Oracle® Cloud

Using Oracle Internet of Things Asset Monitoring Cloud Service

23.3.1
E80558-42
July 2023

Oracle Cloud Using Oracle Internet of Things Asset Monitoring Cloud Service, 23.3.1

E80558-42

Primary Author: Oracle Corporation

Contents

3 Work with Your Assets

8 Use the Oracle Internet of Things Asset Monitoring Mobile Application

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

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

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

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 or visit 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
- *Getting Started with Oracle Cloud*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 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

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
- Ensure Asset Availability and Utilization

- Prevent Asset Theft and Misplacement
- Reduce Business Process Interruptions and Downtime
- Reduce Capital Expenditures

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.

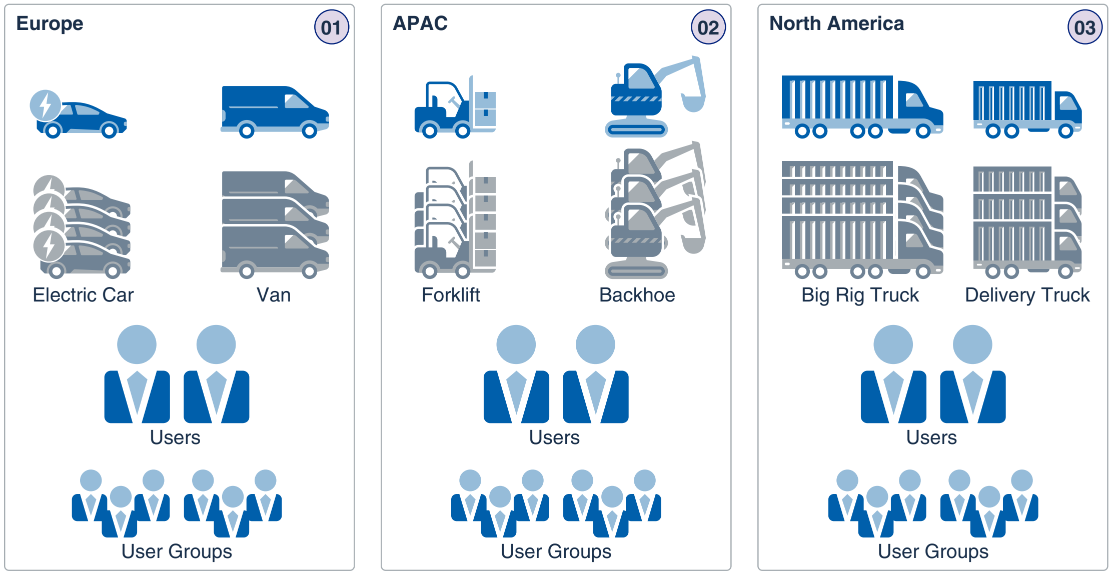
The following sections introduce some of the key building blocks of the Oracle IoT Asset Monitoring Cloud Service application:

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:

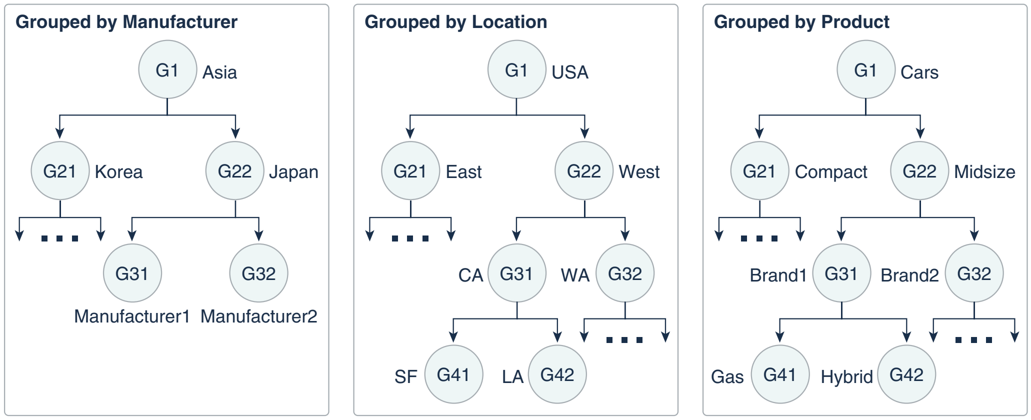
- Create a New Organization
- Create and Manage Users
- Change Your Current Organization
- The Operations Center

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 Type Associations
- Create Asset Type 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:

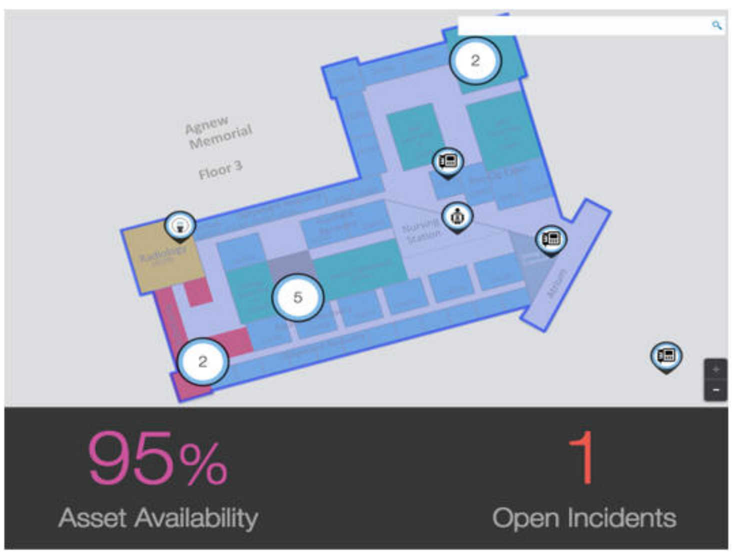
- Define Your Own Metrics
- Track Individual and Cumulative Asset Metrics Using Dashboards
- Track Asset Metrics in the Map View

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:



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 Intelligent Applications Cloud 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:

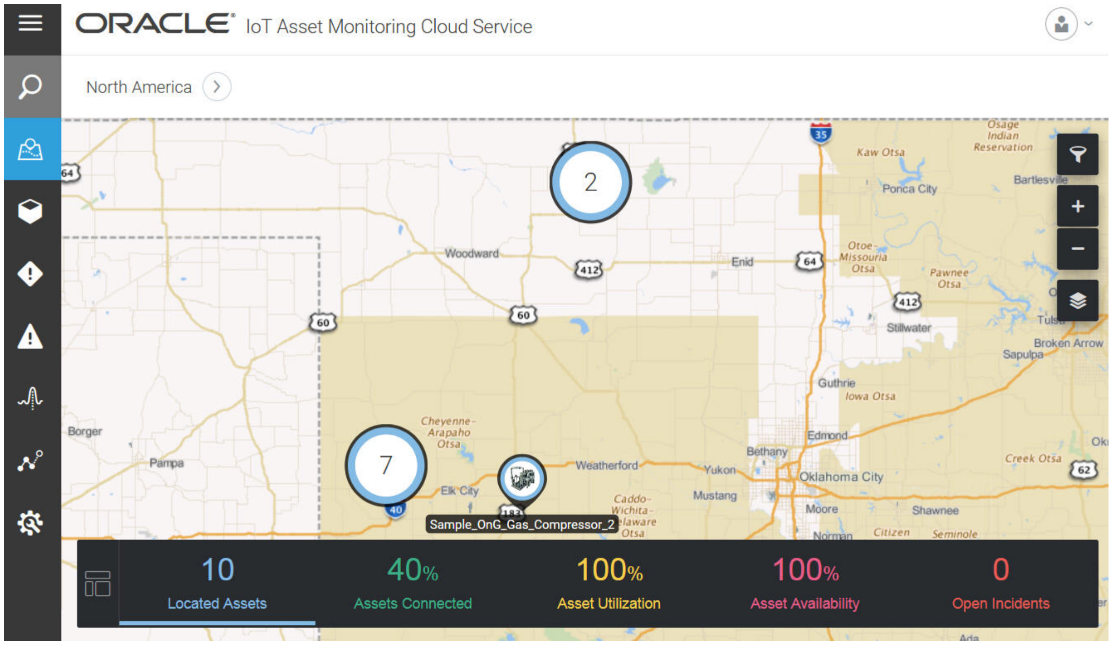
- Use Predictions to Identify Asset Risks
- Create a Prediction Based Rule

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:

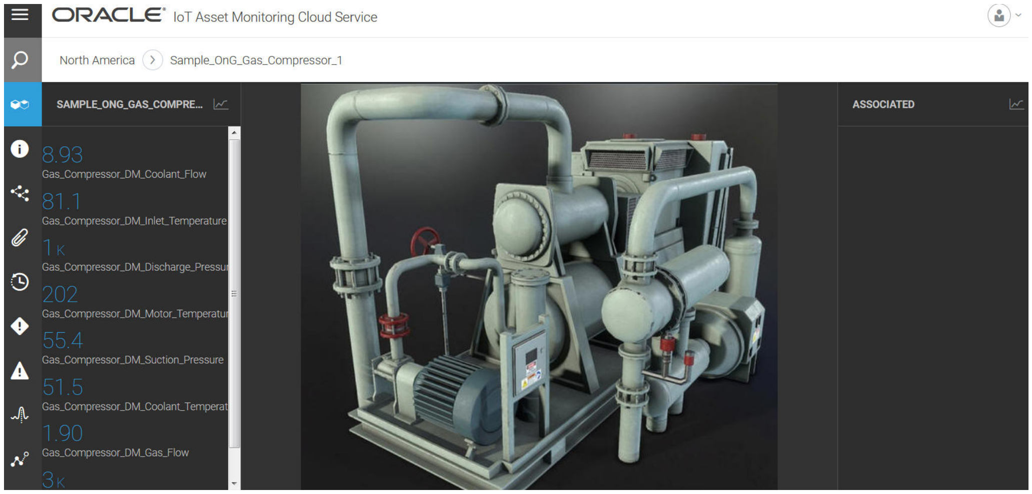


Here are some of the built-in KPI metrics that appear in the map view:

- **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.

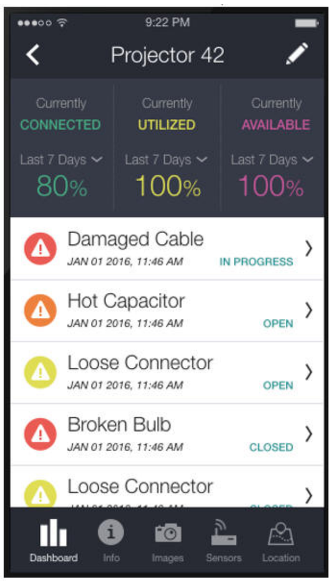
Oracle IoT Asset Monitoring Cloud Service provides the following interfaces:

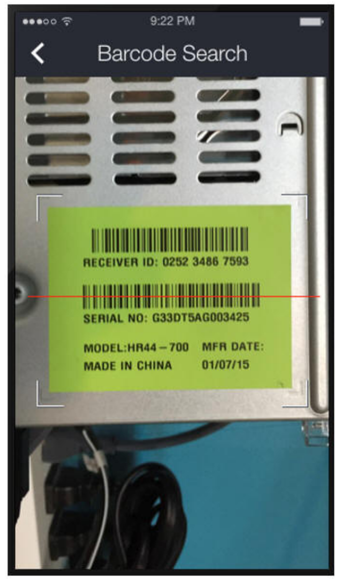
- **Browser Based Application:**

  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.

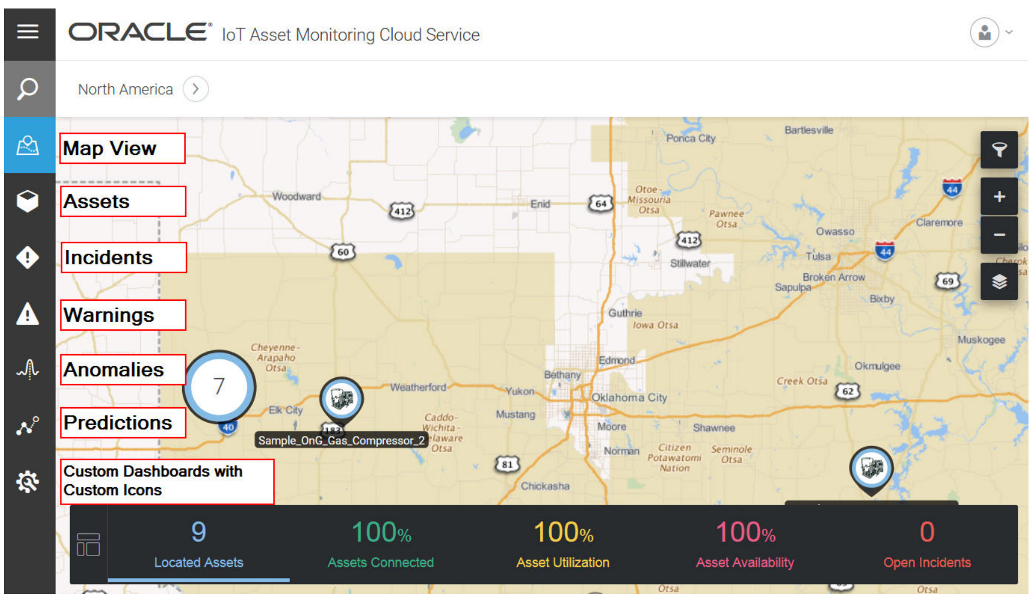
You can return to the operations center from any page by clicking **Menu** and selecting **Operations Center**.

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.

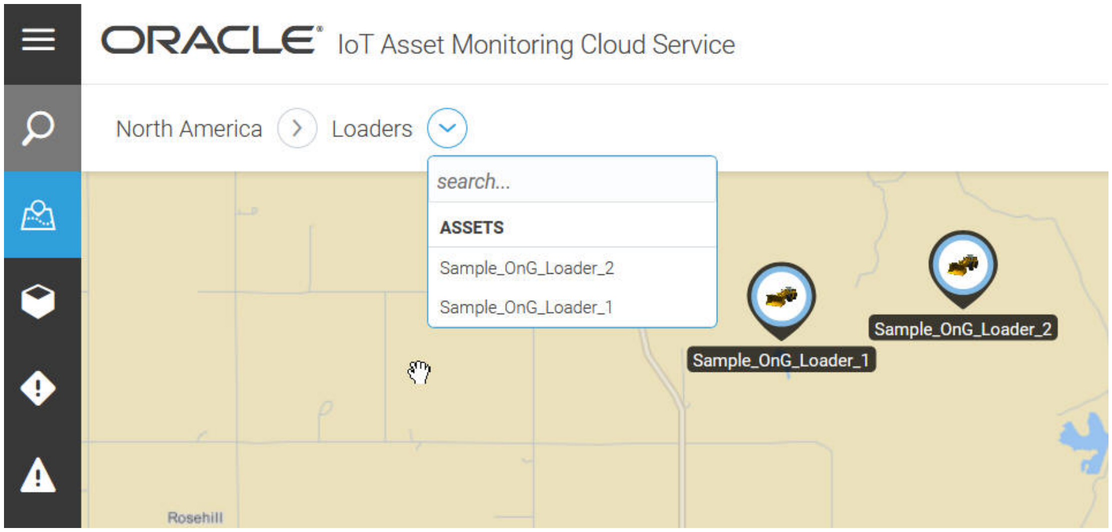
You are placed in the Map view by default. The toolbar on the left lets you access the following pages for the assets visible in the map:

- **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.



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.

The breadcrumbs maintain a trail of the pages and tabs that you used to navigate to a particular page. This trail helps you switch back to the tabs that you used at higher levels in the hierarchy. For example, if you used the **Assets** tab to navigate to the Digital Twin page for a particular asset, then you can use the breadcrumbs to switch back directly to the **Assets** tab without having to go through the **Map**.

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.

> **Note:**
>
> When you switch from the Operations Center to the Design Center, your context in Operations Center is preserved. For example, if you were viewing the Incidents page in Operations Center before navigating to the Design Center, then you automatically land on the Incidents page when you switch back to the Operations Center using the menu.

The design center contains the following pages:

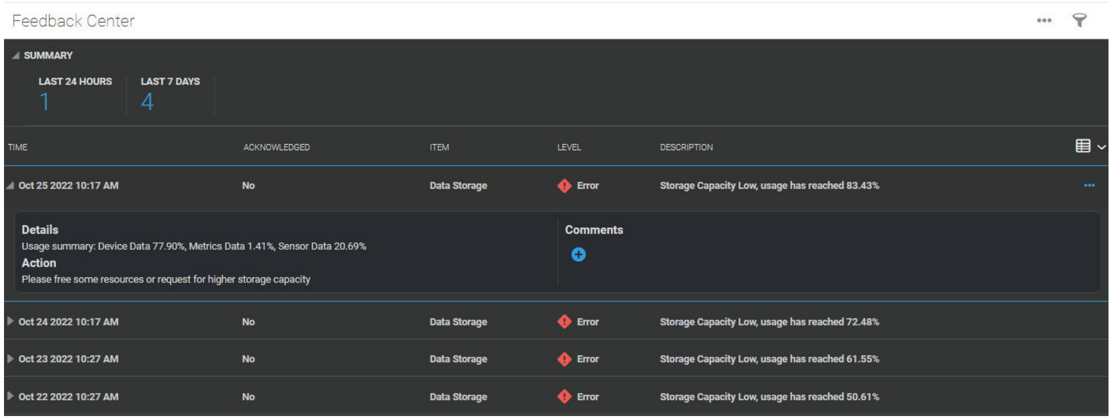
- **Organization:** Use the Organization page to create and edit organizations. You can change the list of users associated with an organization, add dashboards for the organization, and add notification subscribers for the organization.
  Use the Organization page to switch your current organization. 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.

The Feedback Center

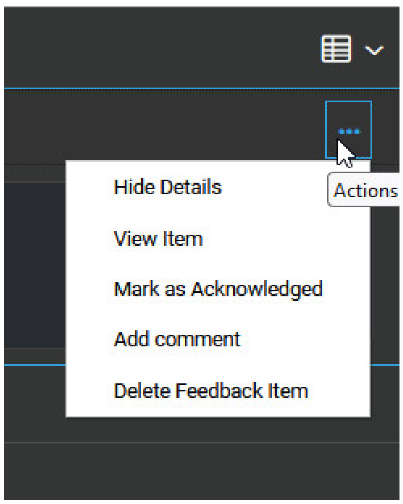
The Feedback Center notifies the administrator about system activity that may require administrator review and action.

For example, the system may need to notify you about storage capacity issues. Or the system may wish to report analytics issues, such as a metric computation being suspended, or a prediction-scoring failing two times in a row. The administrator can review the details for an event of interest, mark the issue as acknowledged, and choose to comment against the event with updates or remarks for other administrators.

When you first log in to the application, you are placed into the Operations Center for your organization. To access the Feedback Center, click **Menu** ≡, and then click **Feedback Center**.



Use the **Actions** menu against a feedback row to see the available options:



Create and Manage 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. 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.

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 your application.

1. In your IoT application, click **Menu** (), and then click **Settings**.

   If you are in the Design Center, you need to click **Previous** () before you see the **Settings** option in the menu.
2. Click **IoT Organizations**, and then click **Manage Organizations**.
3. Click **Create Organization** in the Manage Organizations page.

   The Create Organization dialog appears.
4. Specify a **Name** for your organization.

   For example, *North America Operations.*
5. Specify an optional **Description.**
6. Click **Create**.

   The new organization is created along with its required artifacts. The operation status appears on the IoT Organizations page until the organization is ready for use.

Change Your Current Organization

If you are part of more than one organization, then you can change your current organization in the application.

1. In your IoT application, click **Menu** (), and then click **Settings**.

   If you are in the Design Center, you need to click **Previous** () before you see the **Settings** option in the menu.
2. Click **IoT Organizations**, and then click **Manage Organizations**.
3. Click **Switch Organization** in the Manage Organizations page.
4. Under **Switch To**, select the organization name that you wish to change 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.

If you need to assign users to an organization other than your current organization, then make sure that you switch to the organization before performing the following steps. See Change Your Current Organization for more information on switching organization contexts.

1. In your IoT application, click **Menu** (), and then click **Settings**.

If you are in the Design Center, you need to click **Previous** ( ) before you see the **Settings** option in the menu.

2. Click **IoT Organizations**, and then click your organization name.
3. Click **User Access Control** on your organization page.
4. Under Users, select the users that you wish to include in the organization, and click the right-arrow icon ( ).

   The selected user moves to the list of authorized users.

   Tip: You can hold down the *Ctrl* key to select multiple users at a time.
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.

> **Note:**
>
> Import of organizations exported from previous releases is not supported. If you try to import a previously exported organization from an earlier release into the current release of Oracle IoT Asset Monitoring Cloud Service, the import may fail.

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, groups and places.

1. In your IoT application, click **Menu** ( ), and then click **Settings**.

   If you are in the Design Center, you need to click **Previous** ( ) before you see the **Settings** option in the menu.
2. Click **IoT Organizations**, and then click **Manage Organizations**.
3. Click **Export Organization** in the Manage Organizations page.

   The Export Organization dialog appears.
4. Select the **Organization** 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. In your IoT application, click **Menu** (), and then click **Settings**.

   If you are in the Design Center, you need to click **Previous** () before you see the **Settings** option in the menu.

2. Click **IoT Organizations**, and then click **Manage Organizations**.
3. Click **Import Organization** in the Manage Organizations page.

   The Import Organization dialog appears.

4. Under Upload File, click the **Drag and Drop** area to select a previously exported `.iot` archive file. Alternatively, you can also drag and drop the archive file to the **Drag and Drop** area in your browser window.
5. Click **Done.**

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, *Forklifts*, 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.

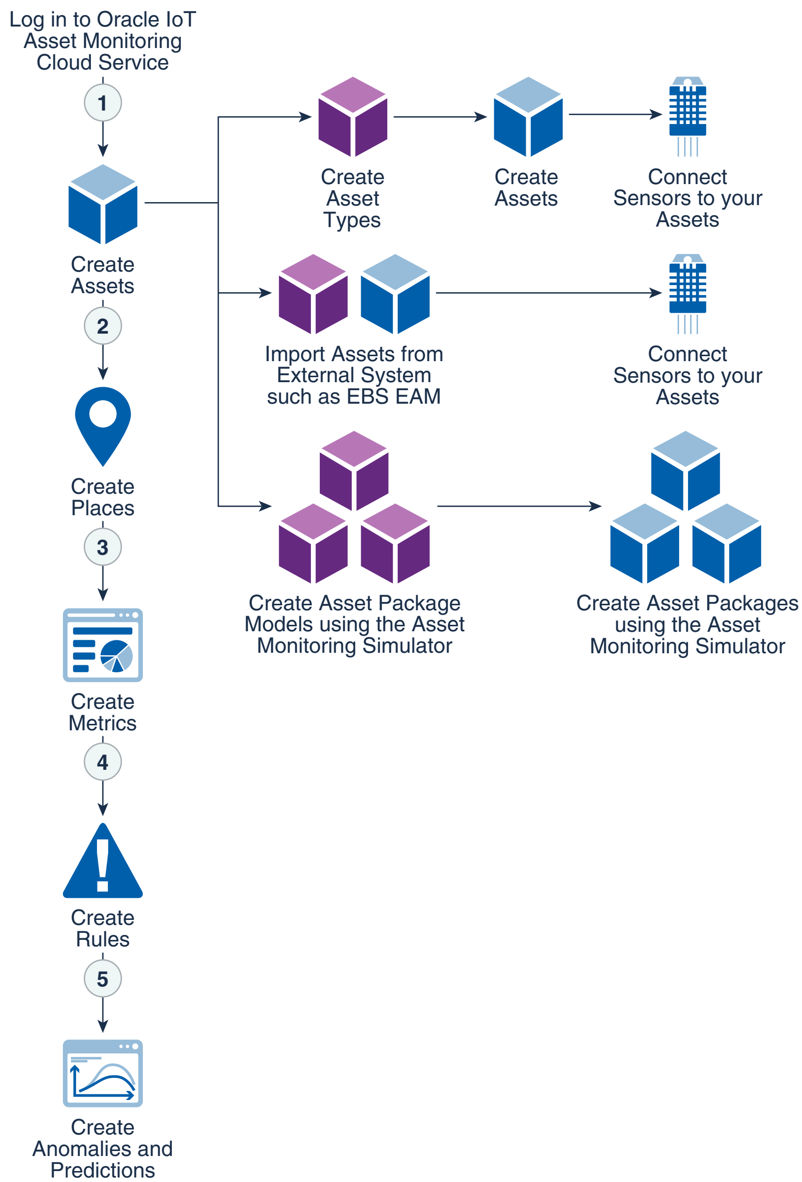
8. Click **Save** to save the new group.
9. Click **Back** to return to the Groups page.

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:



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

Task	Description	More Information
Assign the Device Models to the Cloud Service	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 Intelligent Applications Cloud Management Console.	Assign Device Models to the Oracle IoT Asset Monitoring Cloud Service Application
Create Assets	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.	Create and Manage Asset Types Create and Manage Assets
Create 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.	Create and Manage Places
Create Metrics/ KPIs	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.	Use Asset Metrics or Key Performance Indicators
Create 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

Task	Description	More Information
Create Anomalies and Predictions	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 Intelligent Applications Cloud 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.	Use Anomalies to Track Deviations in Asset Behavior Use Predictions to Identify Asset Risks

How to Get Support

Use these resources to resolve problems:

- Visit the Oracle Help Center at http://docs.oracle.com/en/.
- If you're an Oracle Premier Support Customer, visit My Oracle Support.
- Contact Oracle Technical Support. See Contacting Oracle Support in *Getting Started with Oracle Cloud*.

2

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 application users. Roles are a set of privileges assigned to a user.

Oracle IoT Intelligent Applications Cloud includes global and application-specific roles. Global roles apply across all your IoT applications, such as Asset Monitoring, Production Monitoring, Connected Worker, and Fleet Monitoring. Application specific roles are specific to a particular application, such as Asset Monitoring.

Oracle Identity Cloud Service provides a centralized identity store for your IoT 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.

Asset Monitoring uses the following roles:

- **Administrator (*IoTAdministrator*):** The administrator is responsible for the overall administration of the application. The Administrator role is a global superuser role applicable across Oracle IoT Intelligent Applications Cloud applications.

  The administrator sets up and maintains the application. The administrator:

  - Creates organizations.
  - Creates and manages users.
- **Asset Manager (*IoTAssetManager*):** The asset manager is responsible for life-cycle management and monitoring of asset instances. This includes defining asset types and their corresponding analytics artifacts, creating asset instances, and monitoring key metrics using dashboards. The asset manager has access to both the Design Center and Operations Center.

The asset manager, called operations manager in pre-22.1.1 releases, manages and ensures the day-to-day availability of assets. The asset manager:

- Defines groups.
- Defines asset types and related analytics artifacts.
- Creates asset instances.
- Accesses and manages dashboards.
- Accesses Digital Twin views, executes actions and *what-if* scenarios.
- Accesses and manages the asset inventory.
- Assigns assets to locations and jobs that require them.

> **Note:**
>
> Oracle Service Monitoring for Connected Assets uses the Service Asset Manager role in place of Asset Manager.

- **Technician (*IoTTechnician*):** The technician is responsible for the onboarding and management of entities. This includes creating entity instances and configuring device connections. The technician also performs troubleshooting, and has access to the entity inventory, Digital Twin views, and incident updates.

  The Technician role is a global role applicable across Oracle IoT Intelligent Applications Cloud applications. The technician:

  - Onboards/Removes entities.
    - Creates/Deletes entity instances.
    - Configures connectivity:
      - Creates connectors.
      - Downloads schemas.
      - Creates interpreters.
  - Troubleshoots issues.
  - Resolves incidents:
    - Views related rules.
  - Accesses Digital Twin views:
    - Executes actions, what-if scenarios
  - Accesses entity inventories.
  - Edits custom attributes.
- **Viewer (*IoTViewer*):**The Viewer has read-only access to IoT applications. The Viewer role is a global role applicable across Oracle IoT Intelligent Applications Cloud applications.

  The Viewer role was called User in pre-22.1.1 releases. A viewer can access the following entities in Operations Center:

  - Dashboards
  - Digital Twins

– Notifications

A non-admin application user must have explicit Viewer role to be able to log into the management console (`/ui`).

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 **Settings**.

   If you are in the Design Center, you need to click **Previous** (<) before you see the **Settings** option in the menu.

2. Click **User Management**.
3. Click **Create User** (+).
4. Under **ROLES**, select one or more of these roles for the user from the **Common** or **Asset Monitoring** section:
   - **Administrator**
   - **Asset Manager**
   - **Technician**
   - **Viewer**

   See Understand Roles and Users for detailed information on these application roles.

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** and close the window to return to the User Management page.

Make sure you assign the newly created user to the organization that the user should belong to. See Assign Users to an Organization for more information on assigning users to an organization. You can also assign a user to more than one organization.

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 **Settings**.

   If you are in the Design Center, you need to click **Previous** () before you see the **Settings** option in the menu.
2. Click **User Management**.
3. Click **Edit** () against the appropriate user row.
4. Make the necessary changes under the **ROLES**, **NAME**, **EMAIL** and **TELEPHONE** sections.
5. Click **Save** and close the window to return to the User Management 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 **Settings**.

   If you are in the Design Center, you need to click **Previous** () before you see the **Settings** option in the menu.
2. Click **User Management**.
3. Click **Filter** to open the Filters dialog.
4. Click **Add** () to add new filter criteria.
5. Choose one of these options in the 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).
6. Enter your search criteria in the field and then press **Enter**.
7. (Optional) Click **Add** () to add additional filter criteria.
8. (Optional) Click **Remove** () to remove a search criteria.

9. Click **Apply** to apply 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 **Settings**.

   If you are in the Design Center, you need to click **Previous** () before you see the **Settings** option in the menu.
2. Click **User Management**.
3. Click **Delete** () against the user that you wish to delete.
4. Click **Yes**.

3 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

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

Asset types define the templates for your assets. Each real-world asset must use an asset type.

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

The following built-in asset types appear in your organization:

- Transport Equipment
- Transport Item
- Transport Package

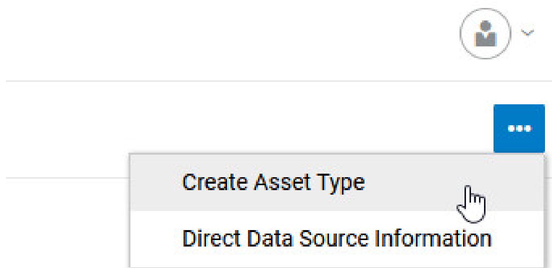
If you are using Fleet Monitoring to manage transportation and logistics, then you can use these asset types for asset-in-transit monitoring, such as for monitoring trailers and RTIs (Returnable Transport Items). You can also use the built-in asset types to monitor cargo conditions.

Oracle recommends that you do not edit the predefined sensor attributes for the transport asset types. You may, however, extend the asset types to create additional attributes if you so require.

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. Select **Create Asset Type** from the **Asset Types** menu.



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.

   If you have the 3D Digital Twin feature, then you can choose to upload and use 3D CAD models in place of asset images. To upload a pre-existing 3D model, click **Upload 3D Model**. See for more information on uploading 3D models.

6. Click **Upload Icon** to upload an icon for the asset type.

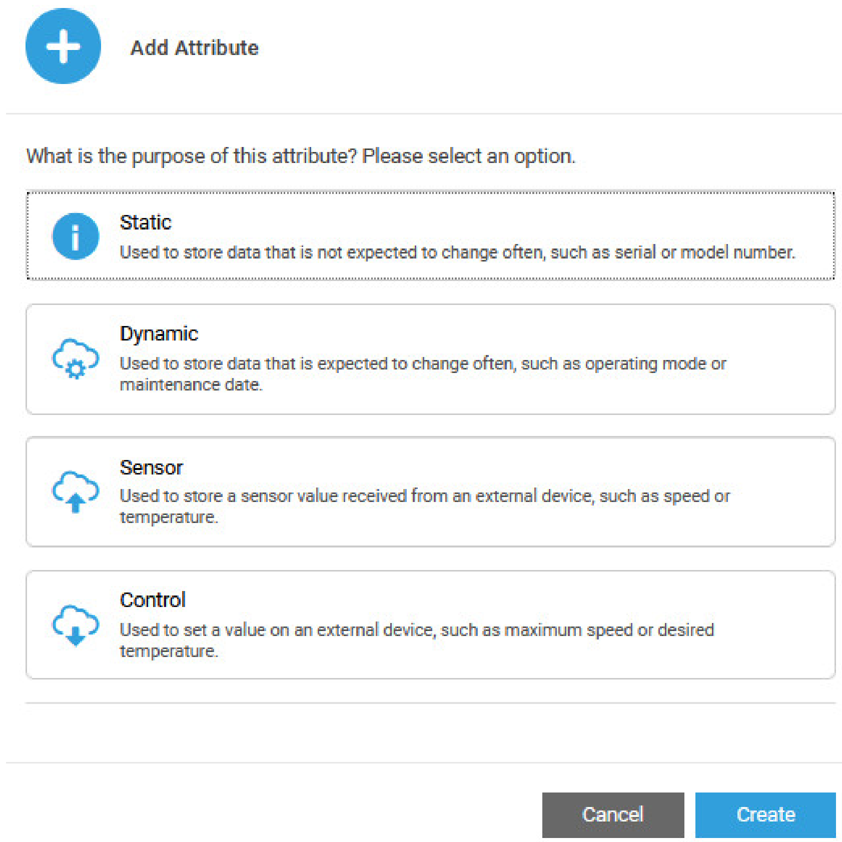
   An icon makes it easier to quickly identify the asset type in the map view.

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 Attributes: 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. Custom attributes can be of the following types:
  – **Static:** Static custom attributes are used to store data that is not expected to change often, such as the serial or model number of an asset.
  – **Dynamic:** Dynamic custom attributes can change often, such as the operating mode or maintenance date for an asset. You can use the operations center, or automatic action-based rules to update the dynamic attribute values.
- **Sensor:** 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.
- **Control:** A control attribute lets you send data back from your digital twin to the actual device. Use control attributes to set the actuator attribute values for your IoT devices. For example, if an HVAC device supports the *Desired_Temperature* attribute, you can set the attribute from your IoT application.

> **Note:**
>
> Control attributes can be currently used for sending MQTT data back to devices using direct ingestion.

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

e. (Optional) Add a **Description** about the attribute.

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

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

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) For static and dynamic attributes, specify a **Default** value of the attribute.

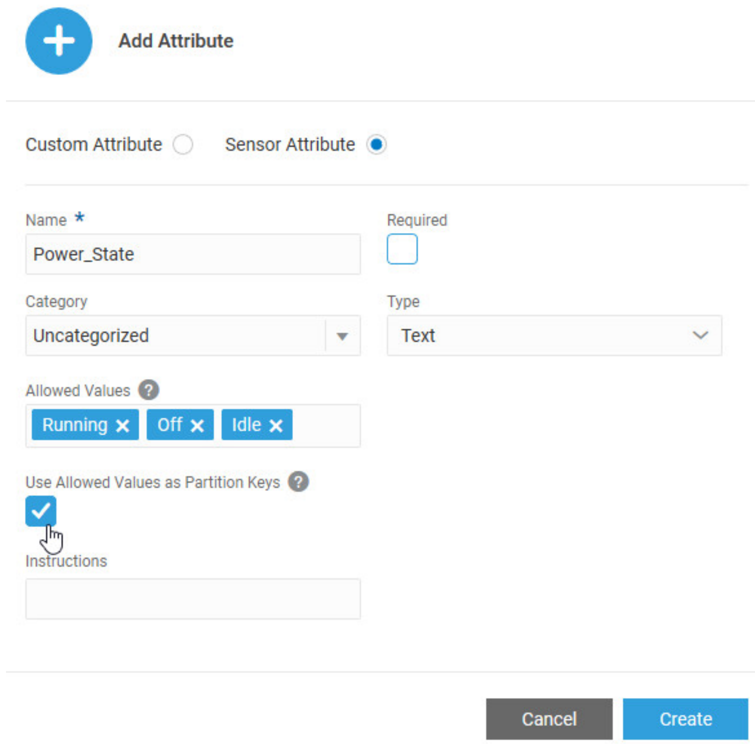
   This field is only applicable to custom attributes. If you do not specify an attribute value when creating an asset, the default value is used.

j. (Optional) You can specify a list of **Allowed Values** for your attribute.

   Press **Enter** after entering each value.

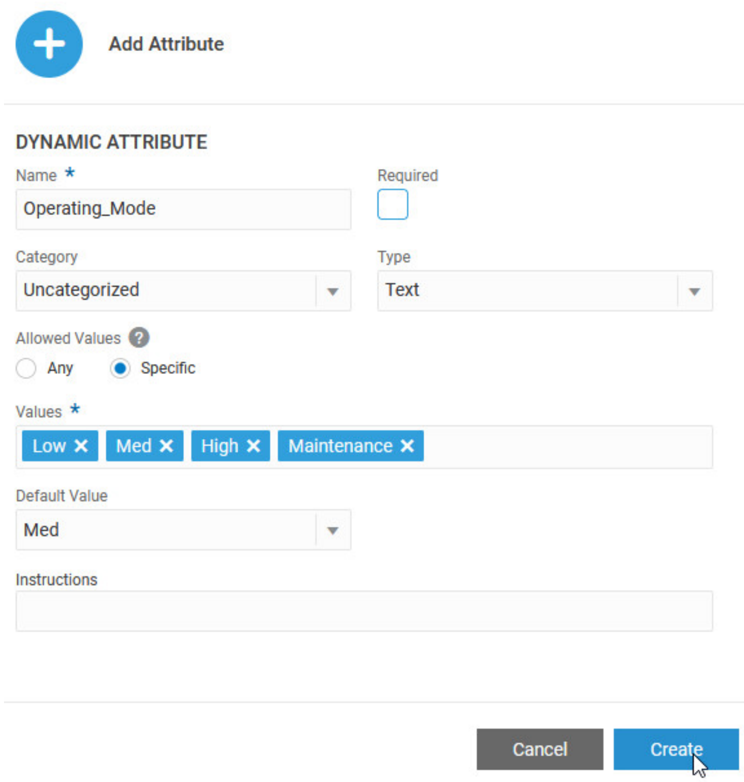
   Some attribute types, such as Number, also allow you to specify a range of allowed values.

k. (Optional) For sensor attributes, if you have used the **Allowed Values** field, you can optionally choose **Use the Allowed Values as Partition Keys**.



Select this option if you intend to use the allowed values as partition keys in your state-aware anomalies. See Define an Automatic Anomaly for more information.

The following example shows a dynamic attribute, `Operating_Mode` that has predefined modes of operation. A default operating mode is also selected.



  l. Click **Create**.
  m. Repeat the above steps to create additional attributes.
8. Click **Save** and then click **OK**.
9. Close the window 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.

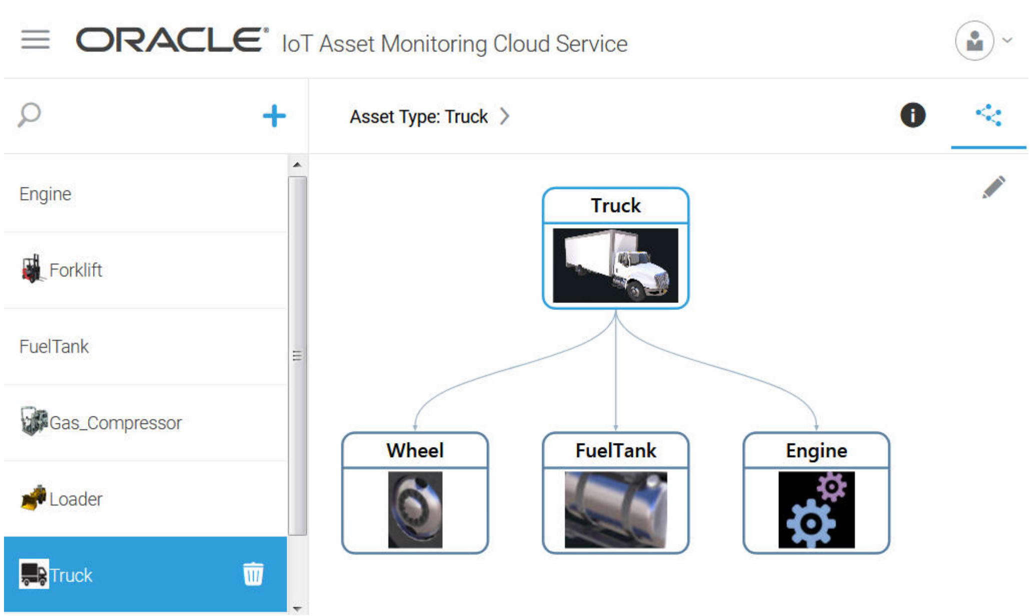
13. Optionally change the order of your action items by using the arrow keys under the **Order** column.

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

About Hierarchical Asset Type Associations

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

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



The asset types may look like the following:

- **Truck**
  - Custom Attributes: Model, Color
  - **Wheels**

        * Custom Attributes: Size
        * Sensor Attributes: Pressure
    – **Engine**
        * Custom Attributes: Make, Model
        * Sensor Attributes: RPM
    – **FuelTank**
        * Custom Attributes: Capacity
        * Sensor Attributes: FuelLevel
        * Alert Attributes: LowFuelAlert

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 Intelligent Applications Cloud.

Create Asset Type Associations

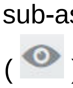
You can create asset type associations when creating or editing an asset type. You can add existing sub-asset types, or create new ones.

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**.

Use 3D Asset Type Models

If you have the 3D (three-dimensional) Digital Twin feature, you can upload and use a pre-configured 3D asset model in place of an asset image when creating a new asset type.

3D CAD models let you contextualize your asset components and data in three-dimensional space. Depending on your model, you can choose to rotate or re-orient the asset in three-dimensional space, separate out the sub-assets, and choose various views, such as shaded, X-Ray, and wireframe.

You may already have a 3D model for your device from your device manufacturer, or you may have one custom-created in your organization. Formats such as `OBJ`, `Sketchup`, `Autocad`, and `COLLADA (DAE)` are supported.

Use the **Upload 3D Model** option to upload a 3D model when creating a new asset type. Depending on the complexity of your model, it may take a few minutes to upload to Oracle IoT Asset Monitoring Cloud Service

After the model is uploaded, you may choose to click and drag the model to change its orientation. Use the mouse control to change your zoom setting. You can also use the various tools to change the appearance and orientation of the model.

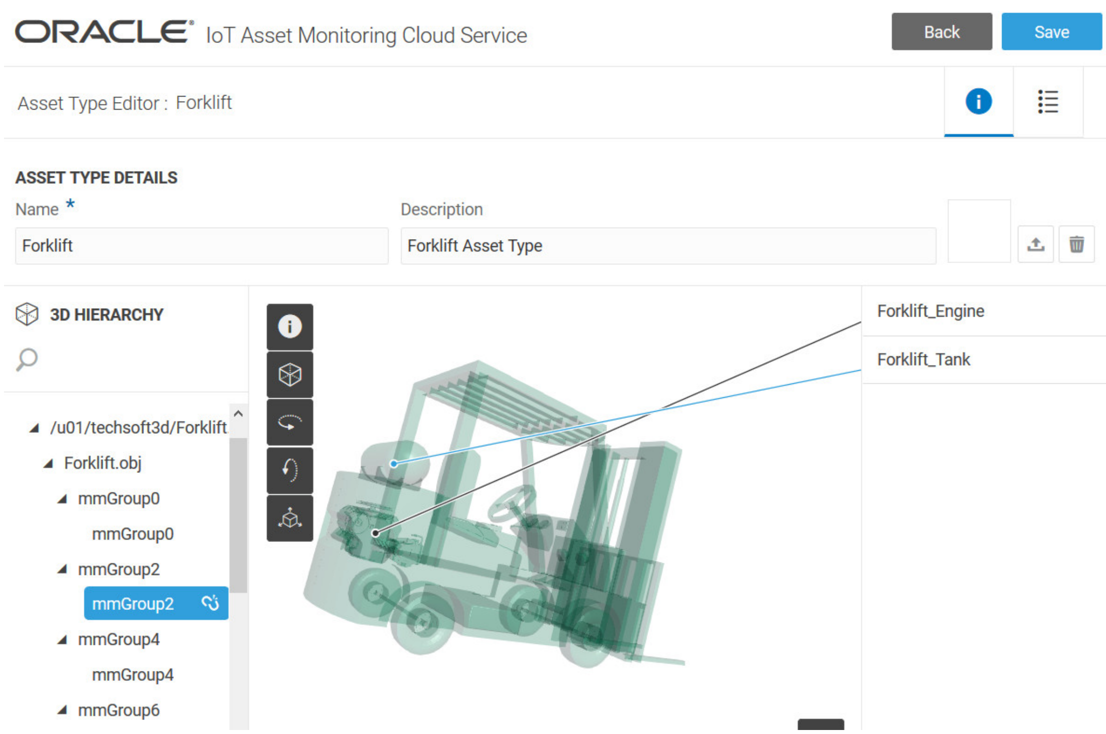
The following tools are available:

- Explode : You can also choose to explode the model, so that the sub-components separate out to varying degrees. Use the slider tool to choose the degree of separation.
- Rendering Style : Choose between the available styles, such as Wireframe, Shaded, and X-Ray.

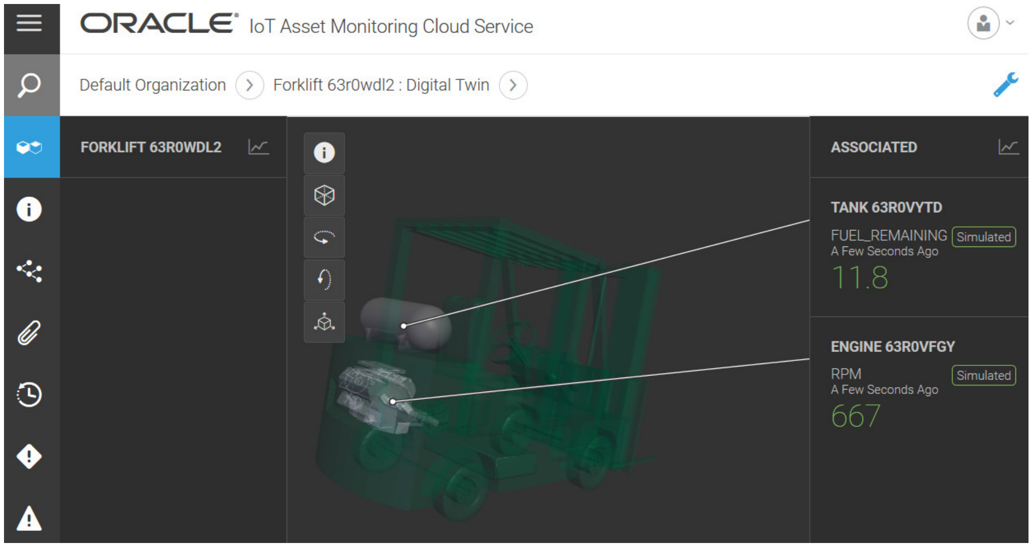
- Rotate Right : Use to rotate the asset model along the horizontal plane.
- Rotate Down : Use to rotate the asset model along the vertical plane.
- Orientation : Use the pin icon to save the current orientation, so that the same default orientation is used in the digital twin view in Operations Center. The reset icon switches back the orientation to the last pinned one.

The 3D Hierarchy shows the various nodes contained in the 3D model. You can choose to create sub-assets for the nodes you choose. Select a component in the exploded asset view, and then click the link icon for the corresponding node in the 3D hierarchy to link the node to a sub-asset type.

The following image shows a forklift asset model. Notice that the `mmGroup2` node in the asset model hierarchy has been mapped to the `Forklift_Tank` sub-asset type.



When you create assets for an asset type using a 3D model, the Digital Twin view uses the 3D model in the Operations Center.



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** () 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 the **Asset Inventory Menu** and select **Create Assets**.
4. To create a single asset, click **Create Single Asset**.
5. Select the **Entity Type** (Asset Type) for the asset.

   The Asset Type must already exist in the application.
6. Enter a **Name** for the asset.

   The application creates a default name for the new asset. You can choose to change this to a name meaningful for your environment. Default names are especially useful when creating assets in bulk.
7. Select **Create Optional Associated 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.

8. (Optional) Select the **Data Source** for the asset sensor attributes.

   If you are using direct data ingestion for your device, you can choose to specify the direct data source details here.

   > **Note:**
   >
   > You can also choose to specify the data source for your sensor attributes in the asset editor after creating the asset.

   - **Direct:** Use for devices that can directly connect with the application.
     - **External ID:** You can enter the external identifier for the device. This is usually the Hardware ID. If you do not enter a value, the default entity ID is used for authentication.
     - **Authentication:** Select between **Client Certificate** and **Client ID/Secret**.

       Client certificate is the recommended option for increased security. The default **Common Name** used for client certificate is the entity ID. If you have specified an External ID, then this is used as the common name.

       If using **Client ID/Secret**, specify a secure password in the **Secret** field. The default **Client ID** used for client certificate is the entity ID. If you have specified an External ID, then this is used as the client ID.
     - **Payload:** Select **Schema** if you are using the standard schema format for data ingestion. Select **Custom** if the payload does not follow the schema. If choosing the custom option, you must specify a previously created **Interpreter** to interpret the payload.
   - **Direct via Any Connector:** Use for devices that connect using a connector.

     External ID: You can enter the external identifier for the device. This is usually the Hardware ID. If you do not enter a value, the default entity ID is used for authentication.
   - **Direct via Specific Connector:** Use for devices that can connect using the specified connector.
     - **Connector:** Select a connector that you have previously created.
     - **External ID:** You can enter the external identifier for the device. This is usually the Hardware ID. If you do not enter a value, the default entity ID is used for authentication.

9. Click **Create** to continue creating the asset and any specified sub-assets.

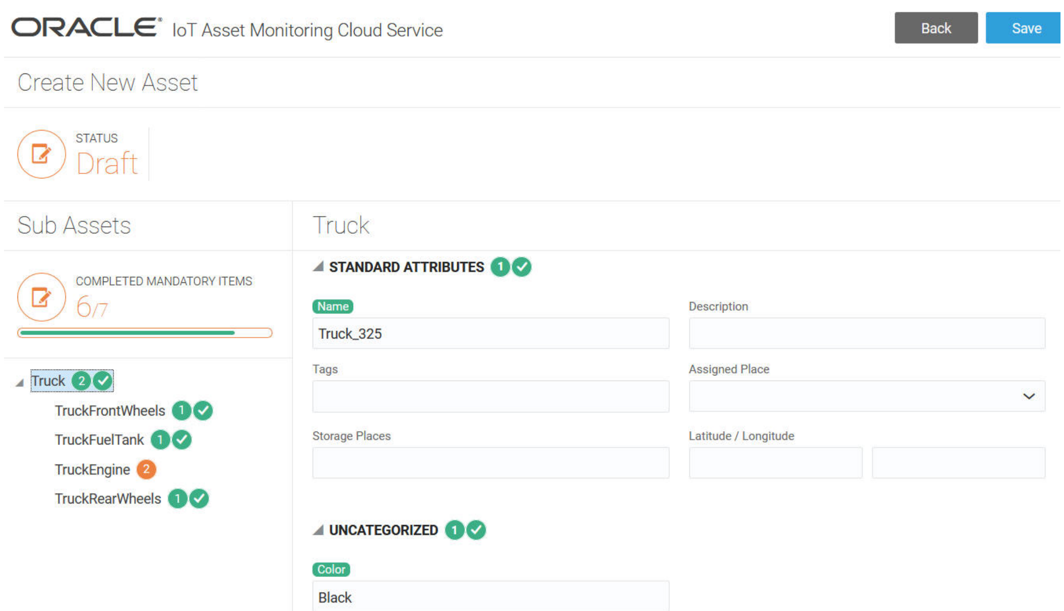
   The draft asset along with any mandatory and specified sub-assets is created. A progress bar indicates the mandatory items that were completed, and the ones that you must complete.

   In the following example, a Truck asset is created. The truck has the following associations:

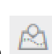
   - TruckFrontWheels
   - TruckFuelTank

- 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.



10. 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.

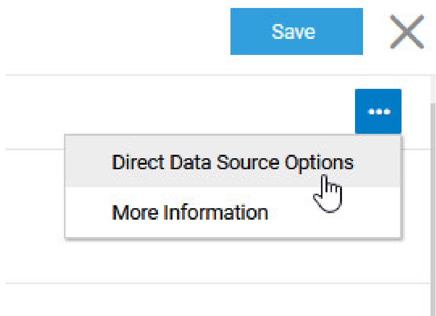
      You can alternatively click **Asset Location**  to select the location in the map. Selecting a location automatically populates the latitude and longitude values.
11. Select the **Data Source** for the asset sensor attributes.
    - **Direct:**
      Select if you are ingesting IoT data from directly connected devices, gateways, and network servers directly into your asset and machine sensor attributes. Choose direct ingestion to eliminate the need for registering devices and device models, and for creating IoT messages.
    - **Linked Device:**

Select to link to an IoT device registered with Oracle Internet of Things Intelligent Applications Cloud.

12. Depending on your choice in the preceding step, complete the direct data source settings, or complete linking the sensor attributes to your device attributes.

    If you selected **Direct** under **Data Source**, complete the direct data source settings:

    a. Select **Direct Data Source Options** from the editor menu.

    b. Select the **Data Source**:

    - **Direct:** Use for devices that can directly connect with the application.
      – **External ID:** You can enter the external identifier for the device. This is usually the Hardware ID. If you do not enter a value, the default entity ID is used for authentication.
      – **Authentication:** Select between **Client Certificate** and **Client ID/ Secret**.

        Client certificate is the recommended option for increased security. The default **Common Name** used for client certificate is the entity ID. If you have specified an External ID, then this is used as the common name.

        If using **Client ID/Secret**, specify a secure password in the **Secret** field. The default **Client ID** used for client certificate is the entity ID. If you have specified an External ID, then this is used as the client ID.
      – **Payload:** Select **Schema** if you are using the standard schema format for data ingestion. Select **Custom** if the payload does not follow the schema. If choosing the custom option, you must specify a previously created **Interpreter** to interpret the payload.
    - **Direct via Any Connector:** Use for devices that connect using a connector.

      External ID: You can enter the external identifier for the device. This is usually the Hardware ID. If you do not enter a value, the default entity ID is used for authentication.
    - **Direct via Specific Connector:** Use for devices that can connect using the specified connector.
      – **Connector:** Select a connector that you have previously created.

- **External ID:** You can enter the external identifier for the device. This is usually the Hardware ID. If you do not enter a value, the default entity ID is used for authentication.

c. Click **OK** in the Direct Data Source Options dialog.

   See Use Direct Data Ingestion for Your Sensor Attributes for detailed information and examples on using direct data ingestion for your asset attributes.

If you selected **Linked Device:** under **Data Source**, complete linking the sensor attributes to the registered 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 Intelligent Applications Cloud, and the corresponding device model should have been selected for the Oracle IoT Asset Monitoring Cloud Service application.

a. Click **Link to Device** ( ) 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 Intelligent Applications Cloud, 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.

13. 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 Intelligent Applications Cloud, 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 Intelligent Applications Cloud, 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.

14. 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.

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

    A Save Progress displays the status of the asset creation.

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

16. Click **OK** after the asset is successfully created.

17. Click **Back** to return to the **All Assets** list.

    The Asset Activity tab keeps track of all asset activity, such as asset creation, edits, and imports.

Create Multiple Assets in Bulk

You can create multiple assets in draft form with a single create operation.

You can subsequently edit and activate these assets by specifying or changing the individual attribute values and creating appropriate device links for the sensor attributes.
Alternatively, you can export the newly-created assets to a `.csv` (comma separated value) file, bulk edit the attributes and device associations, and import back the assets to activate them.

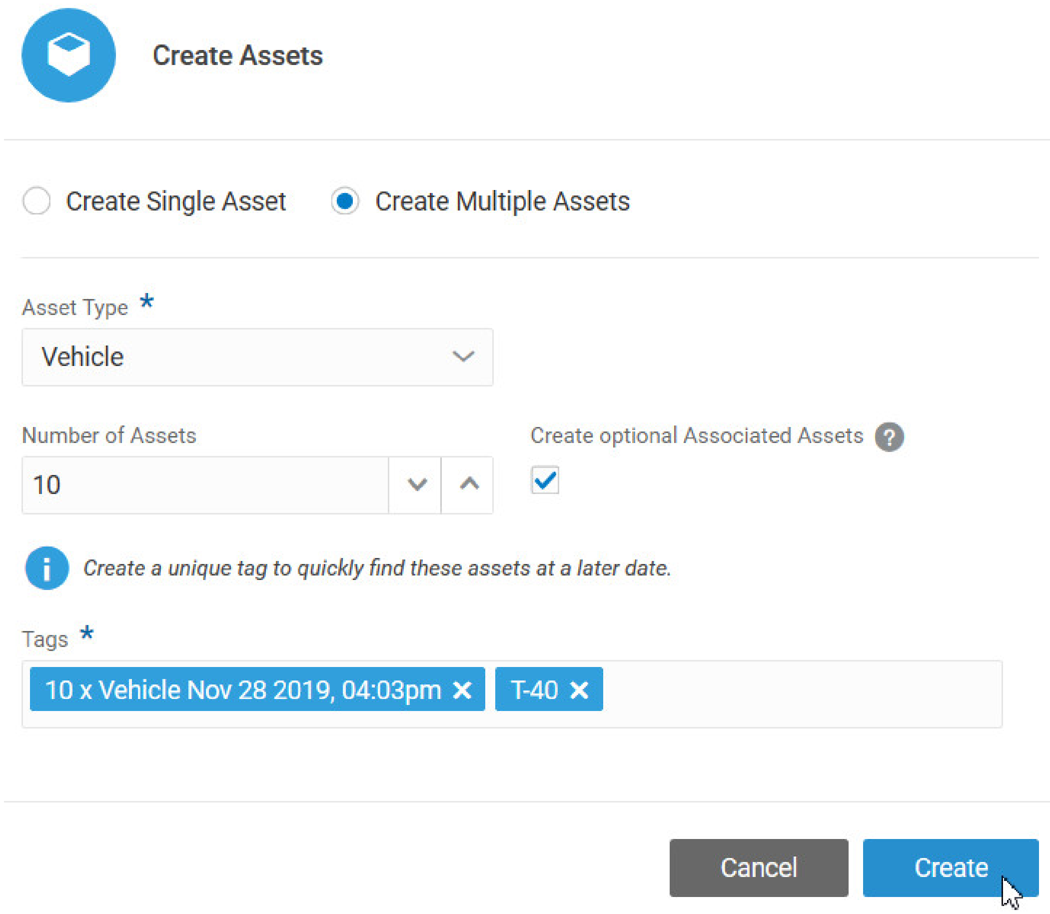
1. Click **Menu** (☰), and then click **Design Center**.
2. Select **Asset Inventory** from the **Design Center** sub-menu.
3. Click the **Asset Inventory Menu** ••• and select **Create Assets**.
4. To create multiple assets, select **Create Multiple Assets**.
5. Select the **Asset Type** for the assets.

   The **Asset Type** must already exist in the application.

6. Enter the **Number of Assets** to be created.
7. Select **Create Optional Associated Assets**, if the asset type has sub-assets that are optional, but you want all optional sub-assets to be created along with the assets.
8. Optionally specify one or more **Tags** for your assets.

   Tags help identify and group assets. Tags are also useful when searching or filtering for assets, say for export.

   A default tag is automatically added, which specifies the number of assets that are being created, the asset type, and the date-time stamp.



9. Click **Create** to continue creating the assets and any specified sub-assets.

   An information message appears confirming that the bulk asset creation has started.

   The application automatically creates default names for the new assets. You can choose to edit these later if required.

   The **Asset Activity** tab keeps track of all asset activity, such as asset creation, edits, and imports.

   After the assets are created, they appear under the **All Assets** tab. You can also refresh the page to check if the assets already appear under **All Assets**.

10. To activate the newly created assets, choose one of the following:
    - Individually edit the assets to specify attribute values and device links.
    - Export the assets to a `.csv` (comma separated value) file to bulk edit them.

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.

Use Direct Data Ingestion for Your Sensor Attributes

Your digital twin entities are now directly addressable over the network, using standard protocols, authentication mechanisms, and payload formats. Ingest IoT data from directly connected devices, gateways, and network servers directly into your asset and machine sensor attributes.

Choose direct ingestion to eliminate the need for registering devices and device models, and for creating IoT messages.

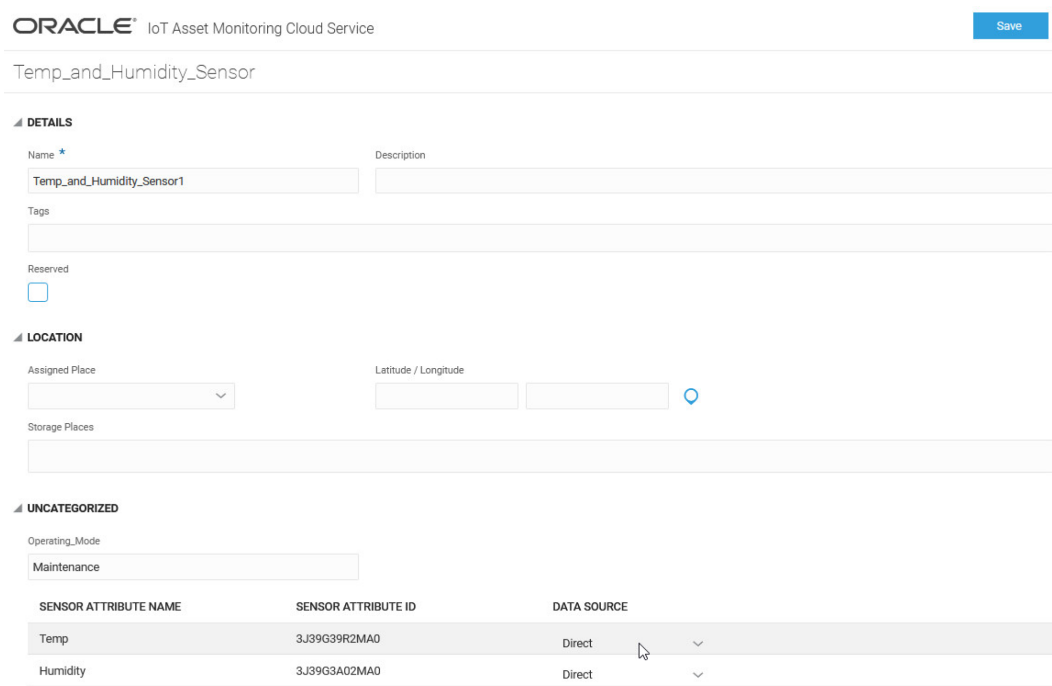
Use standard HTTP or MQTT protocol to send sensor data in JSON or CSV format. The application supports mutual authentication using certificates in addition to basic authentication.

The application lets you download ready-to-use schema samples for your entities. If you have custom payloads, use the interpreter editor interface to create the mappings and routing.

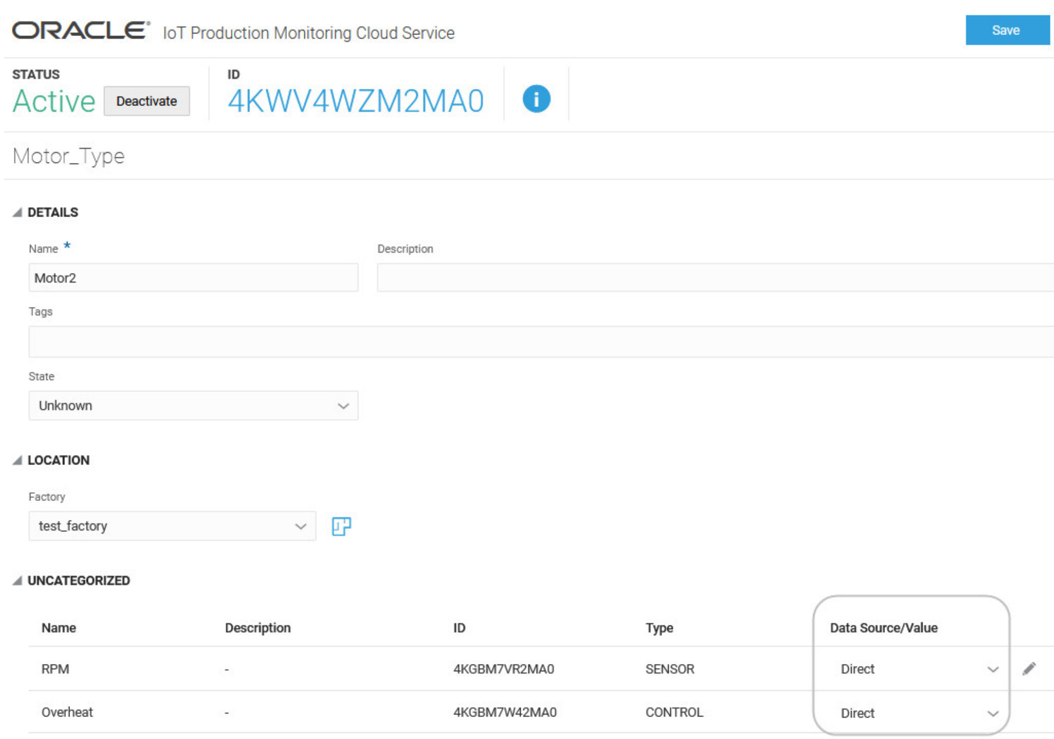
Set Direct Data Options for Your Entity

Use the Create Asset/Machine or Edit Asset/Machine page to set direct data options for the sensor attributes of an entity.

1. On the Create Asset/Machine or Edit Asset/Machine page, set the **Data Source** for one or more sensor attributes to **Direct**.

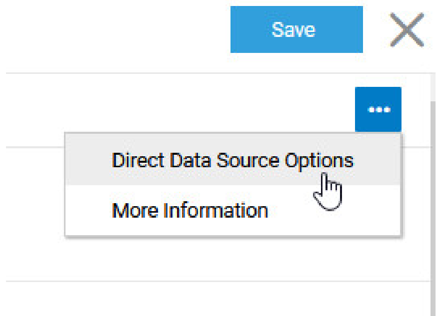


The preceding image shows an asset editor page with two sensor attributes, `Temp` and `Humidity`. The data source for the sensor attributes is set to **Direct**.



The preceding image shows a machine editor page with a sensor attribute, `RPM` and a control attribute, `Overheat`. The data source for the attributes is set to **Direct**.

2. Select **Direct Data Source Options** from the page menu.



3. Select the **Data Source**:
   - **Direct:** Use for devices that can directly connect with the application.
     - **External ID:** You can enter the external identifier for the device. This is usually the Hardware ID. If you do not enter a value, the default entity ID is used for authentication.
     - **Authentication:** Select between **Client Certificate** and **Client ID/Secret**.

       Client certificate is the recommended option for increased security. The default **Common Name** used for client certificate is the entity ID. If you have specified an External ID, then this is used as the common name.

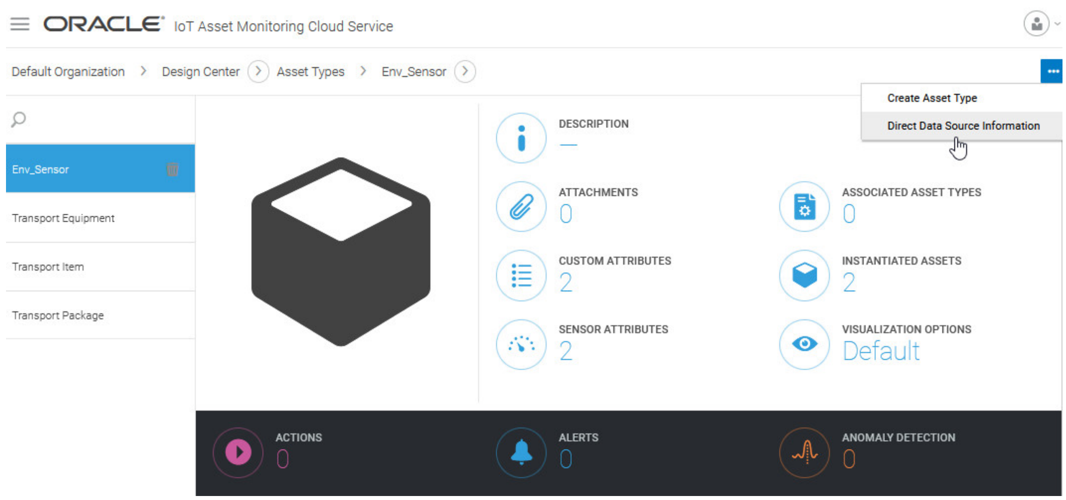
       If using **Client ID/Secret**, specify a secure password in the **Secret** field. The default **Client ID** used for client certificate is the entity ID. If you have specified an External ID, then this is used as the client ID.
     - **Payload:** Select **Schema** if you are using the standard schema format for data ingestion. Select **Custom** if the payload does not follow the schema. If choosing the custom option, you must specify a previously created **Interpreter** to interpret the payload.
   - **Direct via Any Connector:** Use for devices that connect using a connector.

     External ID: You can enter the external identifier for the device. This is usually the Hardware ID. If you do not enter a value, the default entity ID is used for authentication.
   - **Direct via Specific Connector:** Use for devices that can connect using the specified connector.
     - **Connector:** Select a connector that you have previously created.
     - **External ID:** You can enter the external identifier for the device. This is usually the Hardware ID. If you do not enter a value, the default entity ID is used for authentication.
4. Click **OK**, and then click **Save** in the Entity editor.

Download Schema for an Entity Type

Download the JSON or CSV schema for an entity type from the Asset Types page.

1. From the **Menu > Design Center > Asset Types** page, select the asset type for which you wish to download the schema.
2. Select **Direct Data Source Information** from the Asset Types menu.



3. Select **JSON Schema** or **CSV** format.

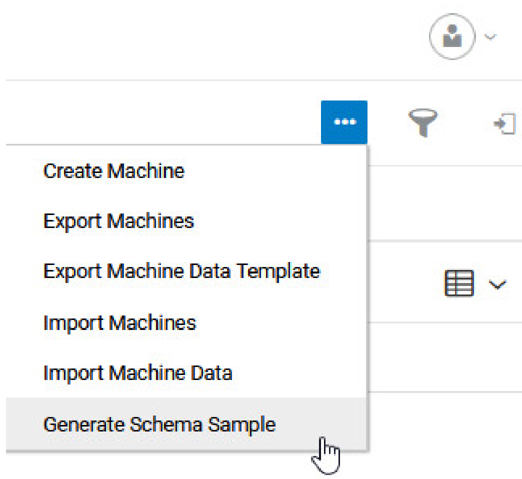
   Choose the schema format that your devices would use to send data for entities of this type.

4. Click **Download** to download the schema file to your hard disk.

Generate Schema Sample for an Entity

Generate the sample schema for an entity to find connection details, such as host, endpoint, topic, and sample payload. You can edit the sample payload values to ingest data.

