
5. Under Asset Information Management (AIM), specify the credentials to connect to the Asset Information Management (AIM) in your Oracle CX Cloud Suite.
   a. Specify the Endpoint URL for connecting to the AIM.
   b. Specify the User Name to connect to the AIM.
   c. Specify the Password to connect to the AIM.
6. Under Oracle Integration Cloud Service, specify the credentials to connect to the Oracle Integration Cloud Service instance.
   a. Specify the Endpoint URL for connecting to Oracle Integration Cloud Service.
   b. Specify the User Name to connect to Oracle Integration Cloud Service.
   c. Specify the Password to connect to Oracle Integration Cloud Service.
7. You can download the ICS par file if you need to configure your Oracle Integration Cloud Service instance to connect to Oracle Engagement Cloud.

   In Oracle Integration Cloud Service, you need to import the package (ICS par file) downloaded from Oracle Service Monitoring for Connected Assets. You can do this from the Menu, Designer, Packages page under Integrations.
   You can then navigate to the Connections page and configure the new connections that are created by providing the connection URL for Engagement Cloud and the integration user credentials.

Import Assets from Asset Information Management

Use the Assets page to import assets from the Oracle CX Cloud Suite Asset Information Management (AIM) into Oracle Service Monitoring for Connected Assets.

1. In Oracle Service Monitoring for Connected Assets, Click the Menu (☰) icon.
2. Click Assets.
3. Click the Import ( 🔗) icon adjacent to the Assets page title.
4. Search for the AIM assets to import using the criteria of your choice.
   a. Select Name, Type (Item in AIM), or Organization Code from the Search By list.
   b. Specify the corresponding Name, Type, or Organization Code value in the Search Value field.
   c. Click Search to search for assets using the criteria you specified.
5. Select the assets to import from the search results.
6. Click Import to import the selected assets into Oracle Service Monitoring for Connected Assets.
The selected assets are imported into Oracle Service Monitoring for Connected Assets. Note that the asset types for the imported assets are derived from the asset data in AIM.

You may next want to associate sensor devices to the imported assets:

1. Edit the asset type to add the required device model and sensor attributes. See Edit an Asset Type for more information on editing asset types.
2. Edit the assets to add the sensor devices. See Edit Asset Details for more information on editing assets.

Configure Rules to Generate Automatic Service Requests

Configure rules to automatically create service requests in Engagement Cloud when an incident is created for an imported asset in Oracle Service Monitoring for Connected Assets.

When creating incident rules in Oracle Service Monitoring for Connected Assets, an additional field appears for assets imported from Asset Information Management (AIM).

If you are creating a rule to generate an incident for an imported asset, click Create Service Request in Oracle Engagement Cloud to automatically create a corresponding service request in Oracle Engagement Cloud.

When an incident for an imported asset appears on the Incidents page, you can go to the Edit page of the incident to view the corresponding Engagement Cloud incident ID and status.

For basic information on using rules in Oracle Service Monitoring for Connected Assets, refer to Use Rules to Monitor and Maintain Assets.

Diagnose and Troubleshoot Connected Assets from Engagement Cloud

When an incident gets created for an imported asset in Oracle Service Monitoring for Connected Assets, the incident rule automatically creates a corresponding service request (SR) in Engagement Cloud.

Oracle Service Monitoring for Connected Assets provides tight integration with Engagement Cloud. You can not only sync incidents to Engagement Cloud, but also take asset actions, and set asset attributes from Engagement Cloud. Diagnostics let you see a graphical plot of your asset sensor attributes and the results of the actions that you execute from Engagement Cloud.

Once you change the status of the SR in Engagement Cloud, the incident status is automatically updated in Oracle Service Monitoring for Connected Assets.

The Connected Asset tab for a service request lets you view information reported by the asset, query the asset for additional information, and remotely execute actions that are available for the asset.