1. On the Asset Inventory or Machine Inventory page in Design Center, select **Generate Schema Sample** from the Asset/Machine Inventory menu.



2. Select the **Entity Type**.

   The entity type is the asset type or machine type.

3. Choose the payload **Format**.

The available formats are **JSON** and **CSV**.

4. Select the **Protocol**.

   You can choose between **MQTTS (Publish)** and **HTTP (Post)**. MQTTS will use the topic in addition to the host.

5. Select an **Entity** for which to generate the schema sample.

   The entity is an asset or machine of the selected type.

6. Under **Target Attribute**, select one or all the direct sensor attributes for the entity.

7. Under **Target Entity**, select whether the target entity information is included in the endpoint or the payload itself.

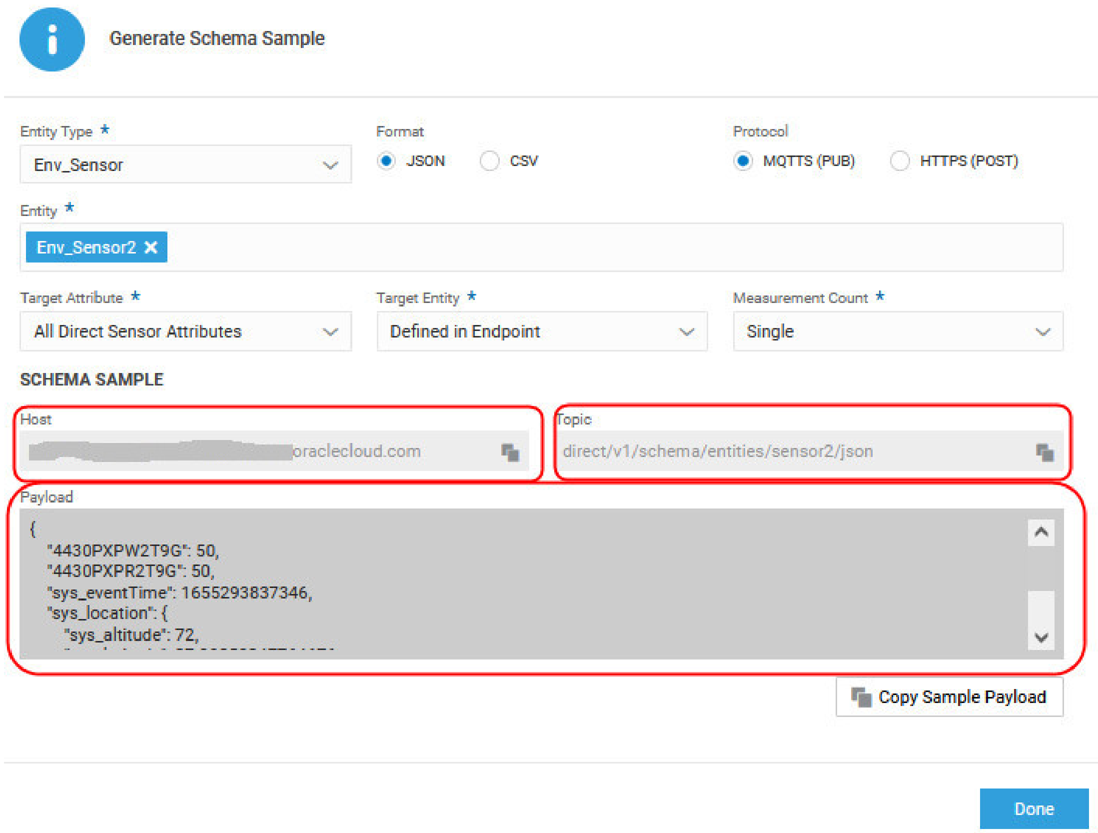
8. Under **Measurement Count**, choose whether the schema sample should include a **Single** reading or **Multiple** readings for the selected attribute.

9. Click **Generate** to generate the shcema sample.

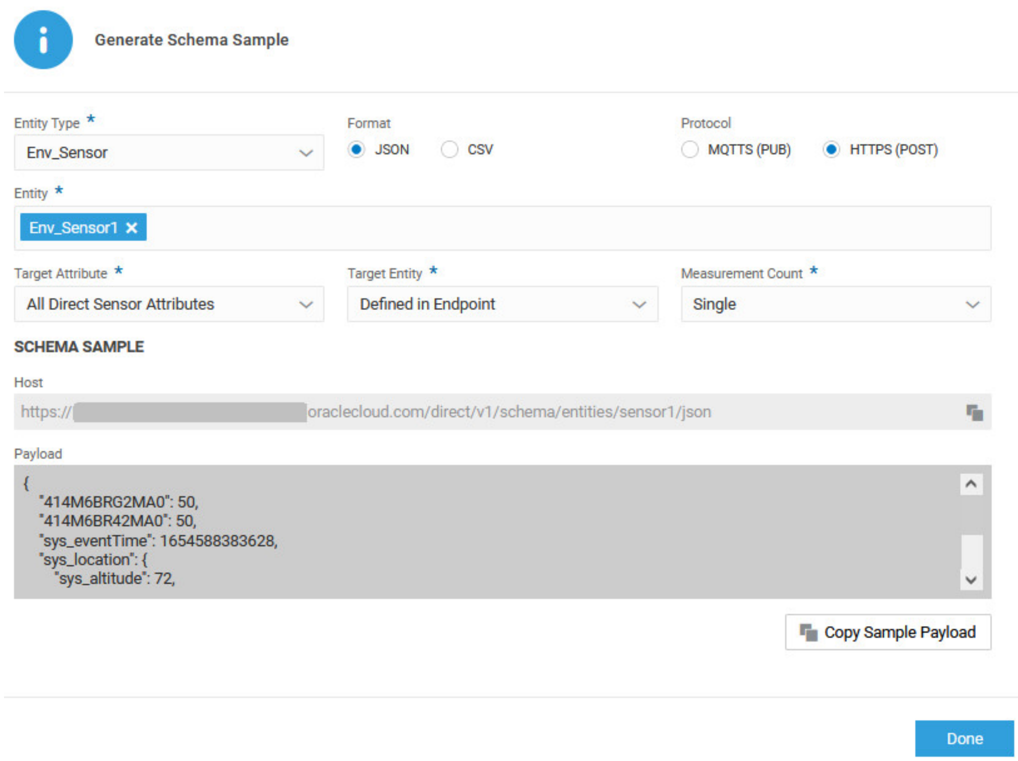
   The schema sample is generated along with the endpoint details of the host and topic (for MQTTS). The payload section contains the generated schema for your asset or machine. For example, the following JSON payload includes sample data for sensor2, where the target entity information is included in the payload itself.

```
{
    "3J39G39R2MA0": 50,
    "3J39G3A02MA0": 50,
    "sys_eventTime": 1650721170666,
    "sys_entityId": "sensor2",
    "sys_location": {
        "sys_altitude": 72,
        "sys_latitude": 37.39353247764676,
        "sys_longitude": -121.95359884794176
    }
}
```

As shown in the following example for MQTTS, it is convenient to copy details, such as the host, topic, and sample payload from the Generate Schema Sample dialog.



The following example uses the HTTPS protocol:

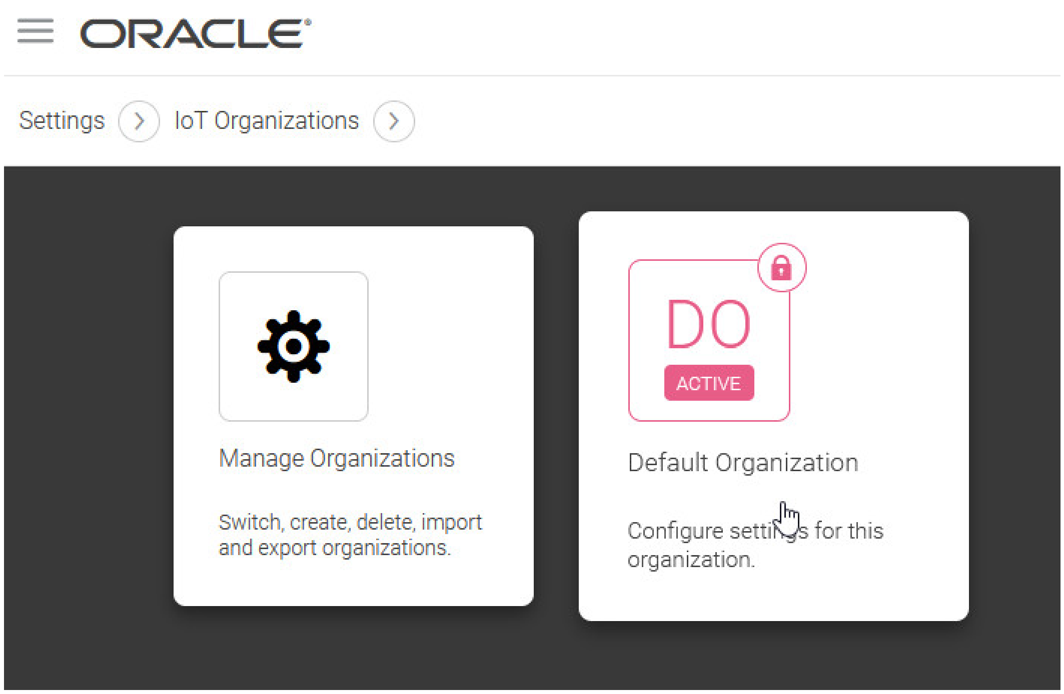


Create a Connector

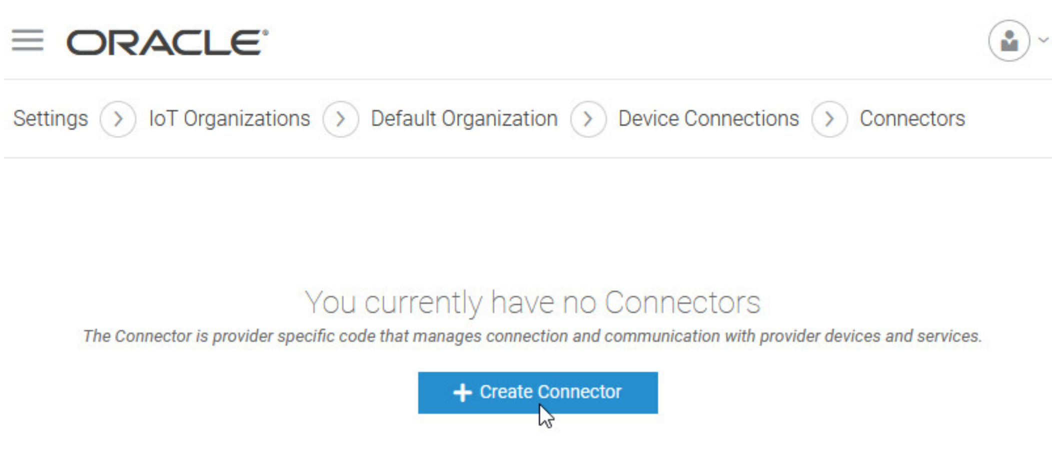
Use a connector to directly ingest data from devices, which are not directly connected.

We use the **Create Connector** option to create a connector from the **Menu >Settings > IoT Organizations >** ***Organization Name*** **> Device Connections > Connectors** page.

1. Click **Menu** (≡), and then click **Settings**.
2. Click the **IoT Organizations** tile, and then click your organization tile.



3. Click the **Device Connections** tile, and then click the **Connectors** tile.
4. Click **Create Connector** to create a new connector.



5. Select between **Gateway** and **Network Server**, and click **Create**.

   The **OPC UA** and **Pi System** connectors are also available for Production Monitoring, like in previous releases.
6. Specify a **Name** and optional **Description** for the connector.
7. Enter an **External ID** for the connector. This is usually the Hardware ID.

   The External ID is used as the common name in certificate-based mutual authentication, or as the client ID in password-based authentication.
8. Enter any optional **Tags**.
9. Optionally specify the location coordinates in the **Location** section.

10. Under the **Security** section, specify the **Authentication** method.

    Client certificate is the recommended option for increased security. The External ID that you specified is used as the common name.

    If using **Client ID/Secret**, specify a secure password in the **Secret** field. The External ID that you specified is used as the client ID.

11. Under **Authorization**, select the target entities for the connector.

    If you select **Specific Entities**, the connector can send data only for entities bound to the connector.

12. Select the **Payload** type.

    Select **Schema** if you are using the standard schema format for data ingestion. Select **Custom** if the payload does not follow the schema. If choosing the custom option, you must specify a previously created **Interpreter** to interpret the payload.

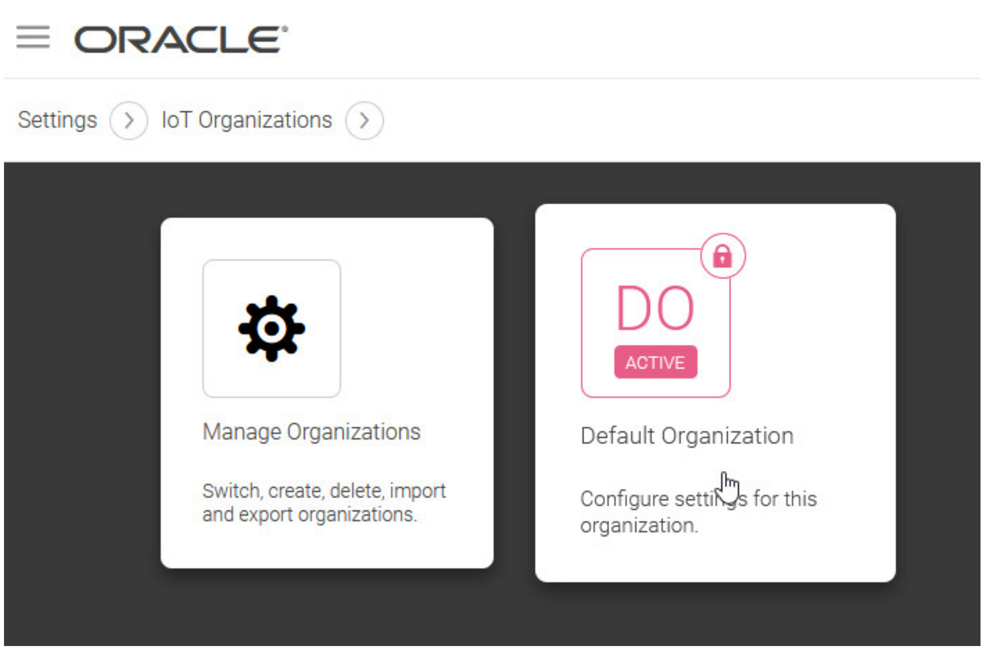
13. Click **Save** to save the connector.

Create an Interpreter

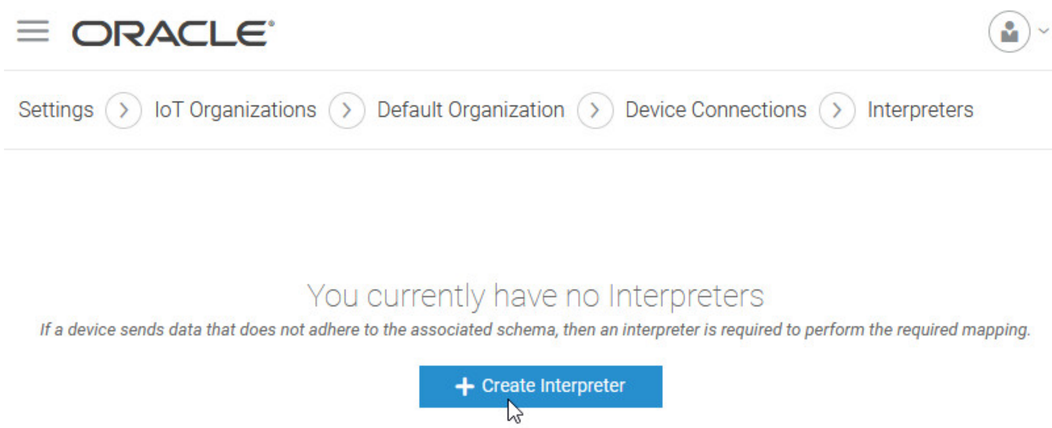
If you are using a custom payload where the payload does not follow the schema, you can create an interpreter to map the payload for the connector.

We use the **Create Interpreter** option to create a connector from the **Menu >Settings > IoT Organizations >** ***Organization Name*** **> Device Connections > Interpreters** page.

1. Click **Menu** (☰), and then click **Settings**.
2. Click the **IoT Organizations** tile, and then click your organization tile.



3. Click the **Device Connections** tile, and then click the **Interpreters** tile.
4. Click **Create Interpreter** to create a new interpreter.



5. Select the interpreter **Type**, and click **Create**.

   Mapping interpreters are the most common use case wherein the payload maps to a single entity type. Use **Routing** interpreters for scenarios where the payload maps to multiple entity types.

6. Provide a **Name** and optional **Description** for the interpreter.

7. Select the **Target Entity Type**.

   This is the target asset type or machine type of the entity. Note that this field is not displayed for routing interpreters where the payload can map to multiple entity types.

8. Select the **Target Entity**.

   This is the asset or machine for which you are ingesting and interpreting the data.

9. Select the **Payload Encoding** format.

   The available options are **JSON** and **CSV**.

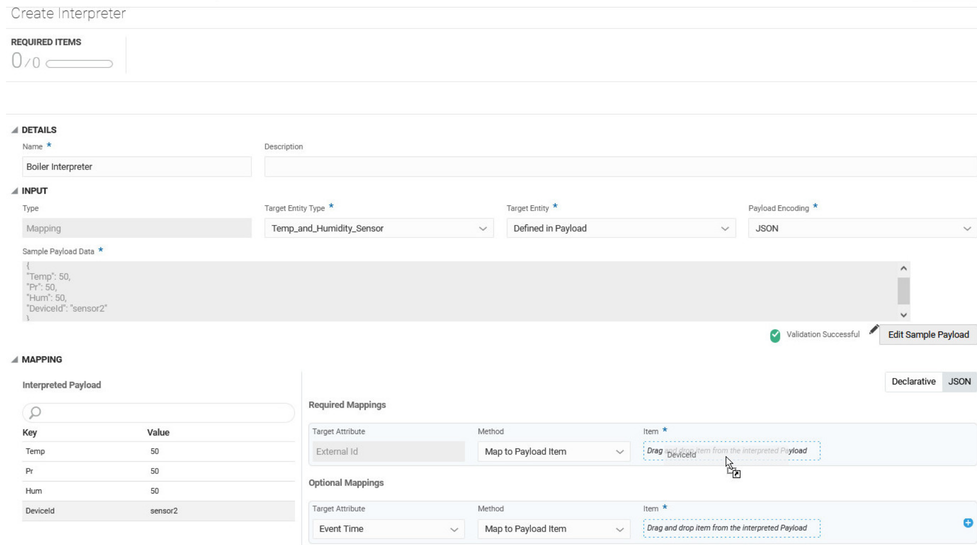
10. Under **Sample Payload Data**, provide the sample JSON or CSV data and click **Validate Data**.

    The sample payload is checked for any syntax/validation errors.

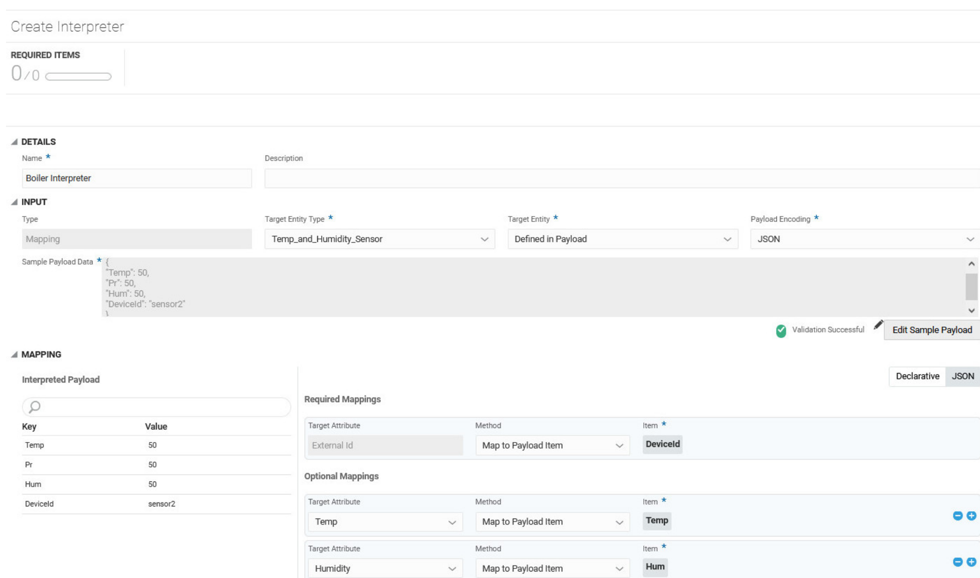
11. In the Mappings section, complete the mappings of the payload to the schema.

    You must complete all required mappings, and any additional mappings that you may have.

    You can drag the payload keys to the appropriate target attributes. The following image shows the `DeviceID` payload key dragged to the `EntityID` attribute.



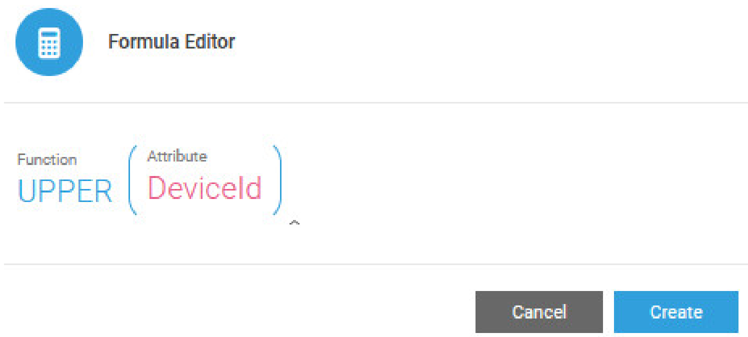
The following image shows a completed mapping.



12. You can also choose **Custom Formula** to complete a mapping.

    Use the formula editor to build and complete your mapping.

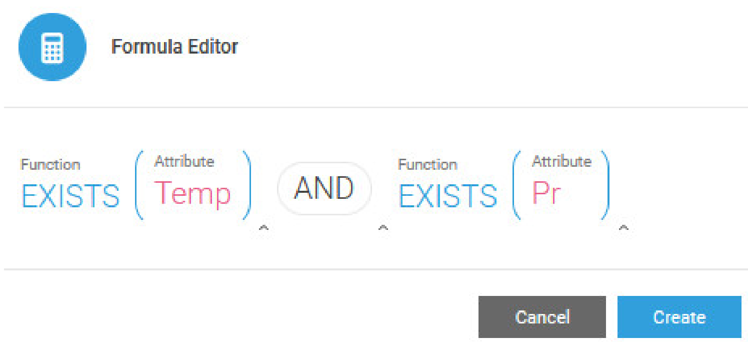
    The following example shows a custom formula for mapping the `DeviceID` to `EntityID`.



13. Define any routing conditions for routing interpreters.

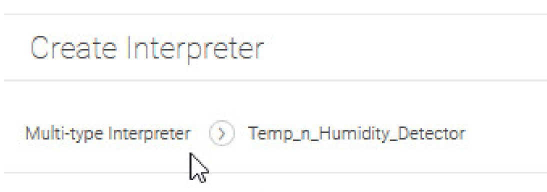
    Use the formula editor to build and complete your condition.

    The following example shows a custom formula for the routing condition.



    a. Select a **Target Entity Type** for the routing condition, and click **Configure Mapping** to complete any required and optional nested mappings for the condition.

       Note that you can navigate back to the main editor using the breadcrumbs that appear at the top of the editor page.



    b. Add more routing conditions, as required.

       The routing will apply to the first applicable routing condition. Once you define more than one condition, you can edit the ordering.

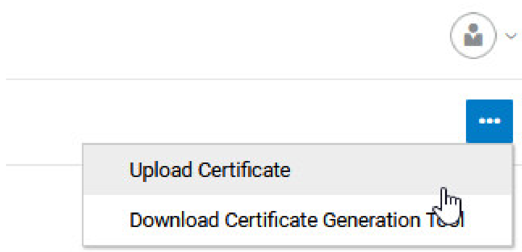
14. Click **Save** to save the interpreter.

Upload and Manage Certificates

As an integrator, you can upload your root certificate, and certificate hierarchy, to your IoT instance. The application can then authenticate your clients devices, gateways, and network servers using the certificate hierarchy. You can also manage your certificates, such as renew or revoke certificates in the application.

The Security area in the Settings section lets you upload and manage certificates. To upload a new certificate:

1. Click **Menu** (≡), and then click **Settings**.
2. Click **Security** on the Settings page.
3. Click **Certificates**.
4. Click **Upload Certificate** to upload a trusted certificate.



5. Specify a **Name**, optional **Description**, and select the `PEM` file to upload.
6. Click **Upload**.
   Oracle recommends that you use a CA certificate. Self-signed certificates are not recommended for production environments.

> **Note:**
>
> You can use the certificate generation tool to generate self-signed certificates. Select **Download Certificate Generation Tool** from the **Certificates** menu to use the same. Use `./gencert.sh help` for usage information on the tool.

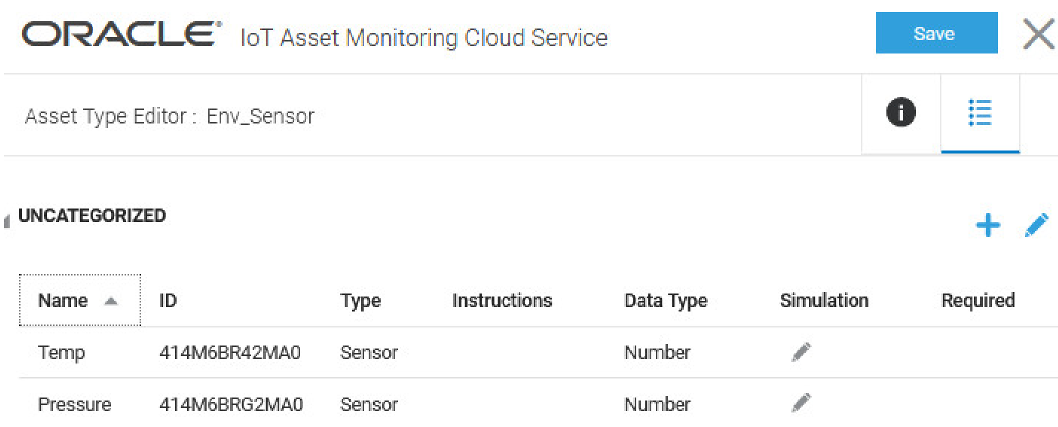
The certificate must be verified before coming into effect. You can choose **Verify Root Certificate** from the Certificates menu to verify the certificate. A verification code is generated, and you need to upload the signed certificate.

You can delegate provisioning to trusted parties by creating intermediate certificates. Create leaf certificates for your devices where the common name is the Entity Id.

Demonstration: Ingest Data for a Directly Connected Device

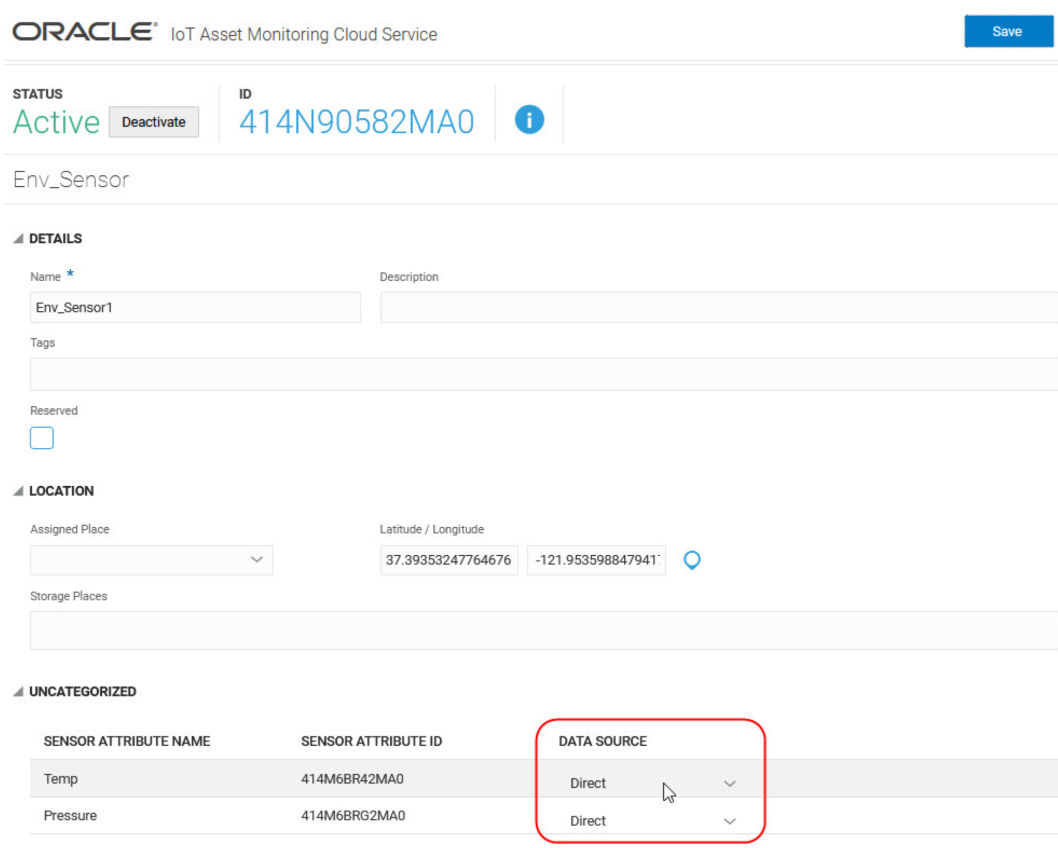
We demonstrate creating an asset and ingesting IoT data for the asset sensor attributes using HTTPS.

1. Create the asset type.



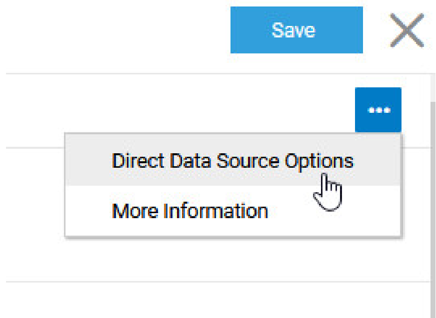
We create an asset type, `Env_Sensor` with sensor attributes for temperature and pressure.

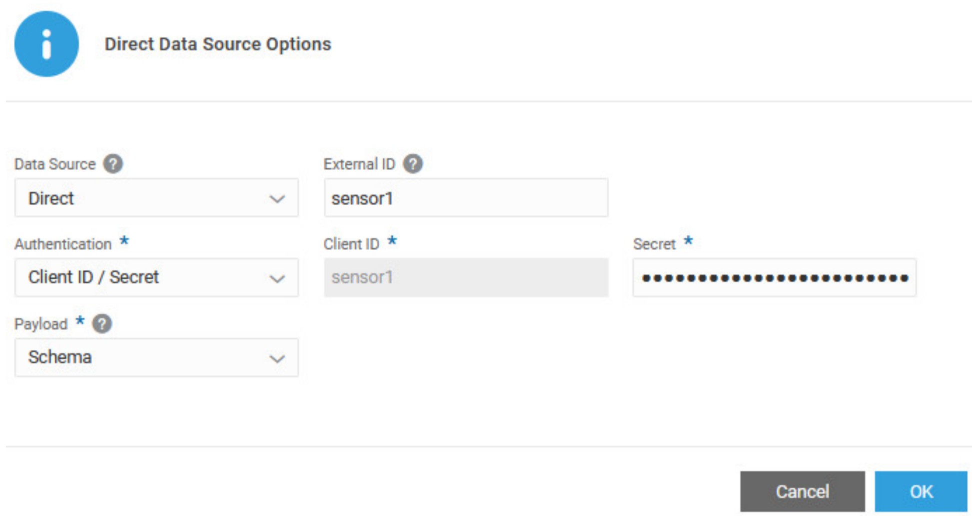
2. Create an asset for the asset type, and set the data source for the sensor attributes to **Direct**.



We create an asset, `Env_Sensor1` for the asset type, and set the Data Source value for the sensor attributes `Temp` and `Pressure` to **Direct.**

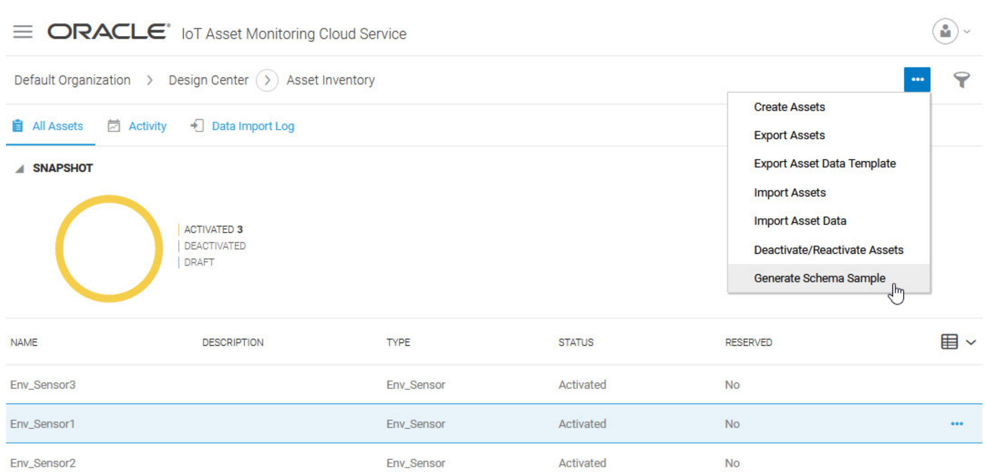
3. Set the **Direct Data Source Options** for the asset in the Asset Editor.

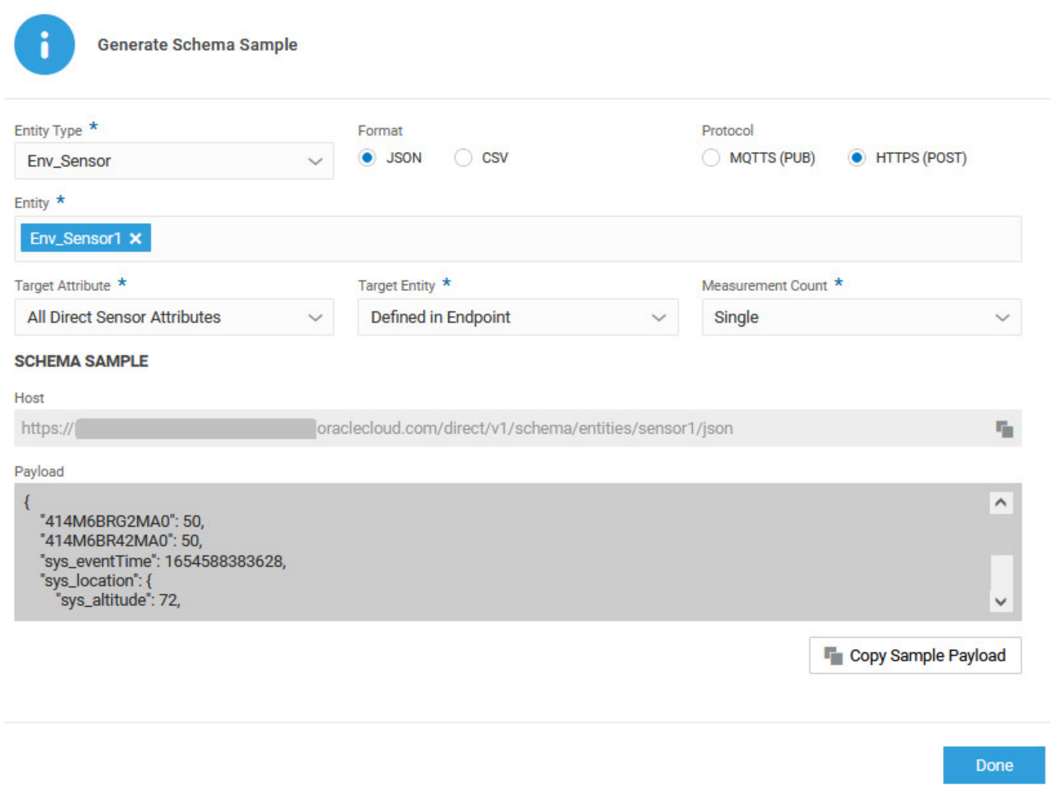




As this is a directly connected device, we choose the **Direct** under **Data Source.** We specify an external ID, `sensor1`. The **External ID** is used as the **Client ID** when the device sends data to the IoT server. We set the authentication method to use **Client ID/Secret** and specify a secure secret password. As we do not need a custom schema, we leave the payload set to the default schema.

4. Generate a sample schema for the asset from the Asset Inventory page.



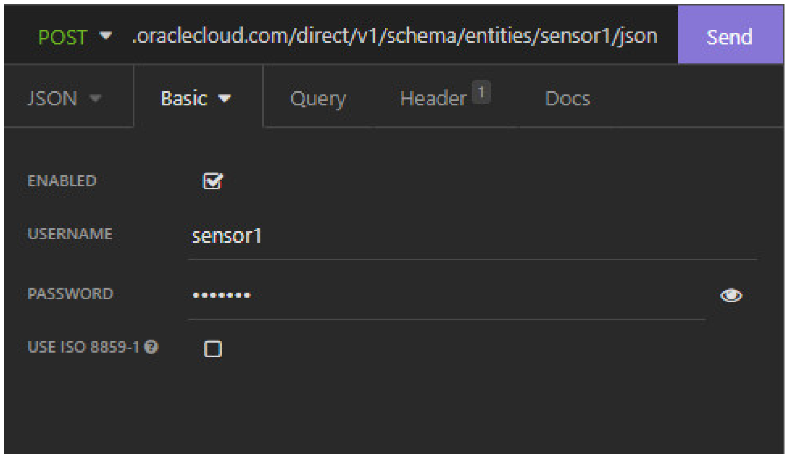


We choose a **JSON** schema and the **HTTPS (POST)** protocol. We select the sensor and choose to generate a sample payload for all its sensor attributes. The sensor ID is included in the endpoint here, but you could also choose to include it as part of payload. We generate a sample schema for a single measurement.

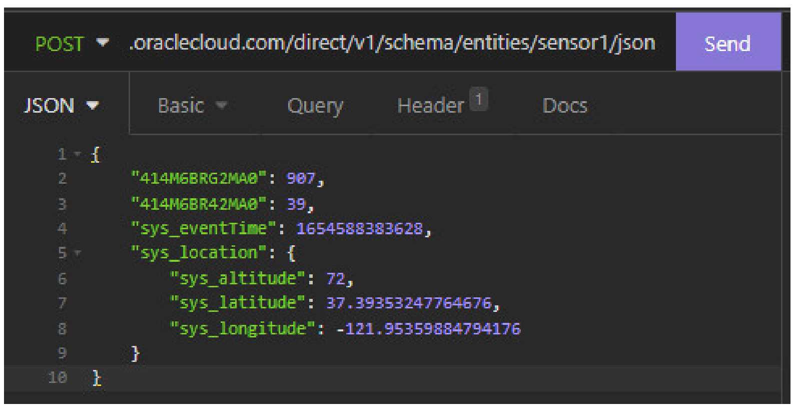
The payload contains sample values for the sensor attributes. Note that the sensor attribute IDs that appear in the payload can be traced to their respective sensor names in the asset editor.

When sending data, say using a REST client or curl command, copy the host, endpoint, and payload from the Sample Schema dialog. Use the client ID as the user name and the secret, set earlier, to authenticate. Edit the payload, as required.

5. Send data using a REST client.



We use the host copied from the sample schema dialog for the POST request. We use the client ID and secret values specified in the Direct Data Source Options dialog, as the user name and password in the REST client.



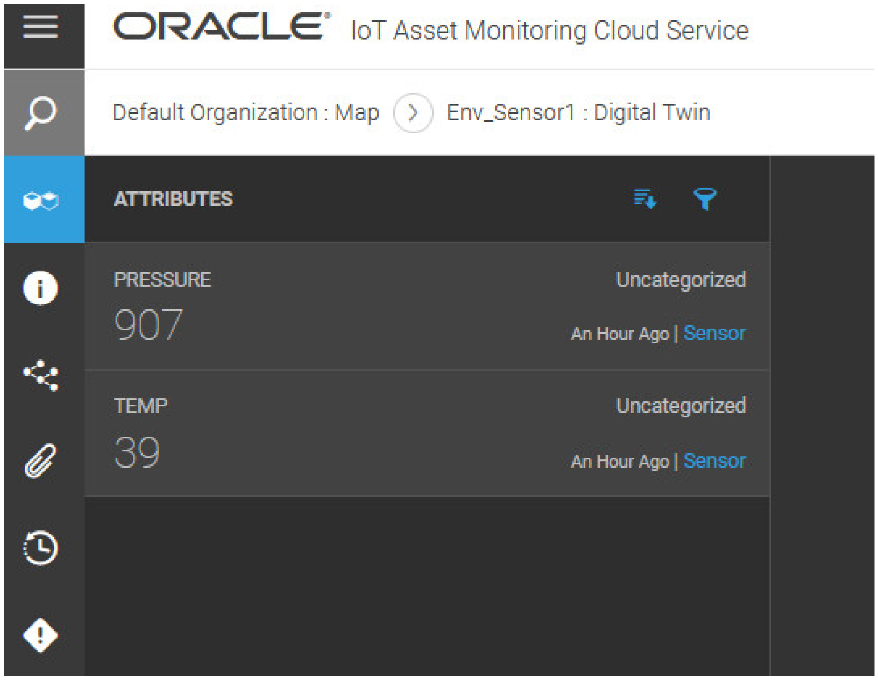
We copy and edit the sample payload from the Direct Data Source Options dialog, and use it as the data for the POST request.

The following shows a sample curl command for the POST request:

```
curl --request POST \
  --url https://iothost.oraclecloud.com/direct/v1/schema/entities/
sensor1/json \
  --header 'Authorization: Basic c2Vuc29yMTpTZWNyZXQx' \
  --header 'Content-Type: application/json' \
  --data '{
    "414M6BRG2MA0": 907,
    "414M6BR42MA0": 39,
    "sys_eventTime": 1654588383628,
    "sys_location": {
        "sys_altitude": 72,
        "sys_latitude": 37.39353247764676,
        "sys_longitude": -121.95359884794176
    }
}'
```

You may choose to use the curl command directly in place of a REST client.

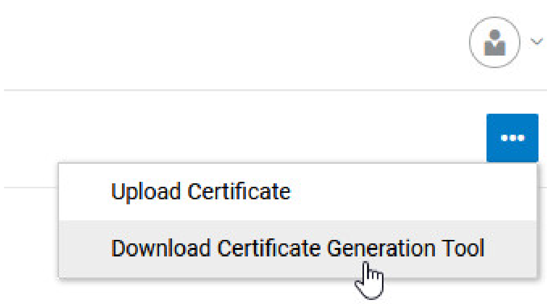
6. Verify that the sent data appears in Operations Center.



Demonstration: Create, Upload, and Verify a Root Certificate

We download and use the **gencert.sh** utility to generate a self-signed root certificate. We next upload the root certificate to the IoT server, and verify it.

1. In your IoT application, navigate to **Menu** ≡ > **Settings** > **Security** > **Certificates**.
2. Select **Download Certificate Generation Tool** from the menu on the Certificates page.

   Save the `gencert.sh` script file on your hard disk.
3. Run the **gencert.sh** utility to generate the root certificate.

   You can use the help option to look at the various options: `gencert.sh help`.

```
bash-4.2$ ./gencert.sh help

./gencert.sh Usage:
        [ help ] prints usage
        [ version ] prints usage
        [ clean ] cleans directory after confirmation
        [ pass <passphrase> ] sets specified passphrase for any future cert that will be generated by this tool
        [ expiry <default-expiration> ] Sets default expiration for all the certs that will be generated by this tool
        [ subject ] Prompt new subject information
        [ root <root-common-name>] generates root prompting for cert details
                 Options:
                 -x | --expiry <expiry> - set expiration
        [ root <root-common-name> -f <public.pem> <private.pem> ] seeds existing root cert
        [ intermediate <intermediate-common-name> [<parent-common-name>] ] generates another intermediate certificate with given common name issued by sp
ecified parent.
                         Default parent is root.
                 Options:
                 -x | --expiry <expiry> - set expiration
                 -p | --parent <parent-common-name> - parent common name. Parent should be root or intermediate
                 -i | --issuer <certificate-path> <private-key-path> - Use external certificate to create intermediate.
                 -l | --pathlen <pathlen> - set custom pathlen.
                         The pathlen parameter indicates the maximum number of intermediate certificates that can appear below this one in a chain
        [ leaf <leaf-common-name> ] generates leaf certificate with given common-name issued by intermediate common-name (default is last used)
                 Options:
                 -x | --expiry <expiry> - set expiration
                 -p | --parent <parent-common-name> - parent common name. Parent should be root or intermediate
                 -i | --issuer <certificate-path> <private-key-path> - Use external certificate to create leaf.
        [ verify <cert-common-name> <verification-code> ] generates verification certificate for the given cert (CN) and the verification code
        [ verify <certificate-file> <private-key-file> <verification-code> ] generates verification certificate for the certificate and the verification
code
        [ crl <CRL-distribution-URL> ] sets Certificate Revocation List distribution URL for all certs that will be generated by this tool.
                CRL-distribution-URL is base URL where all the CRL files are located.
        [ revoke <common-name> ] revokes the cert specified by given common-name
        [ certificate <common-name> ] show certificate
```

We use **visioncorp** as the root common name for our root certificate.

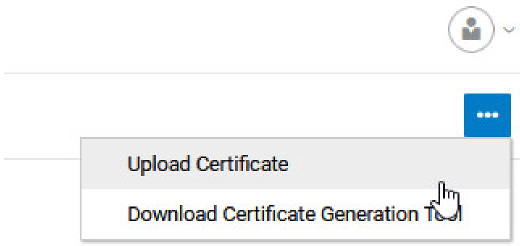
Issue the following command: `gencert.sh root visioncorp`. We use the default options for other parameters, such as *Country* and *State*. Press Enter when the command prompts for these options, so as to accept the default option.

```
bash-4.2$ ./gencert.sh root visioncorp
Type certificate information
Country[US]:
State[CA]:
Location[San Francisco]:
Organization[Org]:
Unit[San Francisco]:
email[hello@example.com]:
Generating RSA private key, 4096 bit long modulus
..........++
...........................................................++
e is 65537 (0x10001)
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            86:0c:b5:a6:08:62:5e:0c
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN=visioncorp, C=US, ST=CA, L=San Francisco, O=Org, OU=San Francisco/emailAddress=hello@example.com
        Validity
            Not Before: Jun 10 08:42:30 2022 GMT
            Not After : Jun  5 08:42:30 2042 GMT
        Subject: CN=visioncorp, C=US, ST=CA, L=San Francisco, O=Org, OU=San Francisco/emailAddress=hello@example.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
```

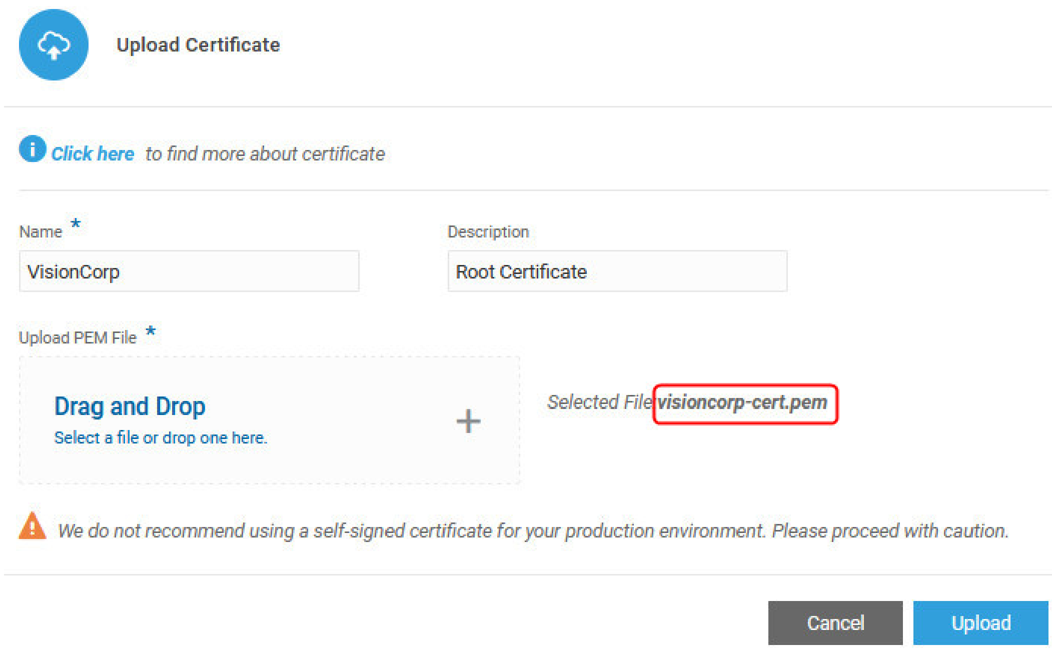
The tool generates files, such as the root certificate file (`visioncorp-cert.pem`) and the private key (`visioncorp-key.pem`) in the `certs\visioncorp` directory.

visioncorp-cert.pem
visioncorp-key.pem
visioncorp-key.pem-pkcs8

4. On the Certificates page, use the **Upload Certificate** menu option to upload the root certificate.



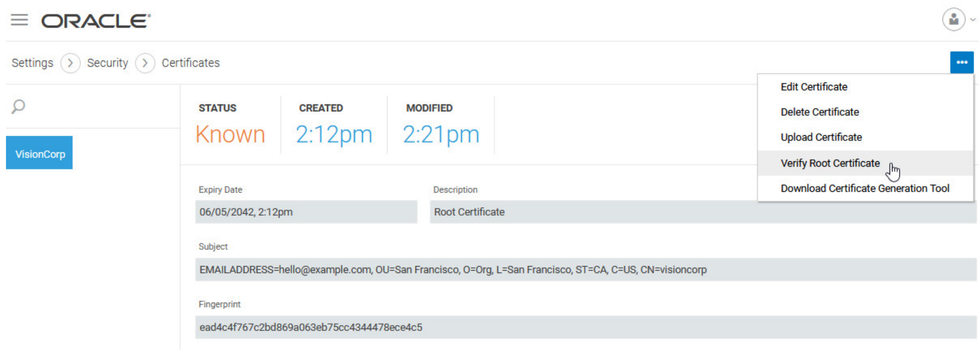
We provide a root certificate name and description, and upload the `visioncorp-cert.pem` file.



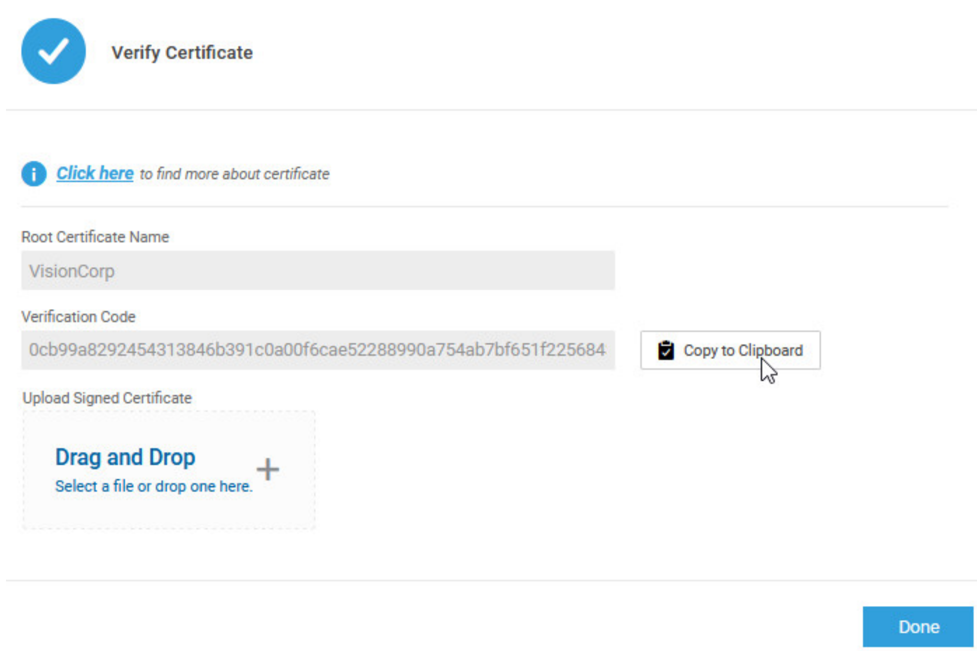
Note:

In your production environment, you would normally use a certificate issued by your CA, as opposed to a self-signed certificate.

5. Use the **Verify Root Certificate** option to verify the root certificate.



The server generates a verification code challenge that we need to sign with the private key to verify the certificate. Click **Copy to Clipboard** to copy the verification code. We'd next use it in the `gencert.sh` utility to generate the verification certificate.



6. Use the `gencert.sh` command to generate the verification certificate by signing the verification code with the private key associated with the root certificate.

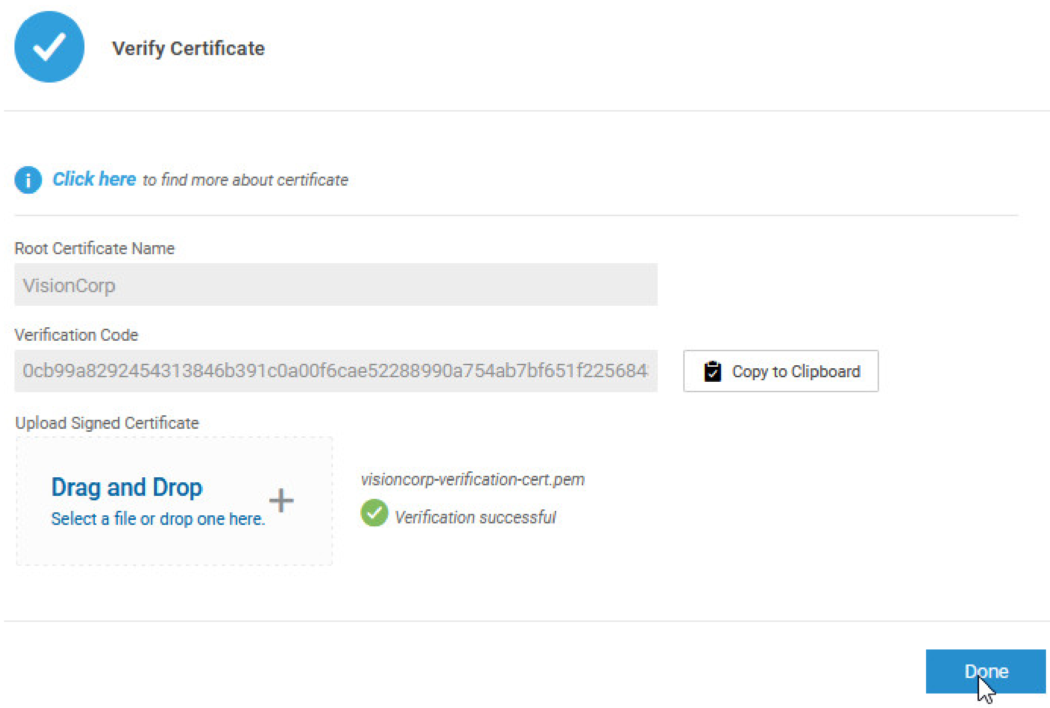
   `gencert.sh verify` *`cert-common-name verification-code`* generates the verification certificate for the given certificate common name (CN) and verification code.

   We use the copied verification code in the following command:

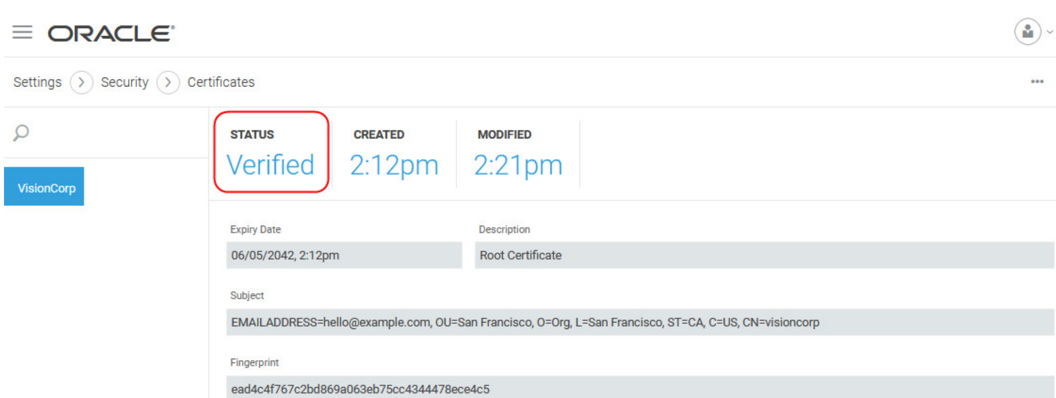
```
bash-4.2$ ./gencert.sh verify visioncorp 0cb99a8292454313846b391c0a00f6cae52288990a754ab7bf651f2256843aa4
Signature ok
subject=/CN=0cb99a8292454313846b391c0a00f6cae52288990a754ab7bf651f2256843aa4
Getting CA Private Key
```

   The `gencert.sh` tool adds the `visioncorp-verification-cert.pem` file to the `certs\visioncorp` directory.

7. Upload the signed certificate (`visioncorp-verification-cert.pem`) in the **Verify Certificate** dialog and confirm successful verification.



Notice that the status of the root certificate changes from *Known* to *Verified*.

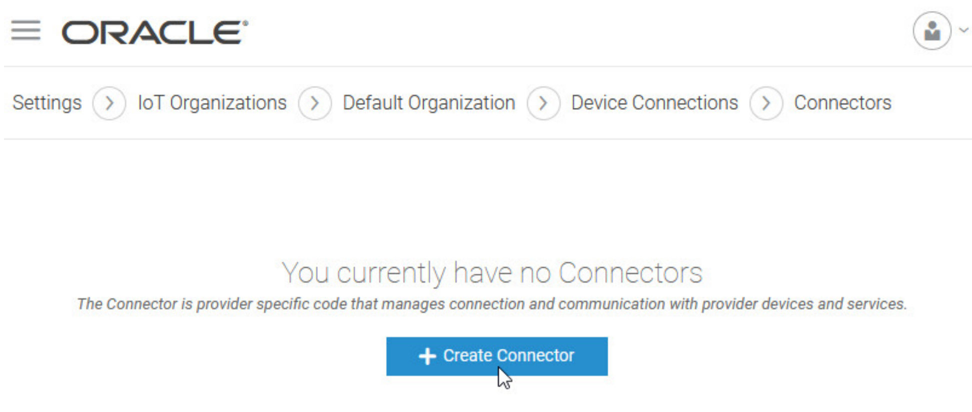


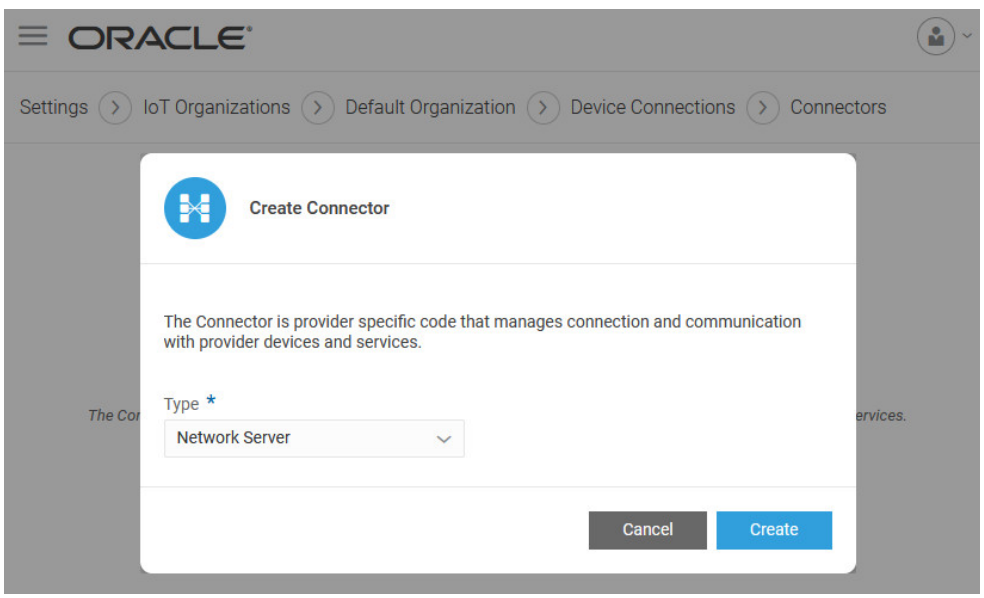
Demonstration: Ingest Data Through a Connector Using Certificate-Based Authentication

We create a connecter, and ingest data for an asset that connects through this connector. We create and use the leaf certificate of the connector to authenticate with the IoT server. We use the MQTTS protocol to publish data.

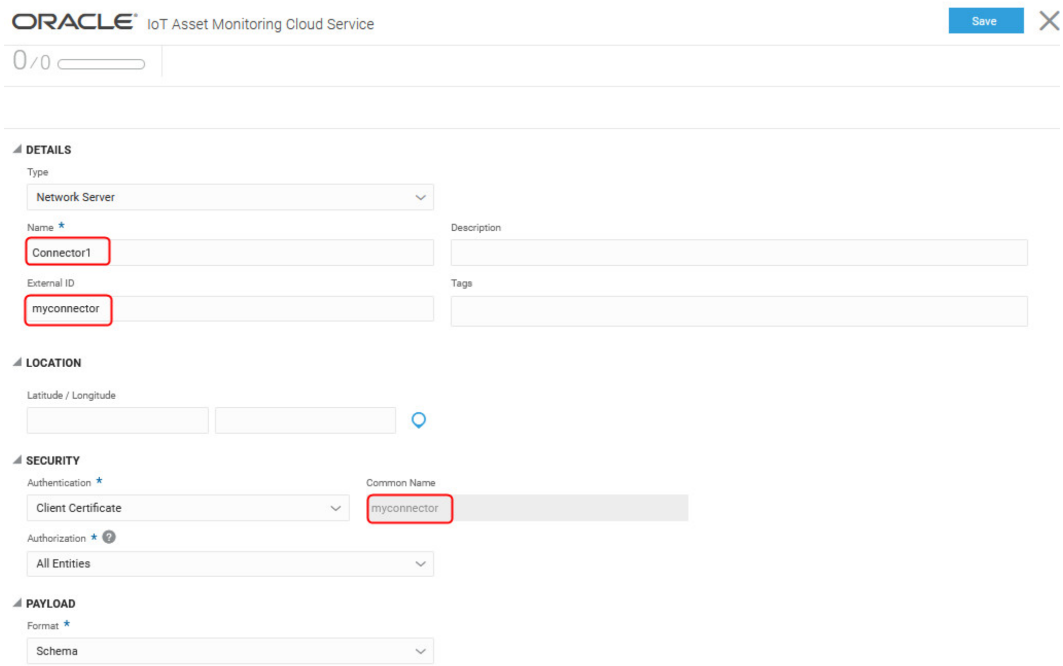
The IoT server traces the certificate chain to the validated root certificate and allows data ingestion for the asset.

1. Use the **Create Connector** option to create a connector from the **Menu >Settings > IoT Organizations > *Organization Name* > Device Connections > Connectors** page.



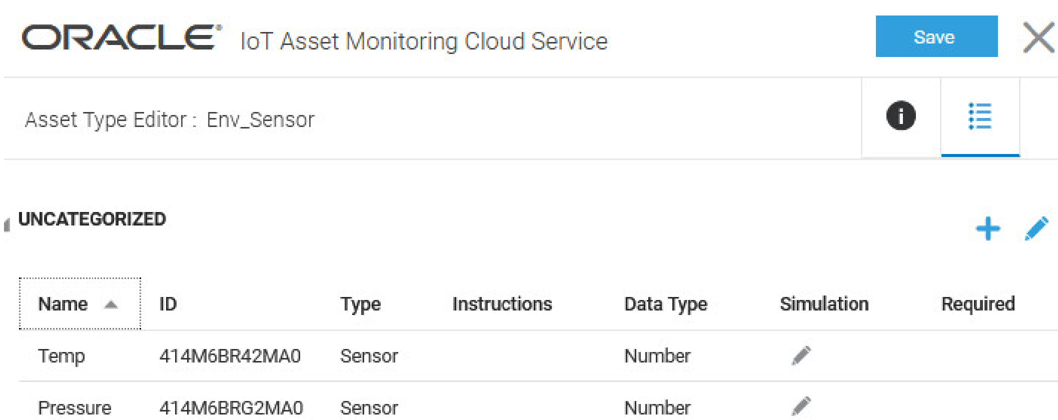


We create a **Network Server** connector here. You could also create a gateway connector.



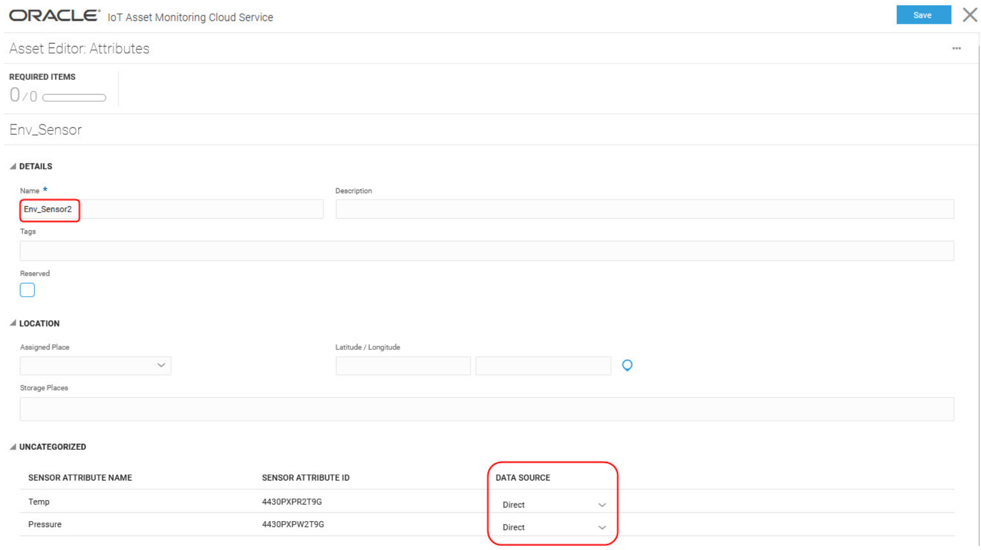
We specify a connector **Name** (`Connector1`) and **External ID** (`myconnector`). We choose **Client Certificate** authentication. The **External ID** of the connector is used as the **Common Name** for client certificate authentication. When creating a leaf certificate for the connector, we must use the same common name.

2. Create the asset type.



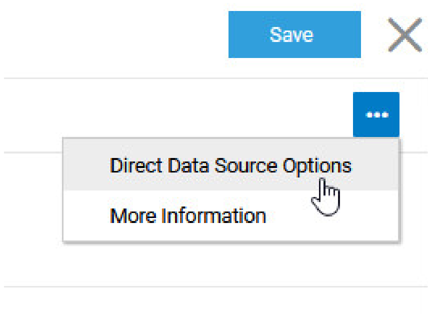
We create an asset type, `Env_Sensor` with sensor attributes for temperature and pressure.

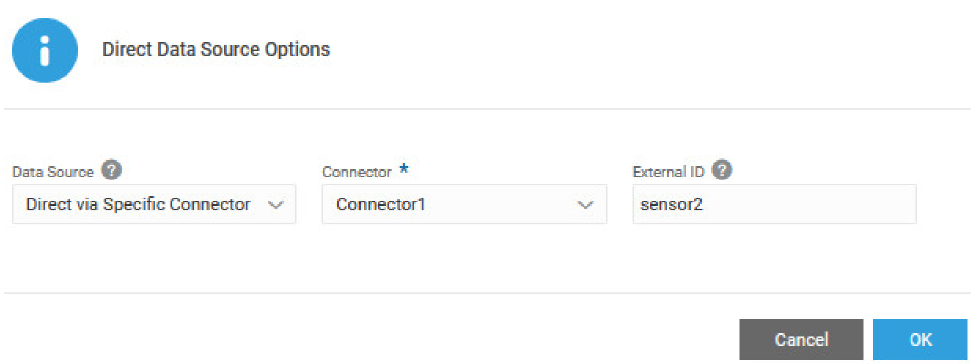
3. Create an asset for the asset type, and set the data source for the sensor attributes to **Direct**.



We create an asset, `Env_Sensor2` for the asset type, and set the **Data Source** value for the sensor attributes `Temp` and `Pressure` to **Direct.**

4. Set the **Direct Data Source Options** for the asset in the Asset Editor.





We configure the asset sensor attributes to use the connector that we created. We specify an external ID, `sensor2` to identify the sensor device in the MQTT topic.

5. Create the certificate hierarchy in IoT and create the leaf certificate for the connector.

We create an intermediate certificate for the verified root certificate and upload it to the IoT server. Next, we create a leaf certificate with the intermediate certificate as its parent. The leaf certificate uses the common name of the connector. The leaf certificate is used by the connector when connecting to the IoT server to send data for the asset.

a. Create an intermediate certificate for the verified root certificate.

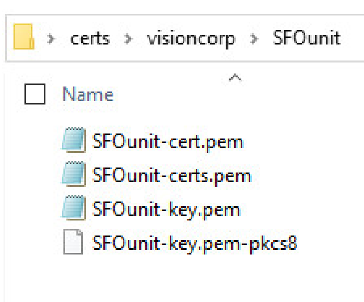
We run the `gencert.sh` utility to generate the intermediate certificate:

`./gencert.sh intermediate` *`intermediate-common-name`* `--parent` *`parent-common-name`*

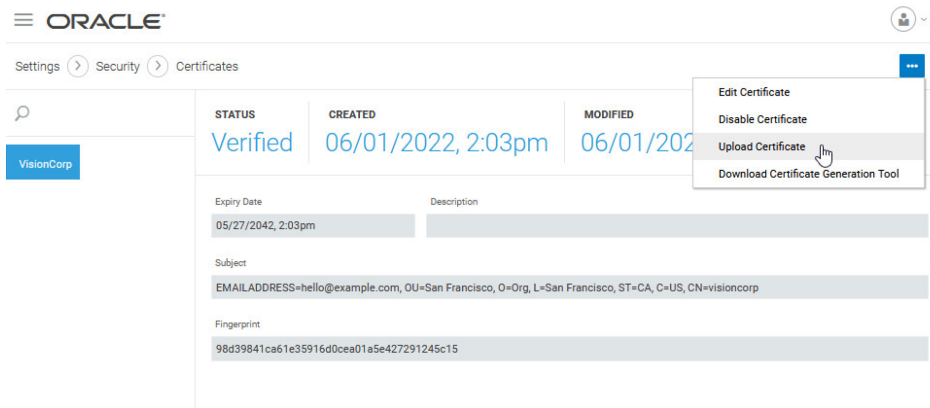
```
bash-4.2$ ./gencert.sh intermediate SFOunit --parent visioncorp
Type certificate information
Country[US]:
State[CA]:
Location[San Francisco]:
Organization[Org]:
Unit[San Francisco]:
email[hello@example.com]:
Generating RSA private key, 4096 bit long modulus
.........................................................................................................++
.....................................................++
e is 65537 (0x10001)
Using configuration from data/config/inter_open_ssl.cnf
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            d0:34:6b:ca:3f:69:86:41
        Validity
            Not Before: Jun 15 06:33:28 2022 GMT
            Not After : Jun 10 06:33:28 2042 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = CA
            localityName              = San Francisco
            organizationName          = Org
            organizationalUnitName    = San Francisco
            commonName                = SFOunit
            emailAddress              = hello@example.com
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                AC:31:C0:E1:AF:33:72:DA:A3:98:AD:D4:19:AB:52:CB:31:3B:F8:D9
            X509v3 Authority Key Identifier:
                keyid:0E:C8:54:53:09:B6:FF:6D:74:6A:29:74:7E:5E:60:AF:48:B6:54:5B
```

We use the common name `SFOunit` for the intermediate certificate and create it under the verified `visioncorp` root certificate.

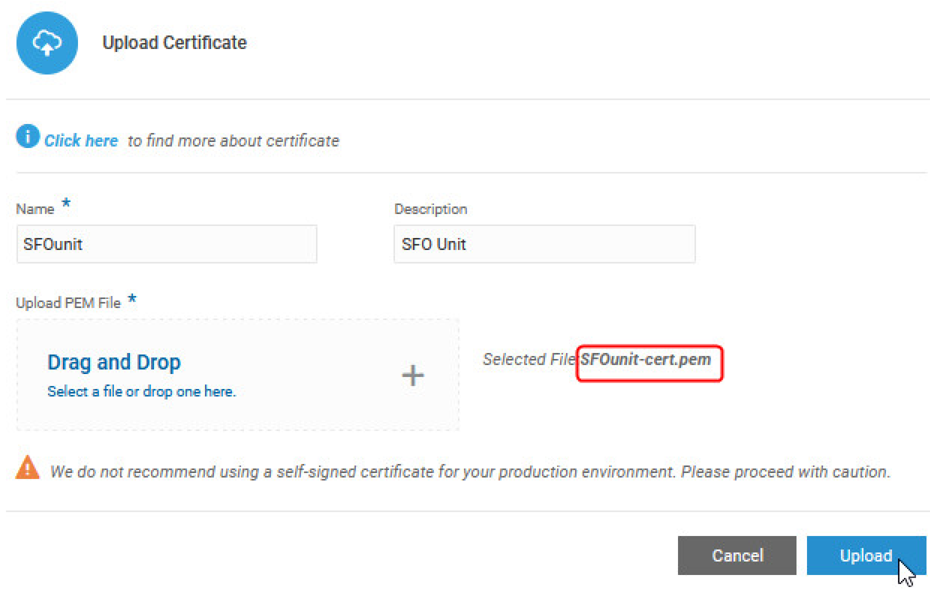
The tool generates files, such as the intermediate certificate file (`SFOunit-cert.pem`) and the private key (`SFOunit-key.pem`) under the `certs\visioncorp\SFOunit` directory.



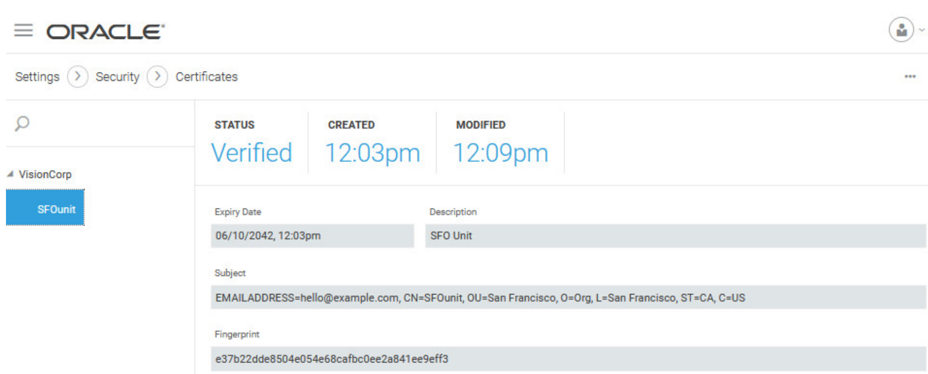
b. Upload the intermediate certificate to the IoT server.



We upload the certificate from the **Settings > Security > Certificates** page.



We specify a name and description for the certificate and upload the `SFOunit-cert.pem` certificate file.



The uploaded intermediate certificate appears on the Certificates page under the root certificate. Note that the SFOunit certificate is already verified, as it was created under the verified root certificate.

c. Create a leaf certificate for the connector.

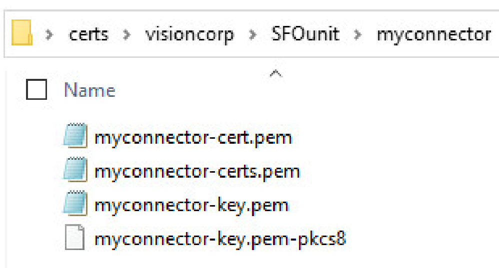
   We run the `gencert.sh` utility to generate the leaf certificate:

   ```
   ./gencert.sh leaf leaf-common-name --parent parent-common-name
   ```

   ```
   bash-4.2$ ./gencert.sh leaf myconnector --parent SFOunit
   Type certificate information
   Country[US]:
   State[CA]:
   Location[San Francisco]:
   Organization[Org]:
   Unit[San Francisco]:
   email[hello@example.com]:
   Generating RSA private key, 4096 bit long modulus
   ...........................................................................................................++
   ..................
   ..................................................................................................++
   e is 65537 (0x10001)
   Using configuration from data/config/inter_open_ssl.cnf
   Check that the request matches the signature
   Signature ok
   Certificate Details:
           Serial Number:
               d0:34:6b:ca:3f:69:86:42
           Validity
               Not Before: Jun 15 09:48:12 2022 GMT
               Not After : Jun 10 09:48:12 2042 GMT
           Subject:
               countryName               = US
               stateOrProvinceName       = CA
               localityName              = San Francisco
   ```

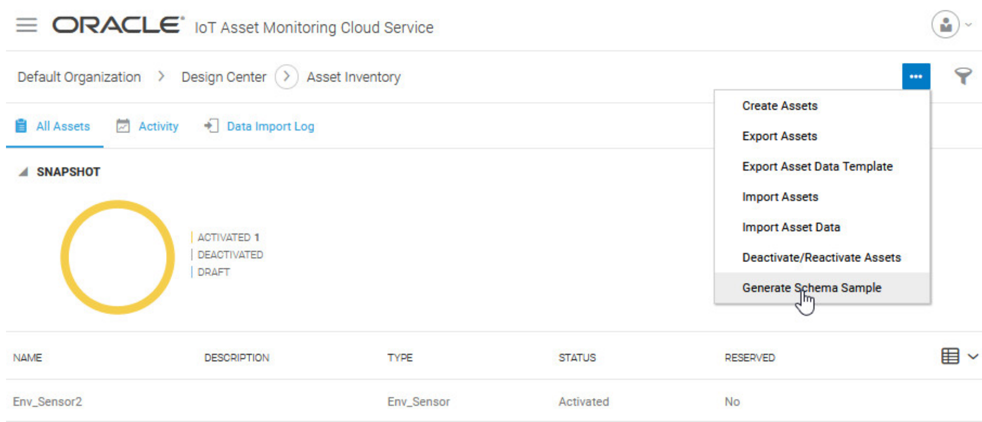
   Note that the common name for the connector leaf certificate (`myconnector`) is the same as the external ID that we specified for our connector. The leaf certificate is created with the intermediate certificate as its parent.

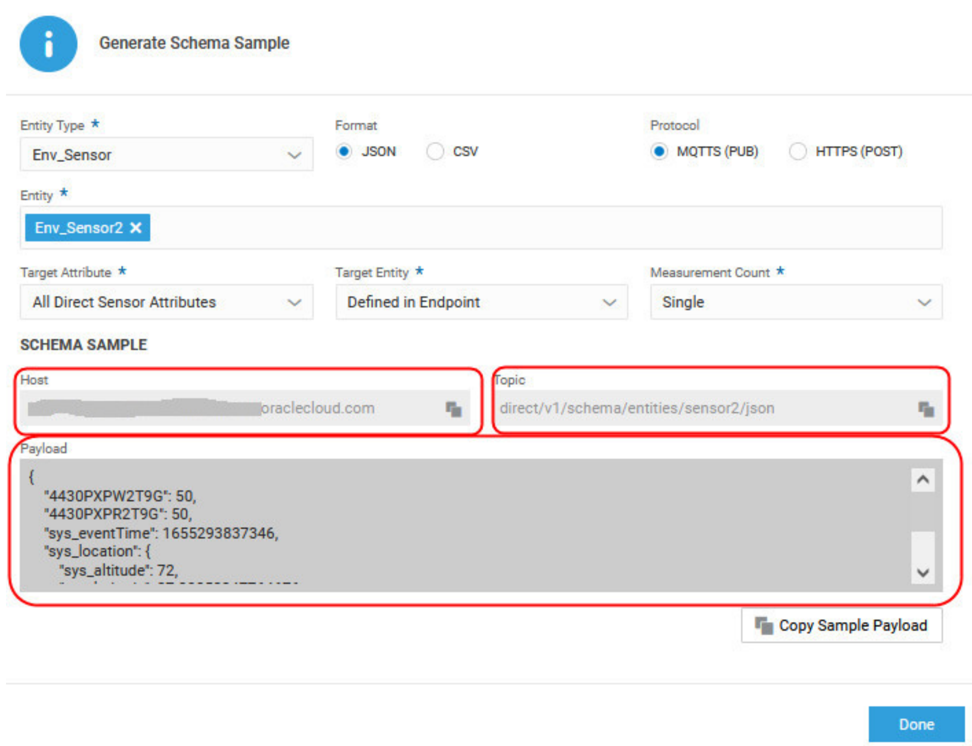
   The tool generates files, such as the leaf certificate file (`myconnector-cert.pem`) and the private key (`myconnector-key.pem`) under the `certs\visioncorp\SFOunit\myconnector` directory.



   We use the leaf certificate of the connector when sending data for the IoT device connected through the connector.

6. Generate a sample schema for the asset from the Asset Inventory page.

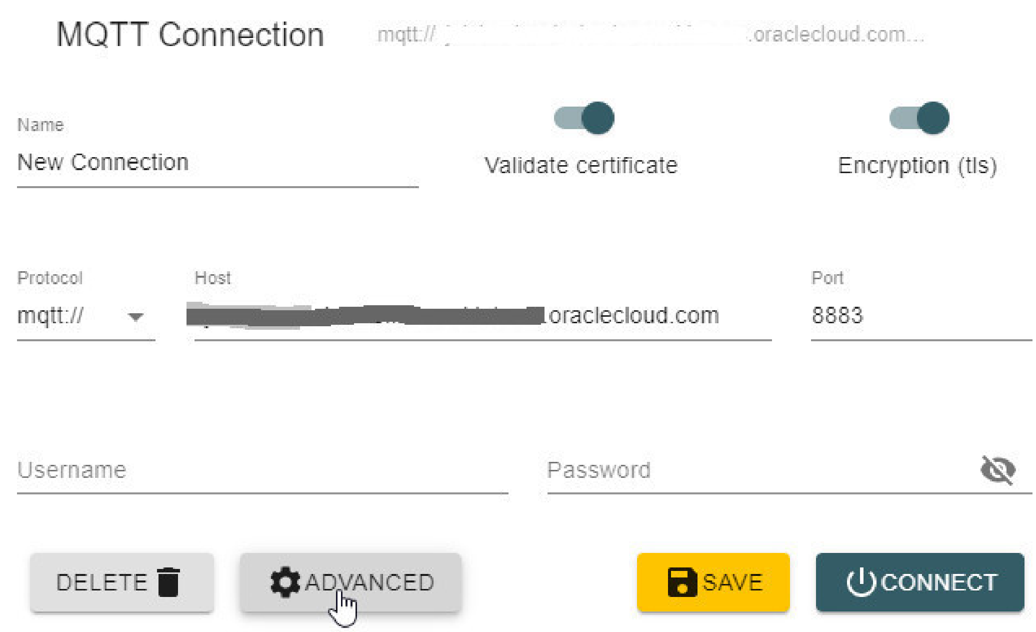




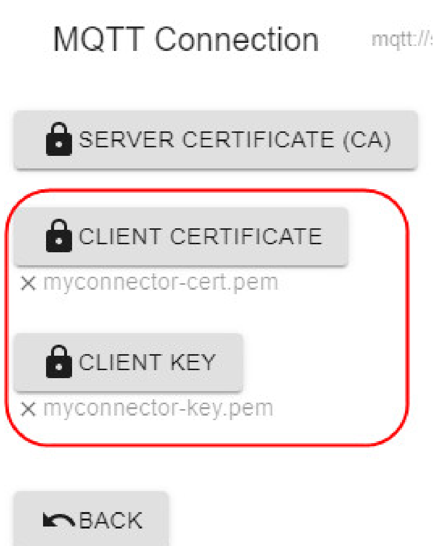
We choose a **JSON** schema and the **MQTTS (PUB)** protocol. We select the asset and choose to generate a sample payload for all its sensor attributes. The sensor ID is included in the endpoint topic here, but you could also choose to include it as part of payload. We generate a sample schema for a single measurement.

When sending data, say using MQTT Explorer, copy the host, topic, and payload from the Sample Schema dialog. Use the connector leaf certificate to authenticate. Edit the payload, as required.

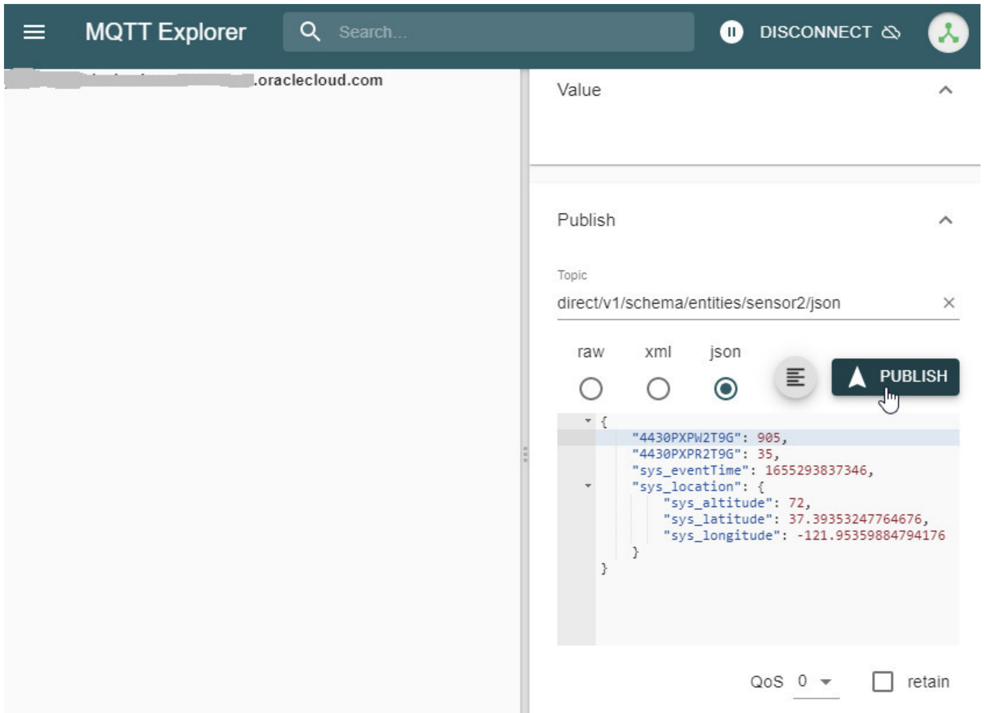
7. Send data for the device connected through the connector using an MQTT client.



We use the host info that we copied from the sample schema dialog. Make sure that the encryption switch is ON, and use the secure port 8883.

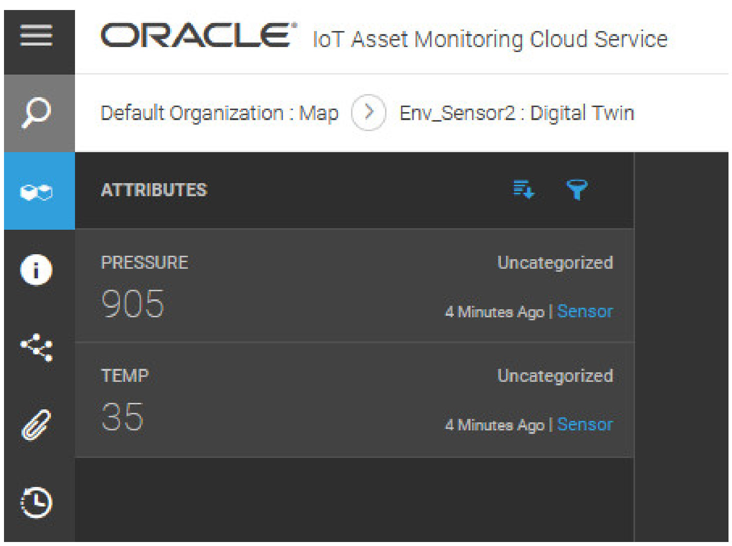


We upload the connector leaf certificate and key under the Advanced section. If you were using a directly connected device, you would use the leaf certificate for the device itself.



Once connected to the IoT server, we use the topic and payload information copied from the Sample Schema dialog. We edit the payload values as necessary, and publish.

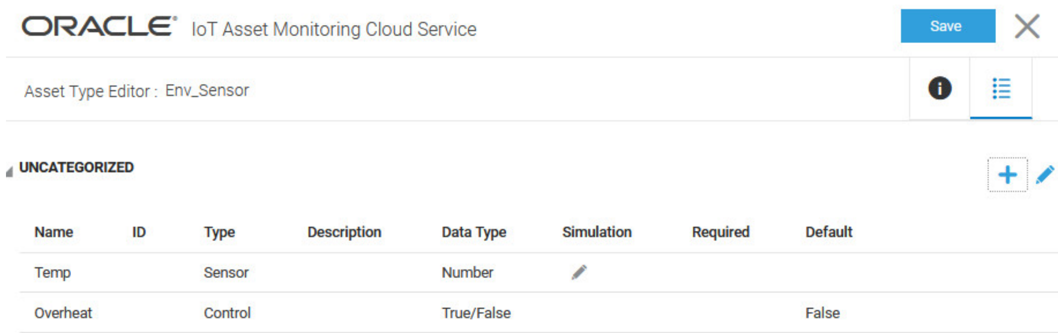
8. Verify that the published data appears in Operations Center.



Demonstration: Send Back Control Data to a Directly Connected Device

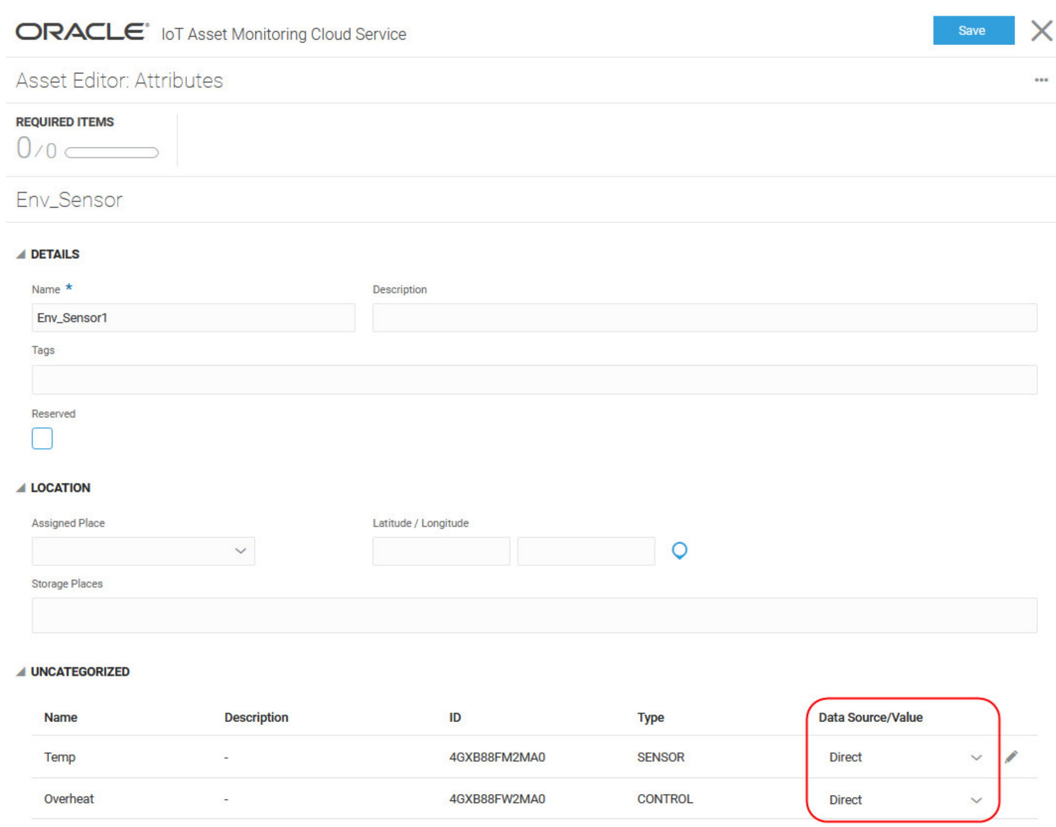
We demonstrate two-way communication with your IoT device using MQTT direct ingestion. Control attributes are used to send back control signals to the IoT device.

1. Create the asset type with sensor and control attributes.



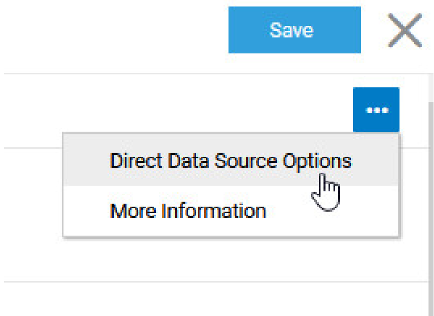
We create an asset type, `Env_Sensor` with one sensor attribute and one control attribute. The sensor attribute `Temp` measures the temperature. The control attribute `Overheat` is used to set the high temperature flag from your IoT application.

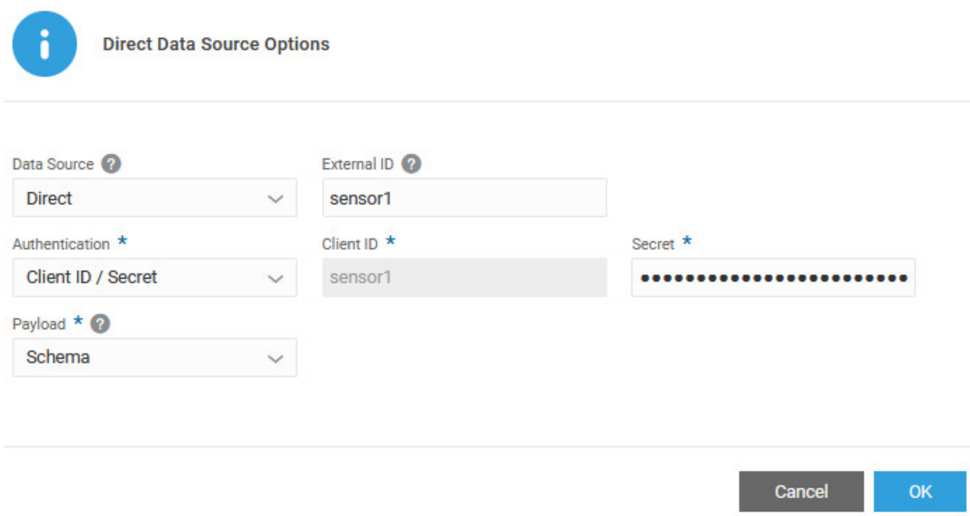
2. Create an asset for the asset type, and set the data source for the sensor and control attributes to **Direct**.



We create an asset, `Env_Sensor1` for the asset type, and set the Data Source value for the sensor attribute `Temp` and control attribute `Overheat` to **Direct.**

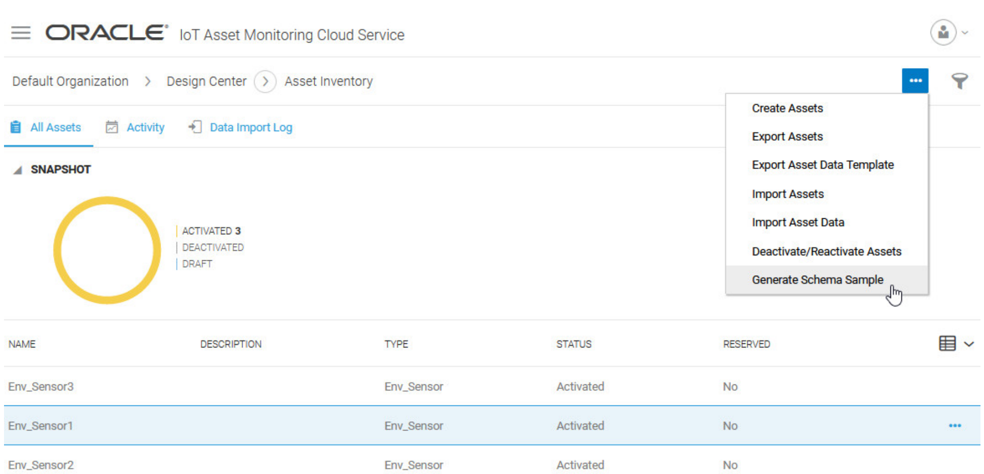
3. Set the **Direct Data Source Options** for the asset from the Asset Editor menu.

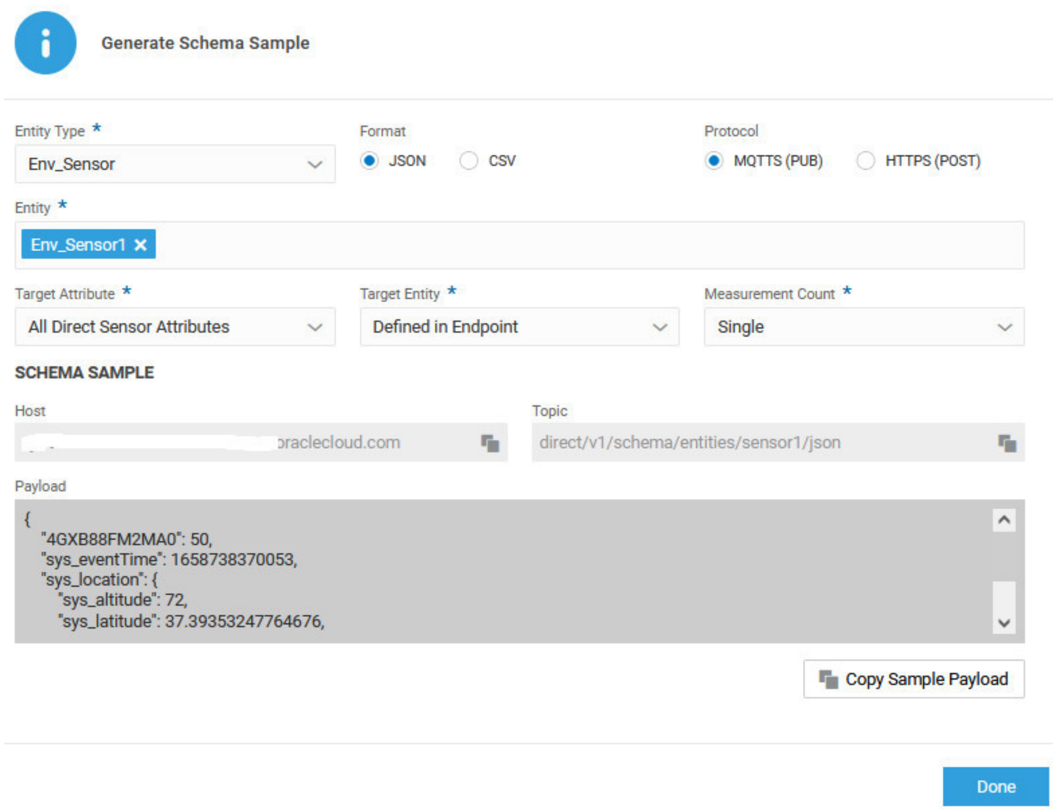




As this is a directly connected device, we choose **Direct** under **Data Source.** We specify an external ID, `sensor1`. The **External ID** is used as the **Client ID** when the device sends temperature data to the IoT server. We set the authentication method to use **Client ID/Secret** and specify a secure secret password. As we do not need a custom schema, we leave the payload set to the default schema.

4. Generate a sample schema for the asset from the Asset Inventory page.





We choose a **JSON** schema and the **MQTTS (PUB)** protocol. We select the asset and choose to generate a sample payload for the sensor attribute. The entity ID is included in the endpoint topic here, but you could also choose to include it as part of payload. We generate a sample schema for a single measurement.

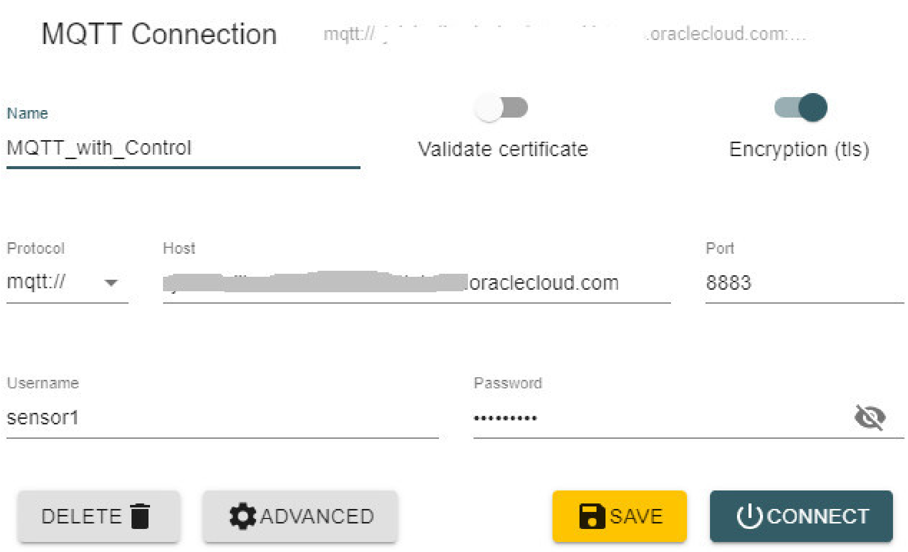
The payload contains a sample value for the sensor attribute. Note that the sensor attribute ID (`4GXB88FM2MA0`) that appears in the payload can be traced to its respective sensor name (`Temp`) in the asset editor.

> **Note:**
>
> The sample schema includes sensor attributes, and not control attributes. While sensor attribute values are generated in the device and passed to your IoT application, control attribute values can be passed back from your digital twin to the actual device.

When sending data, say using MQTT Explorer, copy the host, topic, and payload information from the Sample Schema dialog. Use the client ID as the user name and the secret, set earlier, to authenticate. Edit the payload, as required.

5. Send data for the device using an MQTT client.

   a. Configure the MQTT connection information.



We use the host info that we copied from the sample schema dialog. Make sure that the encryption switch is ON, and use the secure port 8883. Use the external ID of the asset as the user name and the secret, set earlier, to authenticate.

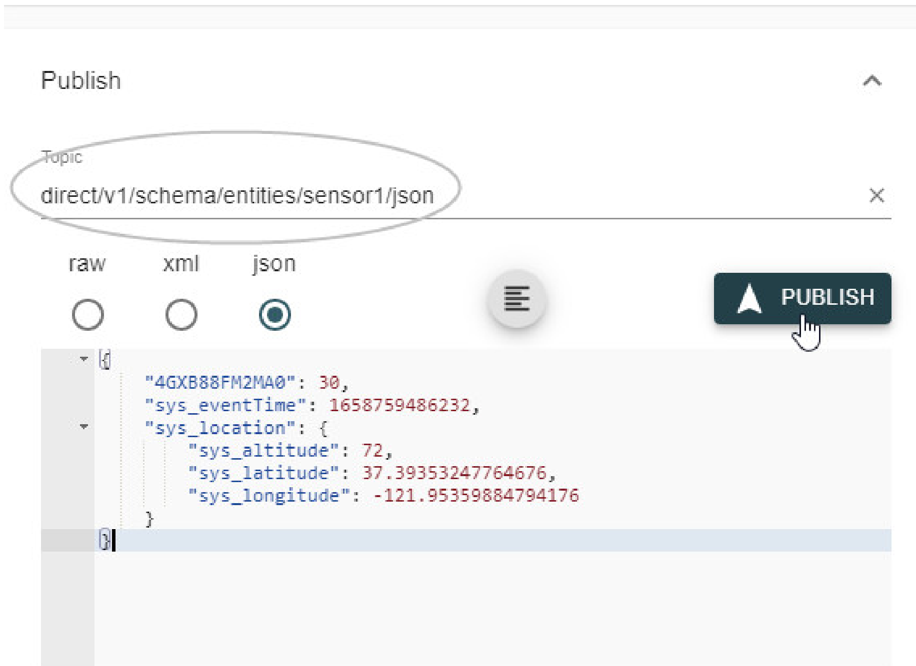
b. Add a topic to be able to pass control attributes back to the device.

You can add the topic using one of the following formats:

- `direct/v1/schema/#`
- `direct/v1/schema/entities/+/attributes/+`
- `direct/v1/schema/entities/+/attributes/`*`attributeID`*

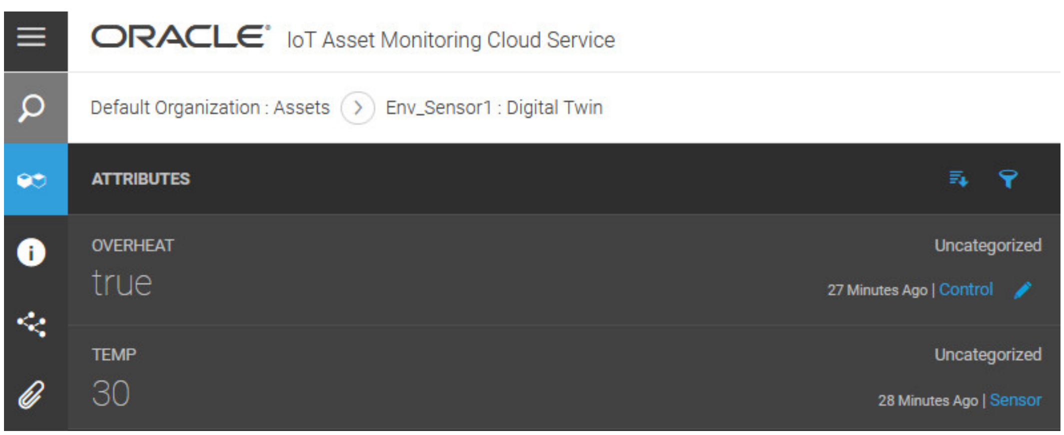
- `direct/v1/schema/entities/`*`externalID`*`/attributes/`*`attributeID`*

c. Connect to the IoT server from the MQTT client, and publish device data to the server.



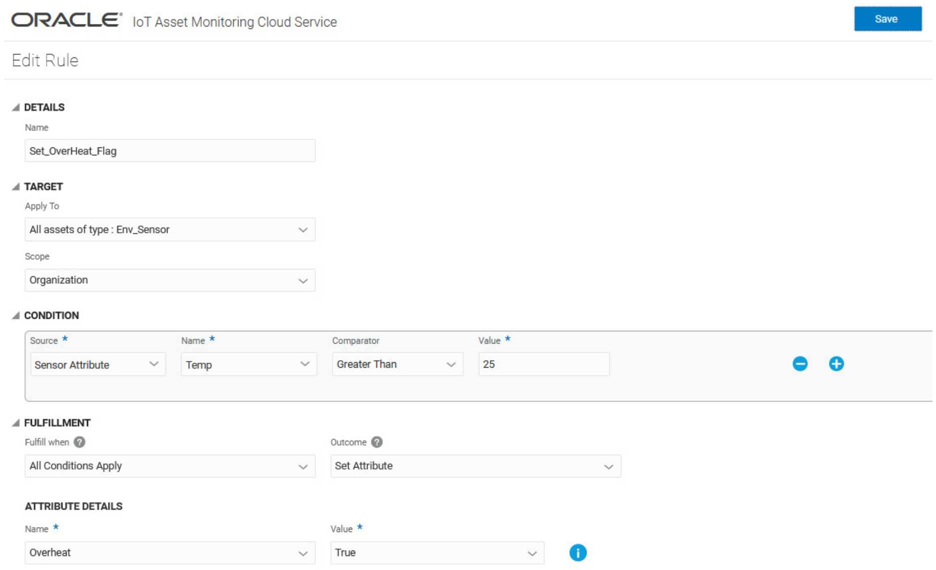
We use the topic and payload information copied from the Sample Schema dialog. We edit the payload values as necessary, and publish.

6. Verify that the published sensor data appears in Operations Center.



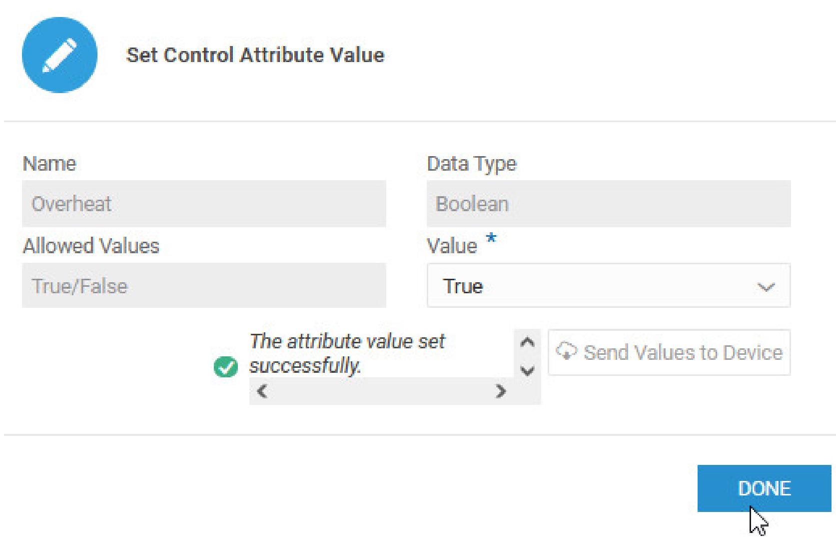
7. Send control data using a rule, or by manually editing the control attribute in Operations Center.

   a. Use a rule to set the control attribute for a device.

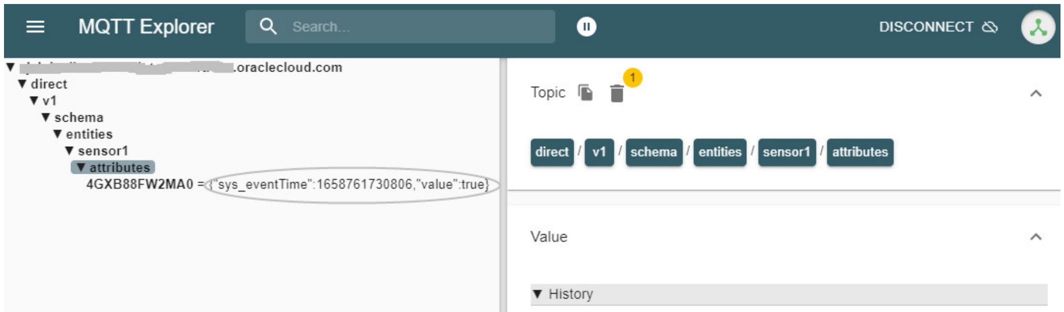


The preceding rule sets the `Overheat` control attribute to `true` if the temperature sensor value received from the IoT device is greater than 25.

b. Alternatively, manually edit the control attribute in Operations Center, and send the data to the device.



You can check the control data received in your MQTT client.



About Exporting and Importing Assets

Export and import assets to copy them from one instance to another. You can also export assets to edit them in bulk. You can then import back the updated assets into the same instance.

For example, you can create a few fully configured assets and export them to a `csv` (comma-separated value) file. You can now add the rest of the assets to the `csv` file, specify the attribute values and device associations, and import back the updated set of assets into your application.

You can also use asset export and import to move your assets from a test instance to a production instance. Each export batch can contain selected assets of a single asset type. The importing instance must already contain the asset type for the assets you are importing.

When you perform an export, the exported assets are added to an *`AssetType`*`.csv` file. Here, *`AssetType`* is the asset type name for the exported assets. The *`AssetType.csv`* file is added to a zip archive (`*.zip`) that you can save to your hard disk. If you are exporting hierarchical assets, then the child assets are also included in the *`ChildAssetType`*`.csv` file, where *`ChildAssetType`* is the asset type name for the associated child assets.

The *`AssetType`*`.csv` file details include the asset names, descriptions, locations, asset statuses, sensor attributes, and custom attributes, together with any asset alerts and function actions. For hierarchical parent assets, the associated child asset references are also included.

Export Assets

Export asset data to a file to bulk-edit assets, or to import them into another instance.

1. Click **Menu** (☰), and then click **Design Center**.
2. Select **Asset Inventory** from the **Design Center** sub-menu.
3. Under **All Assets**, filter the list of assets according to your criteria.

   You can only export assets of the same asset type.

   a. Click Filter to specify the filter criteria.
   b. Build your filter using the **Select Filter** and **Select Search Criteria** fields.

      For example, you can filter based on asset tags and type.

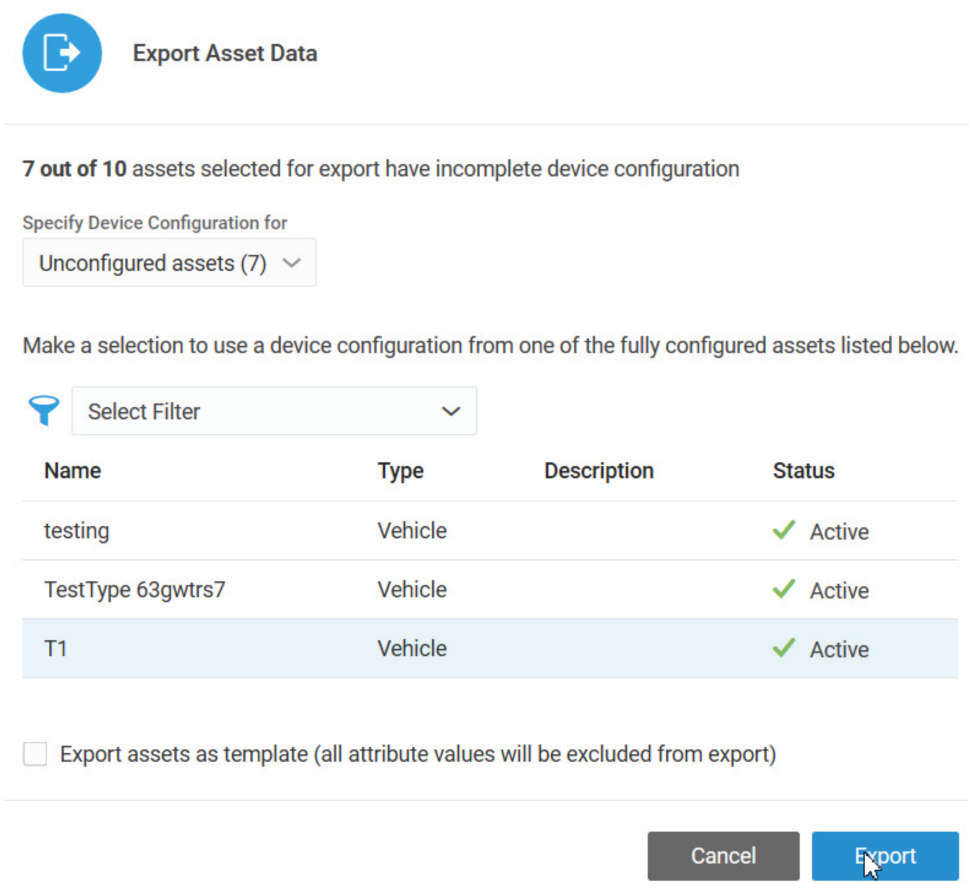
      To specify additional criteria, you can click **Add Search Filter** to add additional filters.

4. Click the **Asset Inventory Menu** and select **Export Assets** to launch the Export Assets wizard.
5. If your list of assets contains assets of more than one type, select an **Asset Type** to export and click **Continue**.

   This dialog appears only if your filtered list of assets includes more than one asset type. Only assets with the same asset type can be exported together.
6. Select an asset with complete device configuration, so that an asset template can be created for the exported assets.

   You must have at least one asset with complete device configuration to successfully export the assets.

   If you have some assets that are not associated with devices, Oracle IoT Asset Monitoring Cloud Service uses the fully-configured asset that you select to create the device model and device attribute template for your unconfigured assets.



> **Note:**
>
> The **Specify Device Configuration for** field appears only if you have Draft (unconfigured) assets in the list.

- If you choose **All Exported Assets** under **Specify Device Configuration for**, then the existing device associations for configured assets are lost.

  Use **All Exported Assets** for cases where you want to create new device associations for all exported assets. Say, you wish to import your assets into another instance of Oracle IoT Asset Monitoring Cloud Service with fresh device associations.

7. (Optional) If you select **Export Assets as Template**, then none of the asset attribute values are included in the export.

   Use this option if you wish to manually create a list of assets and attribute values based on the exported template.

8. Click **Export** to export the list of assets.

   The **Export** button is enabled only after you have selected any one fully configured asset from the list.

9. Select a disk location for the exported assets file and save the file.

   The exported zip archive (`*.zip`) contains the *`AssetType`*`.csv` file. The *`AssetType`*`.csv` file contains the asset names, descriptions, locations, asset statuses, sensor attributes, and custom attributes, together with any asset alerts and function actions. For hierarchical parent assets, the associated child asset references are also included.

Optionally Edit the Exported Assets File

You can choose to add or edit asset attribute values in the exported `csv` (comma-separated value) file before importing the assets back into the same, or another, instance. You can also add additional asset rows in the file and import.

1. Open the exported `*.zip` file on your disk.

   This is the assets file that you exported from Oracle IoT Asset Monitoring Cloud Service.

2. Open the *`AssetType`*`.csv` file in a spreadsheet or text editor.

   The *`AssetType`*`.csv` file fields appear in the following order:

   a. **Name:** The name of the exported asset.

   b. **Description:**The description of the asset.

   c. **Location:** The location co-ordinates of the asset.

   d. **Status:** The current status of the asset (`ACTIVE/DRAFT`).

   e. ***SensorAttributeName*:**
   Various sensor attributes for the asset.

      `SensorAttributeName1, SensorAttributeName2,…,SensorAttributeName`*`n`* contain the sensor attribute references for the asset.

      For sensor attributes, the field values are in the following format:

      ```
      deviceID/deviceModelURN/deviceSensorAttribute
      ```

      For example, `E4125DEF-9691-486E-B229-18333A6177C4/urn:com:oracle:iot:device:pressure_sensor/pressure`.

   f. **Custom Attribute Names:**

Various custom attributes for the asset.

`CustomAttributeName1, CustomAttributeName2,…,CustomAttributeNamen` contain the values for the values custom attributes.

For example, the **`ModelNumber`** custom attribute may contain the value `T400`.

g. ***AlertName***:
Any alerts defined for the asset type.

`AlertName1,AlertName2,…, AlertNamen` contain the alert attribute references for the asset.

For asset alerts, the field values are in the following format:

```
deviceID/deviceModelURN/deviceAlert
```

For example, `198D319A-2DED-409C-B5BD-A72EB918BDC7/urn:com:oracle:iot:device:temperature_sensor/urn:com:oracle:iot:device:temperature_sensor:too_cold`.

h. ***FunctionName/ActionName***:
Actions and action functions.

`FunctionName1/ActionName1,FunctionName2/ActionName1,…` contain the action references for the asset.

For asset actions, the field values are in the following format:

```
deviceID/deviceModelURN/deviceAction
```

For example, `101743FB-A310-4BEF-B4C4-8D82BA48CE04/urn:com:oracle:iot:device:temperature_sensor/reset`.

The following image shows a sample *`AssetType.csv`* extract:

Name	Description	Location	Status	Temp	Temp_Too_Cold	Temp_Too_Hot	Switch/Power Toggle
Room103	Temperature sensor for Room#103		ACTIVE	63712DCB-7689-412E-BD1C-E51F553A806D/urn:com:oracle:iot:device:temperature_sensor/temp	63712DCB-7689-412E-BD1C-E51F553A806D/urn:com:oracle:iot:device:temperature_sensor/urn:com:oracle:iot:device:temperature_sensor:too_cold	63712DCB-7689-412E-BD1C-E51F553A806D/urn:com:oracle:iot:device:temperature_sensor/urn:com:oracle:iot:device:temperature_sensor:too_hot	
Room102	Temperature sensor for Room#102	36.597889133,-118.125000000	ACTIVE	0CB117A4-A49E-4662-AA19-30D009AA25CE/urn:com:oracle:iot:device:temperature_sensor/temp	0CB117A4-A49E-4662-AA19-30D009AA25CE/urn:com:oracle:iot:device:temperature_sensor/urn:com:oracle:iot:device:temperature_sensor:too_cold	0CB117A4-A49E-4662-AA19-30D009AA25CE/urn:com:oracle:iot:device:temperature_sensor/urn:com:oracle:iot:device:temperature_sensor:too_hot	72868454-4453-49A1-8742-363E1AD61739/urn:com:oracle:iot:device:temperature_sensor/reset
Room101	Temperature sensor for Room#101		ACTIVE	72868454-4453-49A1-8742-363E1AD61739/urn:com:oracle:iot:device:temperature_sensor/temp	72868454-4453-49A1-8742-363E1AD61739/urn:com:oracle:iot:device:temperature_sensor/urn:com:oracle:iot:device:temperature_sensor:too_cold	72868454-4453-49A1-8742-363E1AD61739/urn:com:oracle:iot:device:temperature_sensor/urn:com:oracle:iot:device:temperature_sensor:too_hot	

3. Edit the *`AssetType.csv`* file to add or edit rows, as required.

> **Note:**
>
> The details on the device IDs and URNs can be found in the Oracle Internet of Things Cloud Service management console. Navigate to **Menu > Devices > Management** and click **Edit** against a device to see its device ID and device model URN.

Import Assets

Import the assets data into an Oracle IoT Asset Monitoring Cloud Service instance to add assets, or to update existing assets.

> **Note:**
>
> The importing instance must already contain the asset type for the assets you are importing.

If an asset being imported already exists in your Oracle IoT Asset Monitoring Cloud Service instance, then the asset is updated with the attribute data from the imported file. If an asset being imported does not already exist in your Oracle IoT Asset Monitoring Cloud Service instance, the asset gets added.

1. Click **Menu** (☰), and then click **Design Center**.
2. Select **Asset Inventory** from the **Design Center** sub-menu.
3. Click the **Asset Inventory Menu** ••• and select **Import Assets**.
4. Click **Choose File** in the Import Assets dialog and select the previously exported `*.zip` assets file.
5. Click **Import**.

   You get an information message that the import task has started.
6. To check the status of the import at any time, click the **Activity** tab.

   The activity log contains information on the import status and the number of assets that were successfully imported.

   You can also use search filters to filter the activity log.
7. Examine your assets under the **All Assets** tab on the Asset Inventory page to look for new or updated assets.

   You can use the search filters to narrow down your search.

View Asset Details

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

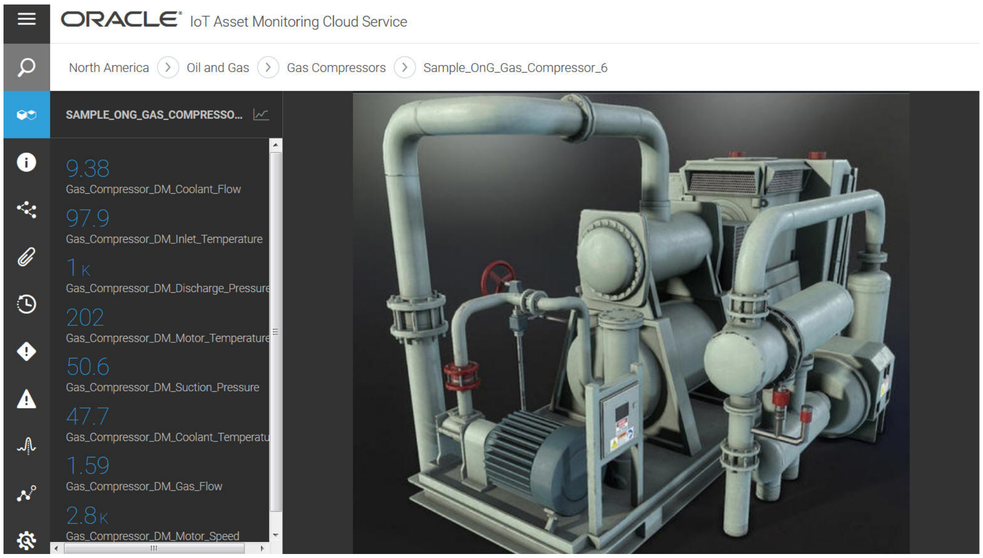
1. In the Operations Center for your organization, click **Assets** .
2. Use the breadcrumbs to navigate to the appropriate group if your asset appears in a group.

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.

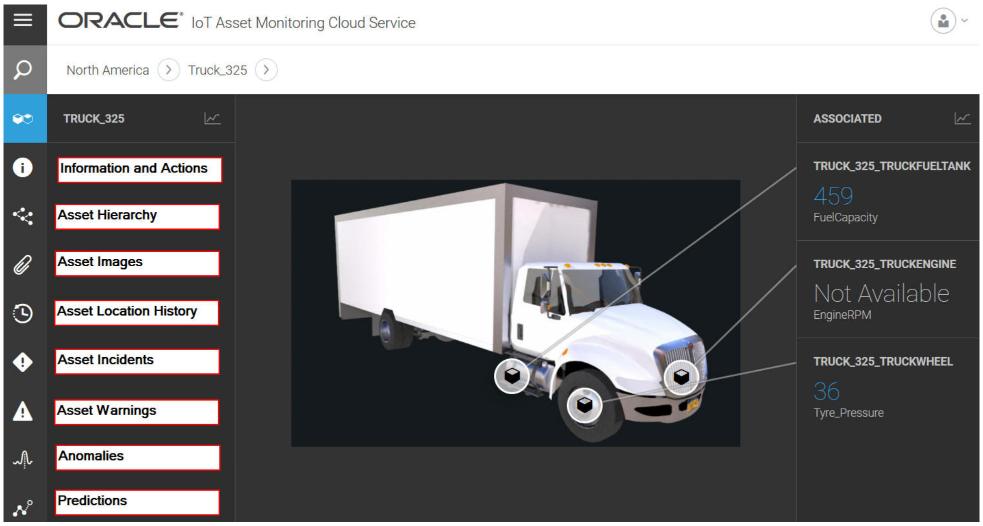
3. Click **Show Details** ( ) against the appropriate asset row.

   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.

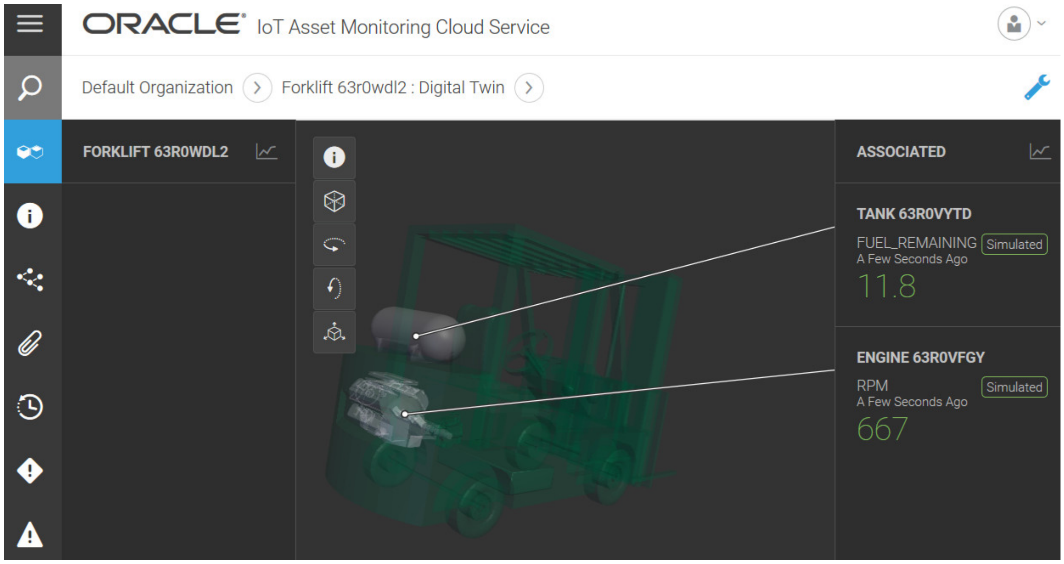
   The following image shows the digital twin version of a gas compressor asset along with its sensor attributes:



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



If your asset uses a 3D model, then the 3D model appears along with the associated viewing tools. The following image shows the digital twin for a forklift asset.



The following tools are available:

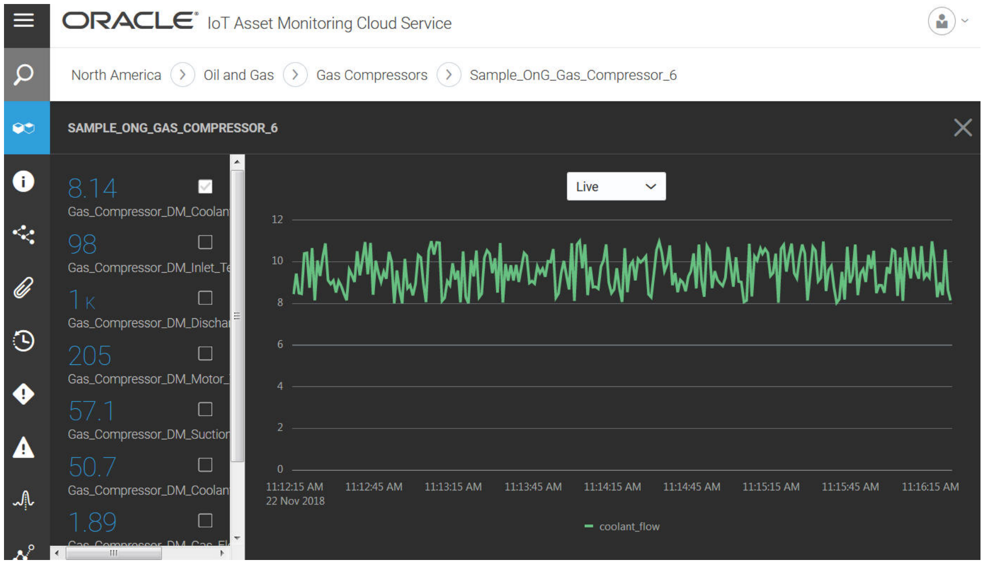
- Explode : You can also choose to explode the model, so that the sub-components separate out to varying degrees. Use the slider tool to choose the degree of separation.
- Rendering Style : Choose between the available styles, such as Wireframe, Shaded, and X-Ray.
- Rotate Right : Use to rotate the asset model along the horizontal plane.
- Rotate Down : Use to rotate the asset model along the vertical plane.
- Orientation : Use the pin icon to save the current orientation, so that the same default orientation is used in the digital twin view in Operations Center. The reset icon switches back the orientation to the last pinned one.

4. Select 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:

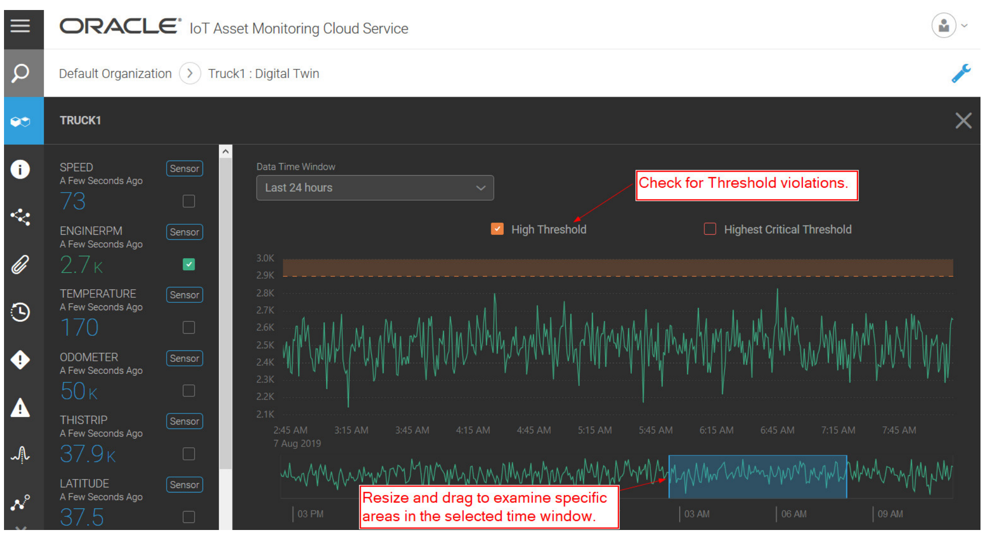
   - **Live**
   - **Last 1 Hour**
   - **Last 24 Hours**
   - **Last 7 Days**
   - **Last 30 Days**
   - **Custom:** Lets you select a custom time period from the calendar.

   The following image shows the live sensor plot for coolant flow data from a gas compressor asset:

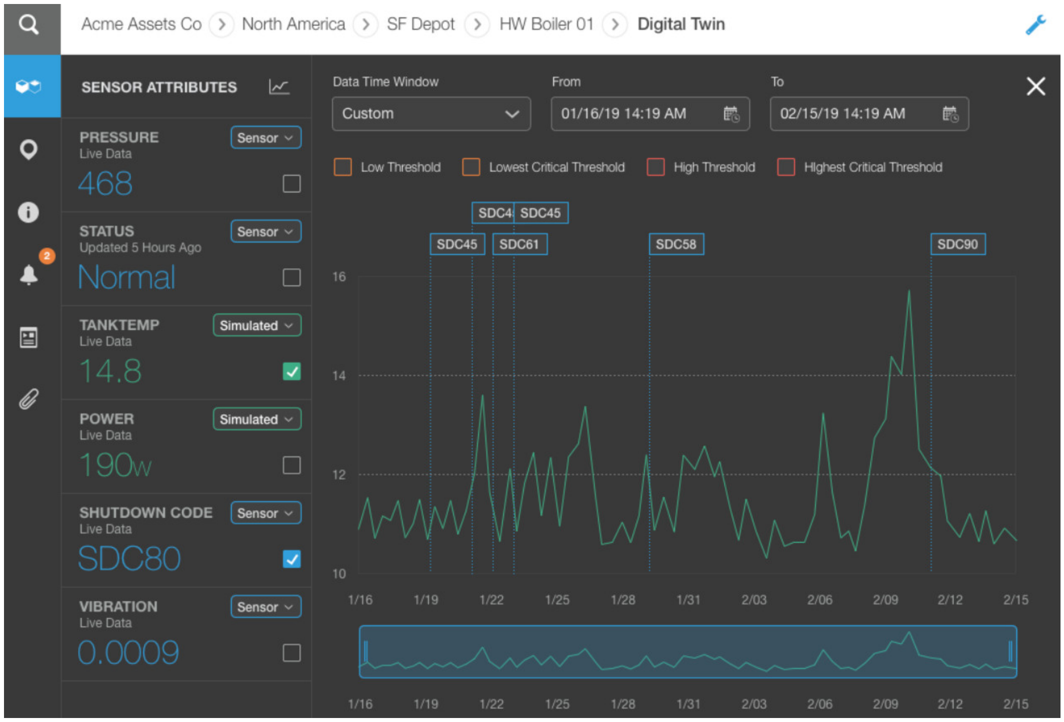


If you have defined high and low threshold values for your sensor attribute, you can choose to display these bars against the plot, so that you can examine threshold violations, if any.
You can choose to re-size and drag the highlighter on the time line to examine a specific portion of the plot more closely.

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

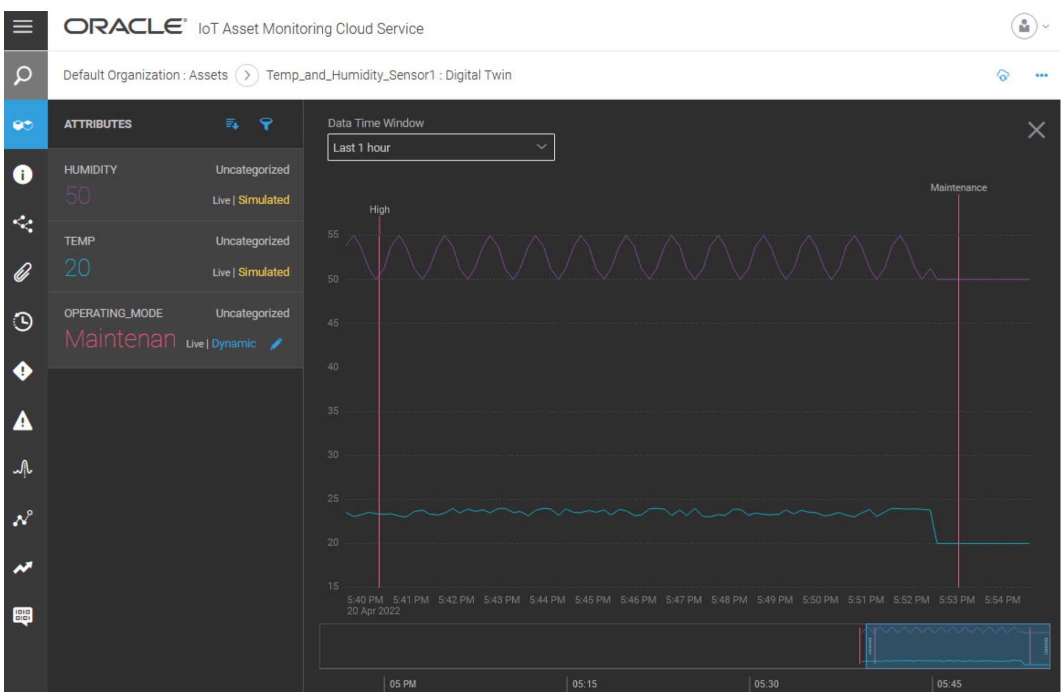


You can also select multiple sensor attributes to compare or correlate them. The following example selects the *tank temperature* sensor attribute. It also selects the *shutdown code* attribute to investigate possible correlation between temperature spikes and shutdown events.



Note that string attribute values can also be displayed on the data plot.

The following image shows a dynamic attribute plotted along with sensor attributes. Notice that you can edit the dynamic attribute value in Operations Center. For example, the operating mode value in the following chart changes from *High* to *Maintenance*.



5. Use the menu bar on the left to navigate to various views:
   - **Search**: Lets you search for other assets, groups, locations and places.

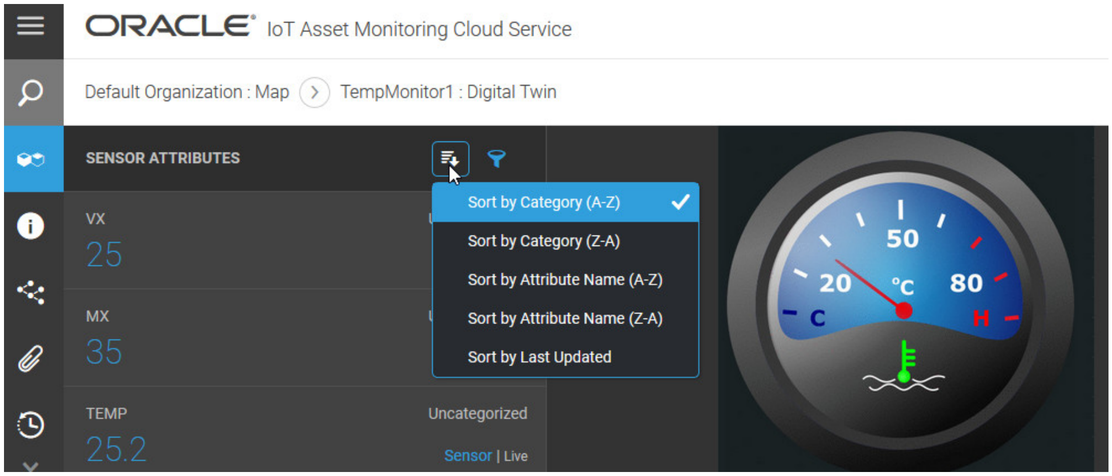
- **Digital Twin**: Shows the digital twin version of the asset along with its current sensor attribute values along with the sensor attribute values of all associated sub-assets.
- **Info**: Shows all standard attribute information and actions available for the asset. You can also use the **Info** page 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.

Sort and Filter Sensor Attributes

The Digital Twin view includes adaptive views and capabilities to filter and sort the sensor attributes for your assets and associated child entities.

The sensor attributes for your assets and associated entities appear category wise, by default. You can change the sort order to arrange attributes by name, or have the attributes with the latest updates appear on top. You can also filter the attributes list based on the attribute name or category.

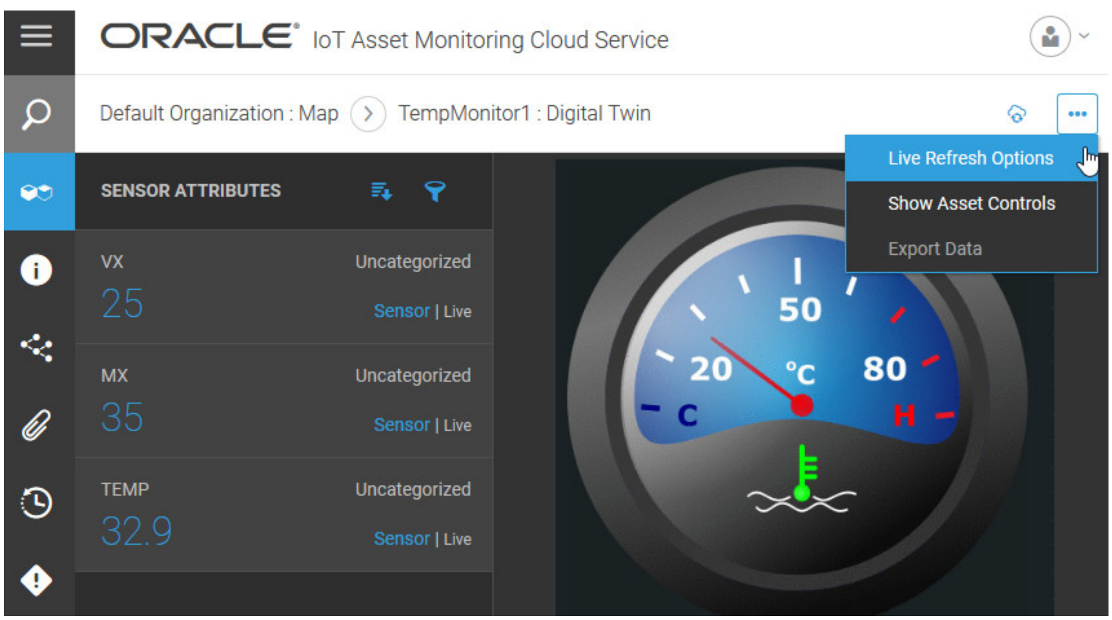


If you have a large number of associated entities for an asset, say fifty or more, then the Digital Twin view automatically creates an additional column for the associated entities. You can conveniently select an associated entity from the column to view its sensor attributes in a separate column.