The following image shows the Connected Asset tab for the Edit Service Request page.
The Actions and Attributes section on the Connected Asset page lets you view the attributes of the connected asset, remotely update the available values, and execute available actions, for troubleshooting and diagnosis. If you have defined an asset action for your asset in Oracle Service Monitoring for Connected Assets, then it is available for use in Engagement Cloud. For example, a connected refrigerator might have an action defined to cycle the power, and might let you remotely set the attribute for the target temperature to any value between 35 and 39 degrees.

You can do the following:

- To execute an action on the connected asset, select an action from the Asset Actions list, and click Execute Action.
- To modify the attribute values, edit the values and click Update Attribute.

The IoT Incident Details section on the Connected Asset page displays the Oracle Service Monitoring for Connected Assets incident details for which this SR is created.

The Diagnostics section on the Connected Asset page lets you review the graphical data reported from the asset sensors. For example, with a connected refrigerator, you might notice that the temperature started increasing a few data points after the motor slowed to half speed. Reviewing this data enables you to focus on why the motor slowed, as the root cause of the issue. You can view up to 200 data points at a time in the line graph, as follows:

- To view data for a specific duration, enter or select the start date and time from which you want to view the data, in the Display 200 Data Points From field.
- To navigate to the previous and next set of 200 data points, click the Previous and Next arrow icons.
- To view the earliest available diagnostic data from Oracle Service Monitoring for Connected Assets, click the Show earliest data icon.
- To view the latest available diagnostic data from Oracle Service Monitoring for Connected Assets, click the Show most recent data icon.
- To view the data stream centered on the time the incident was created in Oracle Service Monitoring for Connected Assets, click the Show data from time of incident creation icon.
- To hide a sensor attribute within the graph, click the sensor attribute name on the graph. To view the sensor attribute, click the sensor attribute name again.
You can update the status of the SR in Engagement Cloud in the Status field of the Service Request Summary page. If you set the status to In Progress, the corresponding incident in Oracle Service Monitoring for Connected Assets changes from New to Work in Progress. When you change the status to Resolved, the status changes to Resolved in Oracle Service Monitoring for Connected Assets as well.

Verify Incident and SR Status Update in Oracle Service Monitoring for Connected Assets

When you make changes to the status of an SR in Engagement Cloud, the associated incident status is automatically updated in Oracle Service Monitoring for Connected Assets.

You can verify the updated status of the incident from the Incidents page.

1. To open the Incidents page, click Incidents ( ) in the Operations Center menu bar. The incidents applicable for your current context appear. You can change your context from the breadcrumbs to navigate to a different group, subgroup, or asset.

2. Use one of the following methods to verify the status of your incident:
   • Check the Status column value corresponding to the incident in the Incidents table.
   • Search for your incident using incident filters. See Search for Incidents Using Filters for more details about searching specific incidents in the Incidents page.

You can also verify the updated work order status in Oracle Service Monitoring for Connected Assets from the Edit Incident page.

Integrate Oracle Service Cloud with Oracle Service Monitoring for Connected Assets

Integrate Oracle Service Monitoring for Connected Assets with Oracle Service Cloud to allow Oracle Service Monitoring for Connected Assets to access Oracle Service Cloud data.

Note:

This integration is available only for Oracle Service Monitoring for Connected Assets, it isn’t available in the standard version of Oracle IoT Asset Monitoring.

1. Download the Iot_Svcs.par file:
   a. Log in to the Oracle Service Monitoring for Connected Assets instance.
   b. Click Menu ( ), and click the Previous ( ) icon to the left of your current organization name.
   c. Click Configuration.
d. Click the Settings tab.

e. Expand Oracle Service Cloud in the Integrations area.

f. Select Oracle Service Cloud.

g. Enter the email address for incident notifications in the Primary Contact for Incidents field.

h. Click Download, browse to a location to save the Iot_Svcs.par file, and then click Save.

2. Log in to Oracle Integration Cloud Service:

   a. Open a web browser, enter the URL for your Oracle Integration Cloud Service instance in the address field, and then press Enter.

   b. Enter your user name and password and then click Sign In.