Change Live Refresh Options for Your Sensor Attributes

You can disable or re-enable automatic refresh for the sensor attribute values of your assets in the Digital Twin view. When enabled, you can choose the refresh frequency.

You can select refresh intervals between 10 seconds and 5 minutes. Use the Digital Twin menu to set the live refresh options.



Customize Asset Visualization Options

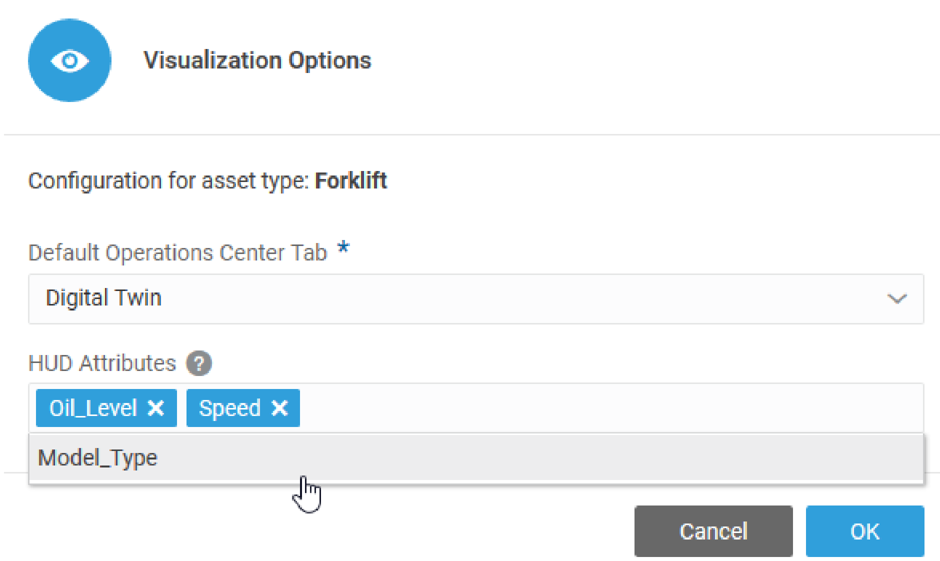
When browsing assets in the map view, you can quickly preview important asset attribute values without leaving the map view. You can also choose the default view or dashboard to launch when accessing asset details from the map.

To set visualization options for all assets of an asset type:

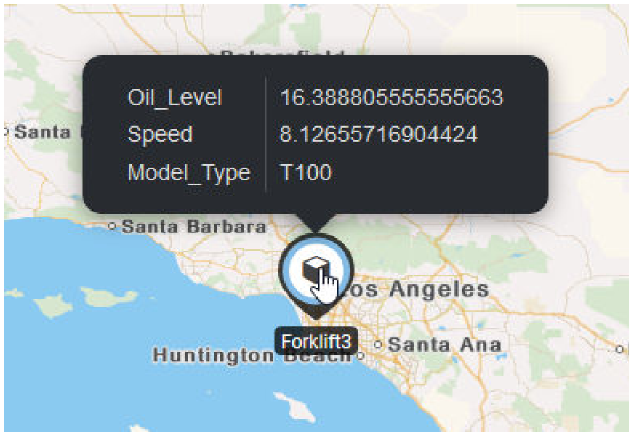
1. Click **Menu** ≡ and then click **Design Center**.
2. Select **Asset Types** from the **Design Center** sub-menu.
3. Select an asset type from the **Asset Types** list.

   You can also search for an asset type.
4. Click **Visualization Options**.
5. Optionally change the **Default Operations Center Tab**.

   When you access an asset in the map, the **Digital Twin** view opens by default. You can change this behavior to open the page of your choice. For example, you can choose to directly open the **Incidents** page for the asset. Or you may choose to launch a custom dashboard that you created for the asset type.
6. Select one or more **HUD Attributes** (Heads-Up Display Attributes).



In the operations center, the selected **HUD Attributes** appear as a pop-up preview when you click an asset in the map. This lets you quickly preview relevant asset attributes without leaving the map view.



If you click on the asset again, the default operations center tab opens up for the asset.

See Locate Your Assets in the Map View for more information on accessing assets in the map view.

7. Click **OK** to close the Visualization Options dialog.

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** ( ) 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.

Deactivate and Reactivate Assets

You can deactivate assets that do not need to be monitored, such as assets created for projects and campaigns that have completed. Deactivated assets are hidden from the Operations Center map, by default. Deactivated assets do not generate device data and rules are not applied to such assets.

For hierarchical assets, you must deactivate the asset at the parent asset level. You cannot deactivate a child asset separately.

You can choose to reactivate a previously deactivated asset.

Deactivate an Asset

You can deactivate an asset from either the **Design Center > Asset Inventory** page or the **Operations Center > Assets** page.

1. Click **Menu** (≡), and then click **Design Center**.
2. Select **Asset Inventory** from the **Design Center** sub-menu.
3. Find your 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 **Edit** against the asset row.
5. Click **Deactivate Asset** adjacent to the asset status.

   If there are any associated sub-assets for the asset, the sub-assets are also deactivated. Any data received from deactivated assets is not included in computations, such as rules, metrics, predictions, anomaly detection, and trends.
6. Click **Apply** to confirm.

7. Click **Save**.
8. Close the Edit Asset window to return to the **Assets** list.

Reactivate an Asset

You can reactivate a previously deactivated asset from either the **Design Center > Asset Inventory** page, or the **Operations Center > Assets** page.

1. Click **Menu** (), and then click **Design Center**.
2. Select **Asset Inventory** from the **Design Center** sub-menu.
3. Find your 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 **Edit** against the asset row.
5. Click **Reactivate Asset** adjacent to the asset status.

   If there are any associated sub-assets for the asset, the sub-assets are also reactivated.

6. Click **Apply** to confirm.
7. Click **Save**.
8. Close the Edit Asset window to return to the **Assets** list.

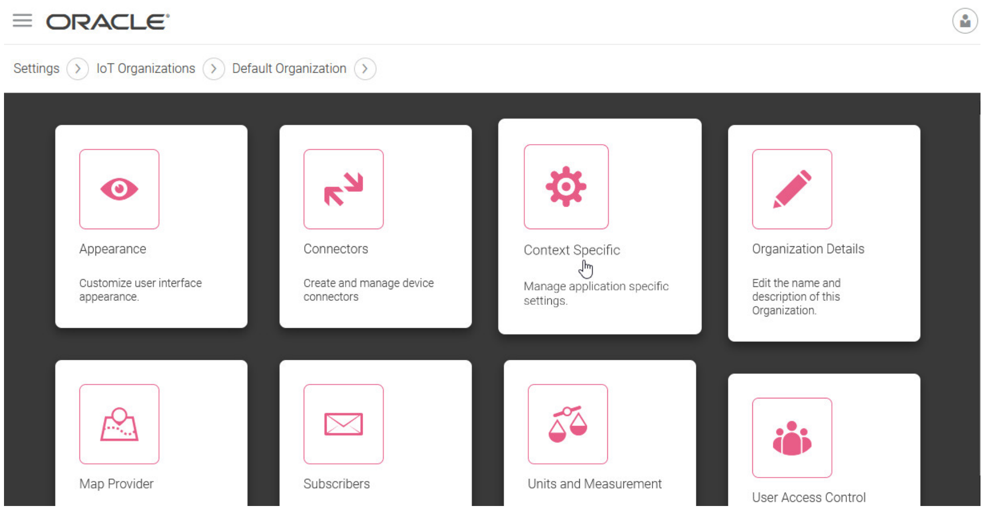
Changing the Default Visibility Option for Deactivated Assets

Deactivated assets are hidden from Operations Center views, such as the map view, by default. You can change the default visibility setting for deactivated assets in the organization from the Settings page.

1. In Oracle IoT Asset Monitoring Cloud Service, click **Menu** (), and then click **Settings**.

   If you are in the Design Center, you need to click **Previous** () before you see the **Settings** option in the menu.

2. On the Settings page, click **IoT Organizations**.
3. Click the name of your organization.
4. Click **Context Specific** to access the context-specific settings for your organization.



5. Click **Assets**.
6. In the Assets dialog, deselect **Hide Deactivated Assets in Operations Center** and click **Save**.

The default option is now changed to show deactivated assets in Operations Center views, such as the map view.

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** (🗑) icon.
5. Click **Yes** to confirm.

Create Asset Clusters Based on Attribute Behavior

The IoT application can automatically cluster entities based on attribute behavior. You can choose to create a clustering configuration for an asset type. This lets IoT group entities with similar attribute behavior over the specified data window.

For example, say you have a temperature sensor entity-type, but different sensors have different normal temperature ranges, depending on whether the sensor is being used to measure ambient temperature or furnace temperature. A cluster is able to separate the ambient sensor entities from the furnace sensor entities.

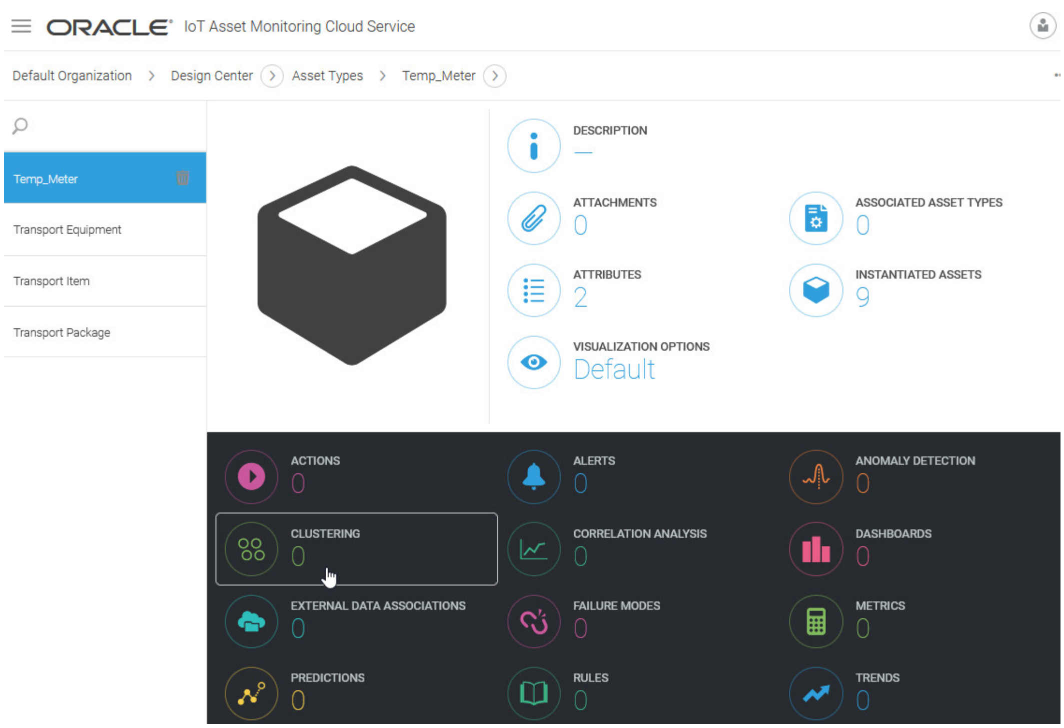
The Clustering tab in Operations Center shows you the details on the clusters, including sensor values and the cluster memberships that the application creates. You can also visualize the tightness of each cluster, and the distances between individual clusters.

Create Clustering Configuration for an Asset Type

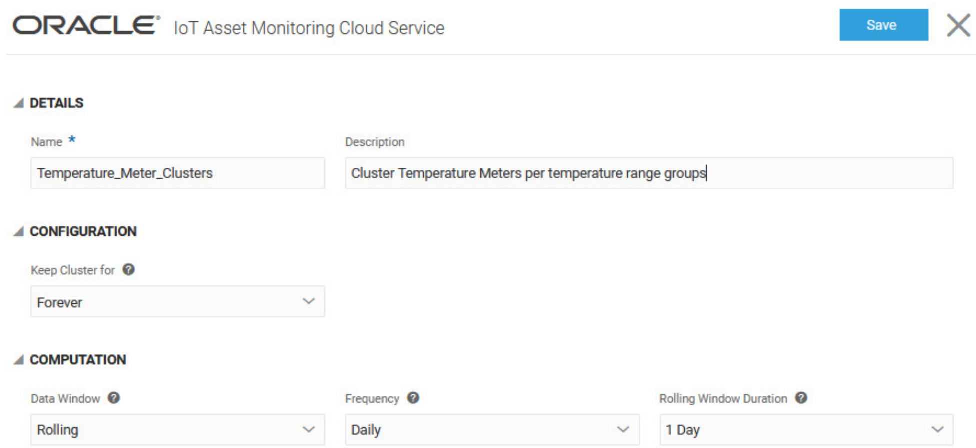
Create a clustering configuration to automatically group assets into clusters based on asset attribute behavior. You can specify a static or rolling data window to train the system for asset grouping.

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 **Clustering**.



5. Select **Create Clustering Configuration** from the page menu ••• .
6. Under the **Details** section, provide a **Name** and **Description** for the clustering configuration.



7. Under **Configuration**, specify the duration for which to keep the cluster configuration.

   The default setting **Last Value Only** stores only the last known configuration.

   If you have unique storage requirements for historical data related to this cluster, you can select an option that is different from the default setting.

8. Under **Computation**, specify a **Data Window** for training the cluster configuration.

   The **Data Window** identifies the historical data that is used to train the system for creating clusters. Asset data collected over the data window is used to determine the clusters.

   - **Rolling**: A rolling data window uses data from a rolling time window to pick the most recent data for training. For example, you can choose to train your cluster configuration with a rolling data window of the last 7 days, and choose to perform the training daily.
     When you use a rolling window, the training model is re-created periodically, as determined by the frequency that you choose.

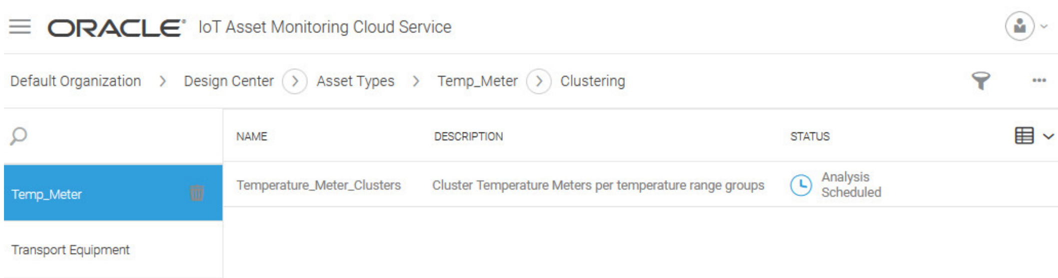
     – **Frequency**: You can optionally change the frequency of the cluster configuration training. For example, if you choose **Daily**, then the training happens every day at 00:00 hours (midnight), UTC time by default.

     – **Rolling Window Duration**: The duration of the rolling window going back from the model training time. For example, if you select **7 Days**, then the last 7 days of target attribute data is used to train the cluster configuration.

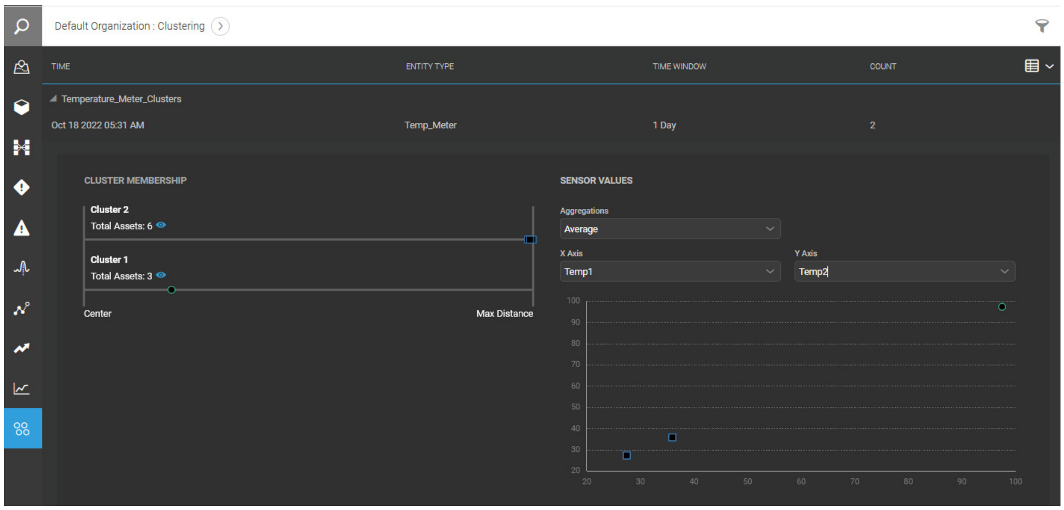
   - **Static**: Uses a static data window to train your cluster configuration. Select the **Window Start Time** and **Window End Time** for your static window period.
     The static data window provides data for a one-time training of your cluster configuration. If your cluster accuracy changes in the future, you should edit the cluster configuration to choose a different static window.

9. Click **Save** to create the cluster configuration.

   The system now schedules analysis for the new cluster configuration.



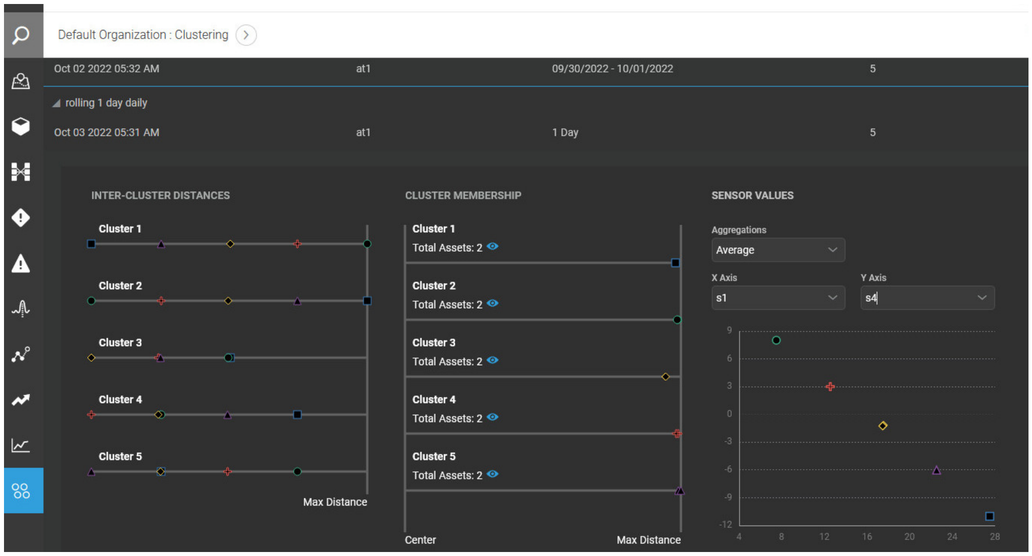
The clusters start appearing in Operations Center once the analysis is complete.



View Asset Clusters in Operations Center

The **Clustering** tab in Operations Center shows you the details on the clusters, including sensor values and the cluster memberships that the application creates. You can also visualize the tightness of each cluster, and the distances between individual clusters.

The clusters are shown at the organizational level in Operations Center.



The cluster membership rows are ordered by cluster size.

An Inter-Cluster Distances pane appears if there are three or more clusters

You can also plot and compare aggregated values (**Max, Min, Sum, Average**) of sensor attributes for each cluster.

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 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.

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

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**.

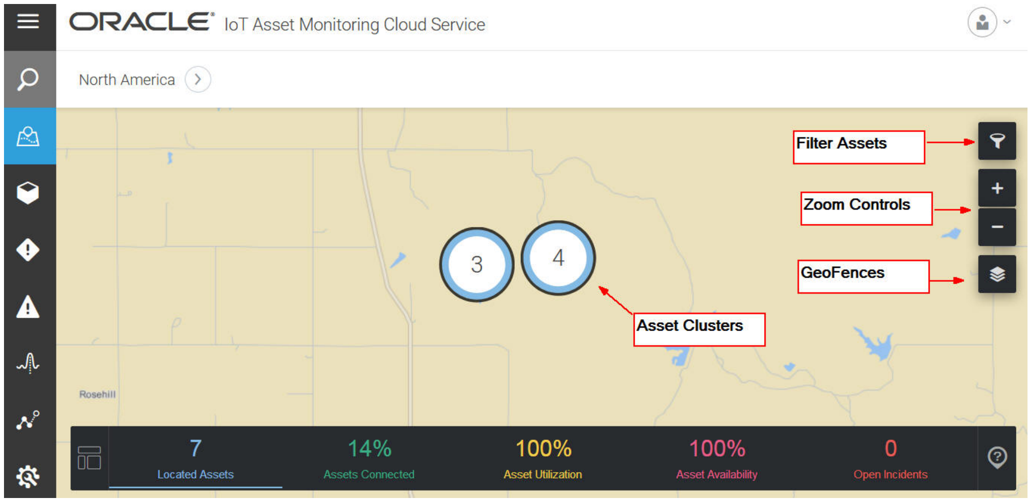
Delete a Place

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

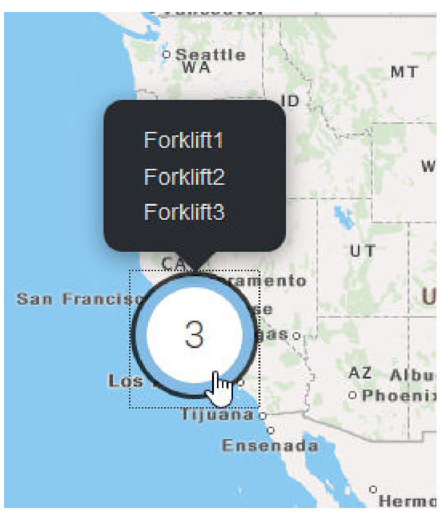
Use the map view to quickly locate the physical locations of your assets. Your assets can appear independently, or clustered together, depending on your zoom level in the map.



1. In the Operations Center, click **Map**  in the menu bar.

> **Note:**
>
> If you are already on an asset page, you can return to the map view by clicking the organization name in the breadcrumb navigation.

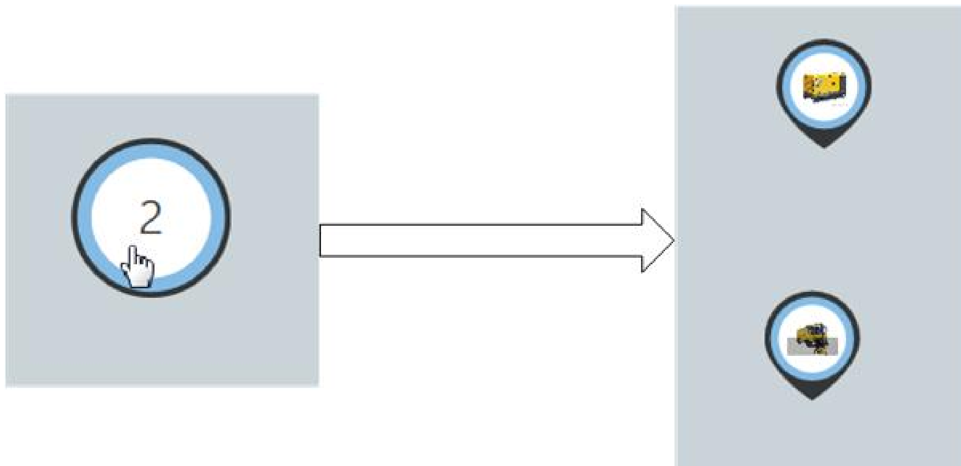
2. Use the zoom buttons (**+** and **-**) to zoom in or out in the map view.
3. Click an asset cluster to show the list of individual assets.



4. Click the asset cluster again to separate out the individual assets. Alternatively, zoom in further to separate the clustered assets.

   > **Note:**
   >
   > You can also double-click a cluster to separate out the individual assets.

   The following image shows how double-clicking a cluster with two assets separates the assets:

5. Click an individual asset to view the asset details.

   If you have configured visualization options, then clicking the asset shows a preview of select attributes in a heads-up display. Click the asset again to open the asset default view.

   See Customize Asset Visualization Options for more information on setting visualization options for an asset type.

   > **Note:**
   >
   > You can always double-click an asset to directly open the default view for the asset.

6. (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.

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

Use Third-Party Map Providers

Oracle IoT Intelligent Applications let 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.

You can also choose to override the map provider for an individual organization from the organization settings.

To use a third-party map provider:

1. In the Operations Center, click **Menu** (☰) and choose **Settings** .

   > **Note:**
   >
   > If you wish to change the map provider for an individual organization only, navigate to **Menu > Settings > IoT Organizations > *Organization Name***.

2. Click **Map Provider**.
3. Select a map provider.

   We currently support **HERE Maps**, as a third-party map provider.
4. Select one of the time options in the **Refresh Time** list. This determines the time interval at which the map data is refreshed in the application.

   If you select **Custom**, enter the number of seconds in **Value**.
5. If you selected HERE Maps, complete these fields:

   > **Note:**
   >
   > - From 22.4.1 release onward, Oracle recommends that you configure HERE maps using OAuth mechanism. In other words, instead of using HERE maps login credentials, generate an access token for authenticating to HERE maps. And to generate the access token, you must first generate OAuth credentials (access key ID and access key secret) as described in the HERE Developer portal at https://developer.here.com.
   > - The **Application ID** and **Application Code** fields are displayed only if you have previously configured HERE maps.

   - **Application ID**: Enter your HERE Technologies application ID.
   - **Application Code**: Enter your HERE Technologies application code.
   - **Access Key ID**: This is the access key credential used for authenticating to HERE maps using OAuth mechanism. Generate and enter the access key from the https://developer.here.com website.

- **Access Key Secret**: This is the secret credential used for authenticating to HERE maps using OAuth mechanism. Generate and enter the access key secret from the https://developer.here.com website.
- **Access Token URL**: Accept the default value or enter the access token URL. The access token URL defines the API used to generate access tokens for authenticating to HERE maps using OAuth mechanism.
- **Base URL**: Accept the default value or enter the base URL. The base URL defines the API used to render the map tiles.
- **Route URL**: Accept the default value or enter the route URL. A route URL defines the API used to determine the route to be covered by a trip or shipment in map view.
- **Geocode URL**: Accept the default value or enter the geocode URL. The geocode URL defines the API used to convert a human-readable address into geographic coordinates.
- **Reverse Geocode URL**: Accept the default value or enter the reverse geocode URL. A reverse geocode URL defines the API used to convert geographic coordinates into a human-readable address.
- **Batch Reverse Geocode URL**: Accept the default value or enter the batch reverse geocode URL. A batch reverse geocode URL defines the API used to convert multiple geographic coordinates into human-readable addresses.
- **Aerial URL**: To display satellite imagery in the map view, accept the default value or enter the aerial URL An aerial URL defines the API used to display satellite imagery.
- **Traffic URL**: To display real-time traffic data in the map view, accept the default value or enter the traffic URL A traffic URL defines the API used to display traffic data.
- **Map Tiles Language**: Select the language in which you want the map tiles to be displayed in map view. Note that map tiles for a selected language is displayed only if the corresponding language data is available in HERE maps. If HERE maps doesn't have the corresponding language map tile, then it defaults to displaying the map tiles in English.

6. Click **Validate Credentials**. After you receive a success message, click **Save** and close the window to return to the Settings page.

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**

The option to see points of interest is also available in all the HERE Maps layers.

If you wish to revert to using the built-in Oracle maps, you can choose **Oracle Maps** from the Map Provider 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**.

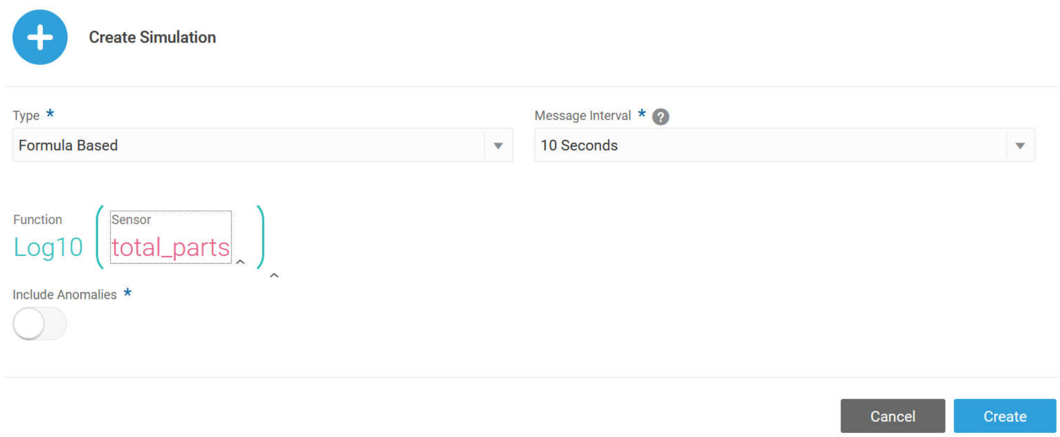
   The message interval is the frequency with which the simulated sensor sends messages.
5. If you chose **Pattern Based** for the simulation **Type**, then select a wave pattern under **Pattern**.

   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.

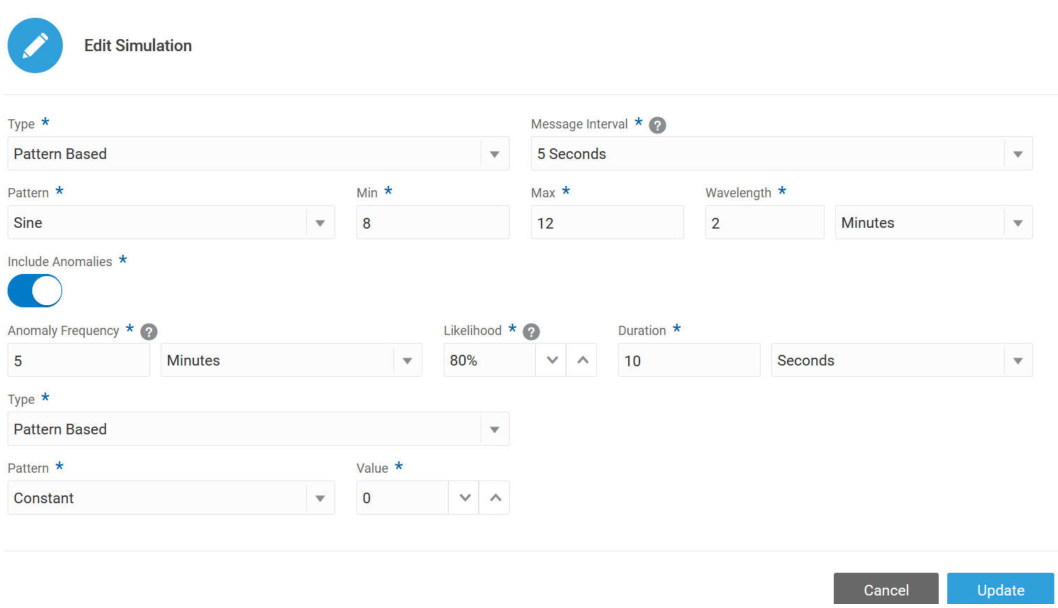
   The formula can use available functions, such as aggregation functions, trigonometric functions, mathematical, string, and time functions. You can also use other sensor attribute values as properties, use various operators such as logical and arithmetic operators, and use constants.

   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.



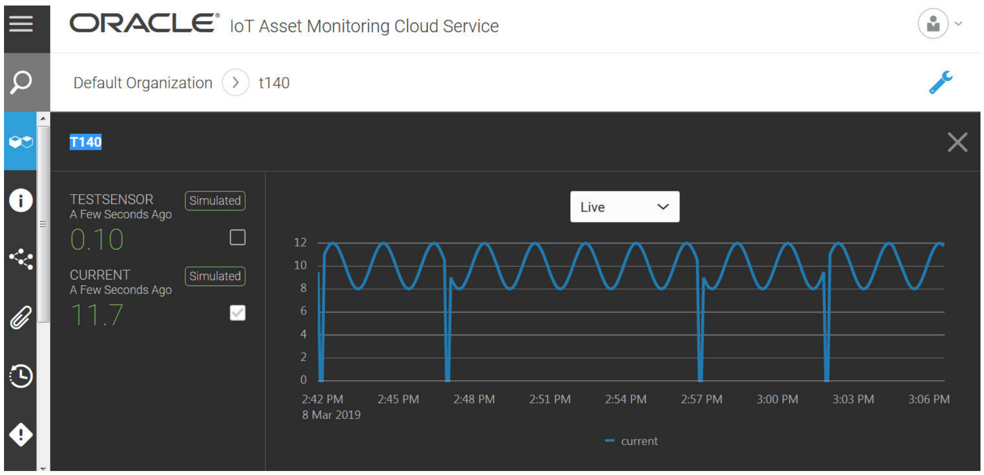
7. If you wish to introduce periodic anomalies in the simulated data, select **Include Anomalies**.
   - **Anomaly Frequency**: The periodic time period with which the anomaly occurs. For example, a value of `5 minutes` will mean that the anomaly would be attempted every 5 minutes.
   - **Likelihood**: 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.

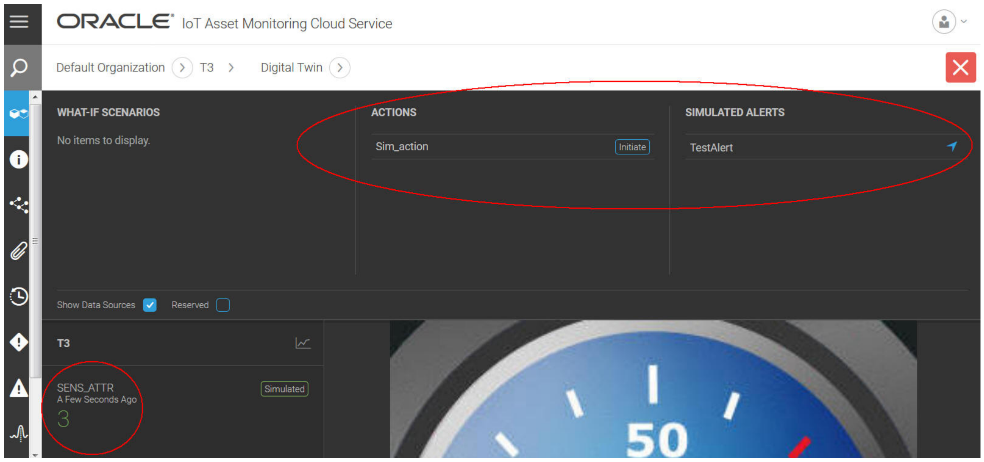
Simulate an Attribute, Action, or Alert for an Asset

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.



Tips and Considerations for Simulated Data and Analytics Artifacts

When generating and using simulated data to test your analytics artifacts, such as anomalies and predictions, keep in mind the data characteristics of your generated data.

When you define simulations for an asset type, any simulated assets that you create for the asset type will generate similar data patterns and values.

When creating random data based simulations, remember that random data patterns are akin to noise, and cannot be predicted. Avoid creating predictions on random data, as the prediction training will fail for random data. You may, however, create a meaningful metric on the sensor generating random data, and base your predictions on the metric.

If you are generating data with a high percentage of anomalies to test anomaly features, then avoid creating predictions on such data. In the real world, if a sensor is reporting large amounts of anomalous data, then the anomalies feature will detect these, and you should use the same to rectify or replace the sensor or asset. Prediction training may fail on data that contains a disproportionately large number of anomalies.

Import Historical Asset Data

If you have your pre-deployment device data in an external system, you can choose to import historical sensor and metric data into Oracle IoT Asset Monitoring Cloud Service and use the data to train your analytics artifacts, such as anomalies and predictions.

Importing historical data is useful for cold start scenarios where you don't have training data already available in Oracle IoT Asset Monitoring Cloud Service. You can also import data for proof-of-concept demonstrations, so that you can use the imported data to train your anomalies, predictions, and trends.

> **Note:**
>
> Pattern anomalies do not support imported historical data. To create pattern anomalies, you must generate training data in Oracle IoT Asset Monitoring Cloud Service.

Use the following steps to import historical sensor and metric data into Oracle IoT Asset Monitoring Cloud Service:

1. In Oracle IoT Asset Monitoring Cloud Service, create and export an asset data template for your asset data.
2. Populate the asset data template with sensor and metric data from the external system.
3. Import the asset data into Oracle IoT Asset Monitoring Cloud Service. The data is available for training after validation and processing.

Export the Asset Data Template

The asset data template defines the schema for your asset data import. It includes fields for asset names and IDs, timestamps, sensor attributes, and metrics.

You should already have your asset type, sensor attributes, metrics, and assets created in Oracle IoT Asset Monitoring Cloud Service before creating the asset data template.

> **Note:**
>
> You can choose to import asset types, assets, and other entities into a new instance by importing a previously exported organization. See Export and Import Organizations for more information.

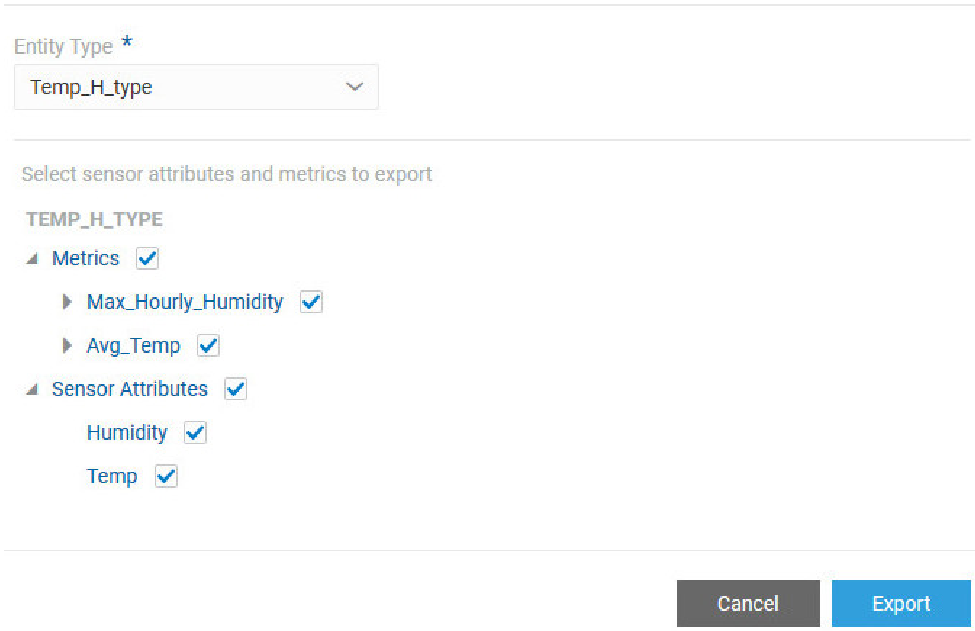
1. Log in to Oracle IoT Asset Monitoring Cloud Service as an administrator.

   Only administrators have the privilege to export asset data templates from Oracle IoT Asset Monitoring Cloud Service.
2. Click **Menu** (≡), and then click **Design Center**.
3. Select **Asset Inventory** from the **Design Center** sub-menu.
4. Click the Asset Inventory Menu ••• and select **Export Asset Data Template**.
5. Select the **Entity Type** (Asset Type) for the asset data template.

   For example, you may want to create an asset data template for forklift assets.

   The existing sensor attributes and metrics for the asset type appear in a tree-like structure under the asset type. If the asset type contains sub-asset types or associated asset types, the attributes for the sub-asset type are also shown.
6. Deselect the sensor attributes and metrics that you do not wish to include in your asset data template.

   For example, if you do not have historical data for a particular attribute in your external system, you can exclude it from the asset data template.



You can click on the **Sensor Attributes** and **Metrics** nodes to expand or collapse them.

7. Click **Export**.

   Save the exported `csv` (comma separated value) file to your local storage.

   The exported `csv` file contains the following fields:

   - `ora_entity_type_name`: The entity type (asset type) for which you created the template.
   - `ora_entity_name`: Name of the entity (asset). You must specify at least one of `ora_entity_name, ora_entity_id, and ora_external_entity_id` for each row of data that you populate in the asset data template.
   - `ora_entity_id`: Identifier (ID) of the entity (asset). You must specify at least one of `ora_entity_name, ora_entity_id, and ora_external_entity_id` for each row of data that you populate in the asset data template.
   - `ora_external_entity_id`: External Identifier of the entity (asset). An external identified would be the identifier of an imported asset in the external system from which it was imported. For example, the asset identifier of an asset in Oracle Fusion Cloud Maintenance.
     You must specify at least one of `ora_entity_name, ora_entity_id, and ora_external_entity_id` for each row of data that you populate in the asset data template.
   - `ora_event_time`: The event time against which the telemetry data is being reported. The epoch long time format and ISO 8061 format are supported. `yyyy-MM-ddTHH:mm:ss.SSSZ`. For example, `2007-07-16T19:20:30.45Z`.
   - `ora_sensor.`*`name`* fields: The sensor attribute values for the attributes that you included in your template.
   - `ora_metric.`*`name`* fields: The metric values for the attributes that you included in your template.

`csvEnv_Sensor2ora_entity_name, ora_entity_id, and ora_external_entity_id`

ora_entity_type_name	ora_entity_name	ora_entity_id	ora_external_entity_id	ora_event_time	ora_sensor.Temp	ora_sensor.Pressure
Env_Sensors	Env_Sensor2			2022-02-22T01:20:37Z	23.30360393	1.049972791
Env_Sensors	Env_Sensor2			2022-02-22T01:20:57Z	23.09586042	0.900000009
Env_Sensors	Env_Sensor2			2022-02-22T01:21:17Z	23.40324418	1.050036272
Env_Sensors	Env_Sensor2			2022-02-22T01:25:07Z	23.72876417	0.95003628
Env_Sensors	Env_Sensor2			2022-02-22T01:25:47Z	23.45777927	0.949963728

Import Asset Data for Sensors and Metrics

Once you have populated your asset data template with asset data, you can import the `csv` file, or a `zip` file containing one or more `csv` files, into Oracle IoT Asset Monitoring Cloud Service.

1. Log in to Oracle IoT Asset Monitoring Cloud Service as an administrator.

   Only administrators have the privilege to import historical asset data into Oracle IoT Asset Monitoring Cloud Service.

2. Click **Menu** (≡), and then click **Design Center**.
3. Select **Asset Inventory** from the **Design Center** sub-menu.
4. Click the Asset Inventory Menu ••• and select **Import Asset Data**.
5. Enter an **Import Task Description** to help you identify the import task later.
6. Select the **Entity Type** (Asset Type) for the asset data that you are importing.
7. Optionally change the number of data lines under **Rejection Threshold**.

   The **Rejection Threshold** specifies the threshold number of erroneous data lines in the imported file before the import is rejected. Typically, users populate the asset data template using an automated process, so if a certain number of data lines are erroneous, it is very likely that the rest of the lines are erroneous too. Oracle IoT Asset Monitoring Cloud Service halts the import once the specified threshold is reached.

   A data line may be rejected for various reasons. For example, the data line might have missing or incorrect entity information.

8. (Optional) Deselect **Review errors before processing** if you wish the file to be auto processed or rejected without prompting you to review the errors, if any.

   Review errors before processing lets you review the error details in case there are validation errors in the imported file. If the number of erroneous rows are below the threshold, you can choose to process or reject the remaining rows.

   If you deselect **Review Errors Before Processing**, then if the number of errors is below the rejection threshold, the import is auto-processed. Else the import is rejected.

9. Click **Choose File** and select the `csv` file or `zip` file to be imported.

   The maximum file size cannot exceed 150 MB. You can choose to compress multiple `csv` files in a single `zip` file.

10. Click **Continue**.

    A notification appears confirming that the upload request was sent.

    The imported file is next validated and processed after which the imported data is available for training. If you are working in other areas of the application, you get periodic notifications about the status of the import. You are also notified if data errors are found in the import file.

11. (Optional) Click the **Data Import Log** tab to monitor the status of the import.

    The Initiated column reflects the time when the import request was initiated.

    The Status column reflects the current status of the import. The status column may reflect one of the following:

    - **Pending Validation:** This is the status just after you have initiated the import.
    - **Validating Data:** The data validation is in progress for the imported file.
    - **Processing Trained Data:** The data processing stage follows the validation stage.
    - **Historical Data Available:** The training data is available in the system.
    - **Some Data Errors Found**: Indicates that there were data errors while processing. You can click the **Show Details** icon to view the error details. Click **Action Required** . to accept or reject the remaining rows.
    - **Request Rejected**: The reason for request rejection is enumerated. For example, the asset data template had a bad schema, or the number of erroneous rows exceeded the rejection threshold. You can click the **Show Details** icon to view the rejection details.

    a. Click the **Show Details** icon to view details about the import, such as any error or rejection details.
    b. Click **OK**.
    c. Click **Action Required** . to complete any user-pending tasks, such as the following:
        - **Process historical data ignoring errors**
        - **Reject Request**

        If you have chosen to review errors before processing, and if the number of erroneous rows are below the rejection threshold, then you can choose to process the historical data in the remaining rows. You can also choose to reject the import request.
    d. Click **OK**.

After you have imported historical sensor and metric data, you can use the data to train your analytics artifacts, such as anomalies and predictions.

Note that historical sensor data will not show up in the digital twin view of your asset. So, you cannot see data plots for imported historical data.

4 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.
- Formula Based 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.
- Duration Based Metric: Tracks asset state durations based on the conditions that you specify. Your conditions can use the asset location, sensor attribute values, and other asset metrics. See Use Duration Tracker Metrics for more information on creating duration based 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.

   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.
4. Click **Metrics**.
5. Click **Create Metric** +.
6. Enter a **Name** to identify the new metric.
7. Select **Formula Based** under **Metric Type**.
8. (Optional) Select a value under **Keep Metric Data For**.

   If you have unique storage requirements for historical data related to this metric, you can select an option that is different from the global settings defined under **Storage Management** on the application **Settings** page.

   For example, if you are calculating frequent metrics across a large number of assets, and the metric data is not required beyond a month, then you can select **30 Days** under **Keep Metric Data For** to optimize storage.
9. Under Calculation Scheduling, choose an option under **Type**.

   Metrics can be calculated per entity (asset), or can be calculated globally for an entity type (asset type). If you select **On Schedule per Entity**, then the metric is calculated for each asset of the asset type. If you select **On Schedule for Entity Type**, then the metric is aggregated across all entities of the asset type. For example, you can calculate the average temperature across all temperature sensors.
   You can also choose to aggregate the metric across all assets in an asset group. This helps compare and rank groups. Select **On Schedule per Group** to create a metric aggregated across assets in a group. You can use both static and filter-based groups. **On Schedule per Group** aggregates data only for leaf groups.
10. Specify a calculation **Schedule**:
    - **Live** calculates the metric every two minutes.

      Use this option sparingly, as it may require a lot of computational and storage resources depending on your number of assets. The **Live** option may be used in special circumstances: For example, when the metric is to be used for anomaly detection purposes.
    - **Hourly** aggregates the metric for every hour.
    - **Daily** aggregates the metric for every day.
    - **Weekly** aggregates the metric for every week.
11. (Optional) Click **Edit** to change the **Data Window** to use.

By default, the **Data Window** is the same as the calculation schedule. For example, if you have set the metric schedule to **Hourly**, the data from the previous hour is used to calculate the metric.

You can also use flexible data windows for your scheduled metric calculations. The data window can be different from the calculation schedule. For example, you may wish to compute the total output for the past twenty-four hours, and calculate this metric hourly.

In addition to sliding data windows, you can also use dynamic custom data windows. For example, you may wish to do an hourly calculation of the cumulative output for the day, starting 9 a.m. in the morning.

a. Select a **Configuration** value:

   - **Default**: Uses the default data window as per the selected schedule. For example, if you have set the metric schedule to **Hourly**, the data from the previous hour is used to calculate the metric.
   - **Data Window Start Time**: Lets you pick from a number of fixed options. For example, you may use data from the last one week, and calculate the metric hourly.
     When choosing larger data windows, ensure that the data life span settings for your custom metrics are large enough in the application settings, so that there is data available for the selected window.
   - **Custom Data Window Start Time**: Lets you choose a fixed start time for the data window. For example, you may wish to do an hourly calculation of the cumulative output for the day, starting 9 a.m. in the morning.
     This option is only available when selecting the **Live** or **Hourly** schedule.

b. Select the **Data Window** value corresponding to the selected configuration:

   - If you selected **Default**, the **Data Window** is automatically selected to match the metric calculation schedule.
   - If you selected **Data Window Start Time**, specify the **Offset** to use. For example, choose **One Week Ago**, to use the data from the past one week.
   - If you selected **Custom Data Window Start Time**, then specify the fixed start **Time** for the data window in the **UTC** (Coordinated Universal Time) time zone.

12. 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:

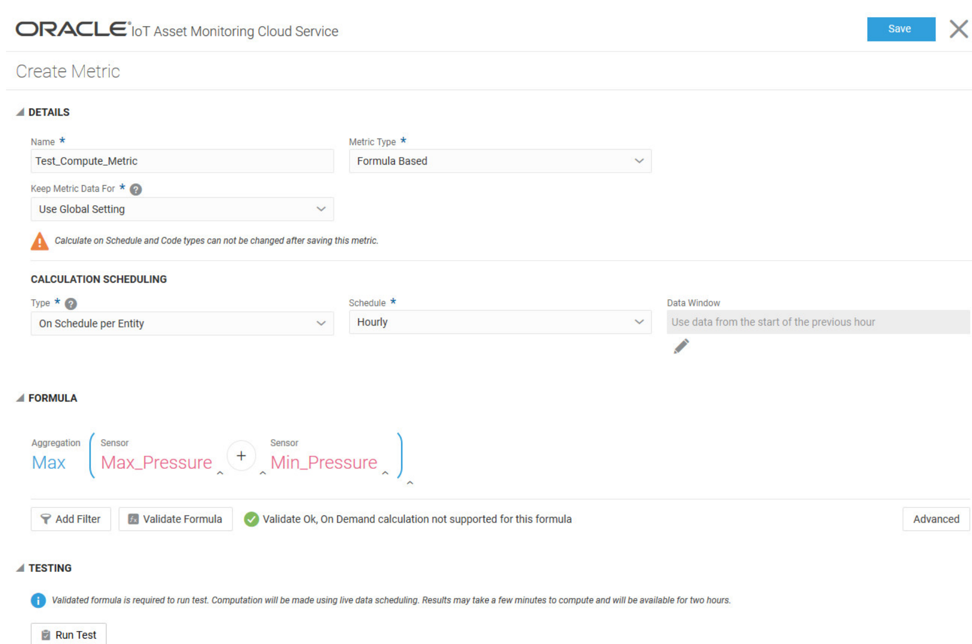
- `AVG (FuelLevel)`: Returns the average `FuelLevel` over the specified time period.
- `MIN(MaxPressure/2 + MinPressure/2)`: First uses the `MaxPressure` and `MinPressure` sensor values to compute the average pressure, and then returns the minimum of this average pressure over the specified time period.

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.



13. Click **Validate Formula** to validate your formula expression.
14. (Optional) Under Testing, click **Run Test** to view sample metric results on live asset data.

> **Note:**
>
> You must successfully validate the formula before **Run Test** is enabled.

Sampling the metric values lets you validate whether your computations work along expected lines. Sampling also lets you determine if the metric can go live, and if the metric is ready to be used in analytics artifacts, such as anomalies and predictions.

Computations are made using live data scheduling. Results may take a few minutes to compute and are available for two hours. Metric results may be shown for a sample selection of assets to cover the range of metric values.

15. Click **Save** to create the metric.

You can now add the metric to a dashboard or to the **Map**.

Metric Usage Examples

This section discusses metric usage examples to help you use the formula editor. It also provides several metric SQL examples.

Example 4-1 Single Asset Metrics and Multi-Asset Metrics

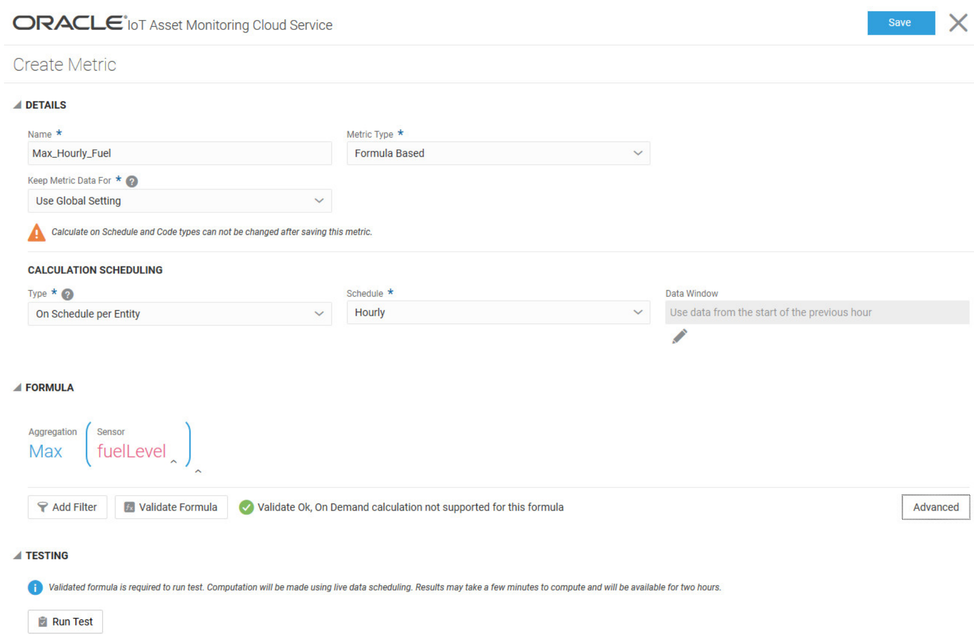
Concepts Covered:

- Aggregation Functions
- Sensor Attributes in Metrics
- Filters
- Relational Operators

Scenario: We create a metric to measure the maximum fuel level for each power generator. Next, we create a metric to measure the count of generators with sufficient fuel.

Metrics:

1. Create a metric, `Max_Hourly_Fuel` that is calculated hourly for each asset.

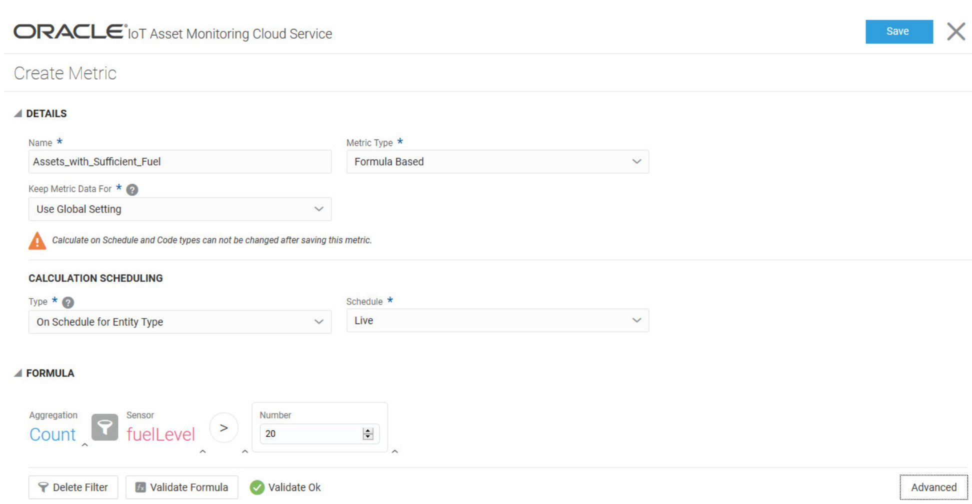


The following SQL is generated corresponding to the metric and calculated hourly:

```
SELECT MAX('Sensors'.'fuelLevel') FROM 'Generator' GROUP BY ENTITY
```

You can put this metric on the machine dashboard to see the hourly maximum fuel level for the selected asset.

2. Create a metric, `Assets_with_Sufficient_Fuel` to calculate the count of assets that have sufficient fuel levels. The metric defines fuel levels above 20 to be sufficient. Note that a filter is applied after adding the `Count` function to add the `Where` clause. A relational operator (>) is used to perform the comparison.



The following SQL is generated corresponding to the metric:

```
SELECT COUNT(*) FROM 'Generator' WHERE 'Sensors'.'fuelLevel'>20
```

You can put this metric on the organization dashboard to see the current count of generator assets with sufficient fuel.

Example 4-2 Nested Metrics and Formulas

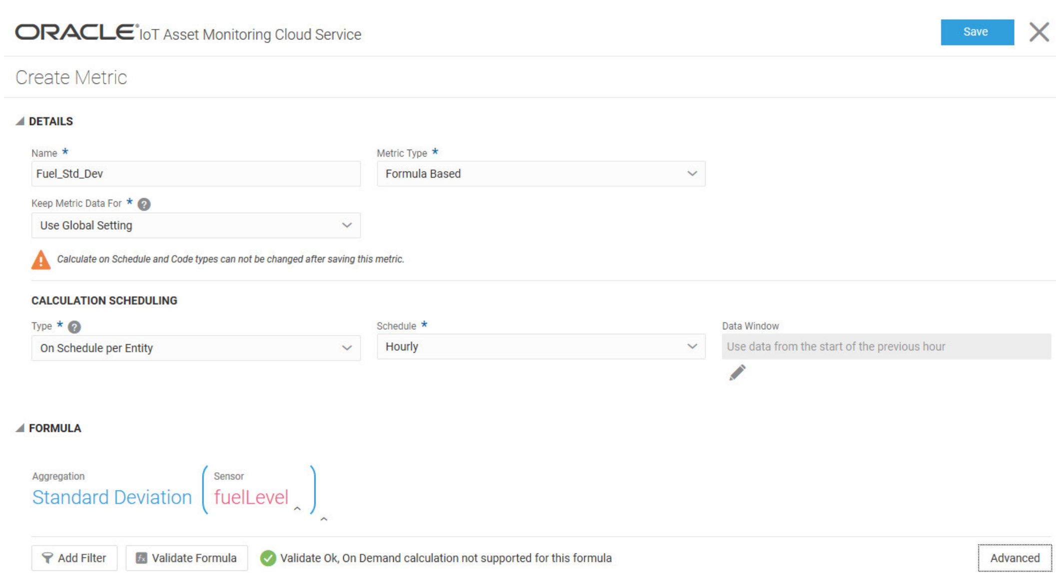
Concepts Covered:

- Functions
- Metrics within Metrics
- Filters
- Relational Operators, Arithmetic Operators

Scenario: We first create a metric to measure the hourly standard deviation value of the fuel level for each power generator. Next, we create a metric specific to our business use case: The metric calculates the number of generators that can be allocated for the project using a custom formula. The formula makes use of the metrics already created.

Metrics:

1. Create a metric, `Fuel_Std_Dev` that is calculated hourly for each asset.

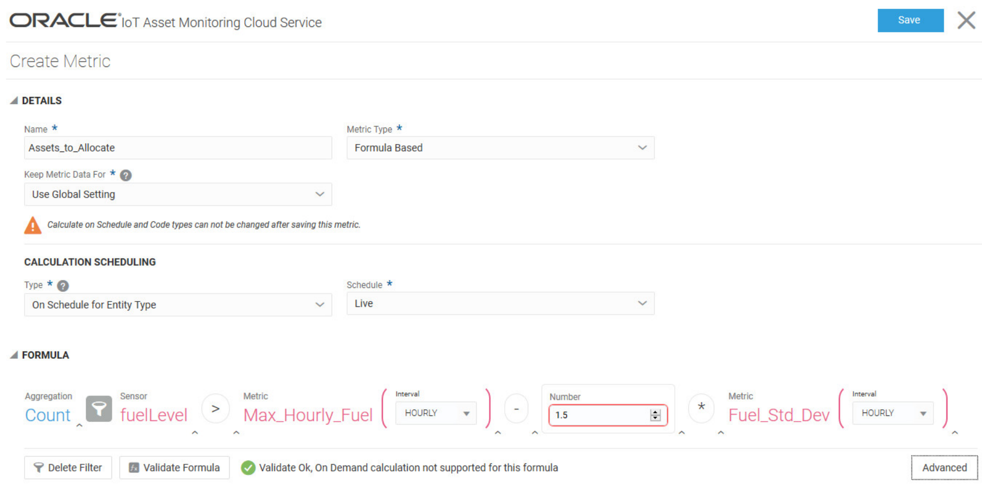


   The following SQL is generated corresponding to the metric and calculated hourly:

   ```
   SELECT STDDEV('Sensors'.'fuelLevel') FROM 'Generator' GROUP BY ENTITY
   ```

   You can put this metric on the machine dashboard to see the hourly standard deviation of the fuel level for the selected asset.

2. Create a metric, `Assets_to_Allocate` to calculate the count of assets that are ready to be allocated to the project. The metric defines the following business-specific formula: Find the count of assets for which the fuel levels are greater than the difference between `Max_Hourly_Fuel` and 1.5 times the `Fuel_Std_Dev` metric. Here, `Max_Hourly_Fuel` and `Fuel_Std_Dev` are the metrics we calculated in the earlier examples.



The following SQL is generated corresponding to the metric:

```
SELECT COUNT(*) FROM 'Generator' WHERE
'Sensors'.'fuelLevel'>'Metrics'.'Max_Hourly_Fuel'['interval':"HOURLY"]
-1.5*'Metrics'.'Fuel_Std_Dev'['interval':"HOURLY"]
```

You can put this metric on the organization dashboard to see the current count of generator assets ready to be allocated.

Metric SQL Examples

Description and Use case for the Metric	Metric SQL Query	Type	Concepts

Number of assets with incidents > 0.
Helps to understand the number of assets that have issues.
	`SELECT COUNT(*)`
	`FROM 'Assets'`
	`WHERE 'Metrics'.'sys_openIncidents' > 0`
		Multi-Asset	• Aggregation Functions
			• System Metrics
			• Relational Operators

Number of assets of specific type with temperature sensor value > 50.
Helps understand the number of assets behaving abnormally.
	`SELECT COUNT(*)`
	`FROM 'AssetWithSensors'`
	`WHERE 'Sensors'.'temperature' > 50`
		Multi-Asset	• Sensor Attribute
			• Relational Operators
			• Aggregation Functions

Description and Use case for the Metric	Metric SQL Query	Type	Concepts

Number of assets of specific type with temperature sensor value > (pressure sensor value * 1.5).
 	
Helps understand the number of assets behaving abnormally.
	`SELECT COUNT(*)`
	`FROM 'AssetWithSensors'`
	`WHERE 'Sensors'.'temperature' >`
	`  'Sensors'.'pressure' * 1.5`
		Multi-Asset	• Multiple Sensor Attributes
			• Arithmetic Operators
			• Relational Operators
			• Aggregation Functions

Number of assets with temperature sensor value > average(temperature value over last 24 hours).
 	
Helps understand the number of assets operating in the above average temperature range.
	`avgTemp[DAILY] ::=`
	`  SELECT AVG('Sensors'.'temperatue')`
	`  FROM 'AssetWithSensors'`
	`  GROUP BY ENTITY`
	
	`SELECT COUNT(*)`
	`FROM 'AssetWithSensors'`
	`WHERE 'Sensors'.'temperature' >`
	`  'Metrics'.'avgTemp'['interval':`
	`"DAILY"]`
		Multi-Asset	• Nested Metrics
			• Relational Operators
			• Aggregation Functions

Number of assets with temperature sensor value * 1.5 + humidity sensor value * 0.75 > 2.7.
 	
You may create formula-based metrics based on your models.
	`SELECT COUNT(*)`
	`FROM 'AssetWithSensors'`
	`WHERE 'Sensors'.'temperature' * 1.5 +`
	`  'Sensors'.'humidity' * 0.75 > 2.7`
		Multi-Asset	• Formula-Based Metric
			• Multiple Sensor Attributes
			• Arithmetic and Relational Operators
			• Aggregation Function

Description and Use case for the Metric	Metric SQL Query	Type	Concepts

Number of assets with average (temperature in last hour) > average (temperature in last 24 hours).
May help identify drifting assets.
	`avgTemp[HOURLY, DAILY] ::=`
	`  SELECT AVG('Sensors'.'temperatue')`
	`  FROM 'AssetWithSensors'`
	`  GROUP BY ENTITY`
	
	`SELECT COUNT(*)`
	`FROM 'AssetWithSensors'`
	`WHERE 'Metrics'.'avgTemp'['interval':`
	`"HOURLY"] >`
	`  'Metrics'.'avgTemp'['interval':`
	`"DAILY"]`
		Multi-Asset	• Nested Metrics
			• Relational Operators
			• Aggregation Functions

Number of assets with average (temperature in last hour) > max (temperature in last 24 hours) - 1.5*standarddev (temperature in last 24 hours)
Helps identify drifting assets.
	`avgTemp[HOURLY] ::=`
	`  SELECT AVG('Sensors'.'temperatue')`
	`  FROM 'AssetWithSensors'`
	`  GROUP BY ENTITY`
	
	`maxTemp[DAILY] ::=`
	`  SELECT MAX('Sensors'.'temperatue')`
	`  FROM 'AssetWithSensors'`
	`  GROUP BY ENTITY`
	
	`stdevTemp[DAILY] ::=`
	`  SELECT STDEV('Sensors'.'temperatue')`
	`  FROM 'AssetWithSensors'`
	`  GROUP BY ENTITY`
	
	`SELECT COUNT(*)`
	`FROM 'AssetWithSensors'`
	`WHERE 'Metrics'.'avgTemp'['interval':`
	`"HOURLY"] >`
	`  'Metrics'.'maxTemp'['interval':`
	`"DAILY"] -`
	`    1.5 *`
	`'Metrics'.'stdevTemp'['interval':`
	`"DAILY"]`
		Multi-Asset	• Nested Metrics
			• Formula-Based Metric
			• Standard Deviation Function
			• Aggregation Functions

(Temperature value + pressure value *1.5 + (humidity value / 3))*0.05-2.7
You may create formula-based metrics based on your models.
	`SELECT LAST(`
	`  ('Sensors'.'temperature' +`
	`   'Sensors'.'pressure' * 1.5 +`
	`   'Sensors'.'humidity' / 3`
	`  ) * 0.05 - 2.7)`
	`FROM 'AssetWithSensors'`
	`GROUP BY ENTITY`
		Single Asset	• `LAST` Function
			• Formula-Based Metric
			• Multiple Sensor Attributes
			• Arithmetic Operators

Description and Use case for the Metric	Metric SQL Query	Type	Concepts

(Avg temperature value in last 24 hours)+(avg pressure value in last 24 hours) *1.5 +(avg humidity value in last 24 hours / 3))*0.05-2.7
You may create formula-based metrics based on your models.
	avgTemp[DAILY] ::=
	  SELECT AVG('Sensors'.'temperatue')
	  FROM 'AssetWithSensors'
	  GROUP BY ENTITY
	
	avgPressure[DAILY] ::=
	  SELECT AVG('Sensors'.'pressure')
	  FROM 'AssetWithSensors'
	  GROUP BY ENTITY
	
	avgHumidity[DAILY] ::=
	  SELECT AVG('Sensors'.'humidity')
	  FROM 'AssetWithSensors'
	  GROUP BY ENTITY
	
	SELECT LAST(
	  ('Metrics'.'avgTemp'['interval': "DAILY"] +
	   'Metrics'.'avgPressure'['interval': "DAILY"] * 1.5 +
	   'Metrics'.'avgHumidity'['interval': "DAILY"] / 3)
	  ) * 0.05 - 2.7)
	FROM 'AssetWithSensors'
	GROUP BY ENTITY
		Single Asset	• Nested metrics
			• LAST Function
			• Formula-Based Metric
			• Multiple Sensor Attributes
			• Arithmetic Operators

Total time in last 24 hours when the temperature value was > 45 Assessing the amount of time the asset is performing beyond specified temperature limits.	SELECT TIME_SUM(*) FROM 'AssetWithSensors' WHERE 'Sensors'.'temperature' > 45 GROUP BY ENTITY	Single-Asset	• Time Function • Sensor Attribute • Relational Operator
Total time in last 24 hours when temperature value - pressure value * 1.5 > humidity value *0.75 / tire pressure Knowledge base anomaly behavior definition	SELECT TIME_SUM(*) FROM 'AssetWithSensors' WHERE 'Sensors'.'temperature' - 'Sensors'.'pressure' * 1.5 > 'Sensors'.'humidity' * 0.75 / 'Sensors'.'tirePressure' GROUP BY ENTITY	Single-Asset	• Time Function • Formula-Based Metric • Multiple Sensor Attributes • Arithmetic Operators and Relational Operator

Description and Use case for the Metric	Metric SQL Query	Type	Concepts
Total in-use time in last 24 hours when vibration > 300 AND temperature > 100 Understanding assets with anomalous behavior.	`SELECT TIME_SUM(*) FROM 'AssetWithSensors' WHERE 'Sensors'.'vibration' > 100 AND 'Sensors'.'temperature' > 300 GROUP BY ENTITY`	Single-Asset	• Time Function • Multiple Sensor Attributes • Relational Operator • Logical Operator

Use Duration Tracker Metrics

Duration tracker metrics let you track asset state durations based on the conditions that you specify. Your conditions can use the asset location, sensor attribute values, dynamic attribute values, and other asset metrics.

For example, your supply chain flow may require you to track the duration that a mobile asset spends in the warehouse. Or you may want to track the amount of time that a cold storage unit door is left open. Manufacturing scenarios may require you to track the duration of time for which sensor attribute values remain out of range.

Like other metrics, you can add duration tracker metrics to your organization and asset dashboards. You can also use duration tracker metrics in your rule conditions to generate incidents, warnings, or alerts if the threshold duration is violated.

Create a Duration Tracker Metric

The metric editor can be used to create a duration tracker metric for one or more assets of 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 **Metrics**.
5. Click **Create Metric** +.
6. Enter a **Name** to identify the new metric.
7. Select **Duration Based** under **Metric Type**.
8. (Optional) Select a value under **Keep Metric Data For**.

   If you have unique storage requirements for historical data related to this metric, you can select an option that is different from the global settings defined under **Storage Management** on the application **Settings** page.

For example, if you are calculating frequent metrics across a large number of assets, and the metric data is not required beyond a week, then you can select **7 Days** under **Keep Metric Data For** to optimize storage.

9. Select a **Mode** for the duration based metric:
   - **Live:** The time duration for which the metric conditions are currently being met. If the metric conditions are currently not met, then the **Live** value is zero.
   - **Last:** The time duration for which the metric conditions were last met.
     When the metric conditions go from *currently being met* to *currently not being met*, the value of **Live** is transferred to **Last**, and the **Live** value becomes zero.
   - **Cumulative:** The total time duration of all occurrences when the metric conditions were met.
     If you select **Cumulative**, you also need to select a **Time Window**. The cumulative occurrences are tracked over the **Time Window** you select. For example, if you select **Weekly**, then the total time duration of all occurrences over the past week is tracked.

   You can select more than one mode if required.
10. Under **Target**, select **All Assets of Type: `AssetType`** to calculate the metric for each asset of the asset type. Alternatively, select **Specific Assets of Type: `AssetType`** and select one or more assets that you wish to monitor.
11. Under **Conditions**, create one or more conditions.

    You can create location conditions based on whether an asset enters or exits a location. You can also create threshold conditions based on whether a sensor attribute, or pre-existing metric, exceeds a set threshold. You can create threshold conditions for dynamic attributes, too.

    To create a location condition:
    a. Select **Location** from the drop-down list.
    b. Select **Entered** or **Exited** in the second drop-down list:
    c. Select the location in the third list.

       The location is the name of a predefined place that you must have previously created in the application.

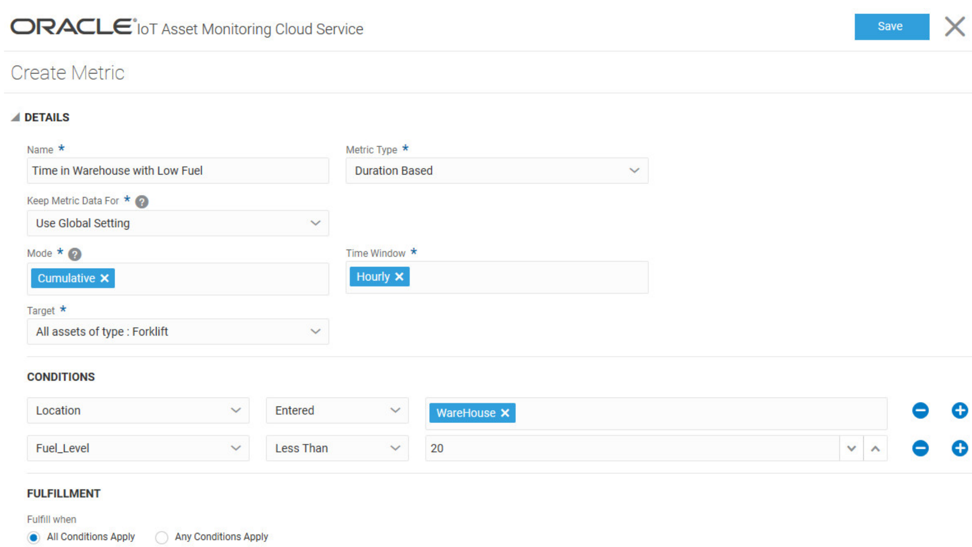
    To create a threshold condition:
    a. Select an asset sensor attribute or existing metric from the drop-down list.
    b. Select a threshold condition for the attribute in the second drop-down list.

       For example, a numeric attribute specifies conditions like **Greater Than** and **Less Than.**
    c. Specify an attribute value in the third field.

       For example, a complete condition may look like: `maxtemp Greater Than 50.`

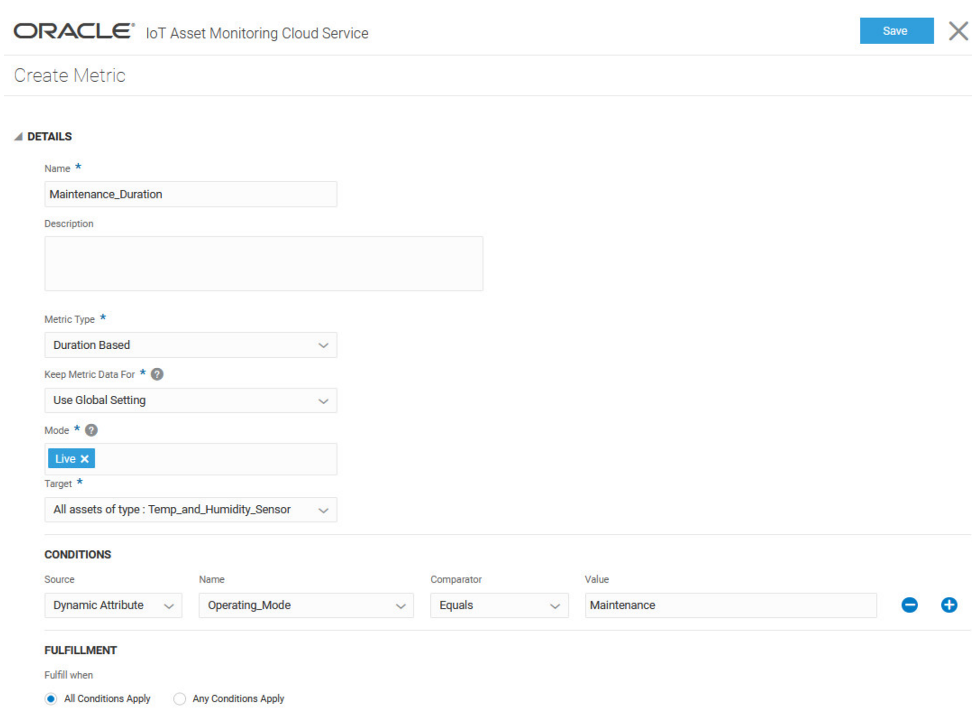
       A complete condition that uses a system metric may look like: `sys_openIncidents Greater Than 5.`
12. (Optional) Add additional conditions, as required.
13. In the Fulfillment section, select an option for the **Fulfill when** field:
    - **All Conditions Apply** : Select this option to track the duration when all the conditions are met.

- **Any Conditions Apply**: Select this option to track the duration when any of the conditions are met.



The preceding example shows the metric editor for a duration-based metric that uses multiple conditions. The duration is tracked when the forklift is inside the warehouse and the forklift fuel level is less than 20.

The following example shows the metric editor for a duration-based metric that uses a dynamic attribute condition. The metric tracks the duration for which an asset remains in maintenance.



14. Click **Save** to create the metric.

You can next add the newly created metric to your dashboards, or use the metric in rule conditions.

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.

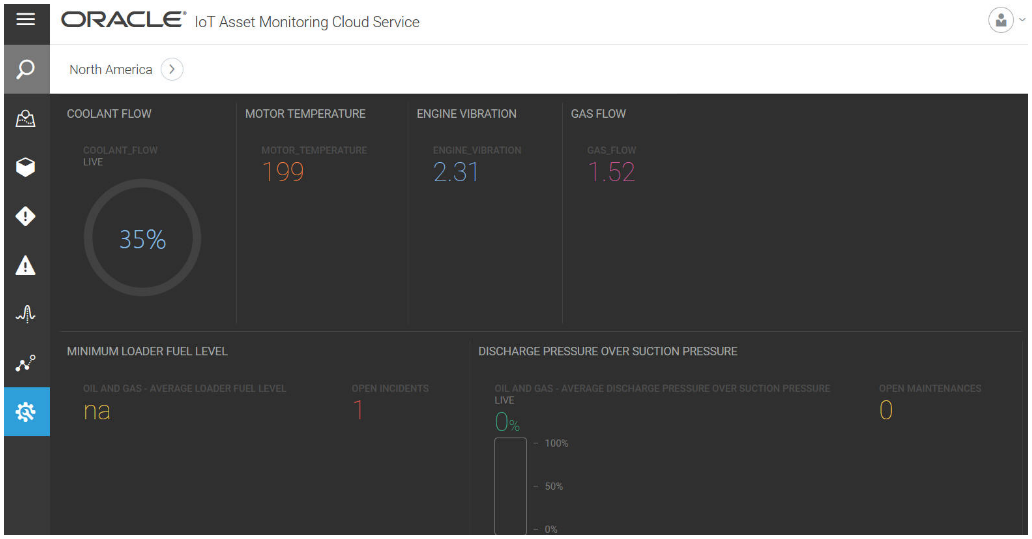
The system metrics are based on live data. A live metric value is refreshed every two minutes.

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 **IoT**, and select one of the available templates or layouts.

   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. Under **Role Access**, optionally change the user roles to which the content of the dashboard should be available.

   The roles you select can view the dashboard in Operations Center.
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 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.

Dashboards currently do not support the newly introduced group-aggregated metrics.

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 **IoT**, and select one of the available templates or layouts.

   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. Under **Role Access**, optionally change the user roles to which the content of the dashboard should be available.

   The roles you select can view the dashboard in Operations Center.
10. 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.
11. 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 **IoT**, and select one of the available templates or layouts.

   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. Under **Role Access**, optionally change the user roles to which the content of the dashboard should be available.

   The roles you select can view the dashboard in Operations Center.

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.

Access the Dashboard Metrics

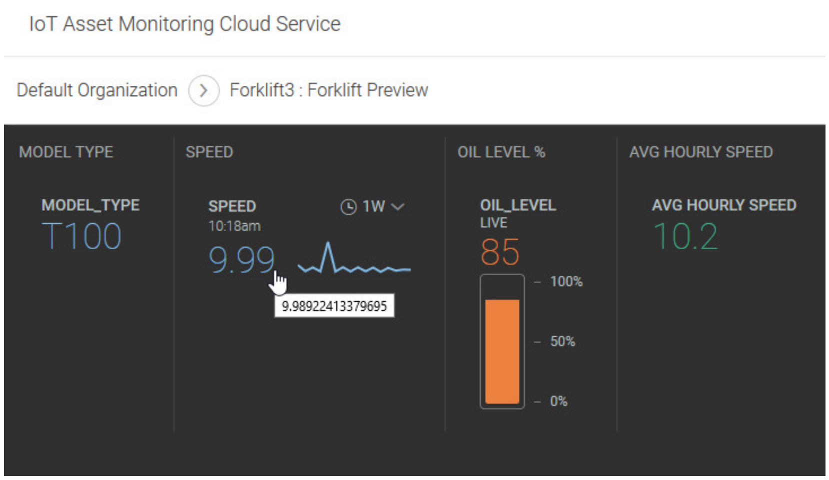
Switch to a previously-created dashboard for an asset, group, or organization to track the cumulative metrics or key performance indicators (KPIs) for your assets.

- 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.

Access Location, Historical Sensor Data, and Sensor Charts for a Sensor Gadget

If your dashboard gadget is a sensor attribute, you can click the gadget on the dashboard to quickly access the location of the corresponding asset in a pop-up window. You can also view historical, tabular sensor data and charts in the pop-up window.

1. In the Operations Center Dashboard view, click the gadget or metric for the sensor attribute.



A pop-window appears with the Location tab selected by default.

2. Click **table** to view tabular data related to the sensor attribute values.
3. Click **chart** to view sensor data charts.

   You can select the time period for which you wish to display the chart.
4. Click **Close** to close the gadget pop-up window.

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 **Histogram** to show a preview chart against the sensor gadget icon.

    This setting is available only if you are adding a sensor attribute metric for an asset-level dashboard.

13. Select an appropriate display type for your metric.

    For certain display types, such as gauges and meters, you need to specify a **Minimum** and **Maximum** value for the gauge range.

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

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

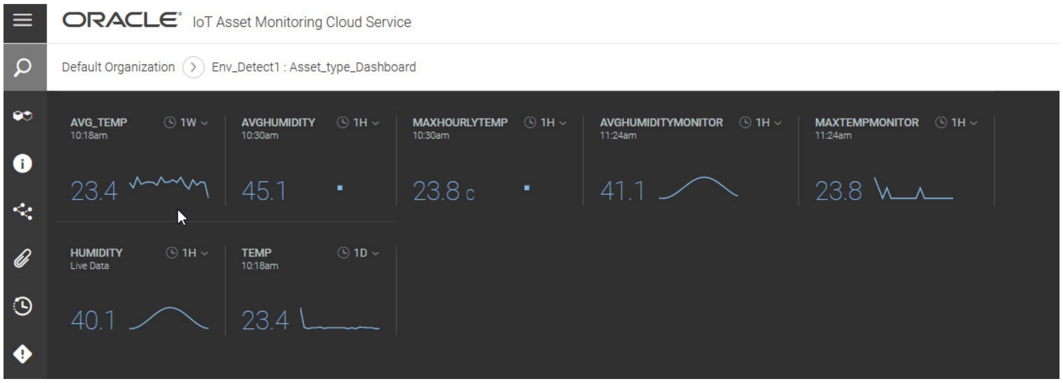
16. Click **Save** to save the dashboard changes.

Visualize and Compare Past Metric Data

You can view past metric data, in addition to the current metric value, for your dashboard metric gadgets. Choose between the chart view and the tabular view to look at data up to 180 days in the past, depending on your metric storage policies. Past metric data is available for both built-in and custom metrics.

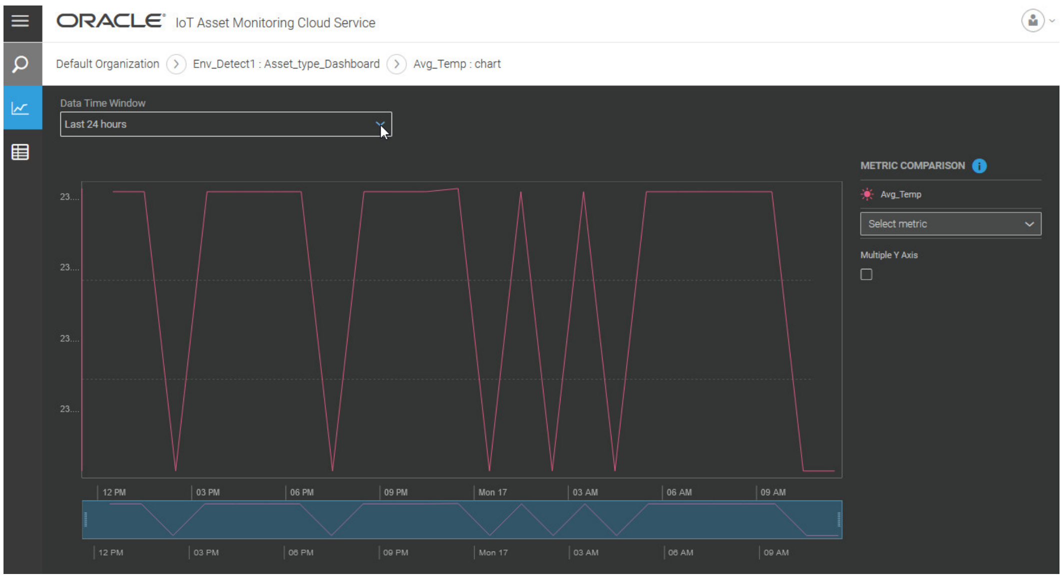
You can also compare up to four metrics in the chart view. For example, you may wish to study possible correlation between two metrics, say *AveragePressure* and *AverageTemperature*. If the metric values are disparate, you can choose multiple y-axes, so that you are able to see each metric plot using the correct scale.

1. In the Operations Center Dashboard view, click the gadget corresponding to the metric.



The metric chart view appears by default.

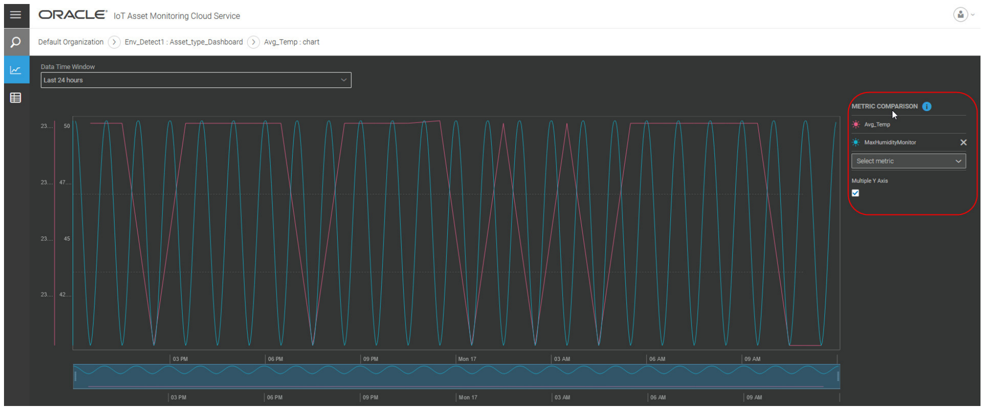
2. Select a pre-defined or custom **Data Time Window** value to see the chart for the specified period.



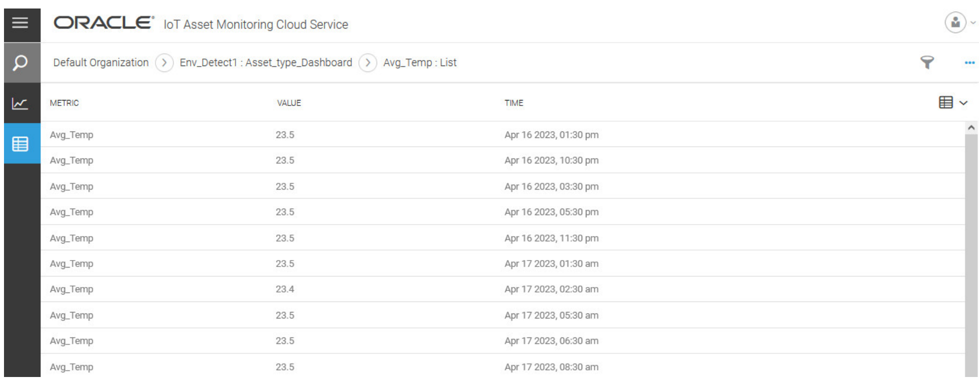
Depending on your metric data storage policies, you can visualize data up to 180 days in the past.

3. Use the **Metric Comparison** area to add metrics to compare.

   You can compare up to four metrics in the chart view. If the metric values are disparate, you can choose multiple y-axes, so that you are able to see each metric plot using the correct scale.

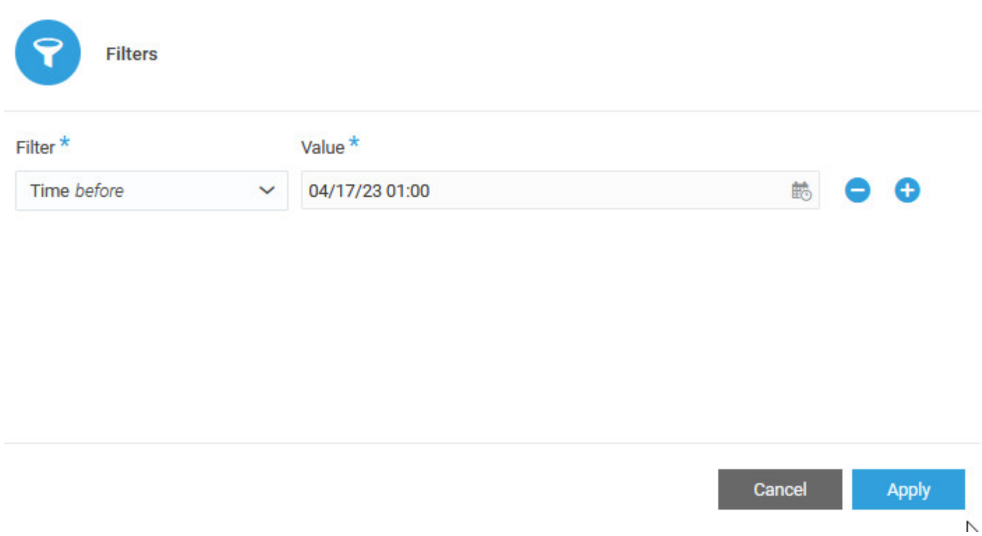


4. Click **List**  in the menu bar on the left to view tabular data for the metric values.



METRIC	VALUE	TIME
Avg_Temp	23.5	Apr 16 2023, 01:30 pm
Avg_Temp	23.5	Apr 16 2023, 10:30 pm
Avg_Temp	23.5	Apr 16 2023, 03:30 pm
Avg_Temp	23.5	Apr 16 2023, 05:30 pm
Avg_Temp	23.5	Apr 16 2023, 11:30 pm
Avg_Temp	23.5	Apr 17 2023, 01:30 am
Avg_Temp	23.4	Apr 17 2023, 02:30 am
Avg_Temp	23.5	Apr 17 2023, 05:30 am
Avg_Temp	23.5	Apr 17 2023, 06:30 am
Avg_Temp	23.5	Apr 17 2023, 08:30 am

5. (Optional) Choose filters to look at data of interest.



6. Use the breadcrumb navigation to go back to the dashboard.

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** ( ) against your dashboard row.
3. Click and drag a metric, or metric group, using the Handle ( ), 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** ( ) against your dashboard row.
3. Click the **Delete** ( ) icon for the metric or metric group that you want to remove from your dashboard.
4. Click **Save** to save your dashboard changes.

Create a Dashboard Using External Content

If you have external reports, visualizations, and pages, such as those created in Oracle Analytics Cloud, you can embed these into custom IoT dashboards. When creating a new custom dashboard, select the **External Content** option to use an external URL that can be embedded into the dashboard.

1. Navigate to the Dashboards page at the organization, group, or asset type level.

   Use one of the following paths:

   - **Menu > Design Center > Organization > Dashboards**
   - **Menu > Design Center > Groups > *Group Name* > Dashboards**
   - **Menu > Design Center > Asset Types > *Asset Type Name* > Dashboards**

2. Click **Create Dashboard** (+).
3. Select **External Content** and click **Create**.
4. Select a **Name** and **Icon** for your dashboard.

   Once the dashboard is created, the chosen icon will appear on the Operations Center menu bar.

5. Under **Role Access**, optionally change the user roles to which the content of the dashboard should be available.

   The roles you select can view the dashboard in Operations Center.

6. Under **URL**, specify the URL of the external page to embed in your IoT dashboard.

   If the external URL supports embed, the URL should load on clicking the preview area below the **URL** field.

   > **Note:**
   >
   > To be able to view Oracle Analytics Cloud visualizations and reports in your IoT application, you should be already logged into Oracle Analytics Cloud.

7. Click **Save** to finish creating the dashboard.

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.

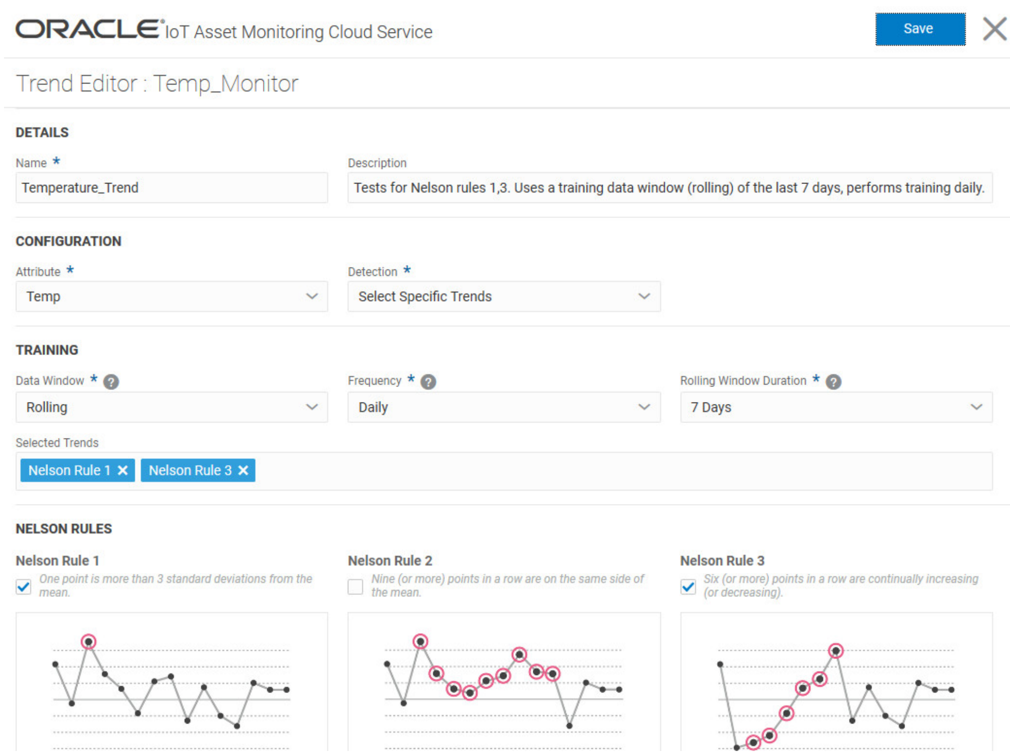
   The Trend Detection Editor appears for the selected asset type.

   The trend detection that you define will apply to all assets of the chosen asset type.
6. Enter a name for the trend in the **Name** field.
7. (Optional) Specify an optional description text for the trend.
8. Under Configuration, select an available **Attribute** to monitor.

   Select from the list of asset sensor attributes and any metrics that you have defined for the asset type.
9. 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.
10. 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.
11. Under Training, select the **Data Window**.

    The **Data Window** identifies the data set that is used to train the system for detecting trends.
    - **Rolling**: A rolling data window uses data from a rolling time window to pick the most recent data for training. For example, you can choose to train your trend model with a rolling data window of the last 7 days, and choose to perform the trend training daily.
      When you use a rolling window, the training model is re-created periodically, as determined by the schedule frequency that you choose.
      – **Frequency**: The frequency of the trend model training. For example, if you choose **Daily**, then the training happens every day at 00:00 hours (midnight), UTC time by default.
      – **Rolling Window Duration**: The duration of the rolling window going back from the model training time. For example, if you select **7 Days**, then the last 7 days of specimen asset data is used to train the trend model.

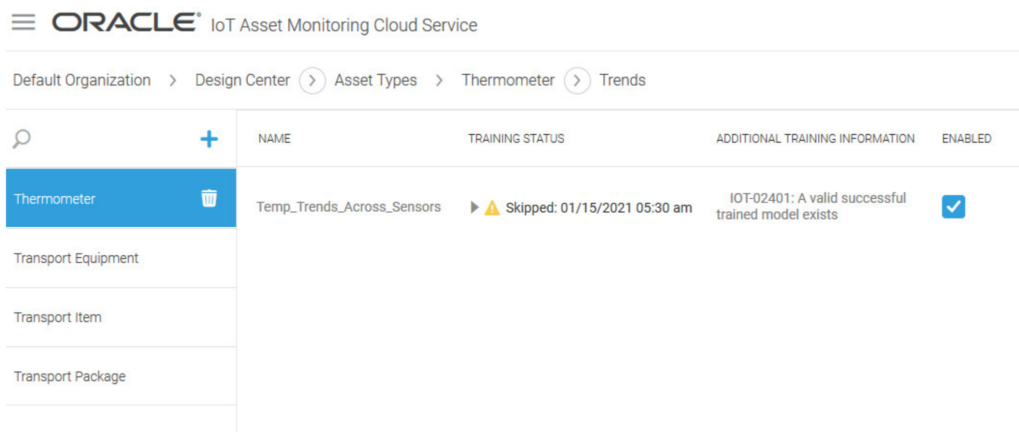


- **Static**: Uses a static data window to train your trend model. Select the **Window Start Time** and **Window End Time** for your static window period.
  The static data window provides data for a one-time training of your trend model. If your definition of typical data changes in the future, you should edit the **Data Window** for the trend, so that the model can be re-trained.

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

    The system now starts building a trend model for the new trend.

The trend is added to the Trends page. The **Training Status** column shows the latest training status for the trend model. Once training is complete, the application starts detecting and reporting trends.
The application reports completed model trainings along with their timestamps. For skipped training, the application includes additional information on the reasons. For example, the presence of a valid trained model may result in skipped training. If training fails, the application includes pertinent information related to the failure.



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 goes 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 Intelligent Applications Cloud. 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 Intelligent Applications Cloud 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 Intelligent Applications Cloud. 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.

      The **Summary** field for incidents and warnings can include dynamic contextual parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
    - **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.

      The **Description** field for incidents and warnings can include dynamic contextual parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
    - **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.

      For asset actions, the **Parameter Value** field can contain dynamic contextual parameters. You can use contextual parameters only in string parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
    - **Subscribers:**Under Notification Subscription, you can add one or more subscriber groups to receive notifications when incidents or warnings are triggered by the rule. See Use SMS, Email, and HTTP Notifications for more information on configuring notifications.
16. If you are creating a rule incident, and you wish to use failure modes for your asset type, select **Include Failure Mode Details**.

    You must have already defined at least one failure mode for your asset type.

    a. Select a pre-existing **Failure Mode** that corresponds to the incident.

    b. Select one or more pre-existing **Failure Causes** that apply to the failure incident.

    See Add Failure Diagnostics Information to Asset Incidents and Anomalies for more information on using failure modes.
17. Optionally specify a weekly or monthly schedule during which the rule is in force.

    A rule is active at all times, by default. You can change this behavior to choose a custom schedule for the rule.

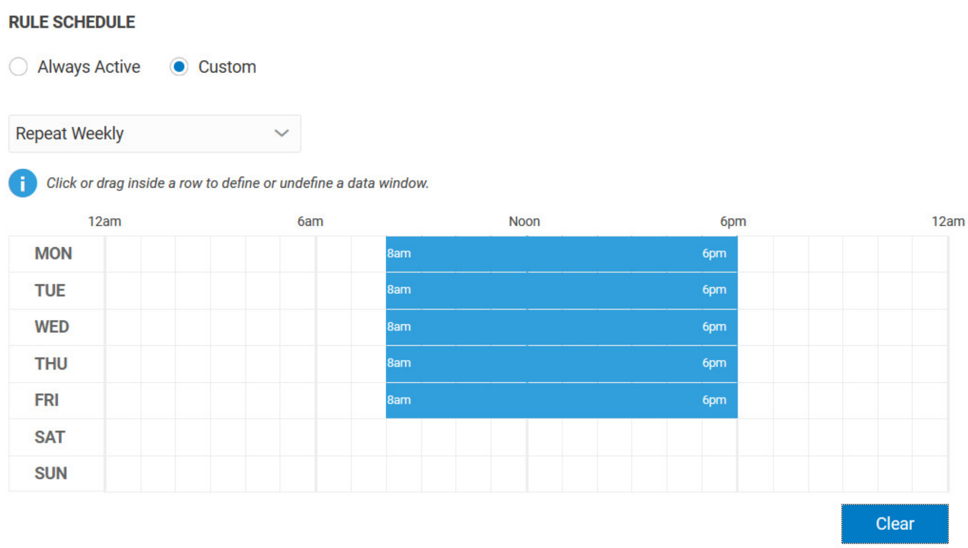
    a. Under Rule Schedule, select **Custom**.

b. Select **Repeat Weekly** to create a weekly schedule. Alternatively, select **Repeat Monthly** to create a monthly schedule.

c. Click or drag inside the rows to select a data window.

   You can click an incorrectly selected cell to deselect it. Alternatively, click **Clear** to start afresh.

The following example shows a weekly schedule for a rule that it is active from 8:00 a.m. to 6:00 p.m. on weekdays.



18. Click **Save**.
19. 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: `metric/sys_openIncidents Greater Than 5.`
10. (Optional) Add additional threshold conditions for attribute values.
11. (Optional) Add additional alert and location conditions.

    See Create an Alert Rule for more information on alert conditions.

    See Create a Location Rule for more information on location conditions.
12. 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.
13. 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 Intelligent Applications Cloud. 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.

14. 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.

      The **Summary** field for incidents and warnings can include dynamic contextual parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
    - **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.

      The **Description** field for incidents and warnings can include dynamic contextual parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
    - **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.

      For asset actions, the **Parameter Value** field can contain dynamic contextual parameters. You can use contextual parameters only in string parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
    - **Subscribers:**Under Notification Subscription, you can add one or more subscriber groups to receive notifications when incidents or warnings are triggered by the rule. See Use SMS, Email, and HTTP Notifications for more information on configuring notifications.
15. If you are creating a rule incident, and you wish to use failure modes for your asset type, select **Include Failure Mode Details**.

    You must have already defined at least one failure mode for your asset type.

    a. Select a pre-existing **Failure Mode** that corresponds to the incident.

    b. Select one or more pre-existing **Failure Causes** that apply to the failure incident.

    See Add Failure Diagnostics Information to Asset Incidents and Anomalies for more information on using failure modes.
16. Optionally specify a weekly or monthly schedule during which the rule is in force.

    A rule is active at all times, by default. You can change this behavior to choose a custom schedule for the rule.

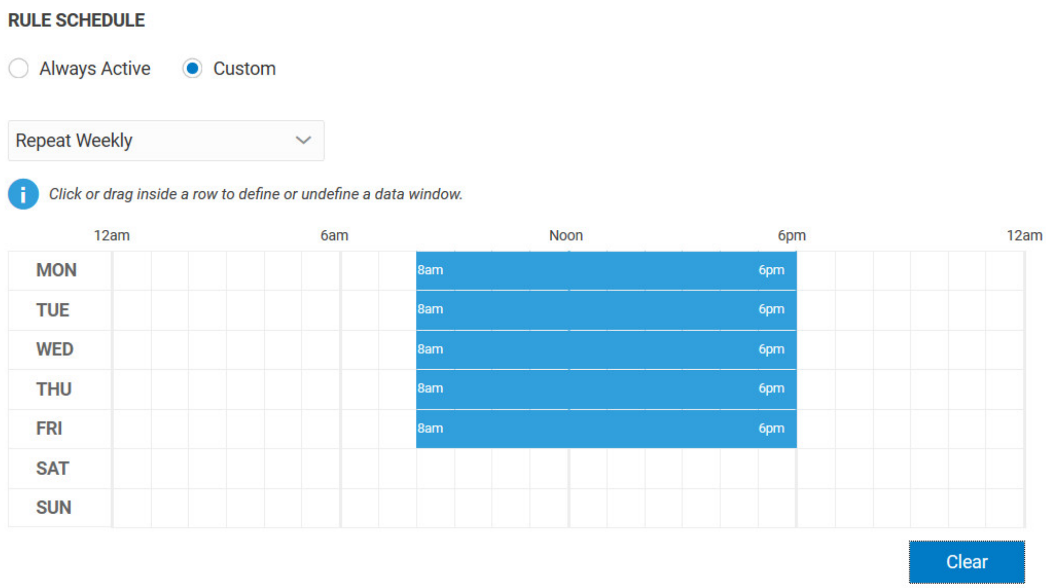
    a. Under Rule Schedule, select **Custom**.

    b. Select **Repeat Weekly** to create a weekly schedule. Alternatively, select **Repeat Monthly** to create a monthly schedule.

c. Click or drag inside the rows to select a data window.

   You can click an incorrectly selected cell to deselect it. Alternatively, click **Clear** to start afresh.

The following example shows a weekly schedule for a rule that it is active from 8:00 a.m. to 6:00 p.m. on weekdays.



17. Click **Save**.
18. 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 Intelligent Applications Cloud. 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.

      The **Summary** field for incidents and warnings can include dynamic contextual parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
    - **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.

      The **Description** field for incidents and warnings can include dynamic contextual parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
    - **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.

      For asset actions, the **Parameter Value** field can contain dynamic contextual parameters. You can use contextual parameters only in string parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
    - **Subscribers:**Under Notification Subscription, you can add one or more subscriber groups to receive notifications when incidents or warnings are triggered by the rule. See Use SMS, Email, and HTTP Notifications for more information on configuring notifications.
16. If you are creating a rule incident, and you wish to use failure modes for your asset type, select **Include Failure Mode Details**.

    You must have already defined at least one failure mode for your asset type.

    a. Select a pre-existing **Failure Mode** that corresponds to the incident.

    b. Select one or more pre-existing **Failure Causes** that apply to the failure incident.

    See Add Failure Diagnostics Information to Asset Incidents and Anomalies for more information on using failure modes.
17. Optionally specify a weekly or monthly schedule during which the rule is in force.

    A rule is active at all times, by default. You can change this behavior to choose a custom schedule for the rule.

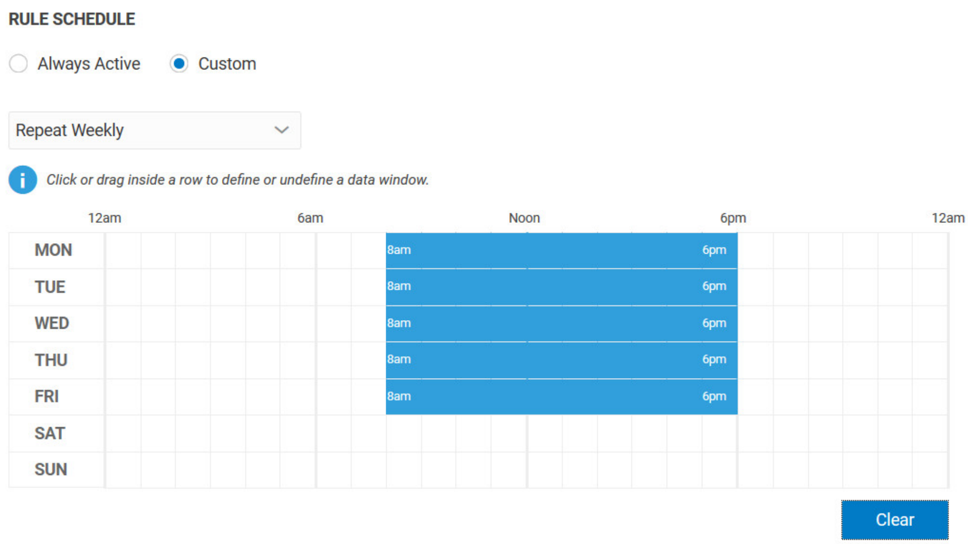
    a. Under Rule Schedule, select **Custom**.

    b. Select **Repeat Weekly** to create a weekly schedule. Alternatively, select **Repeat Monthly** to create a monthly schedule.

c. Click or drag inside the rows to select a data window.

   You can click an incorrectly selected cell to deselect it. Alternatively, click **Clear** to start afresh.

The following example shows a weekly schedule for a rule that it is active from 8:00 a.m. to 6:00 p.m. on weekdays.



18. Click **Save**.
19. 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 Intelligent Applications Cloud. 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.

      The **Summary** field for incidents and warnings can include dynamic contextual parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.

- **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.

  The **Description** field for incidents and warnings can include dynamic contextual parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
- **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.

  For asset actions, the **Parameter Value** field can contain dynamic contextual parameters. You can use contextual parameters only in string parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
- **Subscribers:**Under Notification Subscription, you can add one or more subscriber groups to receive notifications when incidents or warnings are triggered by the rule. See Use SMS, Email, and HTTP Notifications for more information on configuring notifications.

16. If you are creating a rule incident, and you wish to use failure modes for your asset type, select **Include Failure Mode Details**.

    You must have already defined at least one failure mode for your asset type.

    a. Select a pre-existing **Failure Mode** that corresponds to the incident.

    b. Select one or more pre-existing **Failure Causes** that apply to the failure incident.

    See Add Failure Diagnostics Information to Asset Incidents and Anomalies for more information on using failure modes.

17. Optionally specify a weekly or monthly schedule during which the rule is in force.

    A rule is active at all times, by default. You can change this behavior to choose a custom schedule for the rule.

    a. Under Rule Schedule, select **Custom**.

    b. Select **Repeat Weekly** to create a weekly schedule. Alternatively, select **Repeat Monthly** to create a monthly schedule.

    c. Click or drag inside the rows to select a data window.

       You can click an incorrectly selected cell to deselect it. Alternatively, click **Clear** to start afresh.

    The following example shows a weekly schedule for a rule that it is active from 8:00 a.m. to 6:00 p.m. on weekdays.

18. Click **Save**.
19. Click **Back** to return to the **Rules** list.

Create a Trend Based Rule

Create a trend based rule to generate an incident, alert, action, or warning based on trends occurring for your sensor or metric values.

To create trend based rules, you must have the trends defined. See Use Statistical Trends for Your Asset Sensor Attributes and Metrics for more information on trends.

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 a predefined trend:
   a. Select the trend name from the list.

      A second drop-down list appears.
   b. Select one of the following:
      - Select **Occurred** to trigger the rule when the trend occurs.
      - Select **Occurred in Last** to specify a time duration. The rule gets triggered if the trend occurred within 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.
   c. (Optional) If you wish the rule to be triggered only by specific Nelson Rule trends, then select one or more Nelson rules that will trigger the rule.

      If you do not select specific rules, then the rule checks for all Nelson Rules included in the trend by default.

      To select specific Nelson Rule trends, select one Nelson Rule at a time from the list until you have added all the required rules.
10. (Optional) Add additional trend 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 Intelligent Applications Cloud. 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.

      The **Summary** field for incidents and warnings can include dynamic contextual parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
    - **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.

      The **Description** field for incidents and warnings can include dynamic contextual parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
    - **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.

      For asset actions, the **Parameter Value** field can contain dynamic contextual parameters. You can use contextual parameters only in string parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
    - **Subscribers:**Under Notification Subscription, you can add one or more subscriber groups to receive notifications when incidents are triggered by the rule. See Use SMS, Email, and HTTP Notifications for more information on configuring notifications.
16. If you are creating a rule incident, and you wish to use failure modes for your asset type, select **Include Failure Mode Details**.

    You must have already defined at least one failure mode for your asset type.

    a. Select a pre-existing **Failure Mode** that corresponds to the incident.

    b. Select one or more pre-existing **Failure Causes** that apply to the failure incident.

    See Add Failure Diagnostics Information to Asset Incidents and Anomalies for more information on using failure modes.
17. Optionally specify a weekly or monthly schedule during which the rule is in force.

    A rule is active at all times, by default. You can change this behavior to choose a custom schedule for the rule.

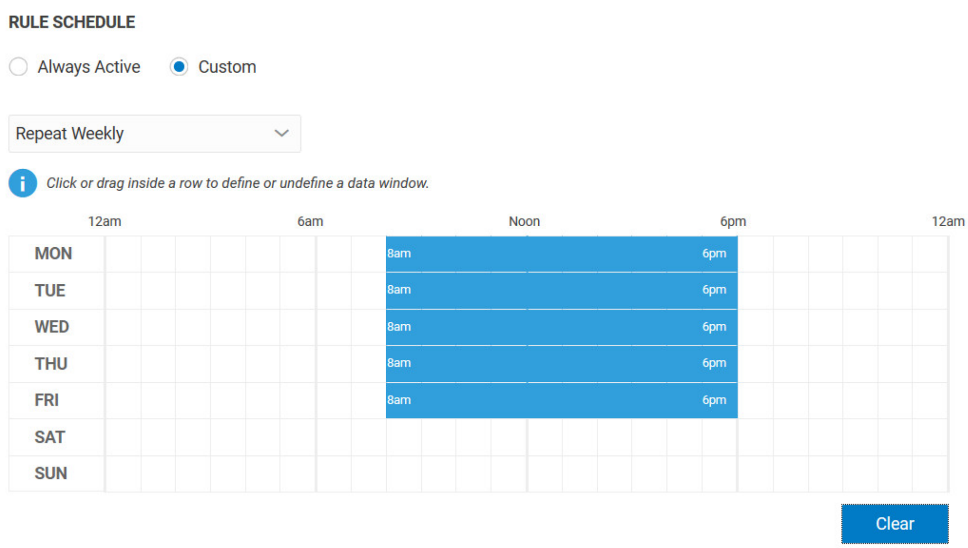
    a. Under Rule Schedule, select **Custom**.

    b. Select **Repeat Weekly** to create a weekly schedule. Alternatively, select **Repeat Monthly** to create a monthly schedule.

c. Click or drag inside the rows to select a data window.

   You can click an incorrectly selected cell to deselect it. Alternatively, click **Clear** to start afresh.

The following example shows a weekly schedule for a rule that it is active from 8:00 a.m. to 6:00 p.m. on weekdays.



18. Click **Save**.
19. 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 Intelligent Applications Cloud. 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.

      The **Summary** field for incidents and warnings can include dynamic contextual parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.

- **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.

  The **Description** field for incidents and warnings can include dynamic contextual parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
- **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.

  For asset actions, the **Parameter Value** field can contain dynamic contextual parameters. You can use contextual parameters only in string parameters. See Use Contextual Parameters in Warnings, Incidents, and Action Messages for more details.
- **Subscribers:**Under Notification Subscription, you can add one or more subscriber groups to receive notifications when incidents or warnings are triggered by the rule. See Use SMS, Email, and HTTP Notifications for more information on configuring notifications.

16. If you are creating a rule incident, and you wish to use failure modes for your asset type, select **Include Failure Mode Details**.

    You must have already defined at least one failure mode for your asset type.

    a. Select a pre-existing **Failure Mode** that corresponds to the incident.

    b. Select one or more pre-existing **Failure Causes** that apply to the failure incident.

    See Add Failure Diagnostics Information to Asset Incidents and Anomalies for more information on using failure modes.

17. Optionally specify a weekly or monthly schedule during which the rule is in force.

    A rule is active at all times, by default. You can change this behavior to choose a custom schedule for the rule.

    a. Under Rule Schedule, select **Custom**.

    b. Select **Repeat Weekly** to create a weekly schedule. Alternatively, select **Repeat Monthly** to create a monthly schedule.

    c. Click or drag inside the rows to select a data window.

       You can click an incorrectly selected cell to deselect it. Alternatively, click **Clear** to start afresh.

    The following example shows a weekly schedule for a rule that it is active from 8:00 a.m. to 6:00 p.m. on weekdays.

18. Click **Save**.
19. Click **Back** to return to the **Rules** list.

Use Contextual Parameters in Warnings, Incidents, and Action Messages

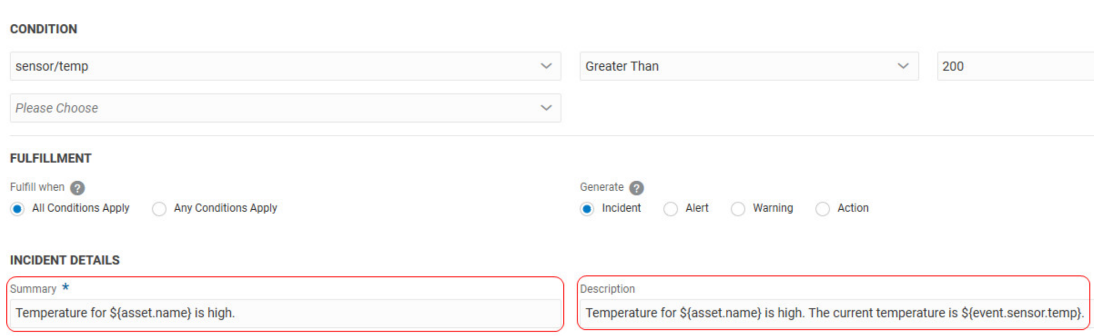
When creating rules, you can use dynamic contextual parameters in the incident and warning details. You can also use contextual parameters in string message values of your asset actions.

Contextual parameters can include variables, such as asset names, sensor values, metric values, and location coordinates of the asset. These variables are dynamically resolved each time the rule is triggered.

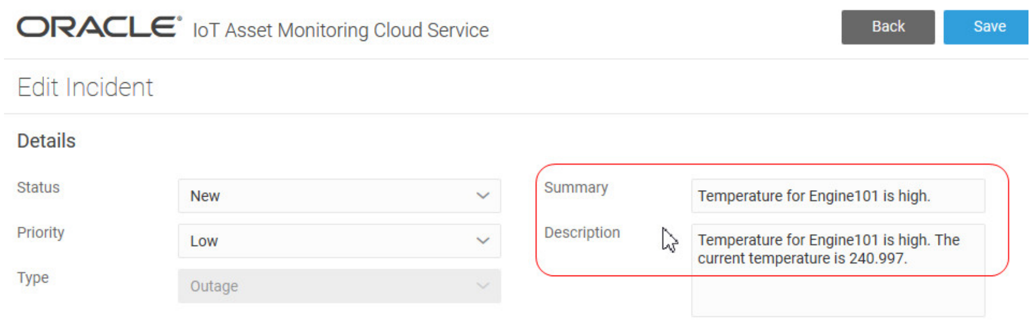
The following warning and incident fields can include dynamic contextual parameters:

- **Summary**
- **Description**

Here's an example of the rule configuration screen containing dynamic contextual parameters in the **Summary** and **Description** fields:



And here's an actual Incident created by the preceding rule:



For asset actions, the **Parameter Value** field can contain dynamic contextual parameters. You can use contextual parameters only in string parameters.

The following contextual parameters can dynamically retrieve asset, sensor, metric, rule, and location related information:

- Asset Parameters
  - `${asset.name}`: Retrieves the name of the asset for which the warning, incident, or action is generated.

    For example: `The asset ${asset.name} has low fuel.`

    May translate to:

    `The asset RedTruck has low fuel.`
  - `${asset.id}`: Retrieves the ID (GUID) of the asset for which the warning, incident, or action is generated.
- Sensor Parameters
  - `${event.sensor.`*`attributeName`*`}`: Retrieves the value of the specifed sensor attribute name.

    For example: `The asset ${asset.name} has low fuel level: ${event.sensor.fuel}%.`

    May translate to:

    `The asset Truck1 has low fuel level: 10%.`

    Here, `fuel` is a sensor attribute for the truck asset.
- Metric Parameters: You can use metric-related parameters only if the rule condition uses the metric.
  - `${event.metric.name}`: Retrieves the name of the metric that triggered the rule.
  - `${event.metric.value}`: Retrieves the value of the metric that triggered the rule.

    For example: `${event.metric.name} for ${asset.name} is High: It is ${event.metric.value}.`

    May translate to:

    `Average Temperature for Engine1 is High: It is 150.`
- Rule Parameter

`${rule.id}`: Retrieves the ID (GUID) of the rule for which the warning, incident, or action is generated.

- Location Parameters: You can use these contextual parameters only in location-based rules.
  - `${event.location.deviceId}`: Retrieves the Device ID of the asset device.
  - `${event.location.latitude}`: Retrieves the latitude co-ordinates of the device.
  - `${event.location.longitude}`: Retrieves the longitude co-ordinates of the device.
  - `${event.location.altitude}`: Retrieves the altitude reading of the device.

    For example: `The asset ${asset.name} has exited its designated location. The asset's co-ordinates are: ${event.location.longitude} ${event.location.latitude}.`

    May translate to:

    ```
    The asset Forklift1 has exited its designated location. The asset's co-
    ordinates are: -122 37.
    ```

Use Built-In Functions to Format Your Contextual Parameters

You can choose to use built-in functions to format the output of your contextual parameters.

For example, string keys can use the following format options:

- `${asset.name`**`?cap_first`**`}` converts the first letter of the string to uppercase.
- `${asset.name`**`?uncap_first`**`}` converts the first letter of the string to lowercase.
- `${asset.name`**`?capitalize`**`}` converts the string into title case (the first letter of every word is capitalized).
- `${asset.name`**`?lower_case`**`}` converts the string to lowercase.
- `${asset.name`**`?upper_case`**`}` converts the string to uppercase.
- `${asset.name`**`?remove_beginning("`*`STRING`*`")`**`}` removes the specified sub string from the beginning of the string.
- `${asset.name`**`?remove_ending("`*`STRING`*`")`**`}` removes the specified sub string from the end of the string.
- `${asset.name`**`?trim`**`}` removes any leading and trailing white spaces from the string.

The following examples describe some available format options for number outputs:

- `${event.sensor.<sensor_name>`**`?abs`**`}` converts a number to its absolute (non-negative) value.
- `${event.sensor.<sensor_name>`**`?c`**`}` converts a numeric value to the *computer language* value, as opposed to the default human readable format. Doesn't use grouping separators (commas, for example), uses dot as a decimal separator. Prints up to 16 digits after the dot. Never uses exponential form.
- `${event.sensor.<sensor_name>`**`?round`**`}` rounds the number to the nearest whole number. In case a decimal number ends with .5, rounds it to the next whole number.
- `${event.sensor.<sensor_name>`**`?floor`**`}` rounds the number downwards.
- `${event.sensor.<sensor_name>`**`?ceiling`**`}` rounds the number upwards.

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** (≡), 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** (≡), 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** (≡), 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 on 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** () icon.
7. Click **Yes**.

Use the Incidents Page to Manage Asset Incidents

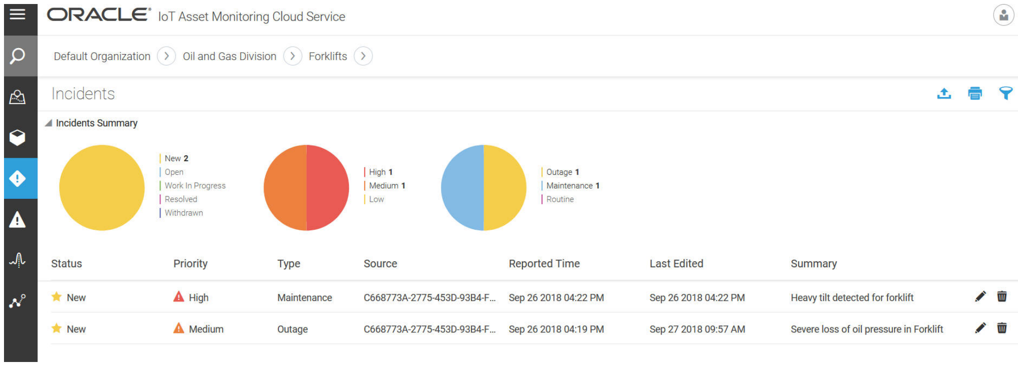
View and manage incidents from the Incidents page. You can also change the status of an incident from this page.

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** ( ) 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 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 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

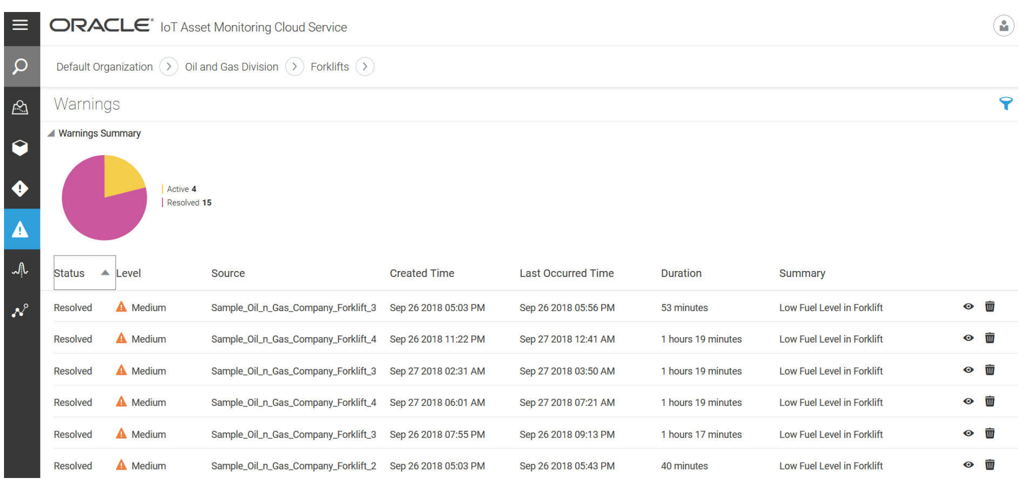
View and manage warnings from the Warnings page. You can also delete warnings from this page.

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.

You can delete both resolved and active warnings. Deleting an active warning may be required in certain scenarios; say, if you are running a what-if simulation scenario.

> **Note:**
>
> If the rule configuration for the warning has **Auto Delete on Resolve** enabled, then warnings are automatically deleted once they are resolved.

Use SMS, Email, and HTTP Notifications

Oracle IoT Asset Monitoring Cloud Service integrates with the Twilio SMS service to help provide seamless SMS notifications. You can also use the default SMTP account, or your own SMTP server, for sending out email notifications. HTTP endpoint notifications are also supported for external applications.

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

You can also send email notifications for asset incidents, warnings, and alerts. When a rule triggers an incident, warning, or alert, email notifications are sent to all configured subscribers. The email notifications also contain a link to the corresponding incident making it easy to navigate to the incident details in the application.

HTTP endpoint notifications are also supported for external applications. For example, an application, such as Oracle Transportation Management (OTM) or Oracle Intelligent Track and Trace can receive alerts and incident notifications from the connected IoT application.

SMS, email, and HTTP notifications eliminate the need to monitor the Oracle IoT Asset Monitoring Cloud Service application continuously. All subscribers are actively informed about incidents, warnings, and alerts 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.

To use the SMS notification service, you must have a Twilio account subscription. 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.

To use email notifications, you can use the built-in, default SMTP account. The default account has a usage limit of 100,000 messages. Alternatively, you can use your own SMTP server to channel Oracle IoT Asset Monitoring Cloud Service email notifications. After choosing your SMTP account, you can add subscribers that need to receive these notifications, and select the rules that should send the notifications.

Add Your SMS 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 Intelligent Applications Cloud 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 **Settings**.

   If you are in the Design Center, you need to click **Previous** () before you see the **Settings** option in the menu.
2. Click **Notification Accounts**.
3. Click **Create Notification Account** ().
4. Select your **Provider**.

   Oracle integrates with Twilio, as the third-party notification service provider.
5. Enter a **Name** for your notification account.

   For example, *My Twilio Account.*
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 **Create** to add the notification account.

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

Add Your Email Notification Account Details

To start using the email notification feature, you can use the built-in, default SMTP service in Oracle IoT Asset Monitoring Cloud Service. Alternatively, you can add your own SMTP server to send unlimited email notifications.

The default SMTP service in Oracle IoT Asset Monitoring Cloud Service lets you send limited email notifications. The usage limit is 100,000 messages per cycle. If your usage needs are different, you can add your own SMTP notification account.

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

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

1. In the Operations Center, click **Menu** (☰), and then click **Settings**.

   If you are in the Design Center, you need to click **Previous** (<) before you see the **Settings** option in the menu.

2. Click **Notification Accounts**.

   Notice that the Notification Accounts section already includes the default SMTP account.

3. To add your own SMTP account, click **Create Notification Account** (+).
4. Under **Provider**, select **SMTP**.
5. Enter a **Name** for your notification account.

   For example, `My SMTP Account`.

6. Enter the **User Name** and **Password** for your SMTP account.
7. Enter the **SMTP Host** server name.
8. Enter the **SMTP Port**.

   The default port number is 465.

9. Under **From**, enter the sender email ID to be used for sending email notifications.
10. Optionally select **Use TLS** (Transport Layer Security) to secure SMTP with an encryption protocol.
11. Click **Create** to create the notification account.

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

Add Your HTTP Notification Account Details

To start using the notification feature, add your notification account details in Oracle IoT Asset Monitoring Cloud Service. For HTTP notifications, add your external application HTTP endpoint URL.

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

1. In the Operations Center, click **Menu** (), and then click **Settings**.

   If you are in the Design Center, you need to click **Previous** () before you see the **Settings** option in the menu.

2. Click **Notification Accounts**.
3. Click **Create Notification Account** ().
4. Under **Provider**, select **HTTP**.
5. Enter a **Name** for your notification account.

   For example, *External HTTP Account.*

6. Enter the endpoint **URL** for your external HTTP application.
7. Select the **Authentication Type**.

   The password-based **Basic** authentication type is currently supported for HTTP notifications.

8. Enter the **User Name** and **Password** credentials for your external HTTP endpoint.
9. Click **Create** to add the notification account.

You can next add subscribers or recipients for the HTTP 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. In the Operations Center, click **Menu** (), and then click **Settings**.

   If you are in the Design Center, you need to click **Previous** () before you see the **Settings** option in the menu.

2. Click **IoT Organizations**.
3. Click the name of your organization.
4. Click **Subscribers** to open the subscribers page for your organization.
5. Click **Create Subscriber** (to add a new subscriber or group or subscribers.
6. Select your **Notification Account**.

   See Add Your SMS Notification Account Details, Add Your Email Notification Account Details, and Add Your HTTP Notification Account Details for more information on adding SMS, email, and HTTP notification accounts.

7. 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.

8. (Optional) Select pre-existing **Rules** to subscribe to events from the selected rules.

   Note that you can also add notification subscribers to an individual rule by editing the rule, or when creating a new rule.

9. Select the **Contact Method**.

   - **Subscribers:** Select to add existing user names as subscribers.

- **Emails:** For email notification accounts, select to add subscribers using their email addresses.
- **Phone Numbers:** For SMS notification accounts, select to add subscribers using their phone numbers.
- **Subscribers and Emails:** For email notification accounts, select if you wish to add some subscribers using their user names and others using their email addresses.
- **Subscribers and Phone Numbers:** For SMS notification accounts, select if you wish to add some subscribers using their user names and others using their phone numbers.

10. If you chose **Subscribers**, select existing users to add them as subscribers.

    Depending on whether you have chosen an SMS or email notification account, the phone numbers or emails of the users are added to the subscriber group.

11. If you are configuring an SMS subscriber group, you can individually enter the subscriber **Phone Numbers**.

    Precede the phone numbers with the country codes. Press enter after entering each phone number.

12. If you are configuring an email subscriber group, you can individually enter the subscriber **Emails**.

    Press enter after entering each email address.

13. Click **Create** 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 use a Database Classic Cloud Service instance to store your data. You can also use an Autonomous Transaction Processing database table.

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 Classic 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:

```
Average(FuelLevel*100/FuelCapacity)
```

Here, `FuelLevel` is a sensor value, and the `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 anAutonomous Transaction Processing table to store historical sensor data for training the prediction model.

Create an External Data Connection to a Database Classic Cloud Service Instance

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

1. Click **Menu** (≡), and then click **Design Center**.
2. Select **Organization** from the **Design Center** sub-menu.
3. Click **External Data Sources** .
4. Click the **Create New** (+) icon.
5. Enter a **Name** and an optional **Description** for the external data connection.
6. Select **DBaaS** in the **Type** list.
7. 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.
8. Enter the URL for the Database Classic Cloud Service instance in the **Connection String** field.
9. Enter the user name for the Database Classic Cloud Service instance in the **User Name** field.
10. Enter the password for the Database Classic Cloud Service instance in the **Password** field.
11. 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.
12. 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.
13. Click **Save** to create the external data connection.

Create an External Data Connection to an Oracle Autonomous Transaction Processing Instance

Create an external data connection to link to an Autonomous Transaction Processing database table. You can use the data in the table for KPI computations and predictive analytics.

1. Click **Menu** (≡), and then click **Design Center**.
2. Select **Organization** from the **Design Center** sub-menu.
3. Click **External Data Sources** .
4. Click the **Create New** (+) icon.

5. Enter a **Name** and an optional **Description** for the external data connection.
6. Under Data Format, select **ATP** as the database **Type**.
7. Enter the name of your ATP database table in the **Table Name** field.
8. Click **Choose File** to select the wallet file required to connect to your ATP instance.

   Oracle client credentials (wallet files) are downloaded from ATP by a service administrator. If you are not an ATP administrator, your administrator should provide you with the client credentials.

   The wallet file for the ATP database can be downloaded from the ATP service console.
9. Enter the **Connection String** to use for the Autonomous Transaction Processing instance.

   For example, a simple connection string would look like the following:

   ```
   database_host[:port][/[service_name]
   ```
10. Enter the user name for connecting to the Autonomous Transaction Processing database in the **User Name** field.
11. Enter the password for the user in the **Password** field.
12. 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.
13. Under **Associations**, you can associate the ATP 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 ATP table column.
    e. Add additional sensor attributes to column associations, as required.
14. 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. Click **Menu** (≡), and then click **Design Center**.
2. Select **Organization** from the **Design Center** sub-menu.
3. Click **External Data Sources** .
4. Select an external data connection in the **External Data** list.
5. Click the **Edit** () icon.
6. Edit the external data connection settings.
7. 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 then click **Design Center**.
2. Select **Organization** from the **Design Center** sub-menu.
3. Click **External Data Sources** .
4. Select an external data connection in the **External Data** list.
5. Click the **Duplicate** ( ) icon.

   A duplicate external data connection opens up for editing.
6. Enter a name for the external data connection in the **Name** field and then add an optional description.
7. (Optional) Edit the remaining external data connection settings.
8. Click **Save**.

Delete a Contextual Data Connection

Delete a contextual data connection when it is no longer required.

1. Click **Menu** (), and then click **Design Center**.
2. Select **Organization** from the **Design Center** sub-menu.
3. Click **External Data Sources** .
4. Select an external data connection in the **External Data** list.
5. Click the **Delete** () icon.
6. Click **Yes** to confirm.

Use Correlation Analysis for Your IoT Sensor Attributes

Use correlation analysis for your asset sensor attributes to visualize and understand the relationships between the various attributes. Correlation analysis can help determine optimal operating and maintenance parameters for your asset. Correlation analysis can also help determine the variables that correlate with unexpected asset failure.

Correlation analysis lets you explore the relationships between the available IoT data measurements and get insights into asset behavior. Correlation analysis also helps perform what-if scenario analyses and root cause diagnostics. Use correlation analysis to help set up your control systems, set up multivariate anomaly detection, and state-aware anomalies.

In addition to sensor attributes, you can also include dynamic custom attributes in your correlation analysis.

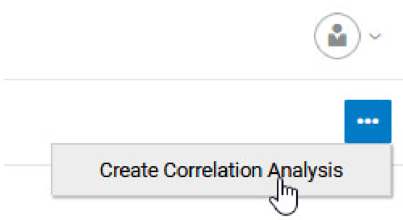
Create a Correlation Analysis for an Asset Type

Create a correlation analysis for an asset type to study the correlation between a target sensor attribute and one or more influencing sensor attributes.

You can apply the correlation analysis to all assets of the asset type, or apply it to specific assets that you wish to study. Use the Asset Type page in Design Center to create the correlation analysis.

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 **Correlation Analysis**.
5. Select **Create Correlation Analysis** from the Correlation Analysis menu.

   The Correlation Analysis editor appears.
6. In the Correlation Analysis editor, specify a **Name** and **Description** for the correlation analysis under the **Details** section.
7. Select a value for the **Publish Results To** field.

   When first creating a correlation analysis, you may want to publish it to **Design Center** only. After you have viewed and analyzed the results, you may want to edit the value to **Operations Center**, so that the results appear in the Operations Center view as well.
8. Under **Target**, choose whether you want the analysis to apply to all assets or specific assets of the asset type.

   Select **All assets of type: *AssetType*** to apply the analysis to all assets. Alternatively, select **Specific assets of type: *AssetType*** to choose the specific assets to analyze.
9. Under **Time Period**, choose the time duration for which to analyze the data.

   For example, choosing **One Hour** will analyze the last hour's data for the chosen assets when you run the analysis.
10. Under **Target Attribute**, select the sensor attribute that you wish to analyze.

    You may also choose a dynamic custom attribute to analyze.
11. Choose the data **Type** for the target attribute.

    Choose **Continuous** if the attribute can take continuous real numbered values. For example, 10.6. Choose **Categorical** if the attribute can take only discrete values. For example, values such as 'High', or '100'.

12. Under **Influencing Attributes**, select one or more sensor attributes that can influence the target attribute.

    You may also include dynamic custom attributes under influencing attributes.

    After selecting an attribute, select the corresponding type, continuous or categorical, before adding another influencing attribute.

    You can add both continuous and categorical influencing attributes.

13. Click **Save** to create the correlation analysis.

The correlation analysis appears as a new row on the Correlation Analysis page for the asset type.

Run and View a Correlation Analysis

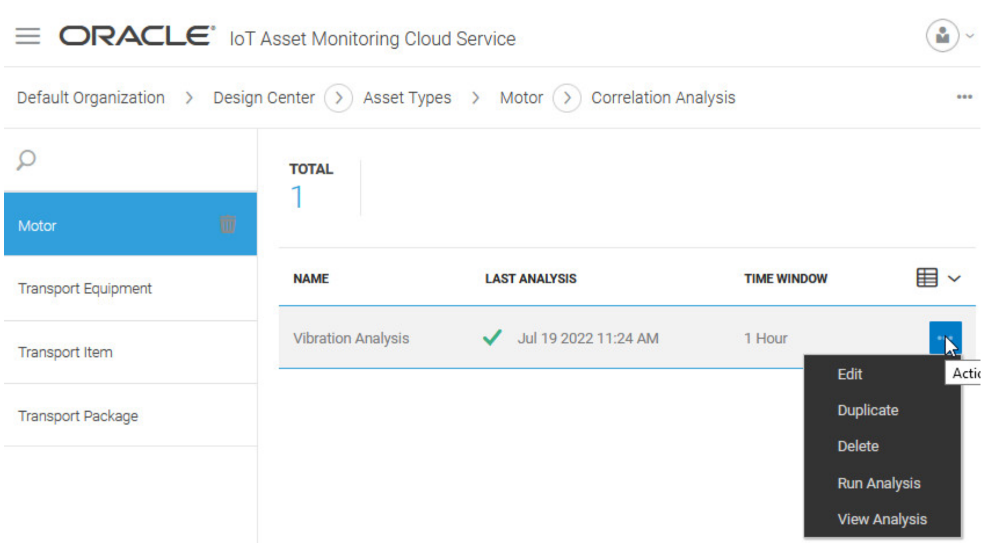
Run a correlation analysis in Design Center to study the correlation between the selected target and influencing attributes. Depending on your correlation settings, the results of the analysis can also be viewed in the Operations Center.

You can run a previously created correlation analysis from the Correlation Analysis page for the asset type.

1. Navigate to the Correlation Analysis page for your asset type.

   Click **Menu > Design Center > Asset Types >** ***Asset Type Name*** **> Correlation Analysis** to navigate to the correct page.

2. Select **Run Analysis** from the **Actions** menu for the correlation analysis row.



> **Note:**
>
> You can also **Edit** the correlation analysis settings from the **Actions** menu.

The Last Analysis column status changes to *Computation in Progress*.

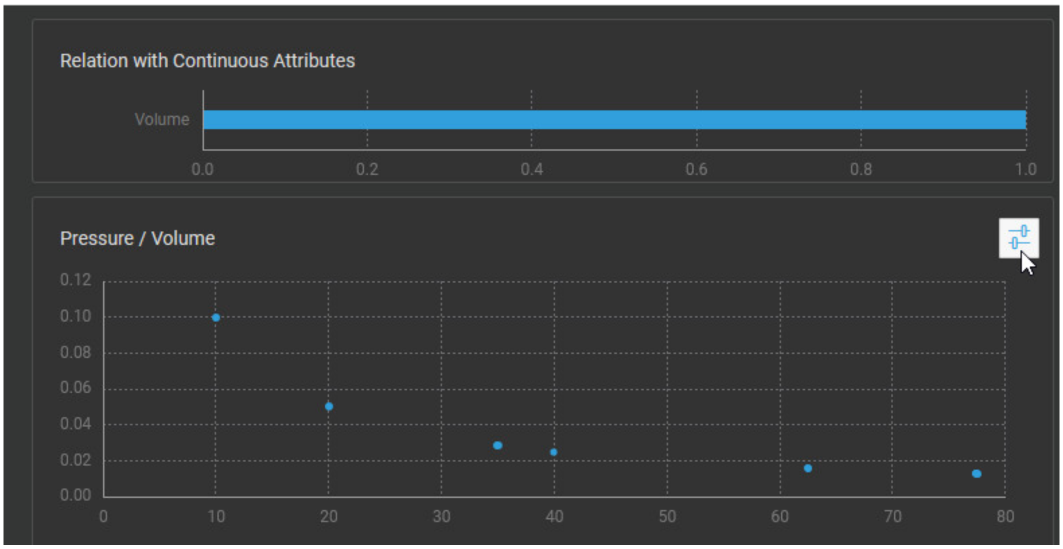
The computation takes between a few seconds to a few minutes. If you navigate away from the page and navigate back to it, you should see the last analysis status as complete along with the timestamp when the analysis completed.