3. Click Integrations.

4. Click the Menu (Ξ) icon next to Oracle Integration Cloud, click Designer, and then click Packages.

5. Import the Iot_Svcs.par file:

   a. Click Import.

   b. Click Browse and browse to the location of the .par file you downloaded in step 1.

   c. Double-click the Iot_Svcs.par file.

   d. Click Import.

6. Click the Menu (Ξ) icon next to Oracle Integration Cloud, click Designer, and then click Connections.

7. Set up the Iot-Svcs RightNow Connection:

   a. Select the Iot-Svcs RightNow Connection.

   b. Click the Menu (Ξ) icon and then select Edit.

   c. Click Configure Connectivity.

   d. Complete the Connection URL field. Use this format: https://<ServiceInstanceHostName>/cgi-bin/<yourinterface>.cfg/services/soap?wsdl=typed

   e. Click OK.

   f. Click Configure Security.

   g. Complete the Username, Password, and Confirm Password fields.

   h. Click Save.

8. Set up the Iot-Svcs dev Connection:

   a. Select the Iot-Svcs dev Connection.

   b. Click the Menu (Ξ) icon and then select Edit.

   c. Click Configure Connectivity.

   d. Select a connection type in the Connection Type list.
e. Select a TLS version in the **TLS Version** list.

f. Complete the **Connection URL** field. Use this format: https://<ServiceInstanceHostName>/services/rest/connect/v1.3

g. Click **OK**.

h. Click **Configure Security**.

i. Complete the **Username**, **Password**, and **Confirm Password** fields.

j. Click **OK**.

k. Click **Save**.

9. Click the **Menu** icon next to Oracle Integration Cloud, click **Designer**, and then click **Integrations**.

10. Select **iotSvcsIncidentGetInteg** and then click the slider to activate the integration.

11. Repeat step 10 to activate these integrations:
   - iotSvcsStatusTypeName
   - iotSvcsBulkIncidentQuery
   - Create SVCS INCIDENT
   - Sales-Product-To-AssetType-Integration
   - SearchContact
   - SvcS Asset Creation
   - SvcsRightNowInteg4Exp
   - UpdateIncident

12. Log out of Oracle Integration Cloud Service.

13. Complete the Oracle Integration Cloud Service settings:
   a. Log in to the Oracle Service Monitoring for Connected Assets instance.
   b. Click **Menu**, and click the **Previous** icon to the left of your current organization name.
   c. Click **Configuration**.
   d. Click the **Settings** tab.
   e. Expand **Oracle Integration Cloud Service Configuration**.
   f. Enter the URL for the Oracle Integration Cloud Service instance in the **Endpoint URL** field.
   g. Enter the user name for the Oracle Integration Cloud Service instance in the **User Name** field.
   h. Enter the password for the Oracle Integration Cloud Service instance in the **Password** field.
Integrate Oracle Enterprise Asset Management with Oracle IoT Asset Monitoring Cloud Service

You can sync assets between Oracle Enterprise Asset Management and Oracle IoT Asset Monitoring Cloud Service. Configure rules to automatically create work orders in Oracle Enterprise Asset Management when an incident is created in Oracle IoT Asset Monitoring Cloud Service.

Oracle Enterprise Asset Management (eAM) is part of Oracle's E-Business Suite and addresses the comprehensive and routine asset maintenance requirements of asset intensive organizations. Using eAM, organizations can efficiently maintain both assets, such as vehicles, cranes and HVAC systems, as well as rotatable inventory items, such as motors and engines. To measure performance and optimize maintenance operations, all maintenance costs and work history are tracked at the asset level.

You can choose to select and sync assets in Oracle Enterprise Asset Management with Oracle IoT Asset Monitoring Cloud Service. Once imported into Oracle IoT Asset Monitoring Cloud Service, you can associate these assets with the appropriate IoT sensors.