3. To view a completed analysis, click the **Actions** menu against the correlation analysis row, and select **View Analysis**.

   The results of the correlation analysis between the target attribute and each influencing attribute appears. For each pair of target and influencing attribute, a correlation value between 0 (no observable correlation) and 1 is returned.

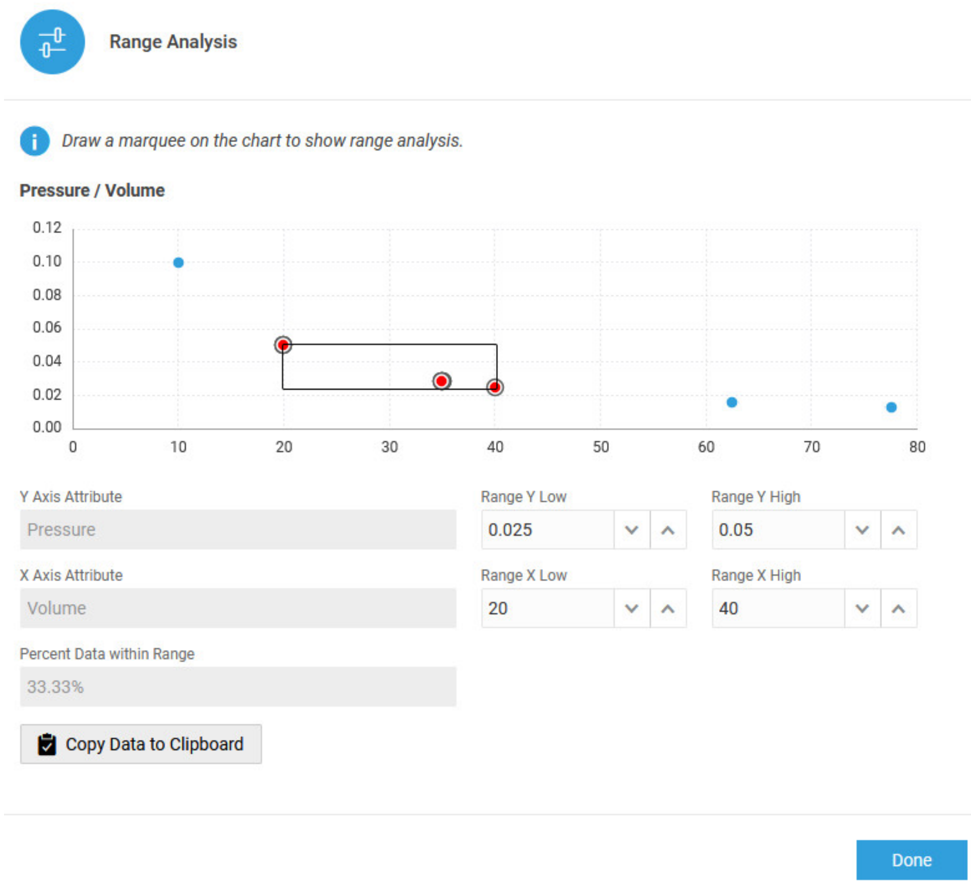
   For each pair of target and influencing attribute, a chart of correlation data is returned. You can also perform additional range analysis by manually selecting the range of values of interest.

   The following example shows a correlation analysis between the Pressure and Volume sensor attributes.

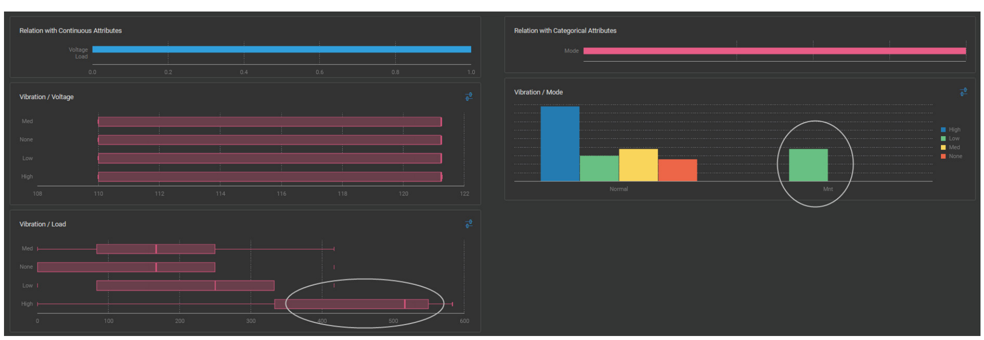


   A close correlation can be seen between the attributes, as the pressure decreases with increasing volume.

   Selecting the Range Analysis button lets you manually select the values of interest.



The following example shows the correlation analysis for a motor. The correlation of the *Vibration* attribute is studied against influencing attributes, such as *Voltage*, *Load*, and operation *Mode*.



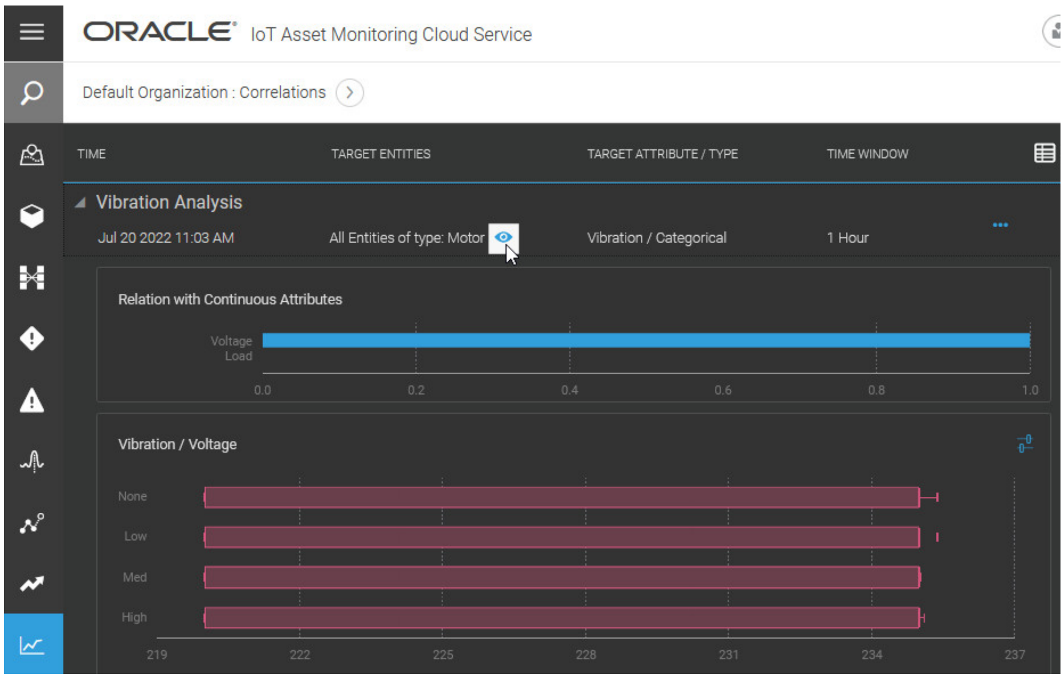
As highlighted in the correlation chart for Vibration/Load, the vibration is consistently high beyond a load value of about 350. This may help you decide on optimum operating modes.

The correlation of vibration against mode of operation shows that the vibration remains low under the maintenance mode. You may want to use operation mode as a partition key when setting up state aware anomalies.

4. To view the correlations in Operations Center, click **Correlations** in the Operations Center menu bar.

To navigate to Operations Center, click **Menu > Operations Center**.

> **Note:**
>
> The **Correlations** button appears in the Operations Center menu bar if you have chosen to publish the results of the correlation analysis to the Operations Center in the correlation analysis settings.



Click the **View** icon under Target Entities to select and view the correlation analysis for a specific asset.

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 sensor or metric (KPI) values. For example, automatic anomalies can help detect an HVAC device that is overheating.

  Sometimes, a set of correlated sensor signals can help identify issues with your asset. For example, a drop in pressure readings coupled with an increase in vibration may indicate cavitation issues in a pump. You can use multivariate automatic anomalies to monitor multiple sensor attributes and metrics simultaneously. Use the Operations Center to view the reported anomalies on the timeline, together with the key signals from your chosen sensor and metric attributes.

Asset sensor values can depend on the asset state. For example, an idling motor has different vibration measurements from a motor running with load. Asset sensor values may also vary with the current process, product or environmental attributes. For example, the baseline fuel consumption may depend on the ambient temperature. The injection pressure of a molding machine may depend on whether it is currently molding steel or aluminum bottles.

If the current asset state determines the threshold sensor values for your anomalies, you can use partition key attributes to partition your anomalies. For example, you can create partitions to look at vibration anomalies when the motor is working, and ignore states where the motor is idling, or under maintenance.

- **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.

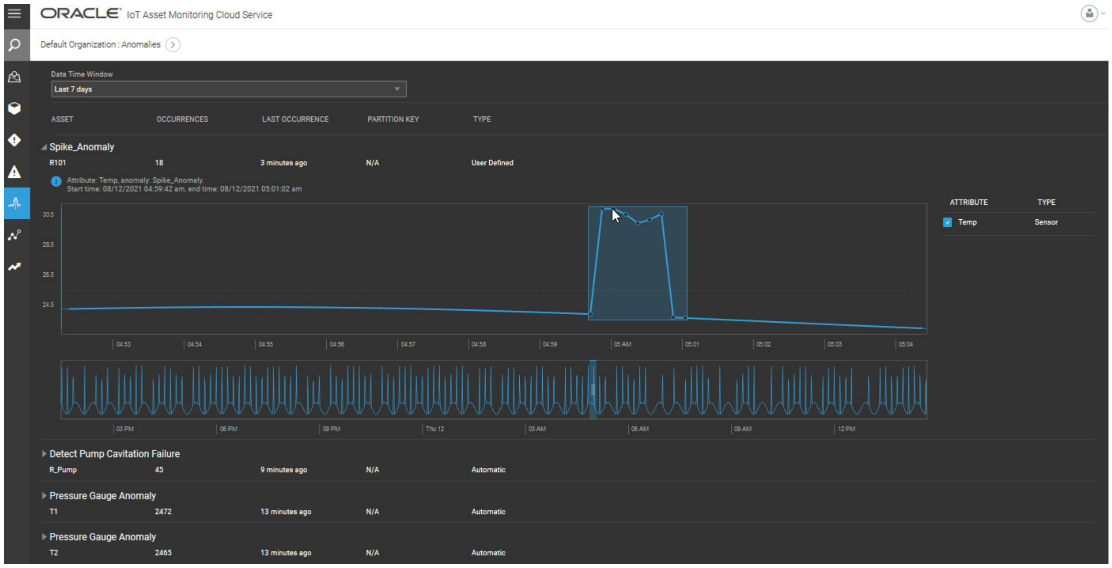
  For acceptable data, you specify a time window containing acceptable patterns of sensor or metric data. The time window is a period of typical operations during which your assets, and associated sensors, behaved normally. The system uses the data pattern that you select to train itself. During day-to-day 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 Classic Cloud Service table, you can overlay these events on the sensor data timeline to define anomalies that occur around the breakdown events.

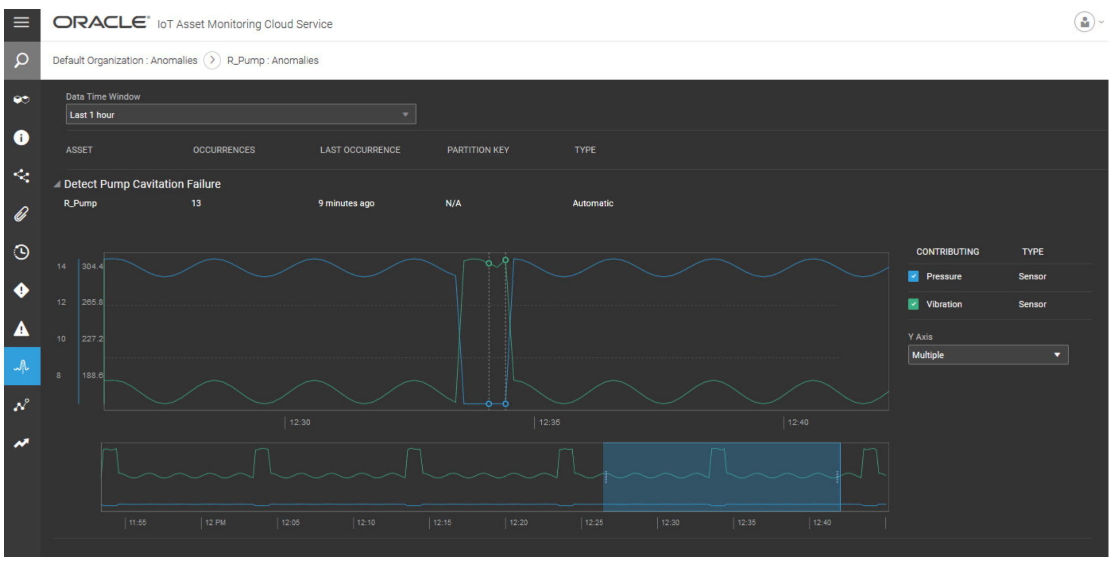
All detected anomalies appear on the Anomalies  page accessible from the Operations Center or Asset Details page of individual assets. The anomalies displayed in the Operations Center depend on your current context (organization, group, subgroup, or asset).

The following image shows some anomalies for the organization context in the Operations Center view. Anomalies for different assets are shown on the same page. You can change your context using the breadcrumbs in the Operations Center. You can filter your view for a group, subgroup, or individual asset.

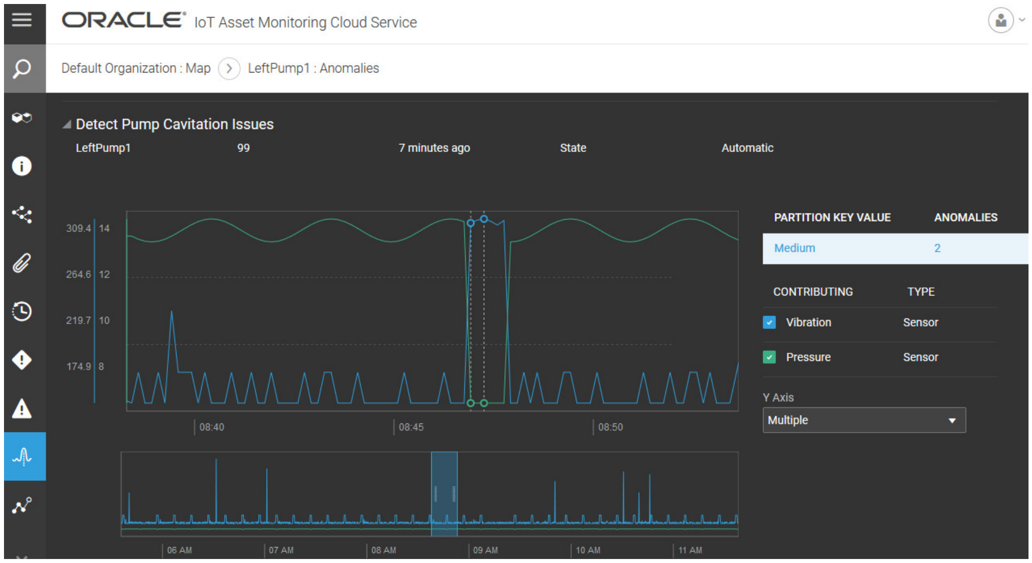
Select a **Data Time Window** to look for anomalies that occurred during the selected period. Expand the anomalies section reported for an asset, and select the desired region in the lower chart to see a magnified version in the upper chart. You can move the mouse over an anomaly to view more details, such as the *Start Time* and *End Time* for the anomaly.



The following Operations Center view shows multivariate anomalies for a pump device. Notice that you can select the sensor signals that you wish to view in the chart. If the sensor values are disparate, you can choose multiple y-axes, so that you can see each signal using the correct scale.



If you are using partition key values corresponding to asset states, then you can select the relevant partition key as well. The following view shows anomalies reported when the running state of the pump is *Medium*.



> **Note:**
>
> If you are using simulated sensor data to test your anomalies, refer to the following sections for more information on the data characteristics of simulated data:
>
> - Define a Simulation for a Sensor Attribute
> - Tips and Considerations for Simulated Data and Analytics Artifacts

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 **Anomaly Detection**.
5. Click the **Create Anomaly** (+) icon.

   The Anomaly Detection Editor appears for the selected asset type.

   The anomaly detection that you define will apply to all assets of the chosen asset type.
6. In the **Details** section, enter a name for the anomaly in the **Name** field.
7. (Optional) Specify an optional **Description** text for the anomaly.
8. (Optional) Select a value under **Keep Metric Data For**.

If you have unique storage requirements for historical data related to this anomaly, you can select an option that is different from the global settings defined under **Storage Management** on the application Settings page.

For example, if you are calculating anomalies across a large number of assets, and the anomaly data is not required beyond a month, then you can select **30 Days** under **Keep Metric Data For** to optimize storage.

9. Under **Detection**, select **Automatic Anomaly** as the **Detection Method**.

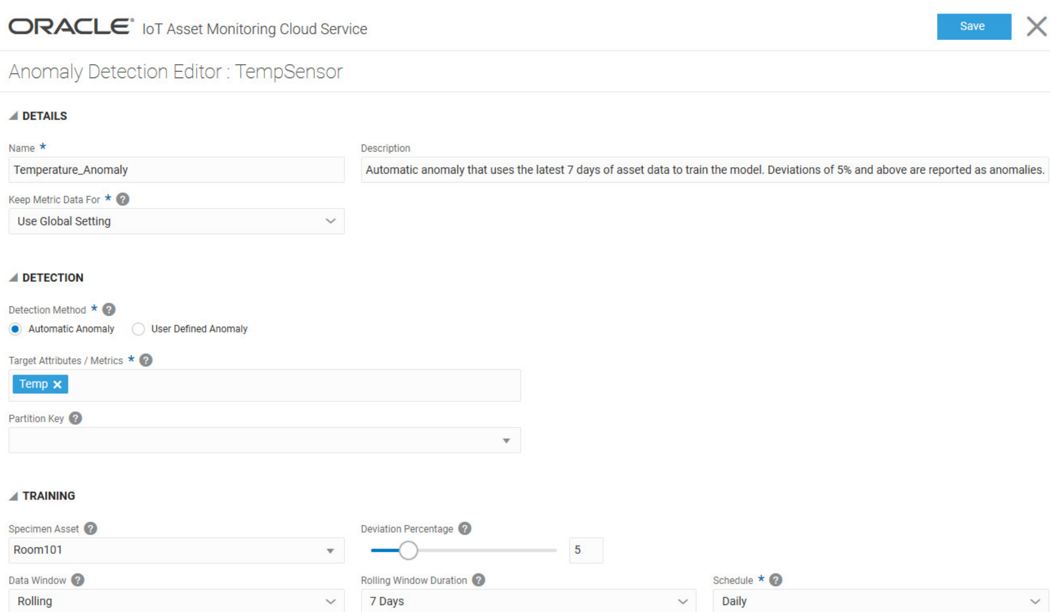
   Use an automatic anomaly to automatically look for deviations in sensor or metric (KPI) values. For example, automatic anomalies can help detect an HVAC device that is overheating intermittently.

10. Select one or more available **Target Attributes/Metrics** to monitor.

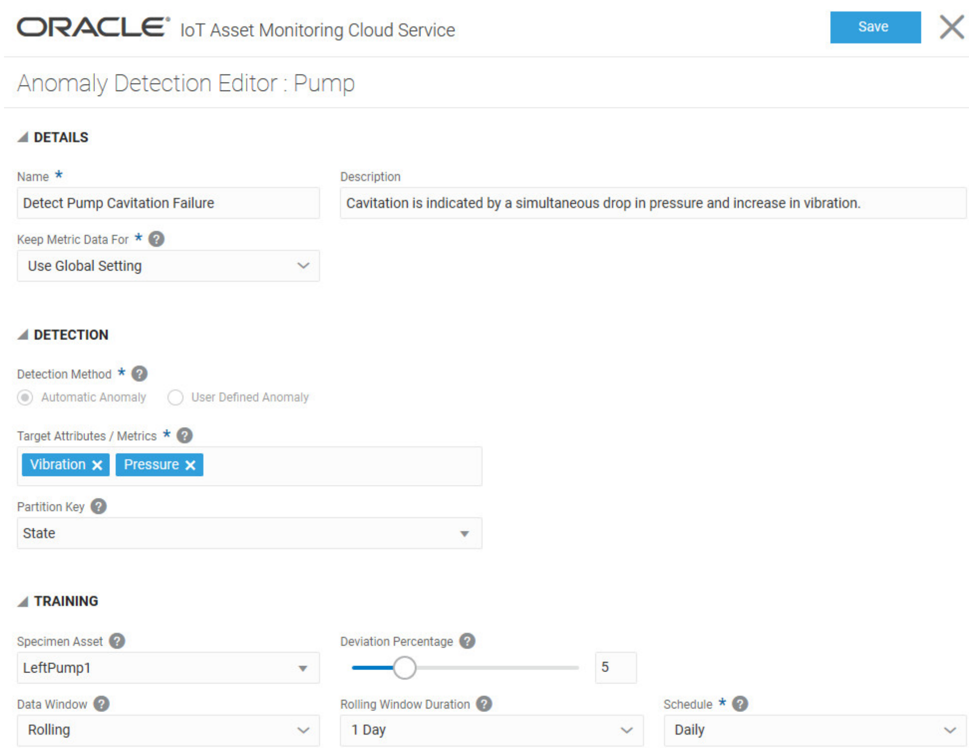
    The list of attributes includes sensor attributes and query-type (computed) metrics.

    Select one sensor attribute or metric if you need to monitor anomalies in a single attribute or metric. Use multiple attributes only if you need to monitor anomalies caused by a combination of correlated attributes. Multivariate anomalies look for anomalies in correlated signals, and are more resource intensive.

    The following example looks for anomalies in the temperature reading:



    The following multivariate example uses the Vibration and Pressure sensor attributes:



11. (Optional) If you have defined sensor attributes that can be used as partition keys to determine the asset state, then you can choose the **Partition Key**.

    For example, you may have defined a sensor attribute called *State* to determine whether the asset is currently running, idling, or under maintenance.

    > **Note:**
    >
    > The asset type must have at least one sensor attribute that can be used as the partition key. See Create a New Asset Type for more information on sensor attributes.

12. Under **Training**, 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.

13. Under Training, select a **Deviation Percentage**.

    Deviation percentage is the acceptable noise in your target attribute data. Use the slider to set a value, or enter a value manually.

    Automatic anomalies choose the best underlying algorithm depending on several factors, such as whether the anomaly uses one or more target attributes, whether the data distribution is Gaussian or non-Gaussian, and the number of records in the data set.

    If you have used a single target attribute or metric, and your data distribution is Gaussian or the number of data points is less than 5000, then the deviation percentage is the percentage deviation from normal distribution. Here, normal distribution implies mean of target attribute value plus/minus twice the standard deviation. Any percentage deviation beyond the deviation percentage results in anomalies.

You can fine-tune your anomaly detection by looking at the reported anomalies and making any required adjustments to the **Deviation Percentage**. For example, if you are getting false positives, you may want to increase the deviation percentage, but if not all anomalies get flagged, then you may need to lower the deviation percentage value.

If your data distribution is non-Gaussian, or if the number of data points is large, or if you are using multiple target attributes or metrics, then an appropriate threshold-based algorithm is chosen to detect automatic anomalies. For such cases, deviation percentage is the threshold deviation percentage. Note that you may need to tweak your deviation percentage value in case you are getting false positives, or in case not enough anomalies are being reported.

> **Note:**
>
> Do not use random data when testing your anomalies. If using simulated test data, do not use random patterns. Note that range-binding simulated data is not enough to make it non-random. Threshold-based algorithms cannot work with random data.

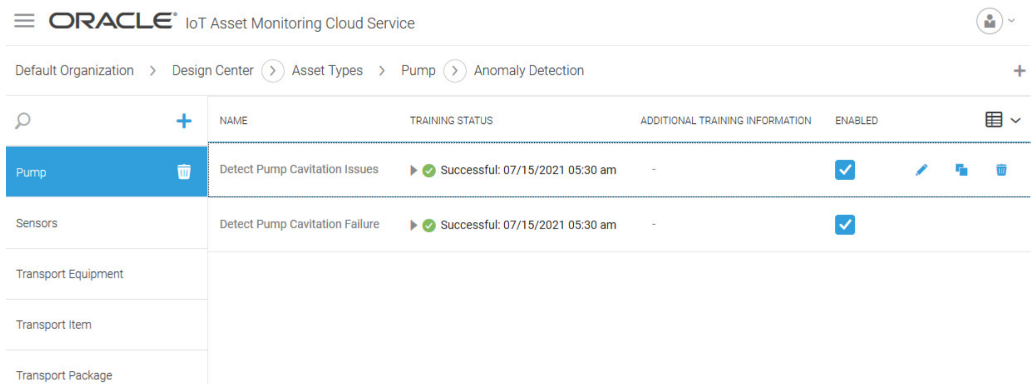
14. Under Training, select the **Data Window**.

    The **Data Window** identifies the data set that is used to train the system for anomaly detection.

    - **Static**: Uses a static data window to train your anomaly model. If you have golden data from a period when your asset worked normally, you can use the same to specify a static window. Select the **Window Start Time** and **Window End Time** for your static window period.
      The static data window provides data for a one-time training of your anomaly model. If your definition of normal data changes in the future, you should edit the **Data Window** for the automatic anomaly, so that the model can be re-trained.
    - **Rolling**: A rolling data window uses data from a rolling time window to pick the most recent data for training. For example, you can choose to train your anomaly model with a rolling data window of the last 7 days, and choose to perform the anomaly training daily.
      When you use a rolling window, the training model is re-created periodically, as determined by the schedule frequency that you choose.
      – **Rolling Window Duration**: The duration of the rolling window going back from the model training time. For example, if you select **7 Days**, then the last 7 days of specimen asset data is used to train the anomaly model.
      – **Schedule**: The frequency of the anomaly model training. For example, if you choose **Daily**, then the training happens every day at 00:00 hours (midnight), UTC time by default.

15. Click **Save**.

The anomaly is added to the Anomalies page. The **Training Status** column shows the latest training status for the anomaly model. Once training is complete, the application starts detecting and reporting anomalies.



The application reports completed model trainings along with their timestamps. If training fails, the application includes pertinent information related to the failure. For example, the chosen training data set's statistical properties might not be suitable. The Feedback Center is also used to notify the Asset Manager about failures.

You can enable or disable an anomaly from within the Anomaly Editor.

Create a User-Defined Anomaly

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

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 **Anomaly Detection**.
5. Click the **Create Anomaly** () icon.

   The Anomaly Detection Editor appears for the selected asset type.

   The anomaly detection that you define will apply to all assets of the chosen asset type.
6. In the **Details** section, enter a name for the anomaly in the **Name** field.
7. (Optional) Specify an optional **Description** text for the anomaly.
8. (Optional) Select a value under **Keep Metric Data For**.

   If you have unique storage requirements for historical data related to this anomaly, you can select an option that is different from the global settings defined under **Storage Management** on the application Settings page.

   For example, if you are calculating anomalies across a large number of assets, and the anomaly data is not required beyond a month, then you can select **30 Days** under **Keep Metric Data For** to optimize storage.
9. Under **Detection**, select **User Defined Anomaly** as the **Detection Method**.

   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.

10. Select an available **Target Attribute / Metric** 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.

11. (Optional) If you have defined one or more failure modes for your asset type, select **Include Failure Mode Details** to associate a failure mode with the anomaly.

    a. Select a pre-existing **Failure Mode** that corresponds to the anomaly.

    b. Select one or more pre-existing **Failure Causes** that apply to the anomaly.

    See Add Failure Diagnostics Information to Asset Incidents and Anomalies for more information on using failure modes.

12. Under **Training**, 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.

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

    > **Note:**
    >
    > Do not use random data when testing your anomalies. If using simulated test data, do not use random patterns. Note that range-binding simulated data is not enough to make it non-random. Threshold-based algorithms cannot work with random data.

    - Choose **Anomalous Data** to select an anomalous data pattern from existing sensor or metric data.

      Make sure that the pattern is clearly identified and selected. Anomaly detection will look for anomalous pattern resemblance, and not necessarily similar values. If anomalous data patterns are not correctly identified, your selected pattern may have too few data points.

      a. (Optional) Change the **Data End Time** for the chart, if required. The current date and time are automatically populated.

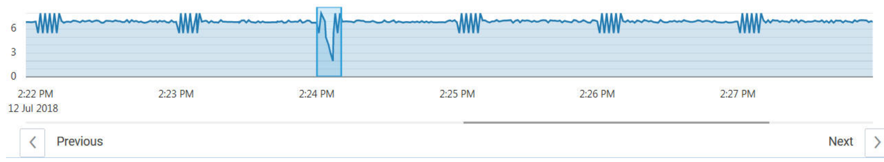
      b. (Optional) If you wish to show contextual annotations using event data stored in a contextual data connection, then select **Show Contextual Annotation.**

         For example, if you have breakdown events and their timestamps stored in a Database Classic 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.

- Choose **Acceptable Data** to select normal behavior data or non-anomalous data from existing sensor or metric data.

  a. Select a **Deviation Percentage.**

  An appropriate threshold-based algorithm is chosen to detect user-defined anomalies. The d**Deviation Percentage.** is the threshold deviation percentage. Note that you may need to tweak your deviation percentage value in case you are getting false positives, or in case not enough anomalies are being reported.

  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.

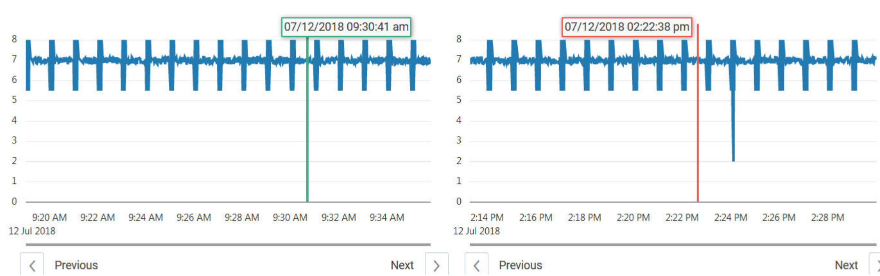
  The data plot for the selected asset attribute appears.

  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.

- 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.

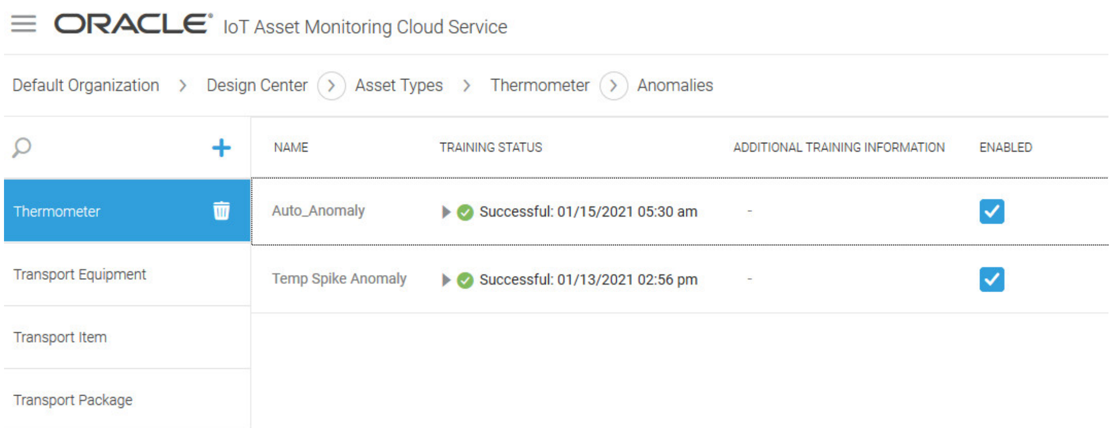
d. Click **Generate Chart.**

   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.

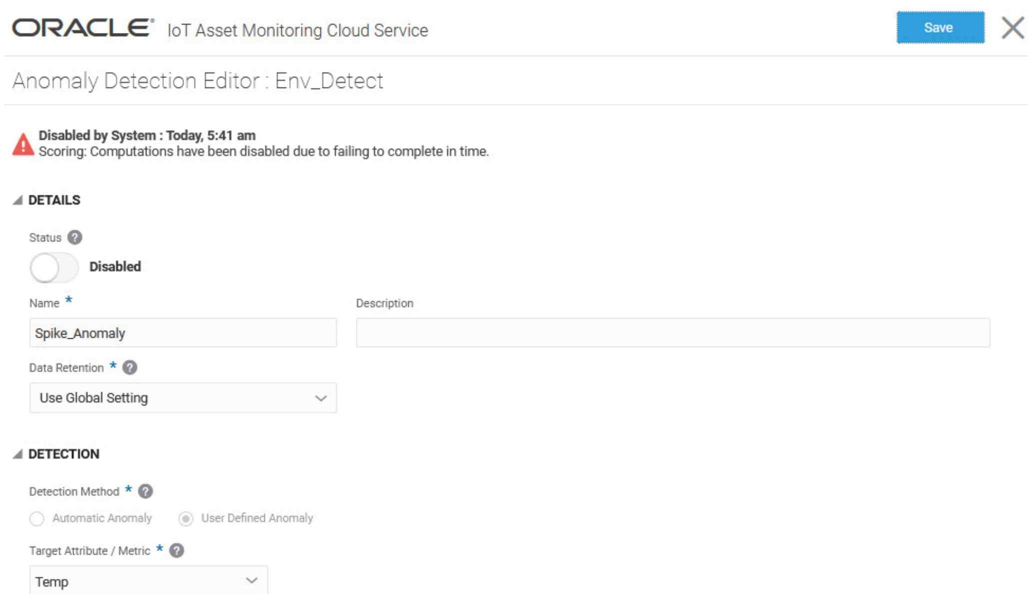
f. Click **Save** to save the anomaly.

The anomaly is added to the Anomalies page. The **Training Status** column shows the latest training status for the anomaly model. Once training is complete, the application starts detecting and reporting anomalies.



The application reports completed model trainings along with their timestamps. If training fails, the application includes pertinent information related to the failure. For example, the chosen training data set's statistical properties might not be suitable. The Feedback Center is also used to notify the Asset Manager about failures.

You can enable or disable an anomaly from within the Anomaly Editor. If an anomaly has been disabled by the system, a relevant message appears inside the Editor. The message also appears on the Anomalies page in Operations Center.



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 Classic 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 Classic Cloud Service or Autonomous Transaction Processing 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** ( ) 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** ( ) 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 OCI Anomaly Detection on Externally Stored IoT Data

If you are using the OCI Anomaly Detection AI Service, you can configure anomaly detection for externally stored IoT data.

OCI Anomaly Detection uses an Oracle-patented multivariate time-series anomaly detection algorithm originally developed by Oracle Labs. OCI Anomaly Detection helps avoid business disruptions through the early detection of multivariate anomalies.

To use OCI Anomaly Detection with IoT data, you must be using Oracle Autonomous Database. You can convert the sensor data stored in Oracle Autonomous Database into the format expected by the OCI Anomaly Detection service, and use this data to create and train the anomaly model.

See the following topics for more information on using Oracle Autonomous Database to externally store your IoT data:

- Use Oracle Autonomous Database to Store Historical IoT Data
- Add an Oracle Autonomous Database Integration
- Enable and Configure the Oracle Autonomous Database Integration

OCI Anomaly Detection expects training data in the following format:

```
TimeStamp, [SensorColumn1], [SensorColumn2]…[SensorColumnN]
```

The following image displays a sample data segment in the desired format:

Timestamp	Temperature_1	Temperature_2	Temperature_3	Temperature_4	Temperature_5	Pressure_1	Pressure_2	Pressure_3	Pressure_4	Pressure_5
2019-01-01T00:00:04Z	0.4328	-0.0723	-0.0057	-0.296	-2.8523	-1.9328	-1.2445	-2.9037	-0.4916	0.0224
2019-01-01T00:01:01Z	0.0671	0.2425	0.201	-0.9488	2.7606	1.4679	-2.2535	-0.9427	2.2233	0.7536
2019-01-01T00:02:06Z	0.106	0.0615	0.1948	2.3834	-0.2861	-0.1715	2.933	-1.5013	-1.6273	-0.154
2019-01-01T00:03:01Z	0.5897	0.098	0.3385	-1.8651	1.3817	-1.4747	0.1926	0.4818	-0.8801	0.4534
2019-01-01T00:04:04Z	-0.017	0.3838	0.511	0.4377	-1.9249	-0.857	0.9831	-0.4732	1.029	1.2375
2019-01-01T00:05:07Z	0.2797	0.291	0.393	1.4511	2.3289	1.6987	-2.5207	0.6959	-2.0131	0.0157
2019-01-01T00:06:08Z	-0.4306	0.5428	0.6012	0.0444	-1.2402	-0.3386	3.2032	0.6636	-0.1432	-0.3818

Extract Distinct Entity Attribute Pairs from External IoT Data

To begin preparing the IoT data stored in Oracle Autonomous Database for OCI Anomaly Detection, we run a query to extract distinct entity-attribute pairs. These entity-attribute pairs will become our column headings in the training data.

Use a database client tool to make a connection with your Oracle Autonomous Database. We use the following query to filter out distinct entity-attribute pairs for the specified entity type and organization.

```
-- Obtains a list of entity/attribute instances which will become 
individual
--  column names in the MSET2 data view.
-- Note:
--  Replace <ENTITY_TYPE_ID> with the actual entity type id value in 
each WHERE clause to filter by entity type id. Remove if not needed.
--  Replace <ORG_ID> with the actual organization id value in each 
WHERE clause to filter by organization id. Remove if not needed.
--  Replace <ENTITIES_TABLE> with name of Data Externalization 
ENTITIES table name.
--  Replace <ATTRIBUTE_VALUES_TABLE> with name of Data Externalization 
ATTRIBUTE_VALUES table name.
--  Replace <ENTITY_TYPE_ATTR_TABLE> with name of Data Externalization 
ENTITY_TYPE_ATTR table name.

SELECT
```

```
    "ENTITY_ID",
    "ENTITY_NAME",
    "ATTRIBUTE_ID",
    "ATTRIBUTE_NAME"
FROM
    (
        SELECT DISTINCT
            "ENTITY_ID",
            "ATTRIBUTE_ID",
            "ENTITY_NAME"
        FROM
            (
                SELECT
                    "ENTITY_ID",
                    "ATTRIBUTE_ID"
                FROM
                    "<ATTRIBUTE_VALUES_TABLE>" inputdataset_0
                WHERE
                    inputdataset_0.ENTITY_TYPE_ID = '<ENTITY_TYPE_ID>' AND
inputdataset_0.ORG_ID = '<ORG_ID>'
            ) selectcolumns_0
            INNER JOIN (
                SELECT
                    "ID",
                    "NAME" entity_name
                FROM
                    "<ENTITIES_TABLE>" inputdataset_1
                WHERE
                    inputdataset_1.ENTITY_TYPE_ID = '<ENTITY_TYPE_ID>' AND
inputdataset_1.ORG_ID = '<ORG_ID>'
            ) selectcolumns_1 ON selectcolumns_0."ENTITY_ID" =
selectcolumns_1."ID"
    ) selectcolumns_1
    INNER JOIN (
        SELECT
            "ID",
            "NAME" "ATTRIBUTE_NAME"
        FROM
            "<ENTITY_TYPE_ATTR_TABLE>" inputdataset_2
        WHERE
            inputdataset_2.ENTITY_TYPE_ID = '<ENTITY_TYPE_ID>'
    ) selectcolumns_2 ON selectcolumns_1."ATTRIBUTE_ID" =
selectcolumns_2."ID"
```

Here is an example query for the preceding script:

```
-- Obtains a list of entity/attribute instances which will become individual
--  column names in the MSET2 data view.
-- Note:
--  Replace <ENTITY_TYPE_ID> with the actual entity type id value in each
WHERE clause to filter by entity type id. Remove if not needed.
--  Replace <ORG_ID> with the actual organization id value in each WHERE
clause to filter by organization id. Remove if not needed.
--  Replace <ENTITIES_TABLE> with name of Data Externalization ENTITIES
```

```
table name.
--  Replace <ATTRIBUTE_VALUES_TABLE> with name of Data Externalization
ATTRIBUTE_VALUES table name.
--  Replace <ENTITY_TYPE_ATTR_TABLE> with name of Data Externalization
ENTITY_TYPE_ATTR table name.

SELECT
    "ENTITY_ID",
    "ENTITY_NAME",
    "ATTRIBUTE_ID",
    "ATTRIBUTE_NAME"
FROM
    (
        SELECT DISTINCT
            "ENTITY_ID",
            "ATTRIBUTE_ID",
            "ENTITY_NAME"
        FROM
            (
                SELECT
                    "ENTITY_ID",
                    "ATTRIBUTE_ID"
                FROM
                    "AI_ATTRIBUTE_VALUES" inputdataset_0
                WHERE
                    inputdataset_0.ENTITY_TYPE_ID = '3JB55AY42T90' AND
inputdataset_0.ORG_ID = 'ORA_DEFAULT_ORG'
            ) selectcolumns_0
            INNER JOIN (
                SELECT
                    "ID",
                    "NAME" entity_name
                FROM
                    "AI_ENTITIES" inputdataset_1
                WHERE
                    inputdataset_1.ENTITY_TYPE_ID = '3JB55AY42T90' AND
inputdataset_1.ORG_ID = 'ORA_DEFAULT_ORG'
            ) selectcolumns_1 ON selectcolumns_0."ENTITY_ID" =
selectcolumns_1."ID"
    ) selectcolumns_1
    INNER JOIN (
        SELECT
            "ID",
            "NAME" "ATTRIBUTE_NAME"
        FROM
            "AI_ENTITY_TYPE_ATTR" inputdataset_2
        WHERE
            inputdataset_2.ENTITY_TYPE_ID = '3JB55AY42T90'
    ) selectcolumns_2 ON selectcolumns_1."ATTRIBUTE_ID" =
selectcolumns_2."ID"
```

Here's some sample data returned by the query:

	ENTITY_ID	ENTITY_NAME	ATTRIBUTE_ID	ATTRIBUTE_NAME
1	3JB5943W2T9G	Temp_n_Humidity_Detector1	3JB55B6W2T90	Humidity
2	3JB5975G2T9G	Temp_n_Humidity_Detector2	3JB55B4W2T90	Temp
3	3JB5943W2T9G	Temp_n_Humidity_Detector1	3JB55B982T90	Pres
4	3JB5975G2T9G	Temp_n_Humidity_Detector2	3JB55B6W2T90	Humidity
5	3JB5975G2T9G	Temp_n_Humidity_Detector2	3JB55B982T90	Pres
6	3JB5943W2T9G	Temp_n_Humidity_Detector1	3JB55B4W2T90	Temp

You can use the data returned by the query to define a naming convention for the column names in your training data. For example, you can choose between the following combinations:

- *ENTITY_ID_ATTRIBUTE_ID*, such as `3jB5943W2T9G_3jB55B6W2T90`.
- *ENTITY_ID_ATTRIBUTE_NAME*, such as `3jB5943W2T9G_Humidity`.
- *ENTITY_NAME_ATTRIBUTE_ID*, such as `Detector1_3jB55B6W2T90`.
- *ENTITY_NAME_ATTRIBUTE_NAME*, such as `Detector1_Humidity`.

When defining columns, choose column names that are unique and contain valid characters. Use a combination of `ENTITY_ID/ENTITY_NAME` and `ATTRIBUTE_ID/ATTRIBUTE_NAME`, making sure to remove any invalid characters. The column names should follow the Oracle rules for Database Object Names and Qualifiers.

Create a Database View Containing Formatted Data

Build the SQL command that creates a database view containing data in the format expected by the OCI Anomaly Detection service

Note that the number of `MAX` statements in the SQL is dynamic, as it depends on the number of Entity-Attribute pairs that you have.

```
-- Creates a database VIEW of MSET2 data out of Data Externalization data
--
-- Note:
--  Replace <ENTITY_TYPE_ID> with the actual entity type id value in each
WHERE clause to filter by entity type id. Remove if not needed.
--  Replace <ORG_ID> with the actual organization id value in each WHERE
clause to filter by organization id. Remove if not needed. --  Replace
<ENTITY_ID> with the actual entity id value.
--  Replace <ATTRIBUTE_ID> with the actual attribute id value
--  Replace <VIEW_NAME> with the actual name of the database VIEW
--  Replace <TIMEZONE_CODE> with the actual code for database timezone --
--  Replace <ENTITIES_TABLE> with name of Data Externalization ENTITIES
table name.
--  Replace <ATTRIBUTE_VALUES_TABLE> with name of Data Externalization
ATTRIBUTE_VALUES table name.
--  Replace <ENTITY_TYPE_ATTR_TABLE> with name of Data Externalization
ENTITY_TYPE_ATTR table name.


CREATE VIEW <VIEW_NAME> AS
SELECT
    TO_CHAR(
        EVENT_TIME AT TIME ZONE '<TIMEZONE_CODE>',
```

```
        'YYYY-MM-DD"T"HH24:MI:SS"Z"'
     ) as TIMESTAMP,
 -- Create a MAX statement for each column-name as described in Step 4.
 ---- Begin MAX statement
    MAX(
        CASE
            WHEN("ATTRIBUTE_ID" = '<ATTRIBUTE_ID>'
                 AND "ENTITY_ID" = '<ENTITY_ID>') THEN
                "NUMERIC_VALUE"
        END
    ) "<ENTITY_NAME>_<ATTRIBUTE_NAME>",
 ---- End MAX statement.  Note: Comma is not needed in final MAX
statement
FROM
    (
SELECT
    "ENTITY_ID",
    "ENTITY_NAME",
    "NUMERIC_VALUE",
    "EVENT_TIME",
    "ATTRIBUTE_ID",
    "ATTRIBUTE_NAME"
FROM
         (
        SELECT
            "ENTITY_ID",
            "ENTITY_NAME",
            "NUMERIC_VALUE",
            "EVENT_TIME",
            "ATTRIBUTE_ID"
        FROM
                 (
                SELECT
                    "ENTITY_ID",
                    "NUMERIC_VALUE",
                    "EVENT_TIME",
                    "ATTRIBUTE_ID"
                FROM
                    "<ATTRIBUTE_VALUES_TABLE>" inputdataset_0
                WHERE
                    inputdataset_0.ENTITY_TYPE_ID = '<ENTITY_TYPE_ID>'
AND inputdataset_0.ORG_ID = '<ORG_ID>'
                        AND inputdataset_0.EVENT_TIME >=
to_utc_timestamp_tz('YYYY-MM-DD"T"HH24:MI:SS"Z"')
                        AND inputdataset_0.EVENT_TIME <=
to_utc_timestamp_tz('YYYY-MM-DD"T"HH24:MI:SS"Z"')
            ) selectcolumns_0
            INNER JOIN (
                SELECT
                    "ID",
                    "NAME" entity_name
                FROM
                    "<ENTITIES_TABLE>" inputdataset_1
                WHERE
                    inputdataset_1.ENTITY_TYPE_ID = '<ENTITY_TYPE_ID>'
```

```
AND inputdataset_1.ORG_ID = '<ORG_ID>'
            ) selectcolumns_1 ON selectcolumns_0."ENTITY_ID" =
selectcolumns_1."ID"
    ) selectcolumns_2
    INNER JOIN (
        SELECT
            "NAME" attribute_name,
            "ID"
        FROM
            "<ENTITY_TYPE_ATTR_TABLE>" inputdataset_2
        WHERE
            inputdataset_2.ENTITY_TYPE_ID = '<ENTITY_TYPE_ID>'
    ) selectcolumns_3 ON selectcolumns_2."ATTRIBUTE_ID" =
selectcolumns_3."ID"    )
GROUP BY
    "EVENT_TIME"
```

The following example helps better understand the script above.

```
-- Creates a database VIEW of MSET2 data out of Data Externalization data
--
-- Note:
--  Replace <ENTITY_TYPE_ID> with the actual entity type id value in each
WHERE clause to filter by entity type id. Remove if not needed.
--  Replace <ORG_ID> with the actual organization id value in each WHERE
clause to filter by organization id. Remove if not needed. --  Replace
<ENTITY_ID> with the actual entity id value.
--  Replace <ATTRIBUTE_ID> with the actual attribute id value
--  Replace <VIEW_NAME> with the actual name of the database VIEW
--  Replace <TIMEZONE_CODE> with the actual code for database timezone --
--  Replace <ENTITIES_TABLE> with name of Data Externalization ENTITIES
table name.
--  Replace <ATTRIBUTE_VALUES_TABLE> with name of Data Externalization
ATTRIBUTE_VALUES table name.
--  Replace <ENTITY_TYPE_ATTR_TABLE> with name of Data Externalization
ENTITY_TYPE_ATTR table name.


CREATE VIEW DATA_VIEW AS
SELECT
    TO_CHAR(
        EVENT_TIME AT TIME ZONE 'UTC',
        'YYYY-MM-DD"T"HH24:MI:SS"Z"'
     ) as TIMESTAMP,
 -- Create a MAX statement for each column-name as described in Step 4.
 ---- Begin MAX statement
    MAX(
        CASE
            WHEN("ATTRIBUTE_ID" = '3JB55B6W2T90'
                 AND "ENTITY_ID" = '3JB5943W2T9G') THEN
                "NUMERIC_VALUE"
        END
    ) "Detector1_Humidity",
 ---- End MAX statement.  Note: Comma is not needed in final MAX statement
```

```
---- Begin MAX statement
    MAX(
        CASE
            WHEN("ATTRIBUTE_ID" = '3JB55B982T90'
                 AND "ENTITY_ID" = '3JB5943W2T9G') THEN
                "NUMERIC_VALUE"
        END
    ) "Detector1_Pressure",
 ---- End MAX statement.  Note: Comma is not needed in final MAX
statement
---- Begin MAX statement
    MAX(
        CASE
            WHEN("ATTRIBUTE_ID" = '3JB55B4W2T90'
                 AND "ENTITY_ID" = '3JB5943W2T9G') THEN
                "NUMERIC_VALUE"
        END
    ) "Detector1_Temperature"
 ---- End MAX statement.  Note: Comma is not needed in final MAX
statement
FROM
    (
SELECT
    "ENTITY_ID",
    "ENTITY_NAME",
    "NUMERIC_VALUE",
    "EVENT_TIME",
    "ATTRIBUTE_ID",
    "ATTRIBUTE_NAME"
FROM
         (
        SELECT
            "ENTITY_ID",
            "ENTITY_NAME",
            "NUMERIC_VALUE",
            "EVENT_TIME",
            "ATTRIBUTE_ID"
        FROM
                 (
                SELECT
                    "ENTITY_ID",
                    "NUMERIC_VALUE",
                    "EVENT_TIME",
                    "ATTRIBUTE_ID"
                FROM
                    "AI_ATTRIBUTE_VALUES" inputdataset_0
                WHERE
                    inputdataset_0.ENTITY_TYPE_ID = '3JB55AY42T90' AND
inputdataset_0.ORG_ID = 'ORA_DEFAULT_ORG'
                        AND inputdataset_0.EVENT_TIME >=
to_utc_timestamp_tz('2022-04-21T01:00:00Z')
                        AND inputdataset_0.EVENT_TIME <=
to_utc_timestamp_tz('2022-04-21T10:00:00Z')
            ) selectcolumns_0
            INNER JOIN (
```

```
                    SELECT
                        "ID",
                        "NAME" entity_name
                    FROM
                        "AI_ENTITIES" inputdataset_1
                    WHERE
                        inputdataset_1.ENTITY_TYPE_ID = '3JB55AY42T90' AND
inputdataset_1.ORG_ID = 'ORA_DEFAULT_ORG'
            ) selectcolumns_1 ON selectcolumns_0."ENTITY_ID" =
selectcolumns_1."ID"
    ) selectcolumns_2
    INNER JOIN (
        SELECT
            "NAME" attribute_name,
            "ID"
        FROM
            "AI_ENTITY_TYPE_ATTR" inputdataset_2
        WHERE
            inputdataset_2.ENTITY_TYPE_ID = '3JB55AY42T90'
    ) selectcolumns_3 ON selectcolumns_2."ATTRIBUTE_ID" =
selectcolumns_3."ID"    )
GROUP BY
    "EVENT_TIME"
```

The following image displays sample data from the view that we created:

TIMESTAMP	Detector1_Humidity	Detector1_Pressure	Detector1_Temperature
2022-04-21T03:39:05Z	50	80.00000012337006	24.999999987662996
2022-04-21T03:39:15Z	50	81.34053146715738	24.865946853284264
2022-04-21T03:39:25Z	50	85.00136041120263	24.499863958879736
2022-04-21T03:40:05Z	50	99.99999987662994	23.000000012337004
2022-04-21T03:31:55Z	50	98.66130104544729	23.13386989545527
2022-04-21T03:32:05Z	50	99.99999731327448	23.00000026867255

Create Vault and Secrets to Store Your Database Credentials and Connection Details

Use the OCI vault to store your Oracle Autonomous Database credentials and connection details. We use these secrets to configure the data asset for OCI anomaly detection.

1. Create your OCI Vault.

   After logging in to Oracle Cloud, navigate to **Menu > Identity & Security > Vault**.

2. Create a master encryption key in the vault.

   The master encryption key is used to encrypt the secrets that you store in the vault.

3. Create the secrets to store your database user credentials and wallet password.
4. Create the secrets for the database wallet files.

   You can download the wallet from the Database Connection page of your Oracle Autonomous Database console. Create secrets for the database wallet files (`cwallet.sso`, `ewallet.p12`, `keystore.jks`, `ojdbc.properties`, `tnsnames.ora`, `truststore.jks`). The wallet files' content should be base64-encoded.

Create and Train the Anomaly Detection Model

Create an anomaly detection project and add a data asset corresponding to your Oracle Autonomous Database view. Next, use the data asset to create and train the anomaly detection model.

For detailed information on OCI Anomaly Detection, refer to the OCI documentation:

Anomaly Detection Documentation

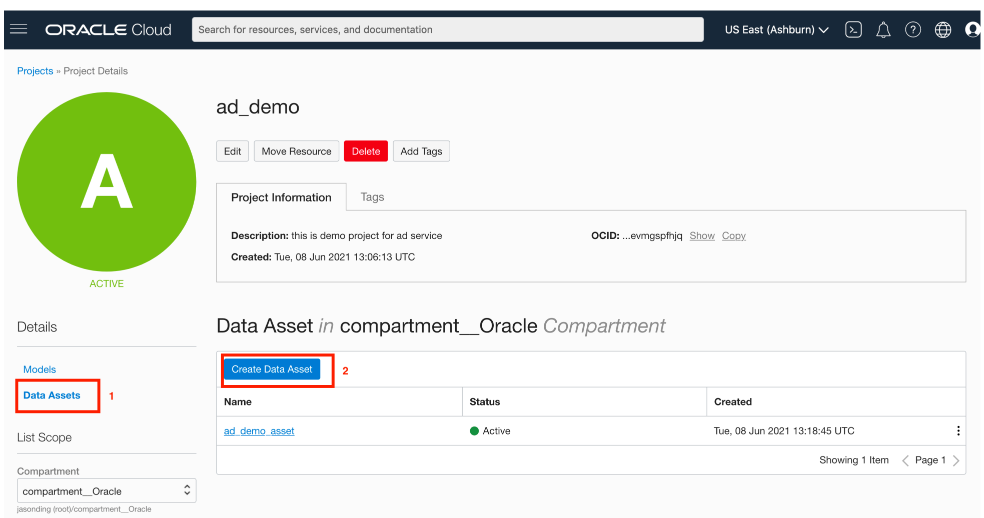
1. Create a new anomaly detection project.

   To create an anomaly detection project in Oracle Cloud, navigate to **Menu > Analytics & AI > Anomaly Detection.**

   Projects are collaborative workspaces for organizing data assets, models, and detection portals.

2. In the project, create a data asset of the Oracle Autonomous Transaction Processing type.

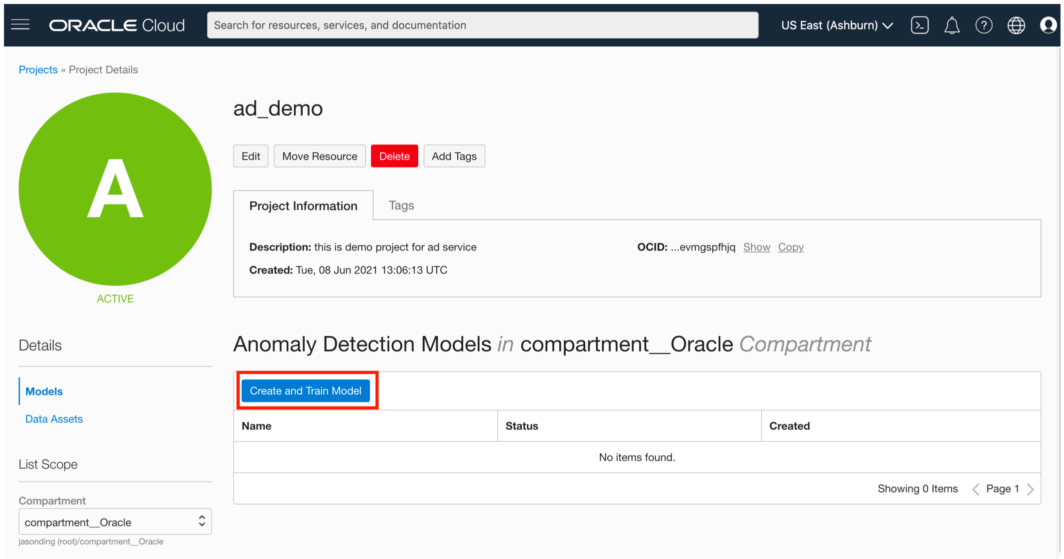
   Click **Data Assets > Create Data Asset** and complete the requisite fields.

   When you select **Oracle Autonomous Transaction Processing**, as the data asset **Type**, you get additional fields for specifying the credentials and vault secrets containing the database connection details.

   Use the view name containing formatted data for the database **Table Name**.

3. Create and train the anomaly detection model.



Use the data asset that you created to create and train the model.

Export Data for Anomaly Detection

Select data for the desired time period, and export it into a `csv` file for anomaly detection.

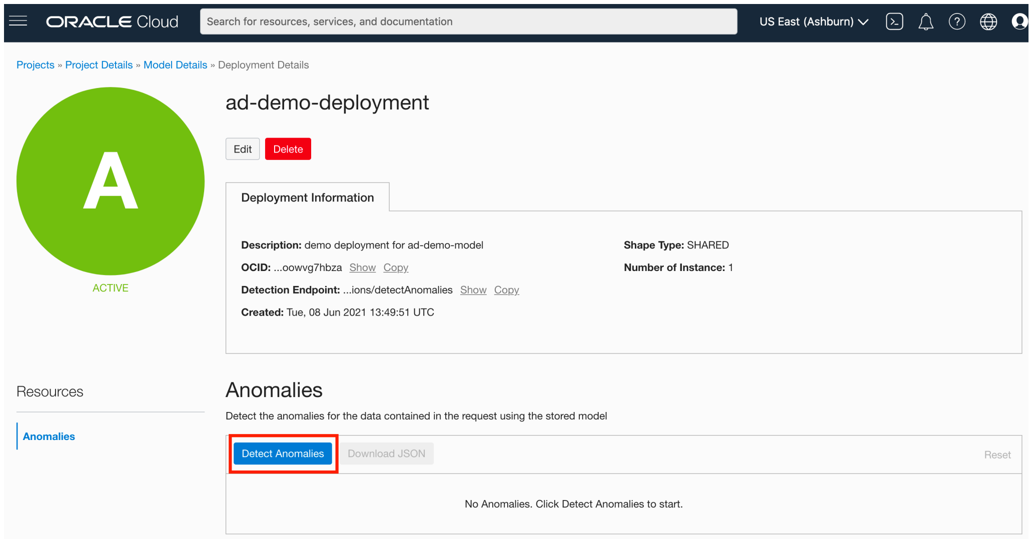
The following sample script exports data from the `DATA_VIEW` view. The view contains the timestamp column and various attribute columns. The script extracts data for the specified time period.

```
set feedback off
set markup csv on quote off
set heading off
spool "output.csv"
select
'timestamp,Detector1_Humidity,Detector1_Pressure,Detector1_Temperature' from
DUAL;
select mv.timestamp as "timestamp", "Detector1_Humidity",
"Detector1_Pressure", "Detector1_Temperature" from (select timestamp,
to_timestamp(timestamp, 'YYYY-MM-DD"T"HH24:MI:SS"Z"') as ts,
"Detector1_Humidity", "Detector1_Pressure", "Detector1_Temperature" from
DATA_VIEW) mv
where mv.ts > to_timestamp('2022-04-21 00:00:00', 'YYYY-mm-DD HH24:MI:SS')
and mv.ts < to_timestamp('2022-04-21 23:55:43', 'YYYY-mm-DD HH24:MI:SS')
order by mv.ts;
spool off;
quit;
```

Detect Anomalies Using OCI Anomaly Detection

Use the exported `csv` file to detect anomalies using a previously created model.

To start the process of anomaly detection, click **Detect Anomalies** on the anomaly model page.



Select an exported `csv` data file to detect anomalies.

For detailed information on OCI Anomaly Detection, refer to the OCI documentation:

Anomaly Detection Documentation

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 Intelligent Applications Cloud data or import and use external device data to help make predictions for your asset.

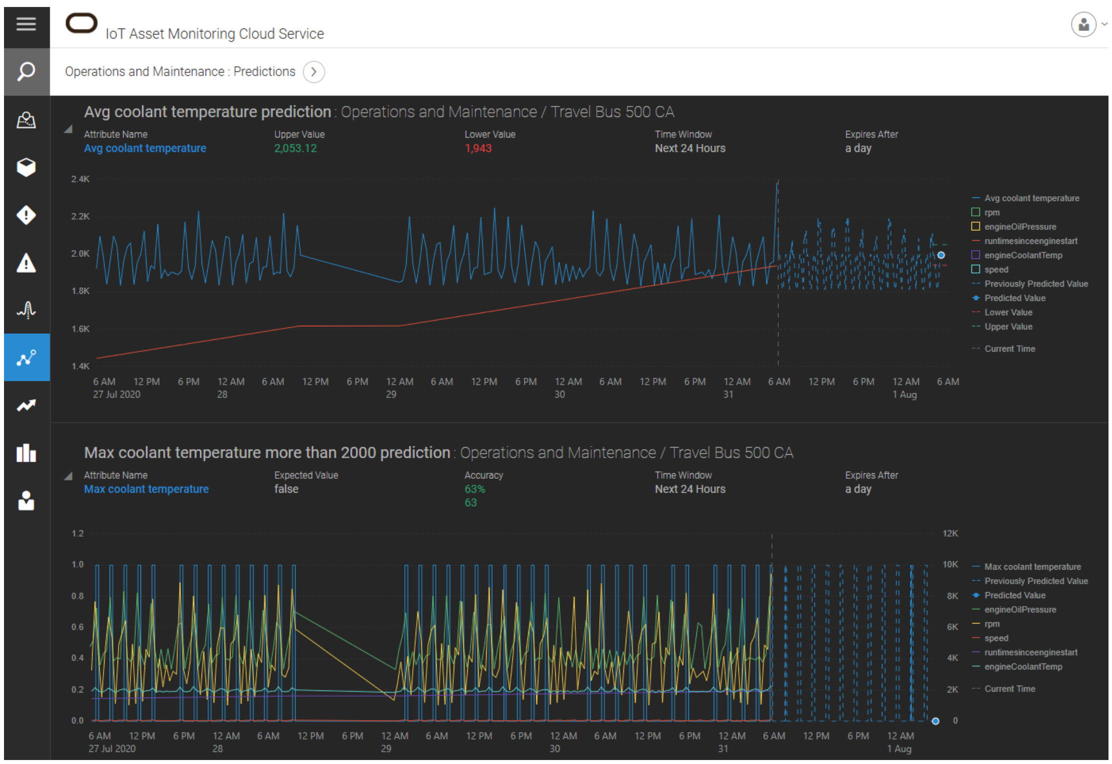
> **Note:**
>
> Before predictions can work, the data source must have at least 72 hours of historical data in it. This requirement may be larger if you have selected a forecast window greater than 72 hours. For example, if you choose to forecast for 7 days ahead, the system must have at least 7 days of historical data before predictive analytics can start training 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.

By default, Oracle IoT Asset Monitoring Cloud Service uses the most appropriate built-in training model to train the prediction. However, if your data scientists have externally trained models for your specific environment, you can use these to replace the training in Oracle IoT Asset Monitoring Cloud Service. Oracle IoT Asset Monitoring Cloud Service then performs the prediction scoring using your pre-trained model. You can use training models supported by PMML4S (PMML Scoring Library for Scala), such as the neural network. When creating a new prediction, upload your PMML file to replace the built-in models used by Oracle IoT Asset Monitoring Cloud Service.

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.



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

Note:

If you are using simulated sensor data to test your predictions, refer to the following sections for more information on the data characteristics of simulated data:

- Define a Simulation for a Sensor Attribute
- Tips and Considerations for Simulated Data and Analytics Artifacts

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.

   The Prediction Editor appears for the selected asset type.

   The prediction settings that you define apply to all assets of the chosen asset type.
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 Configuration section, leave **Automatic Model** selected under **Model**.
9. Select the **Target Attribute** for which you are creating the prediction.

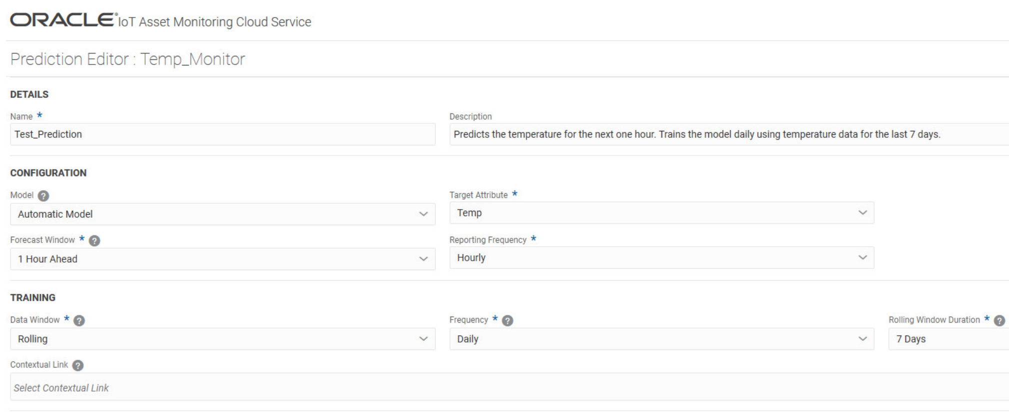
   The list includes both sensor attributes and metrics (KPIs).
10. Under **Forecast Window**, select one of the options:
    - **1 Hour Ahead**: Select this option to create a prediction for the next one hour.
    - **24 Hours Ahead**: Select this option to create a prediction for the next 24 hours.
    - **7 Days Ahead**: Select this option to create a prediction for the next 7 days.
    - **30 Days Ahead**: Select this option to create a prediction for the next 30 days.

    > **Note:**
    >
    > The options that appear depends upon the data life span settings for your device data and metric data. These settings can be managed under **Menu > Settings > Storage Management**.

    If you choose a forecast window of greater than 72 hours, the system will need to collect data equal to the forecast window size before it can start training the prediction. For example, if you choose to forecast 7 days ahead, then the system must have historical data for at least 7 days before the prediction can be trained.
11. Select a **Reporting Frequency** for the prediction.

    For example, if you choose a **Forecast Window** of **24 Hours Ahead** and a **Reporting Frequency** equal to **Hourly**, then the prediction for 24 hours ahead is made every hour.
12. Under Training, select the **Data Window**.

    The **Data Window** identifies the historical data that is used to train the system for making predictions.
    - **All Available Data**: Uses the entire available historical data to train the prediction model.
    - **Rolling**: A rolling data window uses data from a rolling time window to pick the most recent data for training. For example, you can choose to train your prediction model with a rolling data window of the last 7 days, and choose to perform the prediction training daily.



When you use a rolling window, the training model is re-created periodically, as determined by the frequency that you choose.

– **Frequency**: You can optionally change the frequency of the prediction model training. For example, if you choose **Daily**, then the training happens every day at 00:00 hours (midnight), UTC time by default.
– **Rolling Window Duration**: The duration of the rolling window going back from the model training time. For example, if you select **7 Days**, then the last 7 days of target attribute data is used to train the prediction model.

- **Static**: Uses a static data window to train your prediction model. Select the **Window Start Time** and **Window End Time** for your static window period.
  The static window duration must be at least three times the **Forecast Window**, and a minimum of 72 hours.

  The static data window provides data for a one-time training of your prediction model. If your prediction accuracy changes in the future, you should edit the prediction to choose a different static window.

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

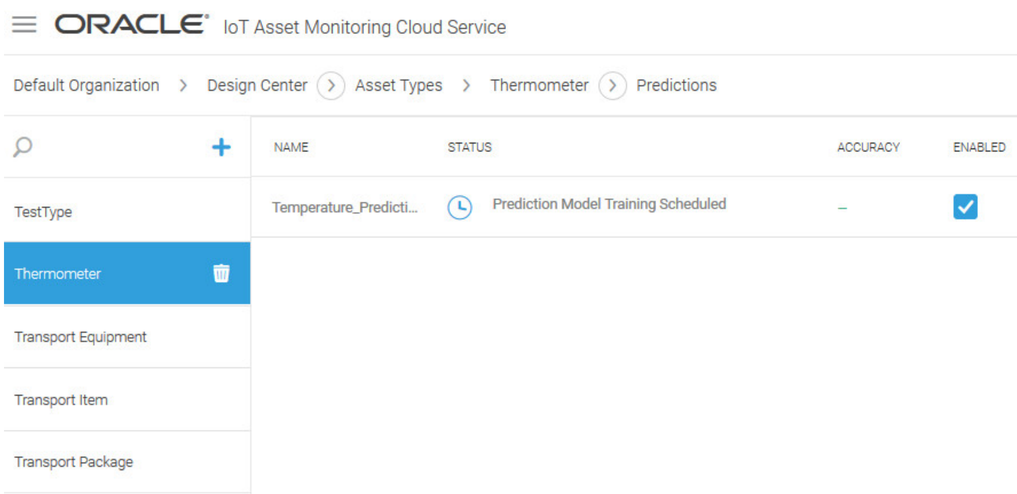
    A contextual link is used to provide additional data to the prediction for training the system. If you have existing contextual data connections that you would like to use as additional data sources for the prediction, you can optionally add them to the prediction.