When creating incident rules for your imported assets, you can configure the rules to automatically create corresponding work orders in the eAM system. The incident details in Oracle IoT Asset Monitoring Cloud Service include the work order details created in Oracle Enterprise Asset Management.

When you update the work order in Oracle Enterprise Asset Management, the corresponding incident status in Oracle IoT Asset Monitoring Cloud Service is automatically updated.

The integration of Oracle IoT Asset Monitoring Cloud Service with eAM provides the following benefits:

- Lets you map the enterprise assets, stored in your eAM system, with field devices and sensors.
- Lets you leverage the features of Oracle IoT Asset Monitoring Cloud Service, such as real-time tracking and monitoring of connected assets.
- Lets you initiate work orders in the eAM system for incidents coming from Oracle IoT Asset Monitoring Cloud Service.

Enable the Integration in Oracle Enterprise Asset Management

Oracle Internet of Things (IoT) Asset Monitoring Cloud Service integration is available in Oracle E-Business Suite (EBS) releases 12.1.3, 12.2.6, and above.

You must ensure that you have the correct EBS-IoT integration patch installed for your Oracle E-Business Suite product. Release 12.1.3 requires patch 25040001 and release 12.2.6 requires patch 25755699. For the latest release, patch details, and installation steps, see Doc ID 2252316.1 on My Oracle Support.
Sync Assets from Oracle Enterprise Asset Management

Use the Assets search page in Oracle Enterprise Asset Management (eAM) to search and sync assets with Oracle IoT Asset Monitoring Cloud Service.

Search for your assets using criteria such as Asset Category or Asset Number. Click Sync Assets to sync the assets returned in the search results.

The synced assets now appear in Oracle IoT Asset Monitoring Cloud Service. The corresponding asset types for the synced assets are also created. The asset types are derived from the asset data in eAM.

You may next want to associate sensor devices with the imported assets:

1. Edit the asset type to add the required device model. See Edit an Asset Type for more information on editing asset types.
2. Edit the assets to add the sensor devices. See Edit Asset Details for more information on editing assets.

Configure Rules to Generate Automatic Work Orders

Configure rules to automatically create work orders in Oracle Enterprise Asset Management (eAM) when an incident is created in Oracle IoT Asset Monitoring Cloud Service.

When creating incident rules in Oracle IoT Asset Monitoring Cloud Service, an additional Work Order section appears for assets imported from eAM.

If you are creating a rule to generate an incident for an imported asset, click Generate Work Order and specify a Work Order Name for the work order that gets created in the eAM system.
For basic information on using rules in Oracle IoT Asset Monitoring Cloud Service, refer to Use Rules to Monitor and Maintain Assets.

Verify and Update the Work Orders Created in Oracle Enterprise Asset Management

When an incident is created for an imported asset in Oracle Internet of Things (IoT) Asset Monitoring Cloud Service, the incident rule automatically creates the corresponding work order in Oracle Enterprise Asset Management.

You can verify the work order details in both Oracle IoT Asset Monitoring Cloud Service and Oracle Enterprise Asset Management.

To verify the work order details in Oracle IoT Asset Monitoring Cloud Service:

1. Open the Incidents page. Click Incidents ( ) in the Operations Center menu bar. The incidents applicable for your current context appear. You can change your context from the breadcrumbs.

2. Click the Edit icon ( ) against the reported incident.

   The Edit Incident page shows additional fields corresponding to the work order created in Oracle Enterprise Asset Management. The WorkOrder and WorkOrderStatus fields display the work order name and status respectively.

You can also verify and update the work order under the Work Orders tab in Oracle Enterprise Asset Management. When you change the status of a work order in Oracle Enterprise Asset Management, the status of the incident in Oracle IoT Asset Monitoring Cloud Service is automatically updated. For example, when you release a work order in Oracle Enterprise Asset Management, the status of the corresponding incident in Oracle IoT Asset Monitoring Cloud Service changes from New to Open. When you close or cancel a work order, the status for the associated incident changes to Withdrawn.
Verify Incident and Work Order Status Update in Oracle IoT Asset Monitoring Cloud Service

When you change the status of a work order in Oracle Enterprise Asset Management, the associated incident status is automatically updated in Oracle Internet of Things (IoT) Asset Monitoring Cloud Service.