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

    The system now schedules training for the new prediction model.

    Note: Predictive analytics may need to collect at least 72 hours of data or data equal to the forecast window size, whichever is higher, before it can start to train the system. Your predictions start showing after the initial training is complete.

The prediction is added to the Predictions page. The **Training Status** column shows the latest training status for the prediction model. Once training is complete, the application starts making predictions.



The application reports completed model trainings along with their timestamps. If training fails, the application includes pertinent information related to the failure. For example, the chosen training data set's statistical properties might not be suitable for predictions. The Feedback Center is also used to notify the Asset Manager about failures.

The application also reports skipped trainings along with an explanation for the same. For example, the system may be waiting to accumulate the minimum amount of data that is required for successful training.

You can enable or disable a prediction from within the Prediction Editor. If a prediction has been disabled by the system, a relevant message appears inside the Editor. The message also appears on the Predictions page in Operations Center.

Create a Prediction Using an Externally Trained Model

If you have a PMML file containing your externally trained model, you can use the PMML file to score your prediction in Oracle IoT Asset Monitoring Cloud Service.

By default, Oracle IoT Asset Monitoring Cloud Service uses the most appropriate built-in training model to train the prediction. However, if your data scientists have externally trained models for your specific environment, you can use these to replace the training in Oracle IoT Asset Monitoring Cloud Service. Oracle IoT Asset Monitoring Cloud Service then performs the prediction scoring using your pre-trained model.

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.

   The Prediction Editor appears for the selected asset type.

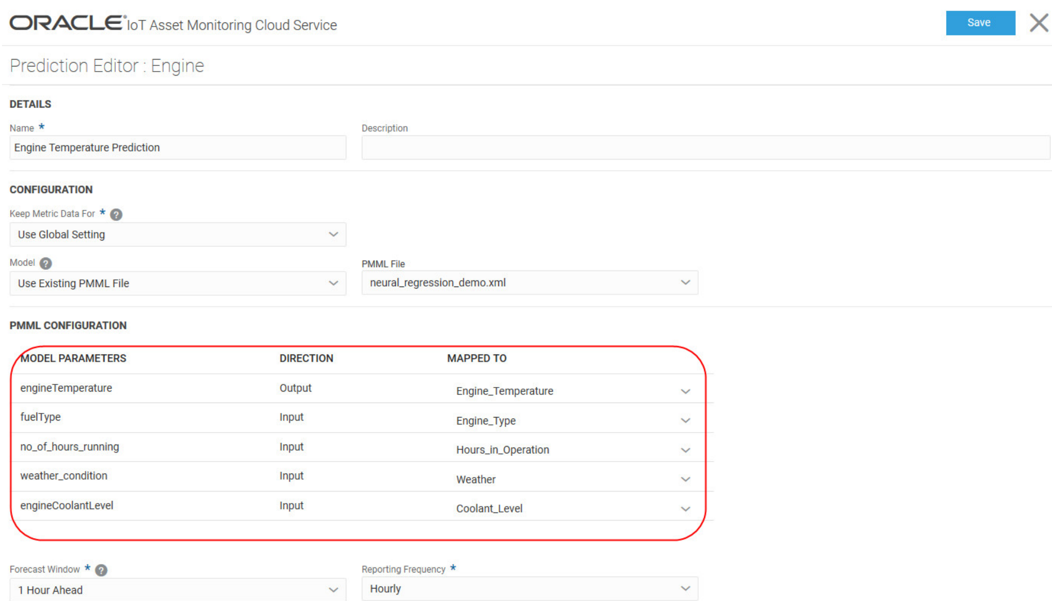
   The prediction settings that you define apply to all assets of the chosen asset type.
6. Enter a name for the prediction in the **Name** field.

7. Enter an optional description for the prediction in the **Description** field.
8. Under **Prediction Model**, select **Upload PMML File** to upload a PMML `xml` file that contains your exported trained model. Alternatively, select **Use Existing PMML File** to use a previously uploaded PMML file.

   For example, you may have completed external training using libraries like PySpark pipeline or R pipeline, and exported the trained model to a PMML file.

   You can only use training models supported by PMML4S (PMML Scoring Library for Scala), such as the neural network. For a list of supported model types in PMML4s, see https://www.pmml4s.org/#model-types-support.
9. Map the PMML model parameters to your asset type sensor attributes and metrics (KPIs).

   The default mapping is performed for you. Verify and change any mappings to match the attributes in your PMML file.



10. Under **Forecast Window**, select one of the options:
    - **1 Hour Ahead**: Select this option to create a prediction for the next one hour.
    - **24 Hours Ahead**: Select this option to create a prediction for the next 24 hours.
    - **7 Days Ahead**: Select this option to create a prediction for the next 7 days.
    - **30 Days Ahead**: Select this option to create a prediction for the next 30 days.
11. Select a **Reporting Frequency** for the prediction.

    For example, if you choose a **Forecast Window** of **24 Hours Ahead** and a **Reporting Frequency** equal to **Hourly**, then the prediction for 24 hours ahead is made every hour.
12. Click **Save** to complete configuring the prediction.

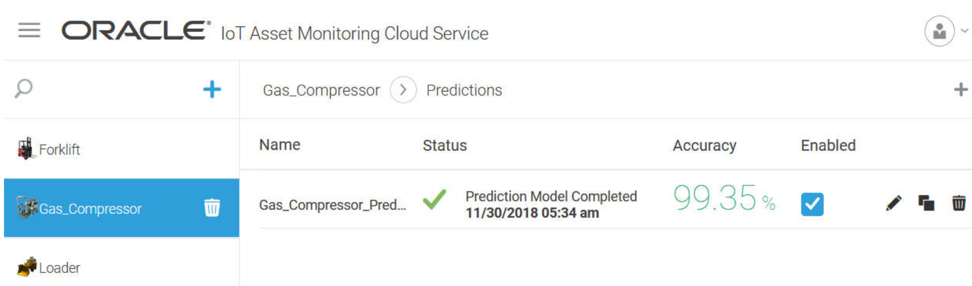
Edit a Prediction

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.

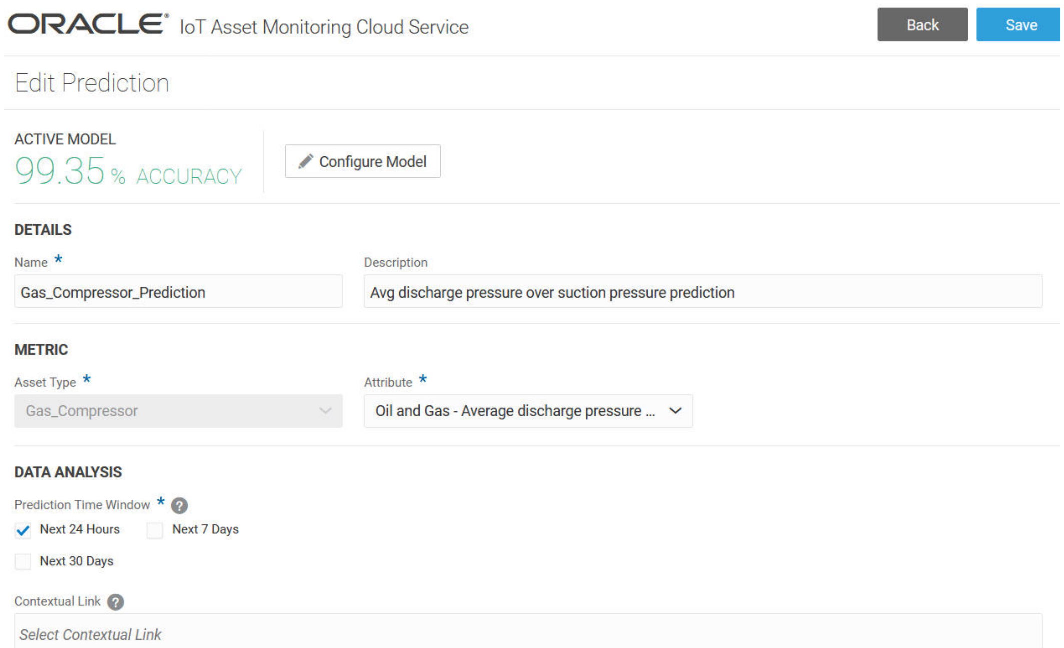
   You can also search for an asset type.
4. Click **Predictions**.
5. Select a prediction from the list.

   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.



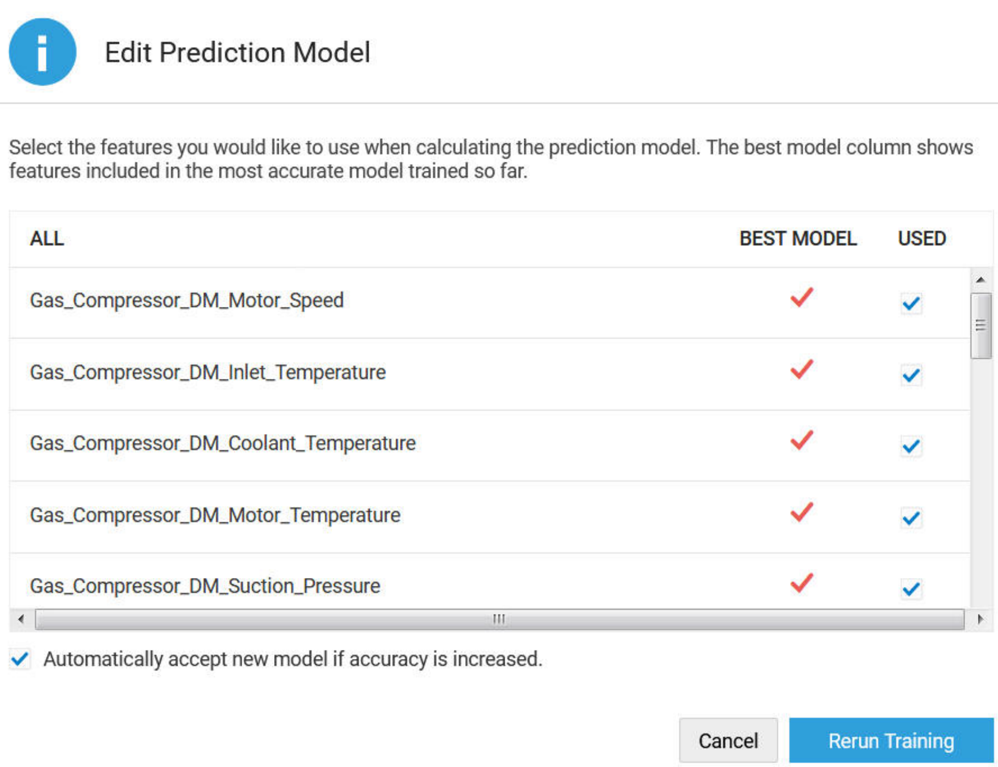
6. Click the **Edit** (✎) icon.
7. (Optional) Under Prediction Model, click **Configure Model** if you wish to re-configure the current prediction model for your prediction.

> **Note:**
>
> The **Configure Model** option to re-configure the current prediction model is available only for metric-based predictions, and not direct sensor-based predictions.



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.



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** () icon.
7. Click **Yes**.

Add Failure Diagnostics Information to Asset Incidents and Anomalies

Use failure modes for your asset components to add failure-related information to associated asset anomalies and incidents. Failure modes include detailed information on the probable failure causes, recommended actions, and failure effects. The asset manager and technicians can use the failure-related information to isolate and resolve the problem.

Define failure modes for your asset type using failure mode templates. When creating a user-defined anomaly or rule, you can choose to associate appropriate failure details with the anomaly or rule incident. Failure details enable easy root cause analysis (RCA) of asset component failures.

Field service personnel and technicians use the failure details and the associated RCA to establish the root cause of an asset incident, perform tests, and take corrective actions. If you have an integration with **Oracle Maintenance Cloud Service**, then the failure cause data and suggested corrective actions associated with the incident are passed to **Oracle Maintenance Cloud Service**.

Define a Failure Mode Using the Failure Mode Template

You can define failure modes for an asset type in the Design Center.

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.

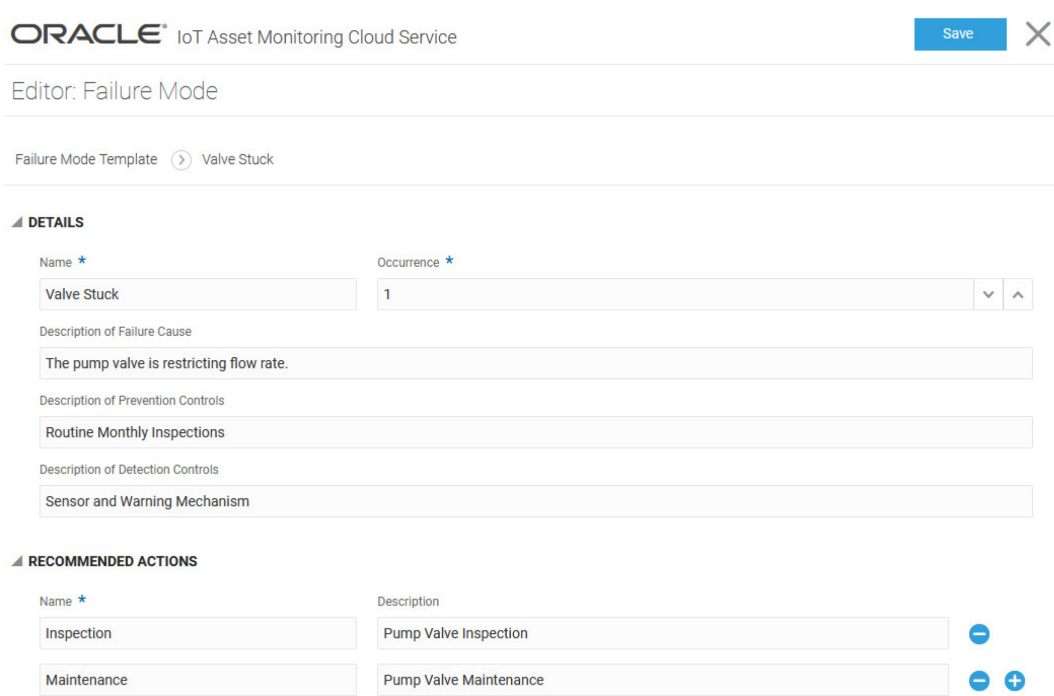
   You can also search for an asset type.
4. Click **Failure Modes**.
5. Click the **Create Failure Mode** () icon.

   The Failure Mode Editor appears for the selected asset type.

   The failure mode that you define will apply to all assets of the chosen asset type.
6. Under the **Details** section, enter a name for the failure mode in the **Name** field.
7. (Optional) Specify an optional description text for the failure mode.
8. Specify a **Severity** level for the fault.
9. Add one or more **Failure Causes** associated with the failure.

   For each failure cause that you add, you can add descriptions and recommended actions.

   The following example shows a failure cause configuration in the Failure Mode editor.



   See Add Failure Causes and Associated Recommendations for a Failure Mode for more details on adding a failure cause.

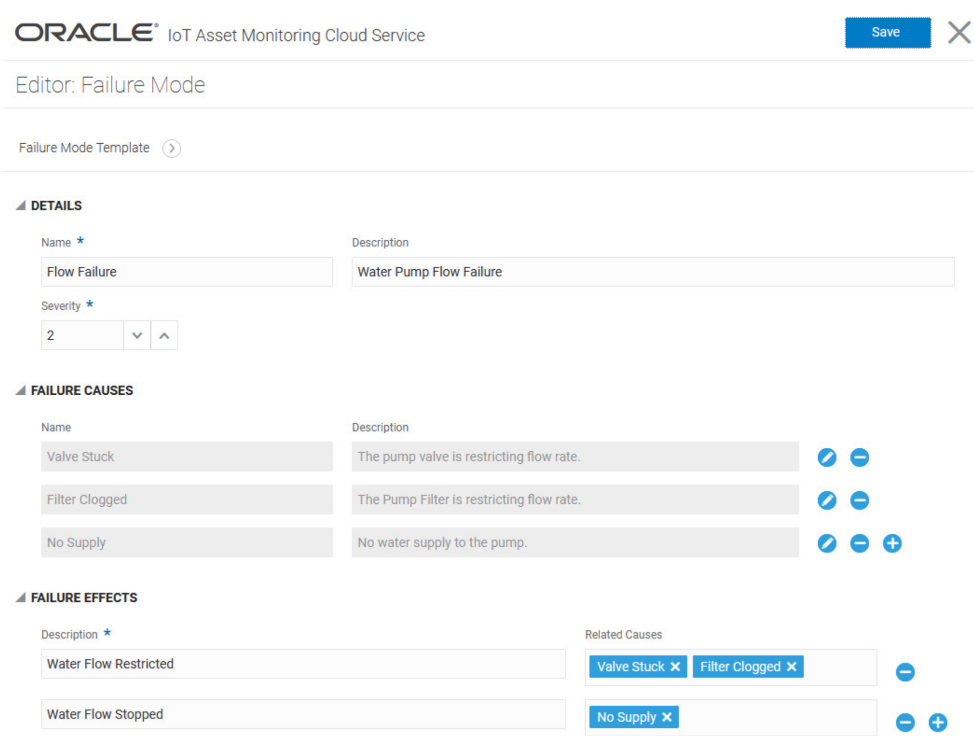
10. Add one or more **Failure Effects** associated with the failure.

    For each failure effect that you add, you can associate appropriate failure causes for the effect. You can choose from the failure causes that you created for the failure.

    See Add Failure Effects and Associate Causes for more details on adding a failure effect.

11. Click **Save** to save the failure mode details.

    The following example shows the Failure Mode editor. The screen shows a sample flow failure for a water pump asset.



Add Failure Causes and Associated Recommendations for a Failure Mode

Add one or more failure causes associated with the failure mode. You must add at least one failure cause for the failure. For each failure cause that you add, you can add descriptions and recommended actions.

1. In the Failure Mode editor, click **Add** under **Failure Causes**.
2. Specify a **Name** for the failure cause.

   For example, `Valve Failure`.
3. Specify an **Occurrence** value.

   The occurrence value specifies the likelihood of the failure happening because of the cause.
4. Optionally add additional information under the description fields.
5. Optionally add recommended actions for the technician or asset manager.

a. To add a recommended action, click **Add** under **Recommended Actions**.
b. Specify a **Name** for the recommended action.

   For example, `Inspect Valve`.
c. Specify additional, optional information under **Description**.
d. Repeat the preceding steps to add more actions.

6. Click **Save** to save the failure cause details.

   You are taken back to the main **Failure Mode Template** editor. You may also use the breadcrumbs to navigate back to the **Failure Mode Template** editor.
7. Repeat the preceding steps to add additional failure causes.

Add Failure Effects and Associate Causes

Add one or more **Failure Effects** associated with the failure. For each failure effect that you add, you can associate appropriate failure causes for the effect. You can choose from the failure causes that you created for the failure.

1. In the Failure Mode editor, click **Add** under **Failure Effects**.

   You must have already created at least one failure cause before you can create a failure effect.
2. Specify a **Description** for the failure effect.

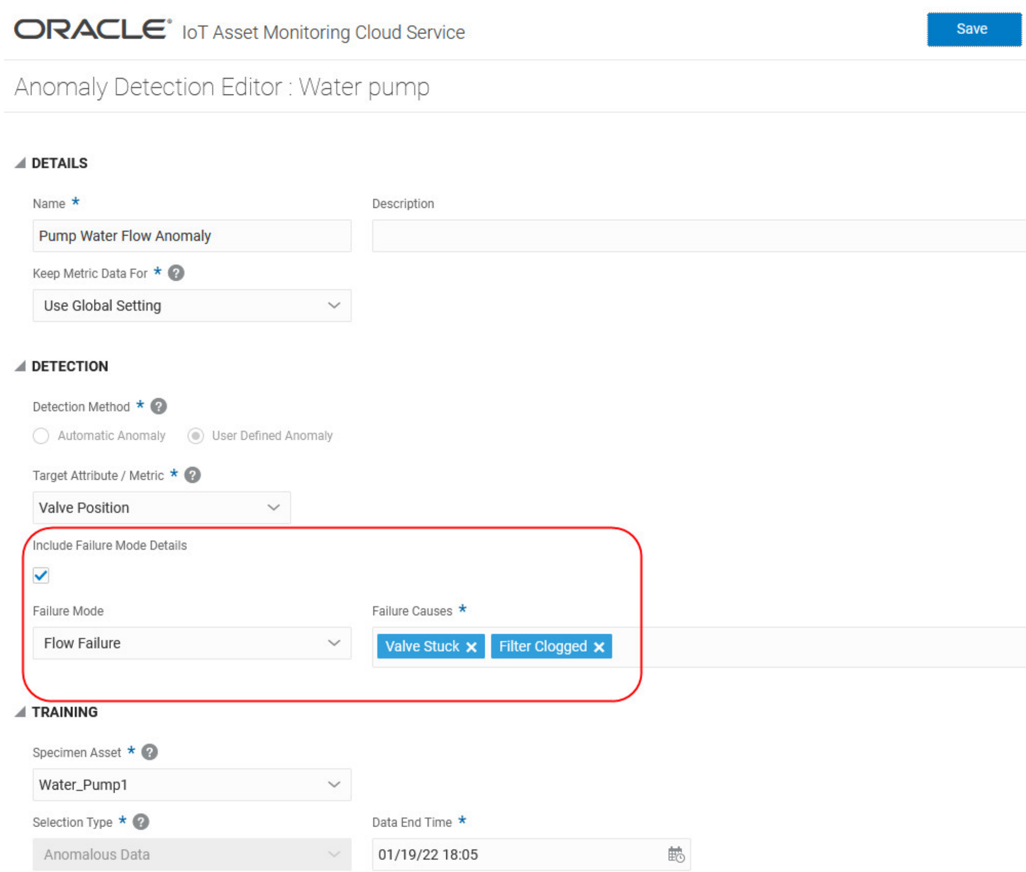
   For example, `Reduced Water Pressure`.
3. Select one or more previously created causes to associate with the failure effect.

   For example, `Valve Stuck` and `Filter Clogged`.
4. Repeat the preceding steps to add additional failure effects.

Use Failure Modes in Your Rules and Anomalies

When configuring rules and user-defined anomalies for your asset type, you can choose to associate failure mode information with the anomaly or rule incident.

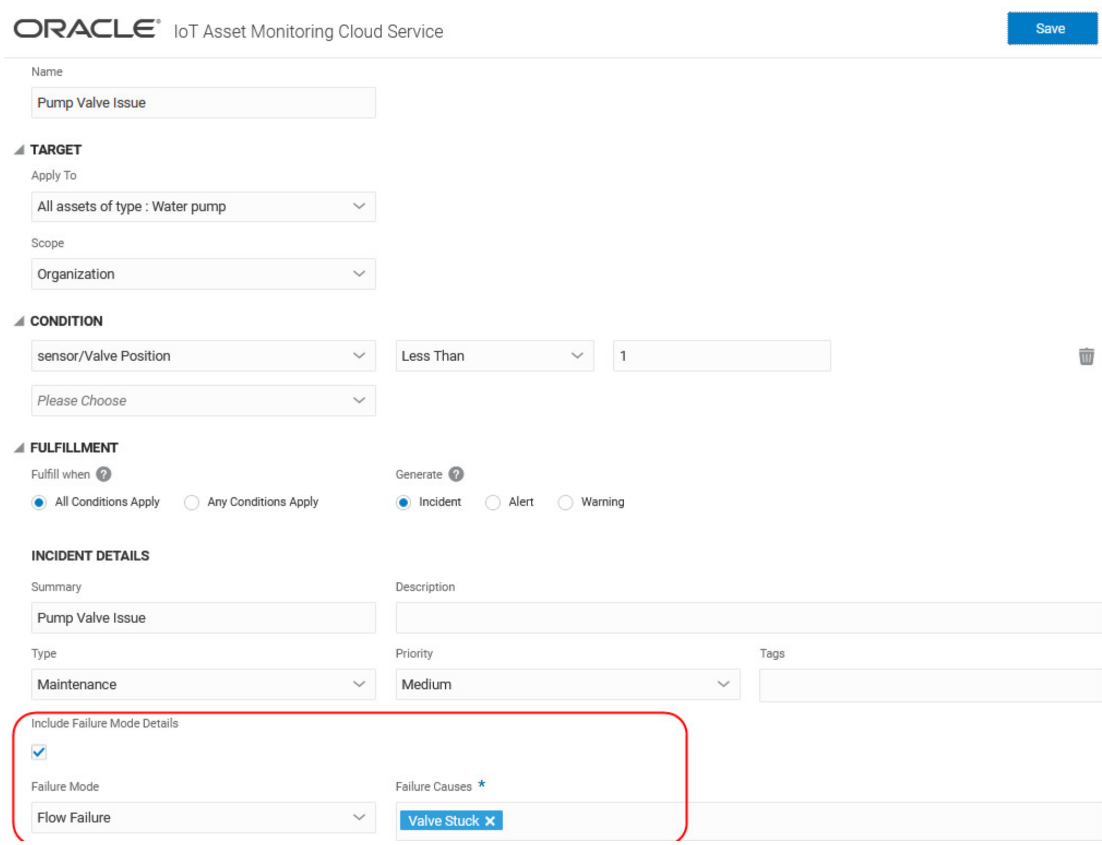
The following sample Anomaly Detection Editor screen depicts associating a failure mode with the anomaly.



> **Note:**
>
> Failure modes can only be associated with user-defined anomalies. Automatic anomalies cannot have failure mode associations.

See Use Anomalies to Track Deviations in Asset Behavior for detailed information on defining anomaly detection.

The following sample Rule Editor screen depicts associating a failure mode with the rule incident.

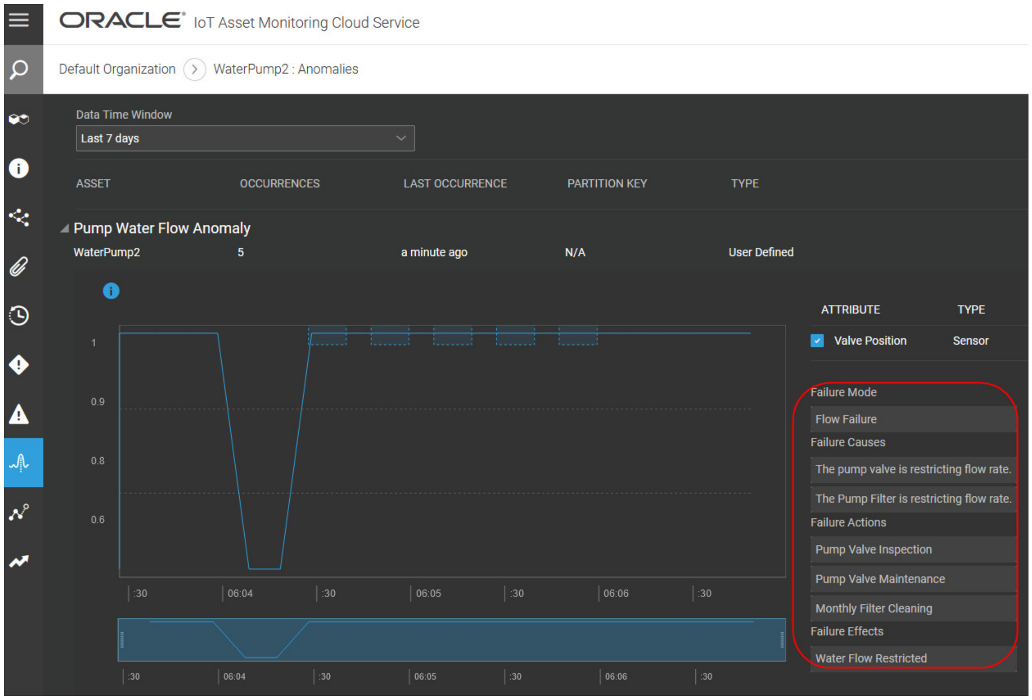


See Use Rules to Monitor and Maintain Assets for more information on creating rules for your asset types.

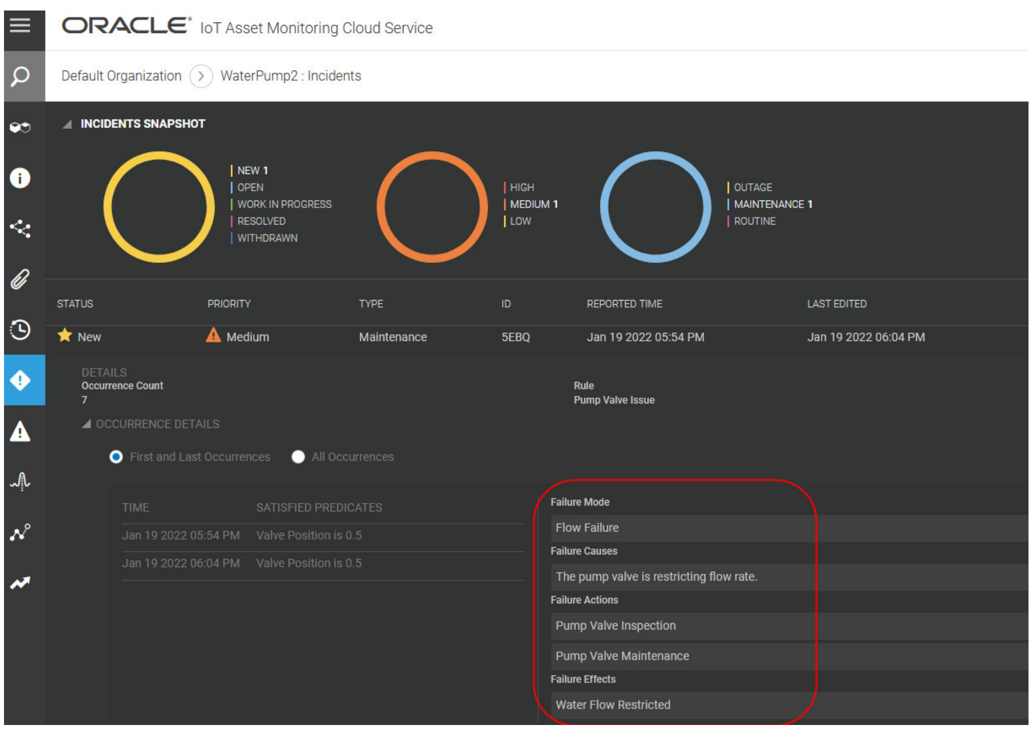
Failure Mode Information in Operations Center

When anomalies and incidents are reported in Operations Center, any associated failure mode information is also included.

The following image shows a sample anomaly reported in Operations Center. The associated failure mode information is included for the technician and asset manager.



The following image shows a sample incident reported in Operations Center. The associated failure mode information is included for the technician and asset manager.



See Use the Incidents Page to Manage Asset Incidents for more information on viewing and managing incidents in Operations Center.

Use What-If Scenarios for End-to-End Simulation Tests

Use what-if scenarios to run scenario-based simulation tests for your assets. What-If scenarios help test and validate your asset monitoring and management setup.

For example, you can simulate a one-minute spike in temperature for your temperature sensor. If you have a rule defined, you can check if a corresponding incident is raised in the system. If you are connected to other enterprise systems like the Oracle Fusion Cloud Maintenance, you can verify that a corresponding maintenance work order is created in the external system.

A what-if scenario lets you override the actual incoming sensor data for an asset with the scenario data. You can choose the period of time for which the scenario runs. The what-if scenario lets you test all the various entities associated with the asset type, such as rules, metrics, and anomalies. So, for example:

- You can create scenarios that trigger your rules, which in turn trigger incidents, warnings, device actions, or device alerts.
- You can look at how the scenario affects metrics (KPIs) that are using the overridden sensor attributes.
- You can verify if anomalies are registered against positive test cases.

To define a what-if scenario for an asset type, create a pattern-based or formula-based simulation for one or more of its sensor attributes. Then run the what-if scenario for a real asset and a chosen period of time.

When the what-if scenario runs for the asset, the real sensor data gets overwritten by the simulation scenario data. The Digital Twin view of the asset reflects the fact that a what-if scenario is active for the asset.

You can verify how the associated organizational entities are affected both during and after the test.

Create a What-If Scenario for an Asset Type

A what-if scenario contains scenario-based simulations for one or more sensor attributes of the asset type. You can run the what-if scenario for any asset of the 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 **What-If Scenarios**.
5. Click the **Create WhatIf** (+) icon.
6. Enter a name for the what-if scenario in the **Name** field.

   For example, `Abnormal Temperature Spikes`.
7. (Optional) Provide an optional **Description** text for the scenario.
8. Click **Upload Image** and upload an optional asset image.

This custom asset image replaces the standard asset image when the what-if scenario is active for an asset.

9. Under **Target**, click **Add** + to add a target sensor attribute.
10. Select a **Sensor Attribute** for the **Asset Reference**.

    This is the asset sensor attribute for which you wish to create a simulation scenario. For example, you may wish to create a voltage fluctuation or a temperature spike.

    The **Asset Reference** is your selected asset type. It's already populated for you.
11. Choose the simulation **Type**.

    You can choose between predefined wave patterns, such as sine curves or square waves, and formula-based simulation values.
12. 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.

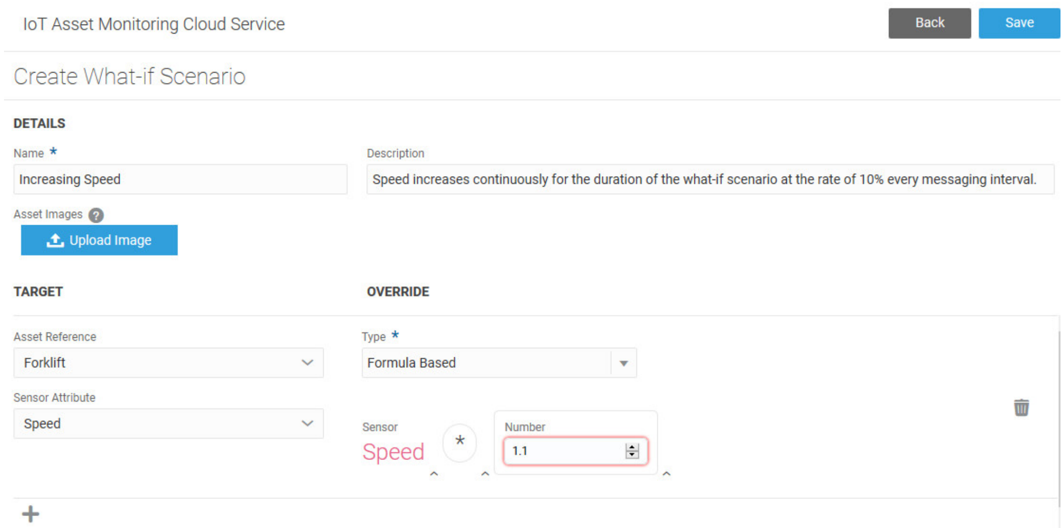
    - For most wave patterns, you need to specify a maximum (**Max**) and minimum (**Min**) value.
    - For regular wave patterns, such as sine waves and square waves, you need to additionally specify the desired **Wavelength** of the patterns.
    - For a constant wave pattern, specify the constant **Value**.

    As an example, say you have a temperature sensor attribute that normally ranges between 10 and 20. You may wish to introduce random spikes by choosing a **Random** pattern between `20` (**Min**) and `30` (**Max**).

    The message interval for the what-if scenario is the same as the message interval for the sensor attribute. When choosing a wavelength, you should keep the message interval in mind, so that the pattern is recognizable in the charts. For example, a sine curve for a sensor attribute with a wavelength of `500 seconds` and a message interval of `10 seconds` will have 50 data point plots in each wave pattern unit.
13. 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 formula increases the speed of a truck by 10% for every message interval of the speed sensor.



> **Note:**
>
> The speed will increase to high values rapidly depending on the messaging interval of the sensor. You should configure the runtime accordingly, and monitor the parameters when playing the scenario for an asset.

14. (Optional) Click **Add** + to add additional target sensor attributes and define corresponding simulations.
15. Click **Save** to save the what-if scenario.

Play a What-If Scenario for an Asset

You can play a what-if scenario for an asset from the digital twin page of the asset. Only one what-if scenario can run at a time.

1. In the Operations Center, navigate to the asset page for your asset.

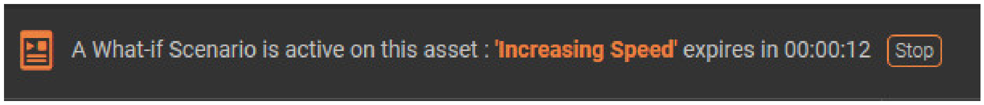
   See View Asset Details if you need help accessing the digital twin page for an asset.
2. Click the Asset Controls icon that appears to the right of the navigation breadcrumbs.
3. Under What-If Scenarios, click **Initiate** against the what-if scenario that you wish to run against the asset.

   To see your what-if scenario, you must have already created the scenario for the corresponding asset type.
4. In the Initiate What-If Scenario dialog that appears, specify an **Expires After** value and click **OK**.

   The **Expires After** value determines the duration for which the what-if scenario remains active.

   The what-if scenario is now active for your asset. You can see the sensor attribute values and charts change per the scenario.

   A banner appears indicating that the what-if scenario is active for the asset.



5. (Optional) Click **Stop** if you wish to stop the what-if scenario before its duration expires.

5

Set Up Your Devices in Oracle Internet of Things Intelligent Applications Cloud

The device model options for asset types and device options for assets are fetched from your Oracle Internet of Things Intelligent Applications Cloud instance.

Topics:

- Create Device Models in Oracle Internet of Things Intelligent Applications Cloud
- 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 Intelligent Applications Cloud

The device model options for asset types are fetched from your Oracle Internet of Things Intelligent Applications Cloud instance.

The Oracle IoT Asset Monitoring Cloud Service application relies on your platform side Oracle Internet of Things Intelligent Applications Cloud for its device models. If you do not already have your device models set up in Oracle Internet of Things Intelligent Applications Cloud, 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 Intelligent Applications Cloud regardless of its manufacturer or operating system.

1. Open the Oracle Internet of Things Intelligent Applications Cloud Management Console.

   You can access the Oracle Internet of Things Intelligent Applications Cloud Management Console from the following URL:

   `https://hostname/ui`

   Here, *hostname* is the host name of your Oracle Internet of Things Intelligent Applications Cloud 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:`urn:<mycompany>:<department>:<mydevice>:<device model>:<message>`.
   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.
   l. 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 Intelligent Applications Cloud.

1. Open the Oracle Internet of Things Intelligent Applications Cloud Management Console.

   You can access the Oracle Internet of Things Intelligent Applications Cloud Management Console from the following URL:

   `https://hostname/ui`

   Here, *hostname* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.

2. Click the **Menu** () icon.
3. Select **Devices** and then select **Model**.
4. In the **Device Models** tab, click the **Import** ( ) 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 Intelligent Applications Cloud Management Console.

   You can access the Oracle Internet of Things Intelligent Applications Cloud Management Console from the following URL:

   `https://hostname/ui`

   Here, *hostname* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.

2. Click the **Menu** () icon.
3. Select **Devices** and then select **Model**.
4. Click the **Duplicate** ( ) 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 Intelligent Applications Cloud Management Console.

   You can access the Oracle Internet of Things Intelligent Applications Cloud Management Console from the following URL:

   `https://hostname/ui`

   Here, *hostname* is the host name of your Oracle Internet of Things Intelligent Applications Cloud 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 Intelligent Applications Cloud Management Console.

   You can access the Oracle Internet of Things Intelligent Applications Cloud Management Console from the following URL:

   `https://hostname/ui`

   Here, *hostname* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.

2. Click the **Menu** () icon.
3. Select **Devices** and then select **Model**.
4. Click the **Device** () 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 Intelligent Applications Cloud Management Console.

   You can access the Oracle Internet of Things Intelligent Applications Cloud Management Console from the following URL:

   `https://hostname/ui`

Here, *hostname* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.

2. Click the **Menu** (☰) 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 Intelligent Applications Cloud Management Console.

   You can access the Oracle Internet of Things Intelligent Applications Cloud Management Console from the following URL:

   `https://hostname/ui`

   Here, *hostname* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.

2. Click the **Menu** (☰) 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 Intelligent Applications Cloud Management Console.

   You can access the Oracle Internet of Things Intelligent Applications Cloud Management Console from the following URL:

   `https://hostname/ui`

   Here, *hostname* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.

2. Click the **Menu** (☰) 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 Intelligent Applications Cloud 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 Intelligent Applications Cloud.

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 Intelligent Applications Cloud Management Console.

   You can access the Oracle Internet of Things Intelligent Applications Cloud Management Console from the following URL:

   `https://hostname/ui`

   Here, *`hostname`* is the host name of your Oracle Internet of Things Intelligent Applications Cloud 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 Intelligent Applications Cloud.

The Oracle IoT Asset Monitoring Cloud Service application relies on your platform side Oracle Internet of Things Intelligent Applications Cloud for its devices. If you do not already have your sensor devices set up in Oracle Internet of Things Intelligent Applications Cloud, 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 Intelligent Applications Cloud.

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 Intelligent Applications Cloud 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 Intelligent Applications Cloud. 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 Intelligent Applications Cloud. 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 Intelligent Applications Cloud, see Registering a Batch of Devices.

Property	Required / *Optional*	Description
`Name`	*Optional*	The `String` data type assigned to the registered device. This value can be modified after device registration.
`Manufacturer`	**Required**	The manufacturer of the device.
`Model Number`	**Required**	The model number of the device
`Serial Number`	**Required**	The serial number of the device.
`Activation ID`	*Optional*	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.
`Activation Secret`	*Optional*	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.
`Latitude`	*Optional*	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.
`Longitude`	*Optional*	The decimal notation of the longitude of the device’s position. For example: , e.g. -43.5723 [World Geodetic System 1984]. If you specify the longitude, then you must also specify the latitude.
`Altitude`	*Optional*	The decimal notation of the altitude of the device’s position, in meters above sea level.
`Accuracy`	*Optional*	The accuracy of the device’s position in meters. This must be a positive number or zero. An accuracy value can only be specified if the latitude and longitude are provided.

Property	Required / *Optional*	Description
`Metadata`	*Optional*	Key/value pairs that are listed in successive columns. There must be an even number of columns containing keys and values. If there is an odd number of columns, an error message is returned.

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 Intelligent Applications Cloud 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:

      ```
      DirectlyConnectdDevice dcd = new
      DirectlyConnectedDevice(configFilePath, configFilePassword);
      ```

   b. Add this statement to the device application code to activate the device:

      ```
      if (!dcd.isActivated())
      { dcd.activate(deviceModelUrn); }
      ```

3. Verify the device has been activated:

   a. Open the Oracle Internet of Things Intelligent Applications Cloud 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 Intelligent Applications Cloud.

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 Intelligent Applications Cloud 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.

6

Customize Your Oracle IoT Asset Monitoring Cloud Service Application

Add a corporate logo or modify the application name to personalize yourOracle IoT Asset Monitoring Cloud Service application.

Topics

- Show or Hide the Application Name
- Add or Update an Application Logo
- Remove an Application Logo
- Customize Visualization Options
- Monitor Data Storage and Manage Capacity Usage

Show or Hide the Application Name

Show or hide the application name when business requirements change.

1. In the Operations Center, click **Menu** (☰), and then click **Settings**.

   If you are in the Design Center, you need to click **Previous** (‹) before you see the **Settings** option in the menu.

   > **Note:**
   >
   > If you wish to change the appearance for an individual organization only, navigate to **Menu > Settings > IoT Organizations > *Organization Name***.

2. Click **Appearance** on the Settings page.
3. Select one of these options:.
   a. Select **Show Application Name** to display the application name on all application pages.
   b. Clear **Show Application Name** to remove the application name from all application pages.
4. Click **Save**.

Add or Update an Application Logo

Add or update corporate logos when business requirements change or a new corporate logo is issued.

1. In the Operations Center, click **Menu** (☰), and then click **Settings**.

If you are in the Design Center, you need to click **Previous** ( ) before you see the **Settings** option in the menu.

> **Note:**
>
> If you wish to change the appearance for an individual organization only, navigate to **Menu > Settings > IoT Organizations > *Organization Name***.

2. Click **Appearance** on the Settings page.
3. Under **Title Bar Logo**, select **Custom**.

   Under Image, click the **Drag and Drop** area to select an image file to upload. Alternatively, you can also drag and drop the image file to the **Drag and Drop** area in your browser window.
4. Click **Save**.

Remove an Application Logo

Remove a logo when an application logo is no longer required.

1. In the Operations Center, click **Menu** ( ), and then click **Settings**.

   If you are in the Design Center, you need to click **Previous** ( ) before you see the **Settings** option in the menu.

> **Note:**
>
> If you wish to change the appearance for an individual organization only, navigate to **Menu > Settings > IoT Organizations > *Organization Name***.

2. Click **Appearance** on the Settings page.
3. Under **Title Bar Logo**, select **None**.
4. Click **Save**.

Set Default Units of Measure

Set the default units of measurement for your application. You can select between the US Imperial and Metric unit systems.

1. In the Operations Center, click **Menu** ( ), and then click **Settings**.

   If you are in the Design Center, you need to click **Previous** ( ) before you see the **Settings** option in the menu.

> **Note:**
>
> If you wish to change the measurement units for an individual organization only, navigate to **Menu > Settings > IoT Organizations > *Organization Name***. For example, you may want to set different measurement units for your US and Europe organizations.

2. Click **Units and Measurement**.
3. Click **Edit** to change the unit system.
4. Under **Unit System**, select between **US Imperial** and **Metric**.

   The US Imperial setting uses the following units for *Distance*, *Speed*, *Temperature*, and *Volume* respectively: *Miles*, *Miles per Hour*, *Fahrenheit*, and *Gallons*.

   The Metric setting uses the following units for *Distance*, *Speed*, *Temperature*, and *Volume* respectively: *Kilometers*, *Kilometers per Hour*, *Celsius*, and *Liter*.
5. Click **Save**.

Customize Visualization Options

You can choose to customize the default view that appears when you log into your organization to access the Operations Center. You can also choose custom default views for your asset types.

The **Map** view is the default view for an organization, and the **Digital Twin** tab is the default view for your assets. You can choose to change the default tab behavior.

For example, if your organization has static HVAC assets that need constant monitoring, you may want to change the default organization view from the Map view to the Incidents view.

As another example, say you have created a custom performance dashboard for your forklifts and you wish this dashboard to appear when you click **Show Details** against a forklift asset. You can change the visualization option for the forklift asset type from **Digital Twin** to your dashboard.

Visualization options can be customized at the organization, group, and asset type levels.

Customize Visualization Options for Your Organization

When you log into your organization, or switch to your organization, to access the Operations Center, the **Map** view is the default view that appears. You can change this setting from the **Visualization Options** setting for the organization.

1. Click **Menu** ≡ and then click **Design Center**.
2. Select **Organization** from the **Design Center** sub-menu.
3. Click **Edit** against **Visualization Options**.
4. Select one of the available options for **Default Operations Center Tab**.

   The default option is **Map**.

For example, if your organization has static HVAC assets that need constant monitoring, you may want to change the default organization view from the **Map** view to the **Incidents** view.

Customize Visualization Options for an Asset Type

When you access the details for an asset, the **Digital Twin** view is the default tab that appears. You can change this setting from the **Visualization Options** setting 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 from the left pane.
4. Click **Edit** against **Visualization Options**.
5. Select one of the available options for **Default Operations Center Tab**.

   The default option is **Digital Twin**.

   For example, say you have created a custom performance dashboard for your forklifts and you wish this dashboard to appear when you click **Show Details** against a forklift asset. You can change the visualization option for the forklift asset type from **Digital Twin** to your dashboard.

Monitor Data Storage and Manage Capacity Usage

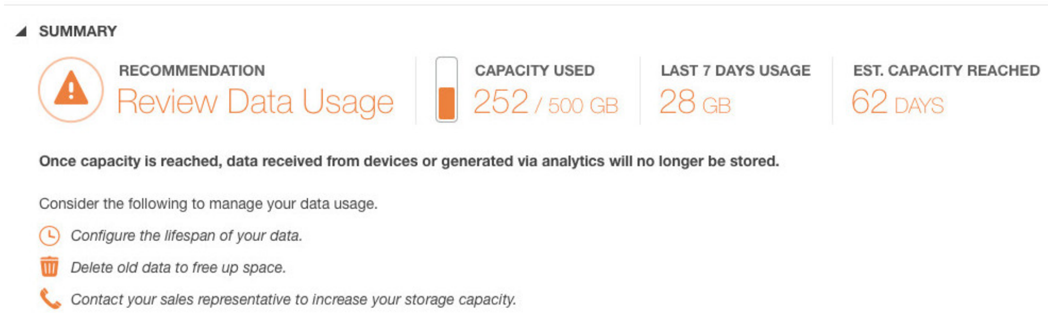
As an administrator, you can monitor the data storage for your Oracle IoT Intelligent Applications Cloud Service. Use the Storage Management page to review storage data in the system, to set up or adjust the time window for data retention, and to run data deletion jobs.

> **Note:**
>
> If you are using more than one application in Oracle IoT Intelligent Applications Cloud Service, then the data storage settings are shared between these applications. Also, any operations that you perform under data management, such as tweaking data life spans or creating deletion jobs, affects data in all these applications.
>
> So, for example, if you are using the Asset Monitoring and Production Monitoring applications, the data usage includes usage across both these applications. Also, if you were to delete metric data older than, say, 30 days, then metric data that is older than 30 days is deleted in both your applications.

When you log in to your IoT application as an administrator, a notification appears with details on the storage capacity used. Notifications may also appear periodically for every 10% of capacity that is used up. High-priority notifications are sent after you have used up more than half of the storage capacity. You can use the Storage Management page to manage your storage capacity.

The **Storage Management** tile under application **Settings** lets you monitor and manage the data storage for your application. The Storage Management page has the following sections:

- **Summary:** Shows you the total data storage capacity available for your account, and the currently used up capacity. Depending on your current usage, the status is indicated using one of the following colors:
  - **Green:** Indicates that more than 50% of the available capacity remains.
  - **Orange:** Indicates that between 25% and 50% of the available capacity remains. A recommendation on ways to manage your data is also included.
  - **Red:** Indicates that less than 25% of the available capacity remains, and you must take steps to manage your storage data.



- **Data Management:** Lets you manage data, change settings, and create data deletion jobs. The data capacity usage percentages are shown category-wise:
  - **Raw Device Data:** Raw time-series data from devices that is stored in a normalized JSON format. Comprises application messages, connector messages, integration-related messages, log messages, and other related messages.
    Oracle recommends a data life span of 7 Days, or less, for this category to avoid high storage consumption.
  - **Sensor Data:** Time-series data from devices and computed attributes used for machine-learning models and anomaly detection. Comprises incoming sensor data, visualization and training data.
    Set the data life span for this category to match your business requirements for data retention.
  - **Custom Metric Data:** Computed values of user-defined metrics. Comprises data specific to custom metrics or KPIs. Custom metrics are metrics that you create in the application for your production environment and scenarios.
    Set the data life span for this category to match your business requirements for data retention.
  - **System Metric Data:** Computed values of built-in system metrics that are automatically computed. Comprises data specific to system metrics or KPIs. System metrics are the built-in metrics that are calculated automatically in your application.
    Oracle recommends a data life span of 90 Days, or less, for this category to avoid high storage consumption.
  - **Transaction Log Data:** Comprises logs related to all shipment transactions that have occurred between Oracle IoT Fleet Monitoring Cloud and OTM or ITT.
    Set the data life span for this category to match your business requirements for data retention.

You can select the data life span for each category. The data life span is the time period for which data is retained. If you set the data life span for a category to **Delete Manually**, then data for that category is never deleted, unless you manually run a data deletion job. Note that this setting may potentially lead to storage capacity issues, as stored data is never deleted.

You can choose to create data deletion jobs to delete selective data. A data deletion job lets you select the data type and time span for which you wish to delete data.

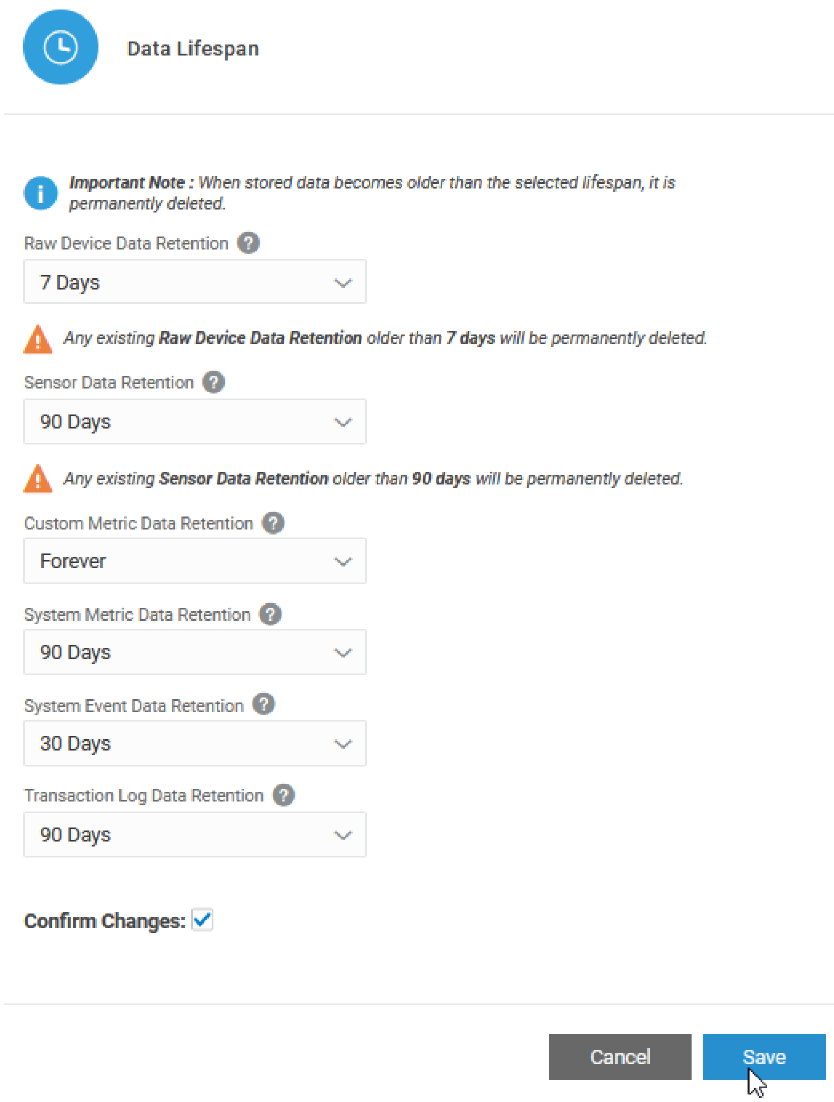
Perform Data Management Tasks

Use the **Data Management** section to manage data storage settings for your application. You can select the data life span for the various data types. You can also create data deletion jobs to delete selective data.

1. Click **Menu** () and then click **Settings** .
2. Click **Storage Management**.

   The Storage Management page appears.
3. To change the data life span, click **Edit** under **Data Life Span**.

   The Data Life Span section appears under the Data Management section.
   a. Select the data life span for **Raw Device Data**, **Sensor Data**, **Custom Metric Data**, **System Metric Data**, and **Transaction Log Data**.



If you select **Forever** for a category, then the data for that category is never deleted automatically. You would need to run a data deletion job, described in the subsequent steps, to select and delete any data for the category.

b. Select **Confirm Changes** and click **Save** to save your settings.

4. (Optional) To run a data deletion job, click the **Create Data Deletion Job** button.

a. In the Create Data Deletion Job dialog box, select one or more data types for which you wish to delete data.

The available choices are:

- **Device**
- **System Metrics and Custom Metrics**
- **Sensor**

b. Under **Delete Data**, choose the time period for which you wish to delete the data.

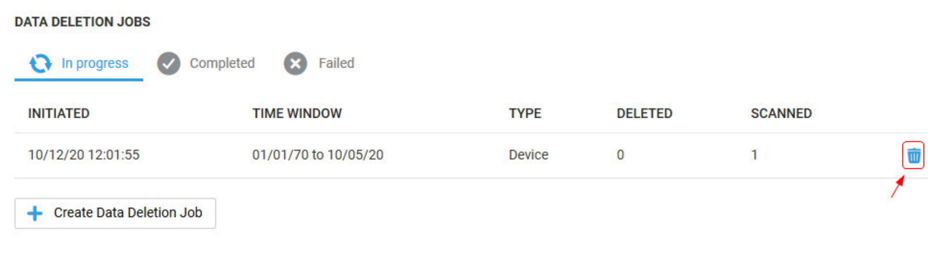
For example, you may want to delete sensor data that is **Older than 30 days**.

You can also choose a custom **Time Range** for which to delete data. For example, you may wish to delete data for a particular day or hour.

c. Click **Delete** to create the delete job.

You can monitor the job progress, and the number of records that were deleted, under the Data Deletion Jobs section. When the data delete job completes, its status changes from **In Progress** to **Completed**.

You can also choose to delete a data deletion job. If the job is still running when you delete it, then the job is terminated and deleted. If the job has already failed or completed, then deleting the job simply removes it from the list of failed or completed jobs.



Use External Storage Options for Long-Term Data Availability and Analysis

You can choose to use one of the external storage options, namely Oracle Autonomous Database or OCI Object Storage, to safely and cost-effectively store your IoT sensor and analytics data for long-term persistence.

The application can use your external storage to store raw or aggregated sensor attribute data, and data related to analytics artifacts, such as metrics, anomalies, predictions, and trends. You can also store your rule incidents and warnings. You can use the historical data for visualization and analysis in external and third party applications.

You can use the rich querying functionality in Oracle Autonomous Database, or chart and analyze the stored data in external applications, such as Oracle Analytics Cloud. For example, you can use analyses, projects, and dashboards in Analytics Cloud to find the answers that you need from key IoT data displayed in graphical formats. You can use applications such as Oracle Visual Builder to create dashboards and mashups.

Use OCI Object Storage to Store Historical IoT Data

The Oracle Cloud Infrastructure (OCI) Object Storage service is an internet-scale, high-performance storage platform that offers reliable and cost-efficient data durability. If you have a subscription for OCI Object Storage, you can use it to store your IoT sensor and analytics data for long-term persistence.

You can learn more about OCI Object Storage here:

- Overview of Object Storage

- Get Started with Object Storage

Use the following steps to add and configure your external OCI Object Storage:

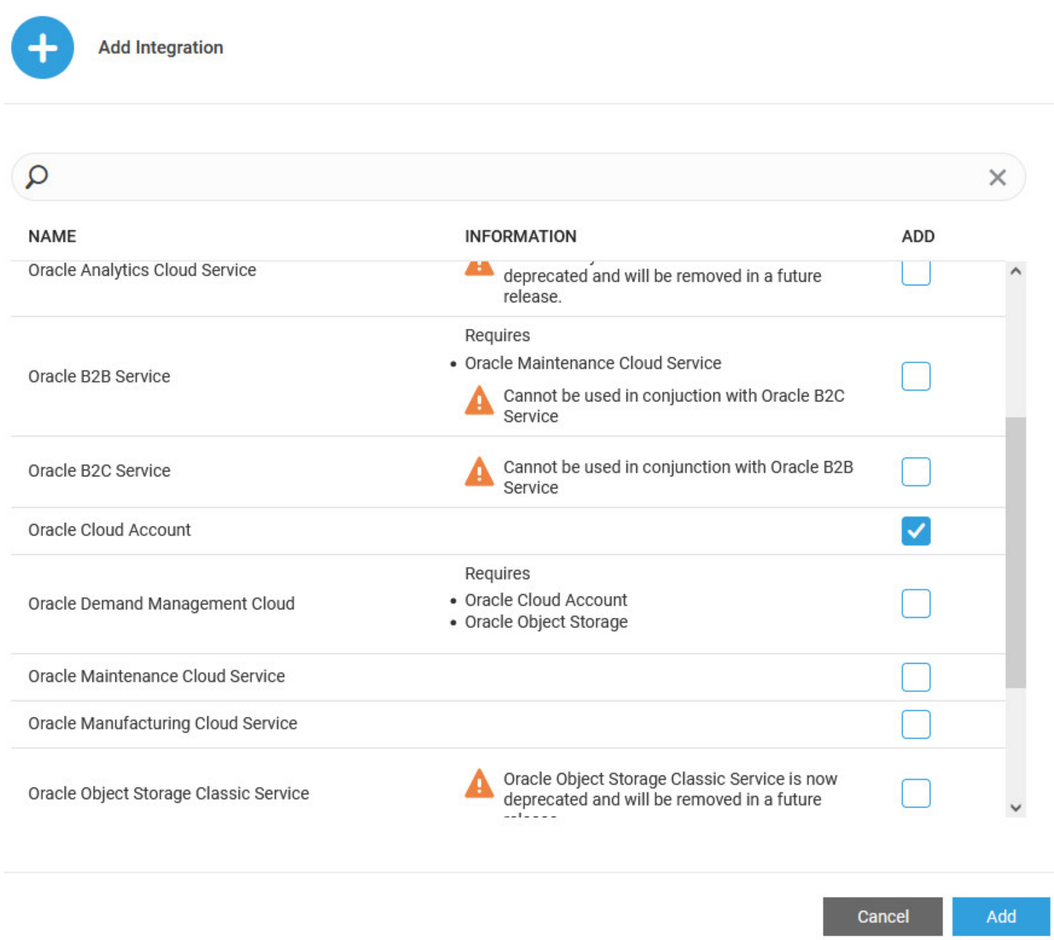
1. Add an Oracle Cloud Account
2. Connect to an OCI Object Storage Instance
3. Add and Configure Your External OCI Object Storage Integration

Add an Oracle Cloud Account

Use the **Settings > Integrations** page in your IoT application to configure an Oracle Cloud account. This Oracle Cloud account is used when specifying integration settings, such as OCI Object Storage settings.

1. In your IoT application, click **Menu** (☰), and then click **Settings**.
2. Click **Integrations**.
3. Click **Add** + to add a new integration.
4. In the Add Integration dialog, select **Oracle Cloud Account** and click **Add**.

   Tip: You can also search for an integration name in the list.

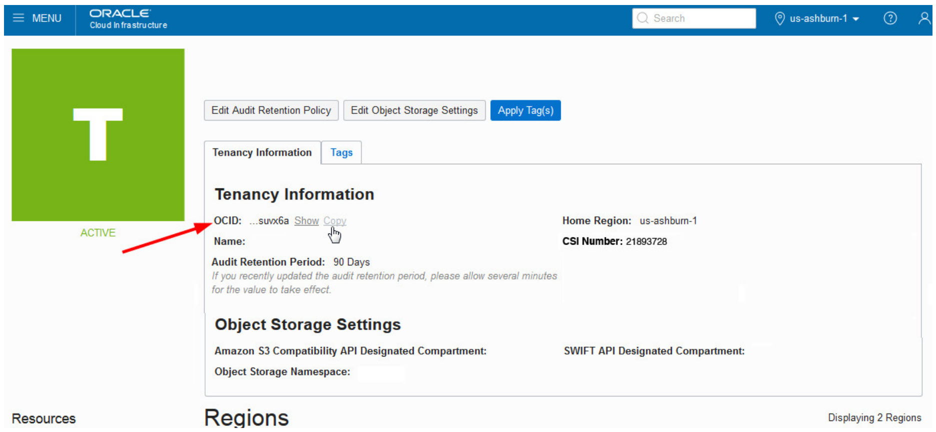
   Oracle Cloud Account integration gets added to the Integrations page.

5. Under **Oracle Cloud Account**, add your cloud account details:

   a. Enter your **Tenant OCID**.

      The tenancy details are available from the Oracle Cloud Infrastructure Console. You need to log in to your Oracle Cloud Infrastructure Console. From the **Profile** menu, click **Tenancy: <YourTenancyName>**.

      The tenancy OCID is shown under Tenancy Information. Click **Copy** to copy it to your clipboard.

      Paste this value under **Tenant OCID** in your IoT application.

   b. Enter the **User OCID**.

      The user details are available from the Oracle Cloud Infrastructure Console. You need to log in to your Oracle Cloud Infrastructure Console. From the **Profile** menu, click **User Settings**.

      The user OCID is shown under User Information. Click **Copy** to copy it to your clipboard.

      Paste this value under **User OCID** in your IoT application.

   c. Under Public Key, click **Generate**.

   d. Click **Close**.

6. Set the public key in OCI Object Storage.

   a. On the **Settings>Integration** page of your IoT application, under **Oracle Cloud Account**, click **Copy** against **Public Key** to copy the public key that you generated earlier.

   b. Log in to your Oracle Cloud Infrastructure Console.

   c. Under the **Profile** menu, click **User Settings**.

   d. Click **API Keys** under **Resources**.

   e. Click **Add Public Key**.

      Note: If three public keys are already listed under API Keys, you have to first delete one public key. An OCI Object Storage service user can't have more than three public keys.

   f. Select **Paste Public Keys** and paste the key that you copied from your IoT application.

g. Click **Add**.

   The fingerprint for the added public key appears under API Keys. The fingerprint should be the same as that displayed on the Settings page of your IoT application.

Connect to an OCI Object Storage Instance

Use the Integrations page in your IoT application to configure OCI Object Storage connection details and to enable Object Storage.

Before configuring the OCI Object Storage connection, you should have already added your Oracle Cloud account on the Settings page.

1. In your IoT application, click **Menu** (≡), and then click **Settings**.
2. Click **Integrations**.
3. Click **Add** + to add a new integration.
4. In the Add Integration dialog, select **Oracle Object Storage Service** and click **Add**.

   Tip: You can also search for an integration name in the list.

   Oracle Object Storage integration gets added to the Integrations page.
5. On the Integrations page, under Object Storage Service, click **Connect**.
6. In the Oracle Object Storage dialog, provide your object storage connection details.
   a. Enter the **Storage URL** for your OCI Object Storage.

      For example, `https://objectstorage.us-phoenix-1.oraclecloud.com`.
   b. Enter the object storage **Namespace** for your tenancy.

      You can find the object storage namespace in your Oracle Cloud Infrastructure Console. You need to log in to your Oracle Cloud Infrastructure Console. From the **Profile** menu, click **Tenancy: <YourTenancyName>**.
   c. Enter the **Default Bucket** name that stores the data.

      The bucket name must already exist in your OCI Object Storage instance.
   d. Click **Verify Connectivity** to verify the connection details and bucket name.
   e. Click **Save** to save the OCI Object Storage connection details.
7. To enable the connection on the Integrations page, click **Edit Configuration** under **Oracle Object Storage**.
8. Toggle the **Integration Status** switch to ON, and click **Save**.

Add and Configure Your External OCI Object Storage Integration

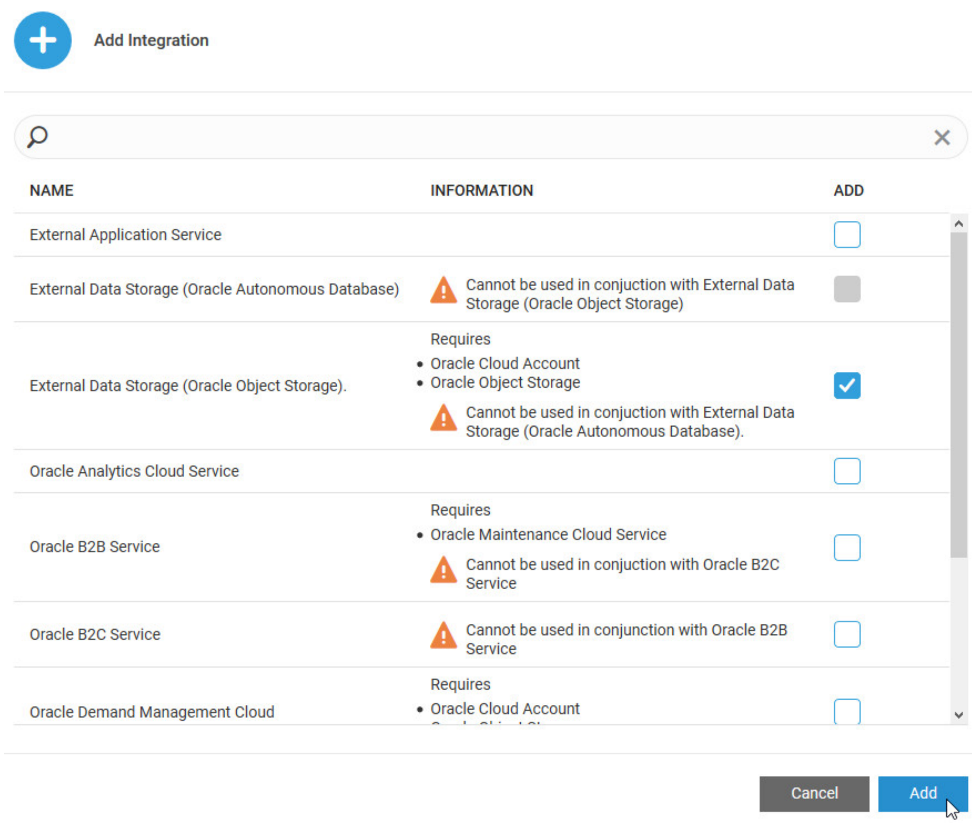
To start storing IoT historical data in your OCI Object Storage, add and configure a new integration for **External Data Storage (Oracle Object Storage)**.

> **Note:**
>
> You should have already added an Oracle Cloud account and specified the connection settings for your OCI Object Storage instance.

Video

1. In your IoT application, click **Menu** (≡), and then click **Settings**.
2. Click **Integrations**.
3. Click **Add** + to add a new integration.
4. In the Add Integration dialog, select **External Data Storage (Oracle Object Storage)** and click **Add**.

   Tip: You can also search for an integration name in the list.

   > **Note:**
   >
   > You can only have one external data storage integration at a time. So, you cannot add both Oracle Autonomous Database and Oracle Object Storage integrations at the same time. If you need to switch from Oracle Autonomous Database integration to Oracle Object Storage, you should first remove the Oracle Autonomous Database integration from the Integrations page.

   The **External Data Storage (Oracle Object Storage)** integration gets added to the Integrations page.

5. On the Integrations page, under **External Data Storage (Oracle Object Storage)**, click **Edit Configuration**.

a. Optionally enter a **File Prefix**.

   Your IoT application prefixes the specified **File Prefix** to the file names that it stores in OCI Object Storage. This helps with easy identification of files.

b. The **Default Bucket** is pre-populated with the bucket that you have used in your Object Storage connection settings.

c. Optionally change the **Export Interval** if you want your application to write more frequently to OCI Object Storage.