1. To open the Incidents page, click **Incidents** in the Operations Center menu bar. The incidents applicable for your current context appear. You can change your context from the breadcrumbs.

2. Use one of the following methods to verify the status of an incident:
   - In the Incidents table, view the **Status** column value that corresponds to the incident.
   - Search for the incident by using incident filters.

You can also verify the updated work order status in Oracle IoT Asset Monitoring Cloud Service from the Edit Incident page.

Integrate with Oracle Analytics Cloud

Oracle IoT Asset Monitoring Cloud Service lets you sync asset, metric, and incident data with Oracle Analytics Cloud. You can use analyses, projects, and dashboards in Analytics Cloud to find the answers that you need from key IoT asset data displayed in graphical formats.

Note:
The Oracle Analytics Cloud Integration is currently available for testing purposes in development environments, and should not be used in production environments. The functionality, compatibilities, interfaces, and APIs are subject to change.

An analysis is a query against your organization’s IoT asset data that provides you with answers to business questions. For example, you may want to know the asset-wise incident numbers. Analyses enable you to explore and interact with information visually in tables, graphs, pivot tables, and other data views. You can also save, organize, and share the results of analyses with others.

A project enables you to dynamically explore multiple data sets in graphical way, all within a single interface. So, for example, you can combine the asset, metric, and incident data sets in a project. You can upload data from many commonly used data sources to create robust sets of information within project visualizations.

Dashboards can include multiple analyses to give you a complete and consistent view of your company’s information across all departments and operational data sources. Dashboards provide you with personalized views of information in the form of one or more pages, with each page identified with a tab at the top. Dashboard pages display anything that you have access to or that you can open with a web browser including...
analyses results, images, text, links to websites and documents, and embedded content such as web pages or documents.

For detailed information on Analytics Cloud, refer to the Oracle Analytics Cloud Help Center Resources.

Enable Oracle Analytics Cloud Integration

Use the Settings page in Oracle IoT Asset Monitoring Cloud Service to enable integration with Oracle Analytics Cloud.

1. In Oracle IoT Asset Monitoring Cloud Service, click **Menu (≡)**, and click the **Previous (🪐)** icon to the left of your current organization name.

2. Click **Configuration**.

3. Click the **Settings** tab (⚙).

4. In the Integrations section, click **Oracle Analytics Cloud Integration**.

5. Select the **Oracle Analytics Cloud Enabled** option, and specify the connection details for your Oracle Analytics Cloud instance.
   
   a. Specify the **Endpoint URL** for connecting to Analytics Cloud. Use the following format: `http://hostname:port`.
   
   b. Specify the **User Name** to connect to Analytics Cloud.
   
   c. Specify the **Password** for the Analytics Cloud user.

6. Click **Sync Data to OAC** to sync the asset, metric, and incident data with your Analytics Cloud instance.

   The default sync interval between Oracle IoT Asset Monitoring Cloud Service and Oracle Analytics Cloud is one hour. However, you can manually sync the data at any time.

7. (Optional) Under Download OAC Project, click **Download** if you wish to save a sample Analytics Cloud project that you can later import into your Analytics Cloud instance.

   The sample project contains sample data sets and visualizations based on the IoT asset, metric, and incident data.

   You can import the sample project into your Oracle Analytics Cloud instance to look at how the various IoT data sets can be joined, used to perform analyses, and create visualizations.

8. (Optional) Click **Download CSV Data** to download a zip file containing the **csv** (comma-separated value) files for your asset, metric, and incident data.

   You may want to download the csv data to keep historical records that you can later import and analyze in Analytics Cloud.

   You can import the **csv** files into your Analytics Cloud instance as data set files.

Import the Sample Project in Analytics Cloud

You can import the sample project downloaded from the Settings page in Oracle IoT Asset Monitoring Cloud Service into Analytics Cloud.
1. If not done already, download the Analytics Cloud project file from the Settings page of Oracle IoT Asset Monitoring Cloud Service.

   Under Download OAC Project, click Download. See Enable Oracle Analytics Cloud Integration for more information.

2. In Oracle Analytics Cloud, click Page Menu in the Projects page.

3. Click Import.

4. Select the .dva file that you downloaded from Oracle IoT Asset Monitoring Cloud Service, and click Import.

   A confirmation message appears.

5. Double click the imported project on the Projects page to open it.

   You can next inspect the various data sets, calculations, data diagrams, and visualizations included in the project.

For more details on working in Oracle Analytics Cloud, refer to the Analytics Cloud Documentation.

Create a New Project in Analytics Cloud Using IoT Data

After you have enabled Analytics Cloud integration in Oracle IoT Asset Monitoring Cloud Service, you can use the synchronized asset, metric, and incident data sets to perform data analyses and create dashboards in Analytics Cloud.

1. From the Oracle Analytics Cloud home page, click Create and choose Project.

   You can also choose to click Create from the Project page.

   The Add Data Set Dialog appears.

2. Choose one or more data sets synchronized from Oracle IoT Asset Monitoring Cloud Service.

   The following data sets are available from Asset Monitoring:

   - **IoTAMAssets**: Contains IoT asset data from Oracle IoT Asset Monitoring Cloud Service.
• **IoTAMIncidents**: Contains IoT incident data from Oracle IoT Asset Monitoring Cloud Service.

• **IoTAMMetrics**: Contains IoT metrics (or KPIs) data from Oracle IoT Asset Monitoring Cloud Service.

• **IoTAMAssetTypes**: Contains IoT asset type data from Oracle IoT Asset Monitoring Cloud Service.

You can also create joins between two or more data set tables in Oracle Analytics Cloud to create visualizations on related data.

3. Prepare your data and use the data to create visualizations and narrations.

You can create calculated columns in your data set tables. You can also create joins between two or more data set tables in Oracle Analytics Cloud to create visualizations on related data.

**Tip:** You may often want to connect the asset and incident data to create reports, such as *Incident report by Assets*. You may want to link the asset identifiers present in the `id` field of the Assets table to the asset ids present in the `contextInformation` field of the Incidents table. You can make use of various functions, such as `Split` and `Replace` to extract information from complex columns. You can also refer to the data diagram in the sample project for ideas.

Refer to Oracle Analytics Cloud documentation for detailed information on Visualizing Data and Building Reports in Oracle Analytics Cloud.

### Use Asset Monitoring Widgets in Your Application

Oracle IoT Asset Monitoring Cloud Service provides a set of pages as widgets that you can embed in your application or Web page.

The following pages are available as widgets:

- Map Page
- Assets Page
- Asset Details Page
- Incidents Page

### Add an Asset Monitoring Widget to Your Application or Web Page

You can copy the URL of an available widget, or copy the embed code for the widget to include it in your application or Web page.

1. Log in to your Oracle IoT Asset Monitoring Cloud Service instance.

2. Navigate to the following URL using the address bar in your browser:

   `Your_AM_URL/syndicatedWidgetExamples.html`

   Here, `Your_AM_URL` is the URL of your Oracle IoT Asset Monitoring Cloud Service instance.

   For example: `https://myAMhost/am/syndicatedWidgetExamples.html`

   The Asset Monitoring Syndicated Widgets Examples page appears.

3. Click **Copy URL** against an available widget to copy the URL for the widget.
4. Click **Copy Embed Code** against an available widget to copy the code that you can embed in your application.

For example:

```html
<iframe src="https://my_am_host/commonui/indexWidget.html?app=AM&root=incidents" width=880px, height=600px></iframe>
```

The code includes the `iframe` element to include in your HTML page or application.

You can now paste the copied URL or code into your page or application.
Use the Oracle Internet of Things Asset Monitoring Mobile Application

Use the Oracle Internet of Things Asset Monitoring Mobile Application to manage and monitor assets on a mobile device.

Topics

• How to Access the Oracle Internet of Things Asset Monitoring Mobile Application
• View Asset Details in the Oracle Internet of Things Asset Monitoring Mobile Application
• Edit Asset Details in the Oracle Internet of Things Asset Monitoring Mobile Application
• Add a New Sensor to an Asset in the Oracle Internet of Things Asset Monitoring Mobile Application
• View Asset Connectivity, Utilization, and Availability in the Oracle Internet of Things Asset Monitoring Mobile Application
• View Sensor Data in the Oracle Internet of Things Asset Monitoring Mobile Application
• Set the Asset Location in the Oracle Internet of Things Asset Monitoring Mobile Application
• View the Asset Location History in the Oracle Internet of Things Asset Monitoring Mobile Application
• View the Oracle Internet of Things Asset Monitoring Mobile Application Version Information
• Log Out of the Oracle Internet of Things Asset Monitoring Mobile Application

How to Access the Oracle Internet of Things Asset Monitoring Mobile Application

Use the Oracle Internet of Things Asset Monitoring Mobile Application to manage and monitor your Oracle IoT Asset Monitoring Cloud Service assets on a mobile device. Before you log in to the Oracle Internet of Things Asset Monitoring Mobile Application, you must have a user account and know the URL of the Oracle IoT Asset Monitoring...
Cloud Service server. Oracle provides user account information when you subscribe to Oracle IoT Asset Monitoring Cloud Service.

Note:
If you have previously installed the Oracle Internet of Things Asset Monitoring Mobile Application, complete steps 3 to 6 of the procedure to open the application.

1. Install the Oracle Internet of Things Asset Monitoring Mobile Application:
   a. Open an internet browser on your mobile Apple or Android device.
   b. Browse to the Apple App Store or Google Play.
   c. Search for Oracle IoT Asset Monitoring.
   d. Install the Oracle IoT Asset Monitoring application on your mobile device.

2. Open the Oracle Internet of Things Asset Monitoring Mobile Application and then read and agree to the legal terms.

3. Enter the Oracle IoT Asset Monitoring Cloud Service URL in the IoT Server URL field.

4. Enter the user name for the Oracle IoT Asset Monitoring Cloud Service server in the Username field.

5. Enter the password for the Oracle IoT Asset Monitoring Cloud Service server in the Password field.

6. Tap Login.

View Asset Details in the Oracle Internet of Things Asset Monitoring Mobile Application

View details about an asset, including its type, description, and registration history.

1. Tap the Menu (≡) icon, and then tap the Search (🔍) icon.
2. Tap an asset in the asset list.

3. Tap the Info (ℹ️) icon.
4. Tap the back icon (←) to return to the asset list.

Edit Asset Details in the Oracle Internet of Things Asset Monitoring Mobile Application

View details about an asset, including its type, description, and registration history.

1. Tap the Menu (≡) icon, and then tap the Search (🔍) icon.
2. Tap an asset in the asset list.

3. Tap the **Info** (ि) icon.

4. Tap the **Edit** (ँ) icon.

5. Edit the fields in the **Description** area.

6. Add or remove sensors.

7. Tap **Update**.

8. Tap **OK**.

---

**Add a New Sensor to an Asset in the Oracle Internet of Things Asset Monitoring Mobile Application**

Add a new sensor to an asset when an existing sensor is replaced.

1. Make sure the device that is being registered is on and connected to the Internet. The device being registered must be on the same subnet as the mobile device for UDP registration.

2. Open the Oracle Internet of Things Asset Monitoring Mobile Application on the mobile device. See How to Access the Oracle Internet of Things Asset Monitoring Mobile Application.

3. Tap the **Menu** (≡) icon, and then tap the **Search** (🔍) icon.

4. Tap an asset in the asset list.

5. Tap the **Edit** (ँ) icon.

6. Tap an existing sensor.

7. Tap the **Add** (+) icon.

8. Tap one of these options:
   - **Scan QR Code**: Select this option to use the device barcode to register the sensor.
   - **Manually Register Device**: Select this option to manually register the sensor.

9. If you are manually registering the device, complete these fields:
   - **Activation ID**: Enter the activation ID in the field. Typically, this the MAC address for the sensor your are registering.
   - **Passphrase**: Enter the password used to access the sensor settings. The password must be accepted by the device being registered.
   - **Name**: (Optional) Enter a unique name to quickly identify the sensor.
   - **Description**: (Optional) Enter a description for the sensor.
   - **Manufacturer**: (Optional) Enter the sensor manufacturer.
   - **Serial Number**: (Optional) Enter the sensor serial number.
- **Model Number**: (Optional) Enter the sensor model number.

10. Tap **Register**.
11. Tap **OK**.

**View Asset Connectivity, Utilization, and Availability in the Oracle Internet of Things Asset Monitoring Mobile Application**

View asset connectivity, utilization, and availability data to determine how an asset is performing.

1. Tap the **Menu** (☰) icon, and then tap the **Search** (🔍) icon.
2. Tap an asset in the asset list.

3. Tap the **Dashboard** (📊) icon.
4. Select a reporting period in the **Connectivity**, **Utilization**, or **Availability** areas.
5. Tap the back icon (↤) to return the asset list.

**View Sensor Data in the Oracle Internet of Things Asset Monitoring Mobile Application**

View sensor data to obtain a detailed view of the data being sent from the assets to Oracle Internet of Things Cloud Service.

1. Tap the **Menu** (☰) icon, and then tap the **Search** (🔍) icon.
2. Tap an asset in the asset list.

3. Tap the **Sensor** icon (📡).
4. Select a sensor in the **Sensor** list.
5. Select a data value in the **Value** list.
6. Tap the back icon (↤) to return the asset list.

**Set the Asset Location in the Oracle Internet of Things Asset Monitoring Mobile Application**

Set the location of an asset when it is moved to a different location.

1. Tap the **Menu** (☰) icon, and then tap the **Search** (🔍) icon.
2. Tap an asset in the asset list.

3. Tap the **Location** (/maps/232) icon.

4. Tap the **Set Location** (/maps/232) icon.

5. Drag the map until the **Target** (/maps/232) icon is centered on a new location.

6. Tap **Save**.

7. Tap **OK**.

---

**View the Asset Location History in the Oracle Internet of Things Asset Monitoring Mobile Application**

Set the asset location of an asset when it is moved to a different location.

1. Tap the **Menu** (/maps/232) icon, and then tap the **Search** (/maps/232) icon.
2. Tap an asset in the asset list.
3. Select a reporting period in the list.
4. Tap the slider to view specific dates and times the asset moved.
5. Tap the back icon (/maps/232) to return the asset list.

---

**View the Oracle Internet of Things Asset Monitoring Mobile Application Version Information**

View Oracle Internet of Things Asset Monitoring Mobile Application version information to determine if you are using the latest version of the software.

1. Tap the **Menu** (/maps/232) icon, and then tap the **Information** (/maps/232) icon.
2. Select one of these options:
   - Tap **Oracle Privacy Policy** to view the current privacy policy.
   - Tap **Legal Terms** to view the current terms of service.

---

**Log Out of the Oracle Internet of Things Asset Monitoring Mobile Application**

Log out of the Oracle Internet of Things Asset Monitoring Mobile Application when you are finished managing and monitoring assets.

1. Tap the **Menu** (/maps/232) icon, and then tap the **Information** (/maps/232) icon.
2. Tap **Logout**.