   The default data export interval is **4 Hours**.

d. Select the IoT data that you wish to store externally:

   - **Attributes:** You can choose to export all raw sensor attribute data. Alternatively, you can choose to export only aggregated attribute data, which exports aggregates, such as *Average*, *Maximum*, and *Minimum* values of your attribute values. Under **Attributes Granularity Level**, select **Aggregated** to export only aggregated attribute data. Under **Attributes Granularity Level Interval** , specify the aggregation interval. This determines the frequency at which the aggregated values are calculated.

     If you select **None (raw data)**, then all raw sensor data is exported.

   - **Metrics:** Select to export metric data corresponding to system metrics and computed metrics.
   - **Anomalies:** Select to export anomaly data.
   - **Predictions:** Select to export prediction data.
   - **Trends:** Select to export data related to trends.
   - **Incidents:** Select to export your rule incidents.
   - **Warnings:**Select to export your rule warnings.

e. Toggle the **Integration Status** switch to **Enabled**.

6. Click **Save** to save your configuration settings.

Use Oracle Autonomous Database to Store Historical IoT Data

Oracle Autonomous Database runs on Oracle Cloud Infrastructure and provides workload-optimized cloud services for transaction processing and data warehousing. If you have a subscription for Oracle Autonomous Database, you can use it to store your IoT sensor and analytics data for long-term persistence.

You can choose either an Oracle Autonomous Transaction Processing database , or an Oracle Autonomous Data Warehouse database to externally store your IoT data.

You can learn more about Oracle Autonomous Database options here:

- Oracle Autonomous Database Solutions
- Getting Started with Autonomous Transaction Processing
- Getting Started with Autonomous Data Warehouse

Use the following steps to add and configure your external Oracle Autonomous Database storage:

Video

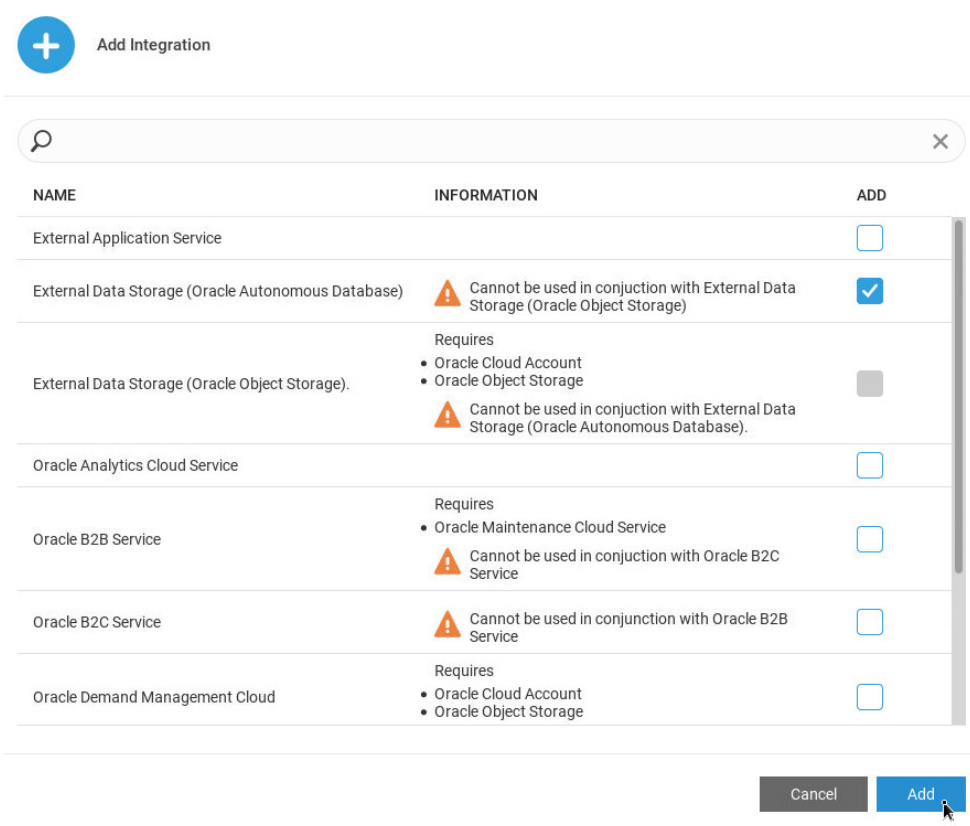
1. Add an Oracle Autonomous Database Integration
2. Enable and Configure the Oracle Autonomous Database Integration

Add an Oracle Autonomous Database Integration

To start storing IoT historical data in an Oracle Autonomous Database, add and configure a new integration for **External Data Storage (Oracle Autonomous Database)**.

1. In your IoT application, click **Menu** (≡), and then click **Settings**.
2. Click **Integrations**.
3. Click **Add** + to add a new integration.
4. In the Add Integration dialog, select **External Data Storage (Oracle Autonomous Database)** and click **Add**.

   Tip: You can also search for an integration name in the list.



> **Note:**
>
> You can only have one external data storage integration at a time. So, you cannot add both Oracle Autonomous Database and Oracle Object Storage integrations at the same time. If you need to switch from Oracle Object Storage integration to Oracle Autonomous Database, you should first remove the Oracle Object Storage integration from the Integrations page.

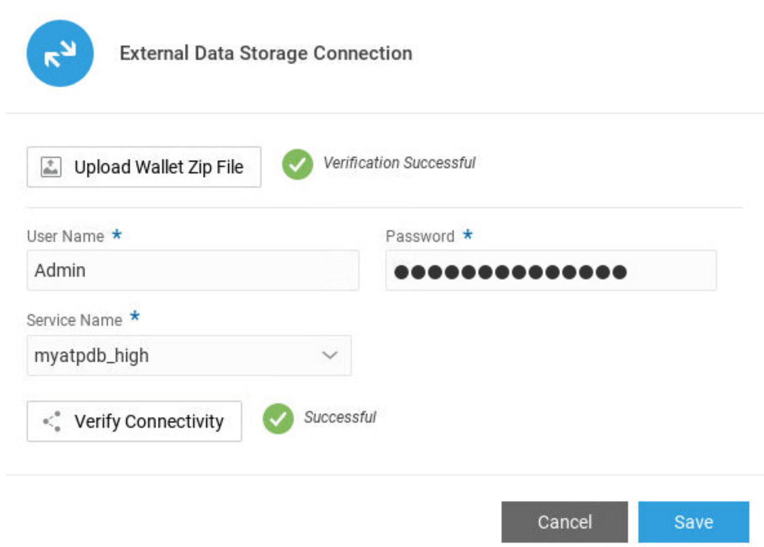
The **External Data Storage (Oracle Autonomous Database)** integration gets added to the Integrations page.

5. On the Integrations page, under **External Data Storage (Oracle Autonomous Database)**, click **Connect** to specify the connection details.
   a. In the External Data Storage Connection dialog, click **Upload Wallet Zip File** to upload the wallet required to securely connect to your database.

      Oracle client credentials (wallet files) are downloaded from Oracle Autonomous Database by a service administrator. If you are not the database administrator, your administrator should provide you with the client credentials. The wallet file for the ATP/ADW database can be downloaded from the ATP/ADW service console.

      After you upload the wallet file, the application verifies the wallet and prompts you for the database login credentials.
   b. Enter the **User Name** and **Password** used to log into the database.
   c. Select the **Service Name** for the database.

      The list of service name options is retrieved from the wallet that you uploaded earlier.
   d. Click **Verify Connectivity** to verify connectivity to your Oracle Autonomous Database instance.



      The **Save** button is enabled after successful verification of the connection credentials.
6. Click **Save** to save your Oracle Autonomous Database connection settings.

Enable and Configure the Oracle Autonomous Database Integration

To start storing IoT historical data in your Oracle Autonomous Database, enable and configure the integration for **External Data Storage (Oracle Autonomous Database)**.

1. In your IoT application, click **Menu** (☰), and then click **Settings**.
2. Click **Integrations**.
3. Under **External Data Storage (Oracle Autonomous Database)**, click **Edit Configuration**.
   a. Optionally enter a **Table Prefix**.

      Your IoT application prefixes the specified **Table Prefix** to the table names that it creates in Oracle Autonomous Database. This helps with easy identification of tables.
   b. Optionally change the **Export Interval** if you want your application to write more frequently to Oracle Autonomous Database.

      The default data export interval is **4 Hours**.
   c. Select the IoT data that you wish to store externally:
      - **Attributes:** You can choose to export all raw sensor attribute data. Alternatively, you can choose to export only aggregated attribute data, which exports aggregates, such as *Average*, *Maximum*, and *Minimum* values of your attribute values. Under **Attributes Granularity Level**, select **Aggregated** to export only aggregated attribute data. Under **Attributes Granularity Level Interval** , specify the aggregation interval. This determines the frequency at which the aggregated values are calculated.

        If you select **None (raw data)**, then all raw sensor data is exported.
      - **Metrics:** Select to export metric data corresponding to system metrics and computed metrics.
      - **Anomalies:** Select to export anomaly data.
      - **Predictions:** Select to export prediction data.
      - **Trends:** Select to export data related to trends.
      - **Incidents:** Select to export your rule incidents.
      - **Warnings:**Select to export your rule warnings.
   d. Toggle the **Integration Status** switch to **Enabled**.
4. Click **Save** to save your configuration settings.

Use Oracle Analytics Cloud to Chart and Analyze Externally Stored Data

You can chart and analyze the stored data in external applications, such as Oracle Analytics Cloud. For example, you can use analyses, projects, and dashboards in

Analytics Cloud to find the answers that you need from key IoT data displayed in graphical formats.

Video

7 Integrate with Other Cloud and Oracle Services

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 Fusion Cloud Maintenance with Oracle IoT Asset Monitoring Cloud Service

You can import assets from Oracle Fusion Cloud Maintenance into Oracle Internet of Things (IoT) Asset Monitoring Cloud Service.

You can choose the Oracle Internet of Things (IoT) Asset Monitoring Cloud Service organization into which your Oracle Fusion Cloud Maintenance assets are imported. Alternatively, you can choose to create one-to-one mappings between Oracle SCM Cloud organizations and Oracle IoT Asset Monitoring Cloud Service organizations. Oracle IoT Asset Monitoring Cloud Service then creates a separate organization for each Oracle SCM Cloud organization from which assets are imported.

After you import assets and associate them with sensors, an incident generated for an imported asset in Oracle IoT Asset Monitoring Cloud Service automatically generates a work order in Oracle Fusion Cloud Maintenance. For example, if a threshold rule triggers an incident when a device associated with an asset overheats, a work order that corresponds to the incident is automatically created in Oracle Fusion Cloud Maintenance.

When you release, close, cancel, or modify a work order in Oracle Fusion Cloud Maintenance, the status of the corresponding incident is automatically updated in Oracle IoT Asset Monitoring Cloud Service. You can configure the synchronization frequency between Oracle IoT Asset Monitoring Cloud Service and Oracle Fusion Cloud Maintenance.

> **Note:**
>
> If you manually modify the status of an incident in Oracle IoT Asset Monitoring Cloud Service, the change is not synchronized with the work order in Oracle Fusion Cloud Maintenance.

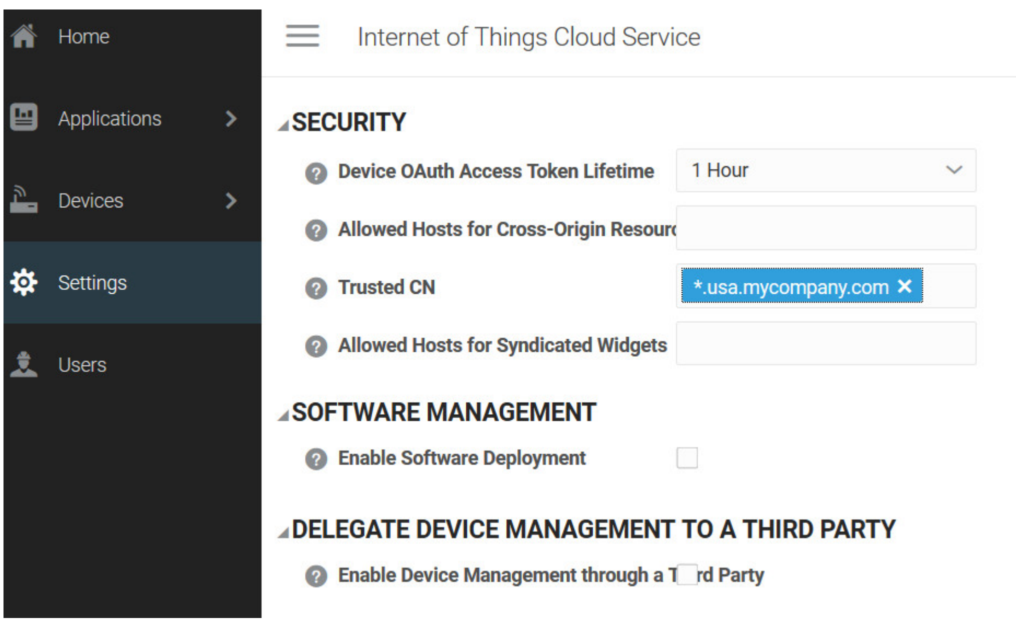
See Also: Integrate Oracle Maintenance Cloud with Oracle IoT Asset Monitoring Cloud in the *Implementing Manufacturing and Supply Chain Materials Management* guide.

Add an Oracle Fusion Cloud Maintenance Integration

Use the Integrations page in Oracle Internet of Things (IoT) Asset Monitoring Cloud Service to add an integration for Oracle Fusion Cloud Maintenance.

Before you configure Oracle Fusion Cloud Maintenance integration, make sure your Oracle Fusion Cloud Maintenance host is trusted by your Oracle Internet of Things Intelligent Applications Cloud domain.

Host names with `.oraclecloud.com` and `.oraclecloudapps.com` suffixes are always allowed. If your Oracle Fusion Cloud Maintenance domain name is different, then add the domain as a trusted CN in the Oracle Internet of Things Intelligent Applications Cloud management console. To do this, add `*.`*`YourDomain`*`.com` under **Trusted CN** in the Settings page.



You can access your Oracle Internet of Things Intelligent Applications Cloud management console at the following URL:

```
https://hostname/ui
```

Here, *`hostname`* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.

To enable integration with Oracle Fusion Cloud Maintenance:

1. In Oracle IoT Asset Monitoring Cloud Service, click **Menu** (≡), and then click **Settings**.

   You can access Oracle IoT Asset Monitoring Cloud Service at the following URL:

   `https://`*`hostname`*`/am`

   Here, *`hostname`* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.

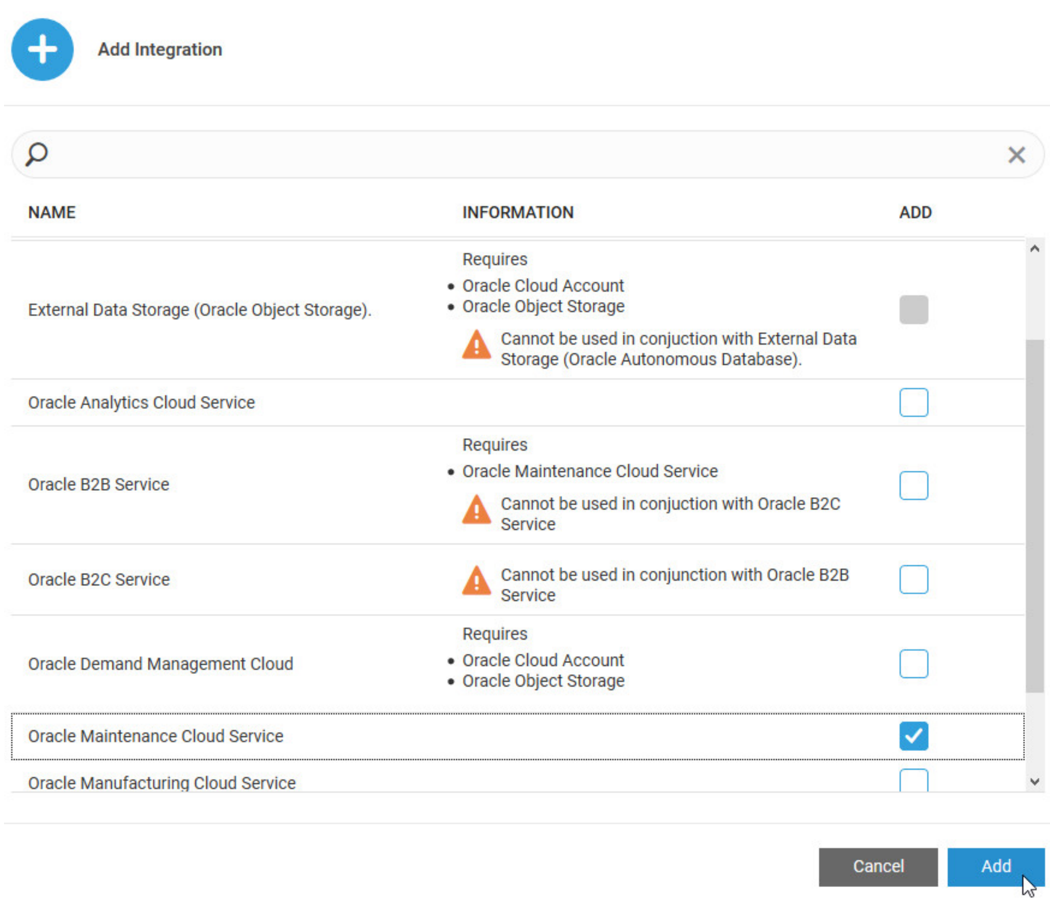
   If you are in the Design Center, you need to click **Previous** (<) before you see the **Settings** option in the menu.

2. Click **Integrations**.

3. Click **Add** + to add a new integration.

4. In the Add Integration dialog, select **Oracle Maintenance Cloud Service** and click **Add**.

   Tip: You can also search for an integration name in the list.



   Oracle Maintenance Cloud Service integration gets added to the Integrations page.

5. On the Integrations page, under **Oracle Maintenance Cloud Service**, click **Connect**.

6. Specify the **Service URL** for your Oracle Fusion Cloud Maintenance instance.

   The Service URL is the URL of your Oracle Fusion Cloud Maintenance host. No port number is necessary here.

   For example: `https://MyMntCloud.oraclecloud.com`.

7. Specify the **User Name** for your Oracle Fusion Cloud Maintenance instance.
8. Specify the **Password** for your Oracle Fusion Cloud Maintenance instance.
9. Click **Verify Connectivity** to verify connectivity to the Oracle Fusion Cloud Maintenance instance.

   If the connection succeeds, then the **Save** button gets enabled.
10. Click **Save** to save the connection settings.

Enable and Configure the Oracle Fusion Cloud Maintenance Integration

To start using Oracle Fusion Cloud Maintenance integration, enable and configure the integration for **Oracle Maintenance Cloud Service** on the Integrations page.

1. In Oracle IoT Asset Monitoring Cloud Service, click **Menu** (), and then click **Settings**.

   If you are in the Design Center, you need to click **Previous** () before you see the **Settings** option in the menu.
2. Click **Integrations**.
3. Under **Oracle Maintenance Cloud Service**, click **Edit Configuration**.
4. Toggle the **Integration Status** switch to **ON**.

   This enables your Oracle Fusion Cloud Maintenance integration.
5. Specify the **Synchronization** frequency in minutes.

   The sync frequency determines how often Oracle IoT Asset Monitoring Cloud Service syncs with Oracle Fusion Cloud Maintenance.
6. Click **Save** to save your configuration settings.
7. (Optional) Select the **Object Storage Integration** to use for storing external data received from Oracle Fusion Cloud Maintenance.

   External data such as asset data, work order data, and maintenance schedules from Oracle Fusion Cloud Maintenance 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 Fusion Cloud Maintenance.
8. If you chose **Object Storage Integration**, then specify a corresponding **Object Storage Container** name, or bucket name, to store the Oracle Fusion Cloud Maintenance data.
9. Under **Oracle SCM Organizations Mapping**, map your Oracle SCM Cloud organizations to one or more Oracle IoT Asset Monitoring Cloud organizations.

   - **One to One**: Lets you create one-to-one mappings between Oracle SCM Cloud organizations and Oracle IoT Asset Monitoring Cloud Service organizations. Oracle IoT Asset Monitoring Cloud Service automatically creates a separate organization for each Oracle SCM Cloud organization from which assets are imported. This helps separate the assets into their respective organizations in Oracle IoT Asset Monitoring Cloud Service.
   - **Many to One**: Lets you choose one organization in Oracle IoT Asset Monitoring Cloud Service where your Oracle Fusion Cloud Maintenance

assets are imported. Assets imported from different Oracle SCM Cloud organizations are imported into the same Oracle IoT Asset Monitoring Cloud Service organization. **Select an IoT Organization** to use for the many-to-one mapping.

> **Note:**
>
> If you change the mapping settings for an existing Oracle Fusion Cloud Maintenance integration, the changed mapping applies to assets from new Oracle SCM Cloud organizations only. The already mapped Oracle SCM Cloud organizations are not affected.

Automatically Sync New Assets and Asset Attribute Updates

Set up Oracle Fusion Cloud Maintenance to automatically sync new assets with your Oracle Internet of Things (IoT) Asset Monitoring Cloud Service instance. Updates to asset attributes in Oracle Fusion Cloud Maintenance are also pushed to Oracle Internet of Things (IoT) Asset Monitoring Cloud Service.

You need to add your Oracle Internet of Things (IoT) Asset Monitoring Cloud Service information in Oracle Fusion Cloud Maintenance.

1. In Oracle Fusion Cloud Maintenance, click **Menu** ≡, and then click **Setup and Maintenance**.
2. Click **Tasks** and click **Search**.

   Alternatively, you can select **Manufacturing and Supply Chain Materials Management** under **Setup**.
3. Search for the following string: `Manage Asset Maintenance Parameters`.
4. Click **Manage Asset Maintenance Parameters** in the search results.
5. Click **Enable IoT** and specify the connection details for your Oracle Internet of Things (IoT) Asset Monitoring Cloud Service instance.
   - **URL**: Use the following format:

     `https://`*`hostname`*`/assetMonitoring`

     Here, *`hostname`* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.
   - **User Name**: Specify the user name for connecting to your Oracle IoT Asset Monitoring Cloud Service instance.
   - **Password**: Specify the password for connecting to your Oracle IoT Asset Monitoring Cloud Service instance.

   > **Note:**
   >
   > If you change the password for connecting to your Oracle IoT Asset Monitoring Cloud Service instance in future, then you must update the password in Oracle Fusion Cloud Maintenance.
6. Click **Save and Close**.

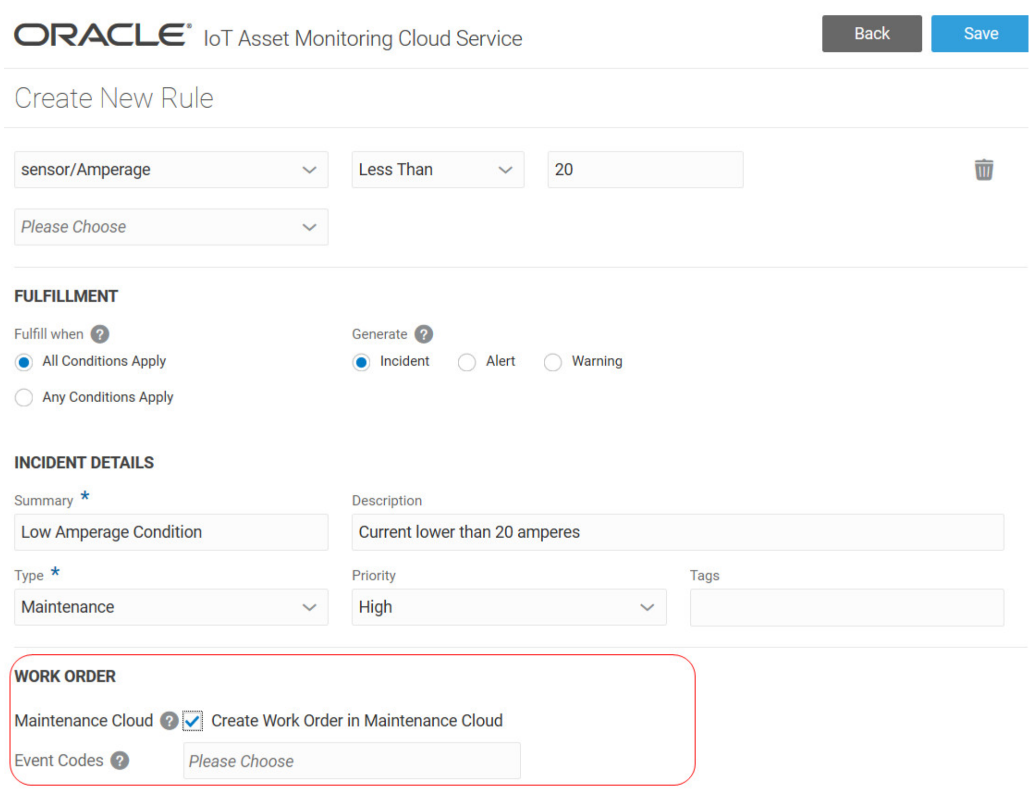
See Also: How Assets are Synchronized with Oracle IoT Asset Monitoring Cloud in the *Oracle SCM Cloud Using Maintenance* guide.

Configure Rules to Generate Automatic Work Orders

Configure rules to automatically create work orders in Oracle Fusion Cloud Maintenance 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 Fusion Cloud Maintenance.
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**.



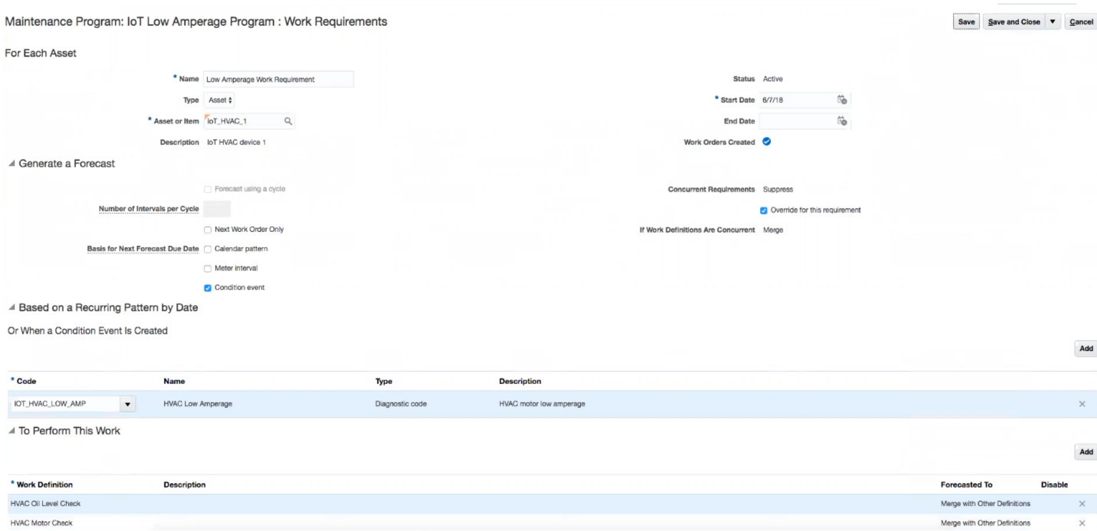
If you have defined condition event codes in Oracle Fusion Cloud Maintenance for your IoT assets, then you can pass the event code corresponding to the incident back to Oracle Fusion Cloud Maintenance. Select the **Event Codes** to pass to Oracle Fusion Cloud Maintenance when the incident rule is triggered.

See Also: How You Manage Condition Event Codes in the *Oracle SCM Cloud Using Maintenance* guide.

You can define maintenance programs in Oracle Fusion Cloud Maintenance 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 Fusion Cloud Maintenance 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 Fusion Cloud Maintenance triggers the HVAC oil check and motor check work orders.



Verify and Update the Work Orders in Oracle Fusion Cloud Maintenance

When an incident is created for an imported asset in Oracle Internet of Things (IoT) Asset Monitoring Cloud Service, a corresponding work order is automatically created in Oracle Fusion Cloud Maintenance.

See Also: How Work Orders Are Automatically Created with Oracle IoT Asset Monitoring Cloud in the *Oracle SCM Cloud Using Maintenance* guide.

> **Note:**
>
> The scheduler job synchronizes Oracle Fusion Cloud Maintenance with Oracle IoT Asset Monitoring Cloud Service every 5 minutes.

1. Sign in to your Oracle Fusion Cloud Maintenance instance.
2. Navigate to **Maintenance Management**.
3. Under **Tasks**, select **Manage Maintenance Work Orders**.
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 Fusion Cloud Maintenance, 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 Fusion Cloud Maintenance, 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 Fusion Cloud Maintenance, the associated incident status is automatically updated in Oracle Internet of Things (IoT) Asset Monitoring Cloud Service.

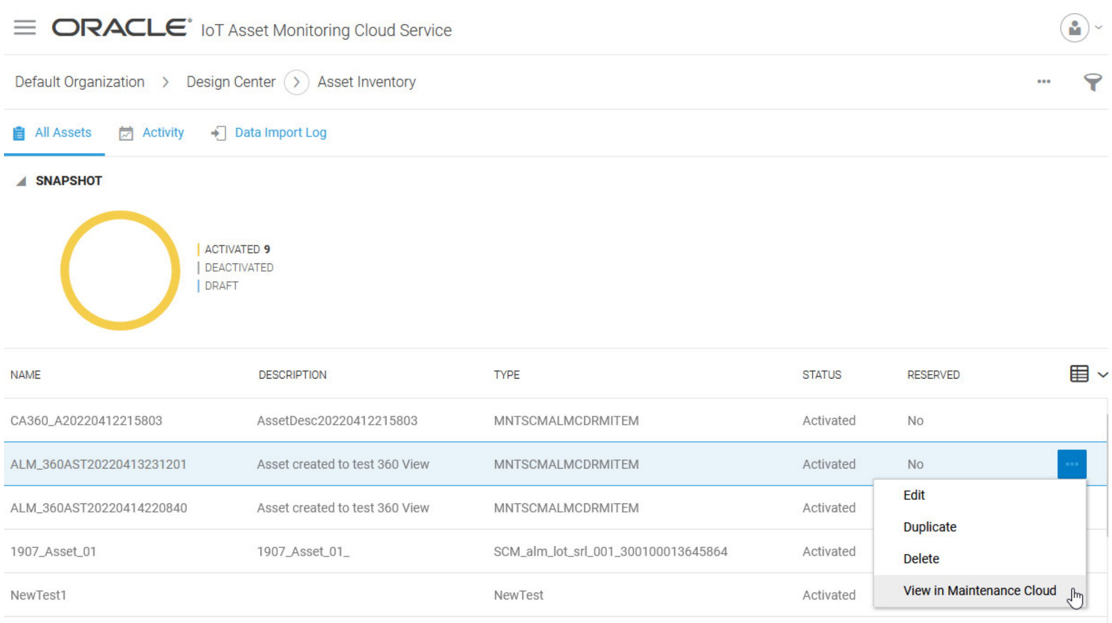
> **Note:**
>
> The scheduler job synchronizes Oracle Fusion Cloud Maintenance with Oracle IoT Asset Monitoring Cloud Service every 5 minutes.

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.

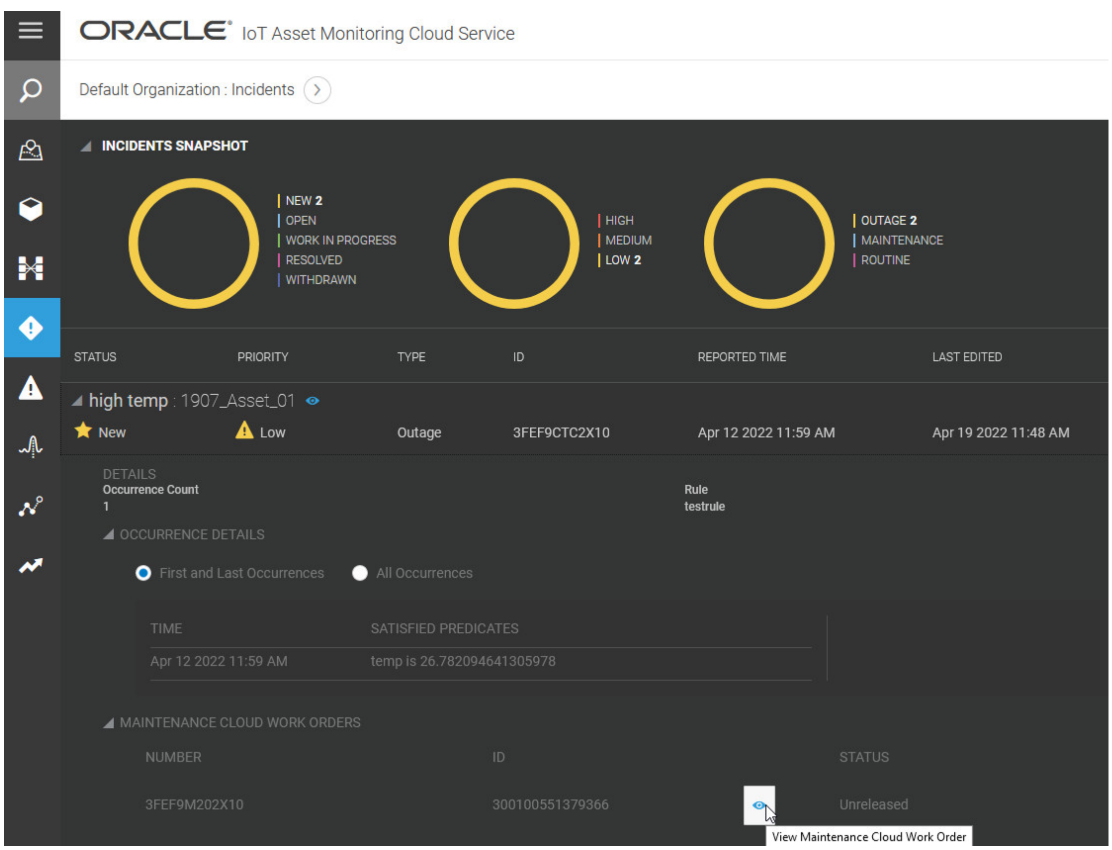
Use Asset and Work Order Maintenance Cloud Links

You can use the Assets page to open an imported asset directly in Oracle Fusion Cloud Maintenance. You can also open a maintenance work order linked to an asset incident from the Incidents page.

Use the **Operations Center > Assets** page or the **Design Center > Asset Inventory** to view your assets. Choose the **View in Maintenance Cloud** option against an asset row to open the imported asset directly in Oracle Fusion Cloud Maintenance.



When a rule incident has an associated work order, you can open the work order directly in Oracle Fusion Cloud Maintenance from the Incidents page in Operations Center. The link is available under the **Maintenance Cloud Work Orders** section for the incident.

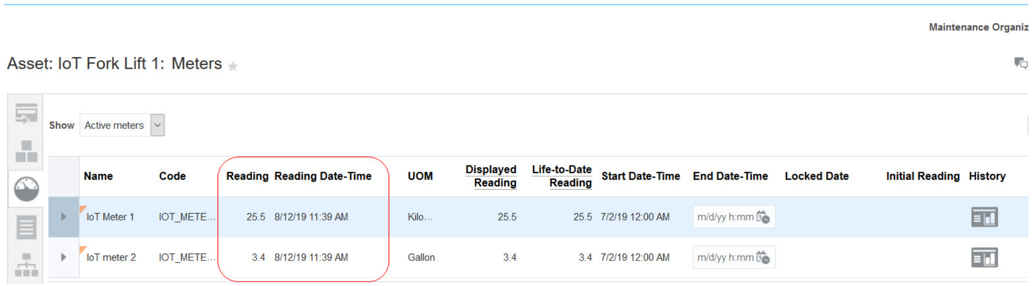


Automatically Update Asset Meters in Oracle Fusion Cloud Maintenance with IoT Data

Oracle Fusion Cloud Maintenance 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 Fusion Cloud Maintenance. 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 Fusion Cloud Maintenance meter readings, which represent the odometer and fuel usage values from sensor devices of a forklift device.

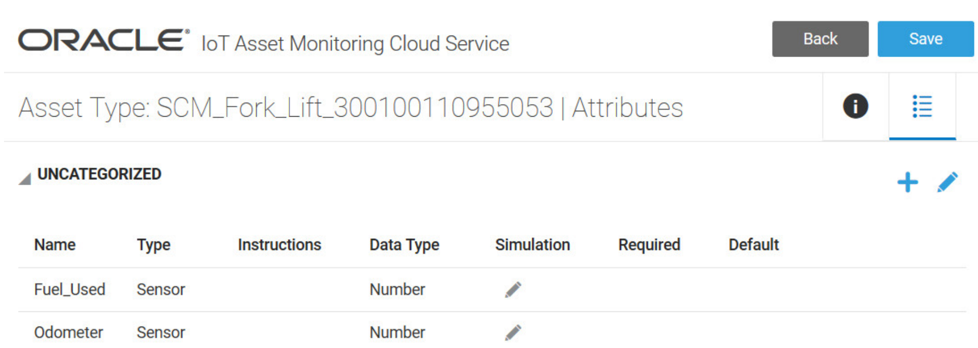


See Also: How Meter Readings Are Automatically Created with Oracle IoT Asset Monitoring Cloud in the *Oracle SCM Cloud Using Maintenance* guide.

If you already have assets with meters in Oracle Fusion Cloud Maintenance, 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 Fusion Cloud Maintenance meters.

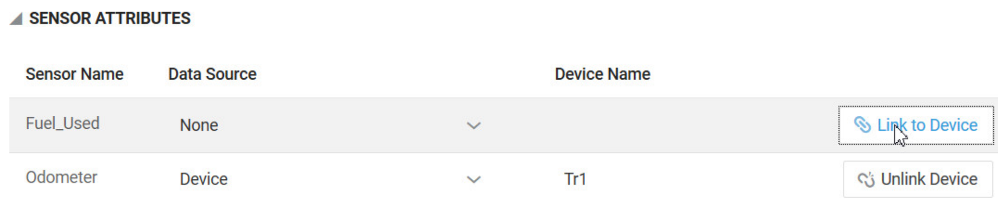
   For example, if you have imported forklift assets that use meters for fuel and distance, you need to add sensor attributes corresponding to the fuel meter and odometer.

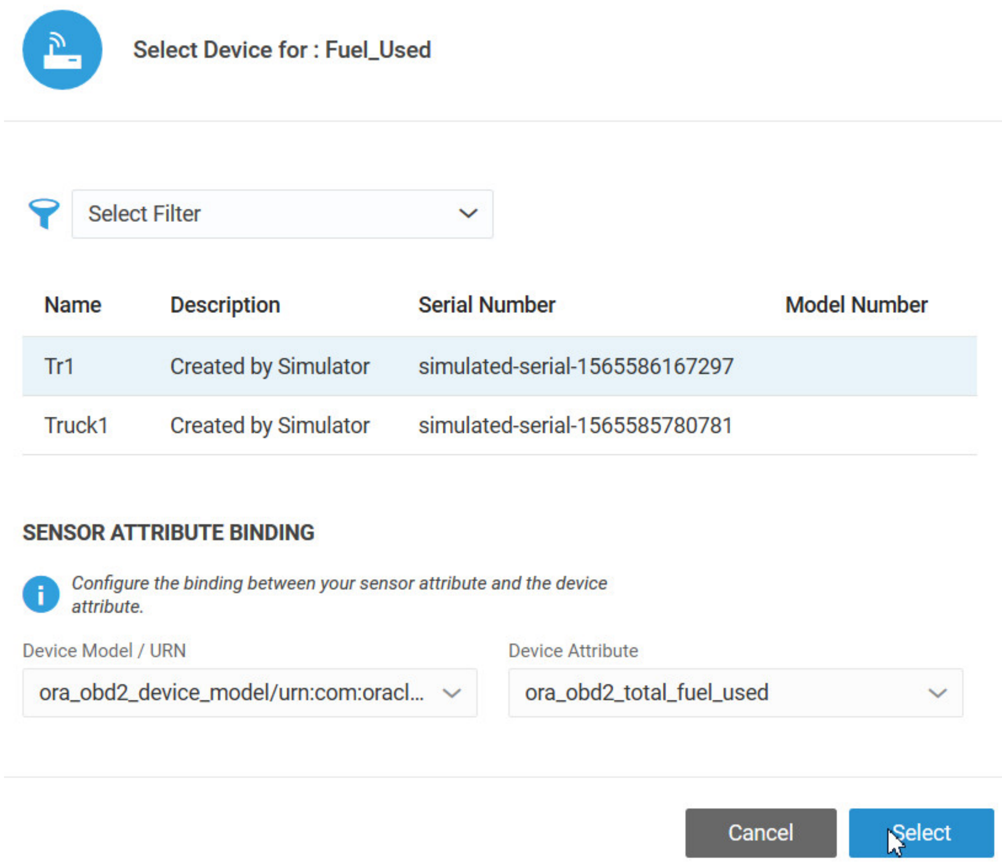


See Edit an Asset Type for more information on editing an asset type to add sensor attributes.

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.



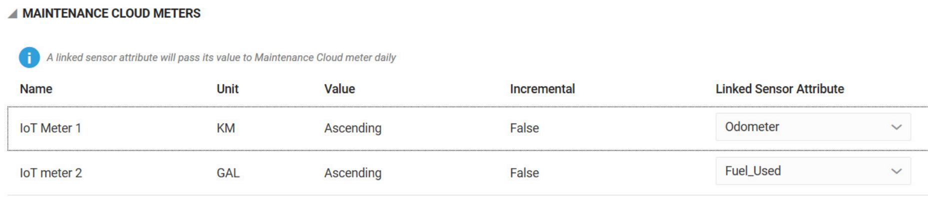


   For more information on editing assets, see Edit Asset Details.

   b. Repeat the previous step for any more sensor attributes that you created.

3. Associate the sensor attributes with their corresponding Oracle Fusion Cloud Maintenance meters.

   a. Under the **Maintenance Cloud Meters** section on the Edit Asset page, select **Linked Sensor Attribute** corresponding to each Oracle Fusion Cloud Maintenance meter.



b. Click **Save** on the Edit Asset page.

The scheduler job sends meter readings back to Oracle Fusion Cloud Maintenance once every day.

Optimize Maintenance Intervals in Oracle Fusion Cloud Maintenance

Oracle Fusion Cloud Maintenance uses maintenance programs for managing asset maintenance. Oracle IoT Asset Monitoring Cloud Service can use IoT analytics on historical data from Oracle Fusion Cloud Maintenance to help provide maintenance interval recommendations for these maintenance programs.

Optimal maintenance of assets reduces unplanned failures, and helps minimize maintenance costs. The key to optimized maintenance is to ensure that assets receive the maintenance they need before parts fail. At the same time, optimization ensures that parts aren't replaced too soon, while they still have significant useful life.

For example, say you wish to optimize the maintenance programs on the data servers in your data center. The preventive maintenance guideline from the manufacturer recommends replacing hard drives every 365 days. Your maintenance programs in Oracle Fusion Cloud Maintenance are designed to follow this recommendation. Over time, some hard drives fail before reaching their scheduled maintenance interval, perhaps because data updates in your environment are more frequent than standard. Optimization helps analyze all the historical failures and replacements, and calculate the anticipated lifespans for critical parts. Oracle IoT Asset Monitoring Cloud Service then makes maintenance interval recommendations for the business' target reliability rate. You may accept these recommendations in Oracle Fusion Cloud Maintenance to slightly reduce the maintenance interval in your environment.

Oracle Fusion Cloud Maintenance provides the required historical data for analysis through OCI Object Storage using BICC (Oracle Business Intelligence Cloud Connector). Oracle IoT Asset Monitoring Cloud Service performs analysis on the ingested data to create recommendations for Oracle Fusion Cloud Maintenance. External data such as asset data, work order data, and maintenance schedules from Oracle Fusion Cloud Maintenance are 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 Fusion Cloud Maintenance.

Set Up Maintenance Interval Recommendations

Set up the Oracle IoT Asset Monitoring Cloud Service URL and credentials in Oracle Fusion Cloud Maintenance. Next, configure the external storage details in BICC (Oracle Business Intelligence Cloud Connector) and Oracle IoT Asset Monitoring Cloud Service. Finally, run the scheduled jobs in Oracle Fusion Cloud Maintenance to ingest data and trigger learning.

1. Enable IoT Integration in Oracle Fusion Cloud Maintenance

2. Enable the Integration and Configure OCI Cloud Storage Details in Oracle IoT Asset Monitoring Cloud Service
3. Configure OCI Object Storage in BICC
4. Configure BICC to Generate Gzip Extract Files
5. Extract Key Maintenance Data from Oracle Maintenance Cloud
6. Perform Learning on Maintenance Data

Enable IoT Integration in Oracle Fusion Cloud Maintenance

Add your Oracle Internet of Things (IoT) Asset Monitoring Cloud Service instance information in Oracle Fusion Cloud Maintenance.

1. In Oracle Fusion Cloud Maintenance, click **Menu** ≡, and then click **Setup and Maintenance** under **My Enterprise**.

   The logged in user should have the SCM Implementation Consultant role in Oracle Fusion Cloud Maintenance to complete this exercise.

2. Click **Tasks** and click **Search**.

   Alternatively, you can select **Manufacturing and Supply Chain Materials Management** under **Setup**.

3. Search for the following string: `Manage Asset Maintenance Parameters`.
4. Click **Manage Asset Maintenance Parameters** in the search results.
5. Click **Enable IoT** and specify the connection details for your Oracle Internet of Things (IoT) Asset Monitoring Cloud Service instance.
   - **URL**: Use the following format:

     `https://`*`hostname`*`/assetMonitoring`

     Here, *`hostname`* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.
   - **User Name**: Specify the user name for connecting to your Oracle IoT Asset Monitoring Cloud Service instance.
   - **Password**: Specify the password for connecting to your Oracle IoT Asset Monitoring Cloud Service instance.

     > **Note:**
     >
     > If you change the password for connecting to your Oracle IoT Asset Monitoring Cloud Service instance in future, then you must update the password in Oracle Fusion Cloud Maintenance.

   - **Confidence Threshold**: (Optional) Specify a confidence threshold between 0 and 1. For example, a value of 0.8 indicates a confidence threshold of 80%. The confidence threshold is used for maintenance interval optimization.
6. Click **Save and Close**.

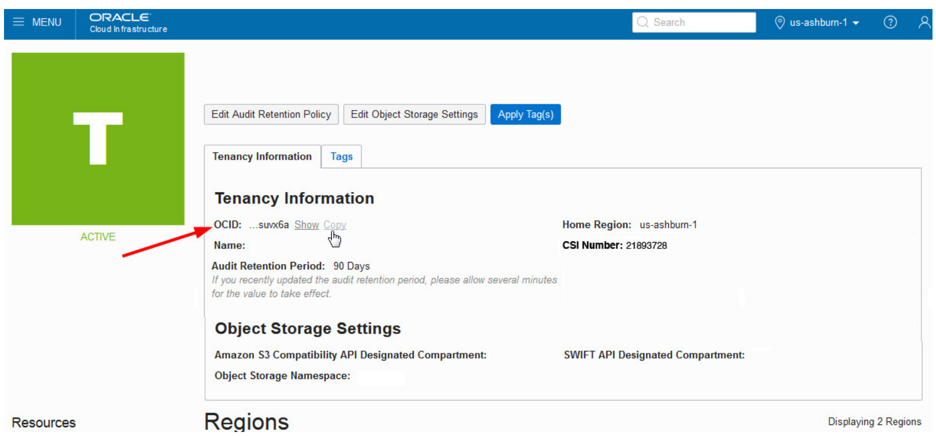
Enable the Integration and Configure OCI Cloud Storage Details in Oracle IoT Asset Monitoring Cloud Service

Use the Settings page in Oracle IoT Asset Monitoring Cloud Service to configure OCI Object Storage settings, and to enable integration with Oracle Fusion Cloud Maintenance.

1. In Oracle IoT Asset Monitoring Cloud Service, click **Menu** (≡), and then click **App Settings**.
2. Click the **Settings** tab (⚙).
3. Under **Cloud Account**, add your cloud account details:
   a. Enter your **Tenant OCID**.

      The tenancy details are available from the Oracle Cloud Infrastructure Console. You need to log in to your Oracle Cloud Infrastructure Console. From the **Profile** menu, click **Tenancy: <YourTenancyName>**.

      The tenancy OCID is shown under Tenancy Information. Click **Copy** to copy it to your clipboard.

      Paste this value under **Tenant OCID** in Oracle IoT Asset Monitoring Cloud Service.
   b. Enter the **User OCID**.

      The user details are available from the Oracle Cloud Infrastructure Console. You need to log in to your Oracle Cloud Infrastructure Console. From the **Profile** menu, click **User Settings**.

      The user OCID is shown under User Information. Click **Copy** to copy it to your clipboard.

      Paste this value under **User OCID** in Oracle IoT Asset Monitoring Cloud Service.
   c. Click **Generate Public Key**.
4. Set the public key in OCI Object Storage.

a. On the Settings page of Oracle IoT Asset Monitoring Cloud Service, under **Cloud Account**, click **Copy** against **Public Key** to copy the public key that you generated earlier.
b. Log in to your Oracle Cloud Infrastructure Console.
c. Under the **Profile** menu, click **User Settings**.
d. Click **API Keys** under **Resources**.
e. Click **Add Public Key**.

   Note: If three public keys are already listed under API Keys, you have to first delete one public key. An OCI Object Storage service user can't have more than three public keys.
f. Select **Paste Public Keys** and paste the key that you copied from Oracle IoT Asset Monitoring Cloud Service.
g. Click **Add**.

   The fingerprint for the added public key appears under API Keys. The fingerprint should be the same as that displayed on the Settings page of Oracle IoT Asset Monitoring Cloud Service.

5. On the Settings page in Oracle IoT Asset Monitoring Cloud Service, provide the object storage details in the Integrations section.

   The OCI Object Storage stores the data extracted by the Business Intelligence Cloud Connector (BICC) from Oracle Fusion Cloud Maintenance.
   a. Under Oracle Object Storage Service, select **Object Storage Enabled**.
   b. Enter the Object **Storage URL** where BICC ingests data.

      For example, `https://objectstorage.us-phoenix-1.oraclecloud.com`.
   c. Enter the **Namespace** of the compartment that contains the storage bucket.
   d. Enter the **Default Bucket** name that stores the data extracted by the Business Intelligence Cloud Connector (BICC) from Oracle Fusion Cloud Maintenance.
6. On the Settings page in Oracle IoT Asset Monitoring Cloud Service, configure Oracle Fusion Cloud Maintenance integration.
   a. In the Integrations section, click **Oracle Maintenance Cloud Service.**
   b. Click **Connect to Mnt**.
   c. Specify the **Service URL** for your Oracle Fusion Cloud Maintenance instance.

      The Service URL is the URL of your Oracle Fusion Cloud Maintenance host. No port number is necessary here.

      For example: `https://MyMntCloud.oraclecloud.com`.
   d. Specify the **User Name** for your Oracle Fusion Cloud Maintenance instance.
   e. Specify the **Password** for your Oracle Fusion Cloud Maintenance instance.
   f. Click **Verify Connectivity** to verify connectivity to the Oracle Fusion Cloud Maintenance instance.
   g. Click **Save**.
   h. Click **Edit Configuration**, and toggle the **Integration Status** to **ON**.

      This enables your Oracle Fusion Cloud Maintenance integration.

i. Specify the **Synchronization** frequency in minutes.

   The sync frequency determines how often Oracle IoT Asset Monitoring Cloud Service syncs with Oracle Fusion Cloud Maintenance.

j. Click **Save**.

k. Select the **Object Storage Integration** to use for storing external data received from Oracle Fusion Cloud Maintenance.

   External data such as asset data, work order data, and maintenance schedules from Oracle Fusion Cloud Maintenance are 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 Fusion Cloud Maintenance.

l. Specify the **Object Storage Container** name, or bucket name, to store the Oracle Fusion Cloud Maintenance data.

7. Under Oracle SCM Organizations Mapping, map your Oracle SCM Cloud organizations to one or more Oracle IoT Asset Monitoring Cloud organizations.

   - **One to One**: Lets you create one-to-one mappings between Oracle SCM Cloud organizations and Oracle IoT Asset Monitoring Cloud Service organizations. Oracle IoT Asset Monitoring Cloud Service automatically creates a separate organization for each Oracle SCM Cloud organization from which assets are imported. This helps separate the assets into their respective organizations in Oracle IoT Asset Monitoring Cloud Service.
   - **Many to One**: Lets you choose one organization in Oracle IoT Asset Monitoring Cloud Service where your Oracle Fusion Cloud Maintenance assets are imported. Assets imported from different Oracle SCM Cloud organizations are imported into the same Oracle IoT Asset Monitoring Cloud Service organization.
     Select an IoT Organization to use for the many-to-one mapping.

> **Note:**
>
> If you change the mapping settings for an existing Oracle Fusion Cloud Maintenance integration, the changed mapping applies to assets from new Oracle SCM Cloud organizations only. The already mapped Oracle SCM Cloud organizations are not affected.

Configure OCI Object Storage in BICC

Configure Oracle Cloud Infrastructure (OCI) object storage in Business Intelligence Cloud Connector (BICC). A data extraction job extracts the file to a specified namespace and bucket in the Oracle Storage Cloud objects store. You need a subscription to Oracle Cloud Storage to complete this setup.

1. Log in to your BICC console.

   Append `/biacm` to your Oracle Fusion Cloud Maintenance URL. For example, `https://`*`hostname`*`/biacm`. Here, *`hostname`* is the host name of your Oracle Fusion Cloud Maintenance instance.

Log in as a user that has permission to perform admin tasks in BICC. The user should have the `ESS Administrator` and `Application Implementation Administrator` roles.

2. Click the **Configure External Storage** task panel.
3. Select the **OCI Object Storage Connection** tab.
4. Click **Add**.
5. Under **OCI Parameters**, complete the following fields:
   - **Name**: Specify a name for the connection.
   - **Host**: Specify the host name for the OCI Object Storage Service. For example, `https://objectstorage.us-phoenix-1.oraclecloud.com`.
   - **Tenancy OCID**: Paste your Tenant OCID. The tenancy details are available from the Oracle Cloud Infrastructure Console. You need to log in to your Oracle Cloud Infrastructure Console. From the **Profile** menu, click **Tenancy: *YourTenancyName***. The tenancy OCID is shown under Tenancy Information. Click **Copy** to copy it to your clipboard.
   - **User OCID**: Paste your User OCID. The user details are available from the Oracle Cloud Infrastructure Console. You need to log in to your Oracle Cloud Infrastructure Console. From the **Profile** menu, click **User Settings**. The User OCID is shown under User Information. Click **Copy** to copy it to your clipboard.
   - **Namespace**: Specify the namespace of the compartment that contains the storage bucket. Namespace is obtained in the OCI Console.
   - **Bucket**: Specify the bucket name that stores the data extracted by BICC from Oracle Fusion Cloud Maintenance.
6. Under OCI API Signing Key click **Generate API Signing Key**.

   A value is displayed in the **Fingerprint** field.

   You need to paste this key in OCI Object Storage service before you can test the connection. To do this, navigate to the User Settings page from the **Profile** menu in OCI Console. Click **API Key > Add API Keys** to import or paste the key in OCI Console.
7. Click **Test Connection** in BICC to test the connection to the OCI Object Storage service.

Configure BICC to Generate Gzip Extract Files

Change the compression type for BICC extracts to `gzip`. Oracle IoT Asset Monitoring Cloud Service connects to the OCI Object Storage service to ingest batches of these compressed `csv` files (`.gz`) for analysis.

1. Log in to your BICC console.

   Append `/biacm` to your Oracle Fusion Cloud Maintenance URL. For example, `https://`*`hostname`*`/biacm`. Here, *`hostname`* is the host name of your Oracle Fusion Cloud Maintenance instance.

   Log in as a user that has permission to perform admin tasks in BICC. The user should have the `ESS Administrator` and `Application Implementation Administrator` roles.
2. Click the **Manage Offerings and Data Store** task panel.
3. On the Offerings page, click the **Actions** drop-down list, and select **Extract Preferences**.
4. Under File Parameters, change the **Compression Type** to **GZip**.
5. Click **Save** to save your changes.

Extract Key Maintenance Data from Oracle Maintenance Cloud

Schedule the **Extract, Transform, and Load Maintenance Data** program in Oracle Fusion Cloud Maintenance to create a machine-learning ready data extract of your key maintenance related data

1. From the home page in Oracle Fusion Cloud Maintenance, select **Menu > Tools > Scheduled Processes**.
2. Click **Schedule New Process**.
3. Click the **Name** drop-down list, and click **Search**.
4. Type `Extract,` in the **Name** search field, and click Search.
5. Select **Extract, Transform, and Load Maintenance Data** from the list of search entries and click **OK**.
6. Click **OK** again to confirm.
7. In the Process Details dialog, select a value for **Extraction Type**.

   You can choose **Incremental** or **Full** load.
8. Enter a **Reliability Rate** between 0 and 1.

   The Reliability Rate is used in calculating the useful lifespan of parts and assets. The reliability rate indicates the maximum allowable failure rate before a part or asset is no longer considered usable.

   For example, a value of 0.8 indicates a reliability rate of 80%.
9. Enter a **Utilization Rate** between 0 and 1.

   The utilization rate indicates the minimum lifespan of a part that must be utilized before it can be replaced.

   For example, a value of 0.5 indicates a utilization rate of 50%.
10. Click **Submit**, and then click **OK**.
11. Click the **Refresh** icon on the Overview page to see the current status of your process.

    Once the **Extract, Transform, and Load Maintenance Data** process prepares key maintenance data, the BICC job packages and copies the data into the OCI Object Storage bucket.

Perform Learning on Maintenance Data

Schedule the **Perform Learning on Maintenance Data** program in Oracle Fusion Cloud Maintenance to trigger learning on the exported maintenance data. Oracle IoT Asset Monitoring Cloud Service then sends recommendations back to Oracle Fusion Cloud Maintenance based on the learning performed in Oracle IoT Asset Monitoring Cloud Service.

1. From the home page in Oracle Fusion Cloud Maintenance, select **Menu > Tools > Scheduled Processes**.
2. Click **Schedule New Process**.
3. Click the **Name** drop-down list, and click **Search**.
4. Type `Perform Learning` in the **Name** search field, and click Search.

5. Select **Perform Learning on Maintenance Data** from the list of search entries and click **OK**.
6. Click **OK** again to confirm.
7. Enter **Reliability Rate** and **Reliability Tolerance** values between 0 and 1.

   For example, a value of 0.8 indicates a reliability rate of 80%.
8. Enter a **Utilization Rate** between 0 and 1.

   The utilization rate indicates the minimum lifespan of a part that must be utilized before it can be replaced.

   For example, a value of 0.5 indicates a utilization rate of 50%.
9. Click **Submit**, and then click **OK**.
10. Click the **Refresh** icon on the Overview page to see the current status of your process.

    Once the **Perform Learning on Maintenance Data** process has succeeded, Oracle IoT Asset Monitoring Cloud Service performs learning on the ingested data and sends back recommendations to Oracle Fusion Cloud Maintenance.

The maintenance manager can check the **Recommendations** infolet on the landing page to look for new recommendations in Oracle Fusion Cloud Maintenance. The maintenance manager can choose to accept, reject, or override these recommendations.

Integrate Oracle B2B Service with Oracle Service Monitoring for Connected Assets

You can integrate Oracle B2B Service (Oracle Engagement Cloud) with Oracle Service Monitoring for Connected Assets to directly manage your IoT connected assets from Oracle B2B Service. 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 Oracle B2B Service.

To export incidents, Oracle Service Monitoring for Connected Assets connects to Oracle B2B Service through Oracle Integration Cloud (Oracle Integration Service).

> **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 B2B Service solution for businesses that want to combine Oracle's sales and service capabilities on a single platform. Oracle B2B Service 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.

Oracle B2B Service uses a tight integration with Oracle Service Monitoring for Connected Assets. You can not only sync incidents to Oracle B2B Service, but also take asset actions, and set asset attributes from Oracle B2B Service. Diagnostics let you see a graphical plot of your asset sensor attributes, and the results of the actions that you execute from Oracle B2B Service.

Once you change the status of the SR in Oracle B2B Service, 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 Oracle B2B Service:

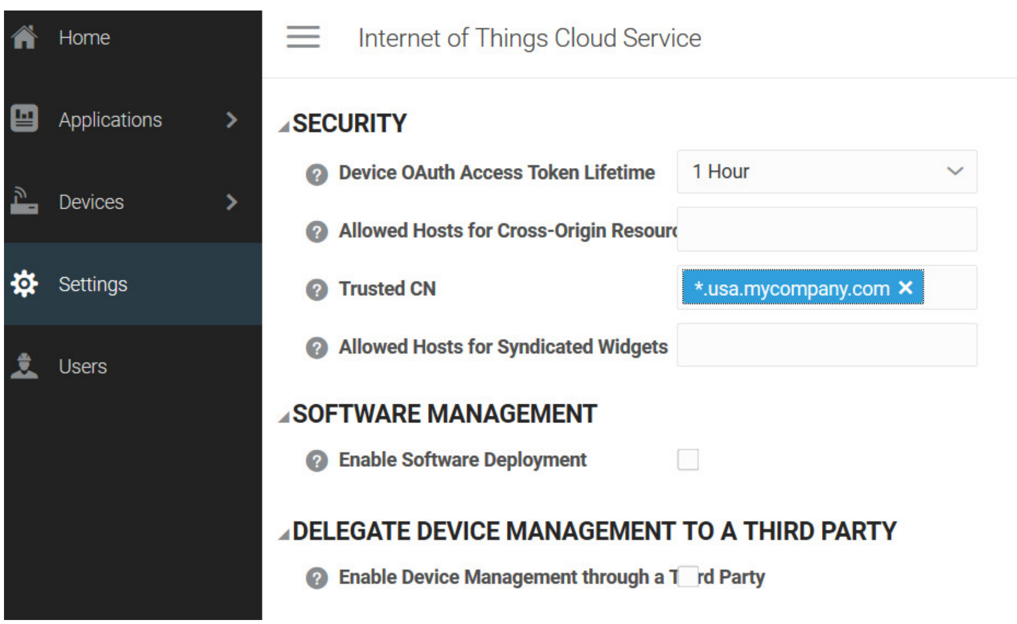
- Add an Oracle B2B Service Integration
- Enable and Configure the Oracle B2B Service Integration
- Configure Oracle B2B Service Settings
- Configure Rules to Generate Automatic Service Requests
- Diagnose and Troubleshoot Connected Assets from Oracle B2B Service
- Verify Incident and SR Status Update in Oracle Service Monitoring for Connected Assets

Add an Oracle B2B Service Integration

Use the Integrations page in your IoT application to add an integration for Oracle Fusion Cloud Maintenance.

Before you configure Oracle B2B Service integration, make sure your Oracle B2B Service host and Oracle Integration Service host is trusted by your Oracle Internet of Things Intelligent Applications Cloud domain.

As host names with `.oraclecloud.com` and `.oraclecloudapps.com` suffixes are always allowed, no action is necessary for these domains. If your Oracle B2B Service or Oracle Integration Service domain name is different, then add the domain as a trusted CN in the Oracle Internet of Things Intelligent Applications Cloud management console. To do this, add `*.`*`YourDomain`*`.com` under **Trusted CN** in the Settings page.



You can access your Oracle Internet of Things Intelligent Applications Cloud management console at the following URL:

https://*hostname*/ui

Here, *hostname* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.

To enable integration with Oracle B2B Service:

1. In your IoT application, click **Menu** (), and then click **Settings**.

   You can access Oracle Service Monitoring for Connected Assets at the following URL:

   `https://hostname/smca`

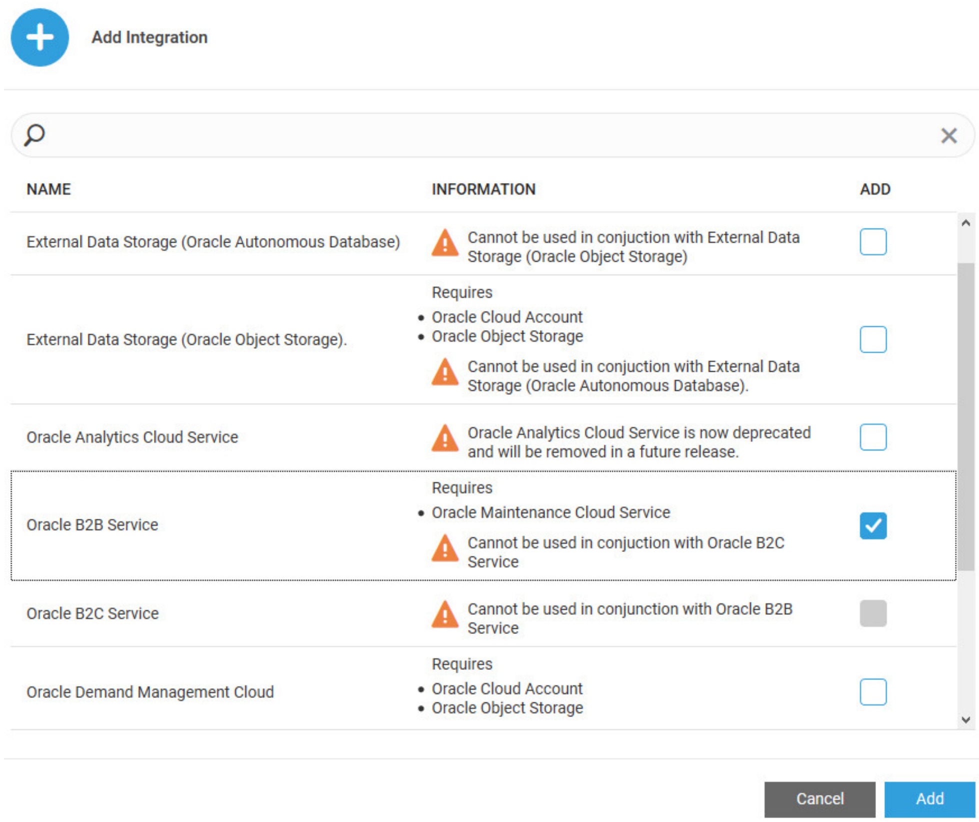
   Here, *hostname* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.

   If you are in the Design Center, you need to click **Previous** () before you see the **Settings** option in the menu.

2. Click **Integrations**.
3. Click **Add** to add a new integration.
4. In the Add Integration dialog, select **Oracle B2B Service** and click **Add**.

   Tip: You can also search for an integration name in the list.

   > **Note:**
   >
   > **Oracle Maintenance Cloud Service** integration is a prerequisite for **Oracle B2B Service**. The Asset Information Management connection information and org mapping information is fetched from the **Oracle Maintenance Cloud Service** integration.
   >
   > If you have not previously added the **Oracle Maintenance Cloud Service** integration, it is automatically selected along with **Oracle B2B Service**.
   >
   > See Integrate Oracle Fusion Cloud Maintenance with Oracle IoT Asset Monitoring Cloud Service for more information on **Oracle Maintenance Cloud Service** integration.



> **Note:**
>
> You cannot use **Oracle B2B Service** integration and **Oracle B2C Service** integration at the same time.

Oracle B2B Service integration gets added to the Integrations page.

5. On the Integrations page, under **Oracle B2B Service**, click **Connect**.
6. Specify the **Service URL** for your Oracle Integration Cloud instance.

   To export incidents, Oracle Service Monitoring for Connected Assets connects to Oracle B2B Service through the Oracle Integration Service.

   The Service URL is the URL of your Oracle Integration Cloud host.

   For example: `https://MyIntCloud.oraclecloud.com`.
7. Specify the **User Name** to connect to Oracle Integration Service.
8. Specify the **Password** to connect to Oracle Integration Service.
9. Click **Save** to save the connection settings.

Enable and Configure the Oracle B2B Service Integration

To start using Oracle B2B Service integration, enable and configure the integration for Oracle B2B Service on the Integrations page.

Oracle B2B Service can automatically sync new installed base assets with your Oracle Service Monitoring for Connected Assets instance.

To export incidents, Oracle Service Monitoring for Connected Assets connects to Oracle B2B Service through the Oracle Integration Service.

To enable integration with Oracle B2B Service:

1. In your IoT application, click **Menu** (☰), and then click **Settings**.
2. Click **Integrations**.
3. Under Oracle B2B Service, click **Edit Configuration**.
4. Toggle the **Integration Status** switch to **ON**.

   This enables your Oracle B2B Service integration.
5. (Optional) Under **Create Incident URL Suffix**, specify an incident suffix string to use when creating the SR in Oracle B2B Service.
6. Download the ICS par file to configure your Oracle Integration Cloud instance to connect to Oracle B2B Service.

   In Oracle Integration Cloud, import the package (ICS par file) downloaded from your IoT application. You can do this from the **Menu > Integrations > Packages** menu**.**

   Next, configure the connections in the imported integration by providing the connection URL for your Oracle B2B Service integration along with the user credentials:

   a. Test and save the ICS Rest Adapter connection.
   b. For the EC SMC Rest connection, specify the B2B Service connection URL along with your B2B Service user credentials:

      For example: `https://`*`MyB2Bservice`*`.oraclecloud.com:443/crmRestApi/resources/latest`.

      Test and save the connection.
   c. For the EC SMC OSC connection, specify the OSC Services Catalog WSDL URL along with your user credentials for the B2B Service:

      For example: `https://`*`MyB2Bservice`*`.oraclecloud.com:443/fndAppCoreServices/ServiceCatalogService?wsdl`.

      Test and save the connection.

   Once the connections are updated and tested, you must re-activate the integration in Oracle Integration Cloud for the changes to take effect.
7. In your IoT application, click **Save** to save the configuration settings you specified in the Oracle B2B Service Configuration dialog.

Configure Oracle B2B Service Settings

You need to enable Oracle B2B Service to use installed base assets, add the Oracle Service Monitoring for Connected Assets URL in Oracle B2B Service, and enable the **Connected Asset** tab for service requests in Oracle B2B Service.

The following topics cover the configuration settings required in Oracle B2B Service:

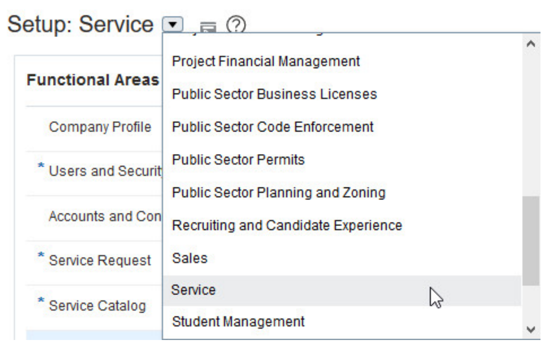
- Manage Assets Using the Common Asset Model
- Automatically Sync New Assets and Asset Attribute Updates
- Manage Service to IoT Cloud Integration
- Enable Connected Asset Tab for Service Requests

Manage Assets Using the Common Asset Model

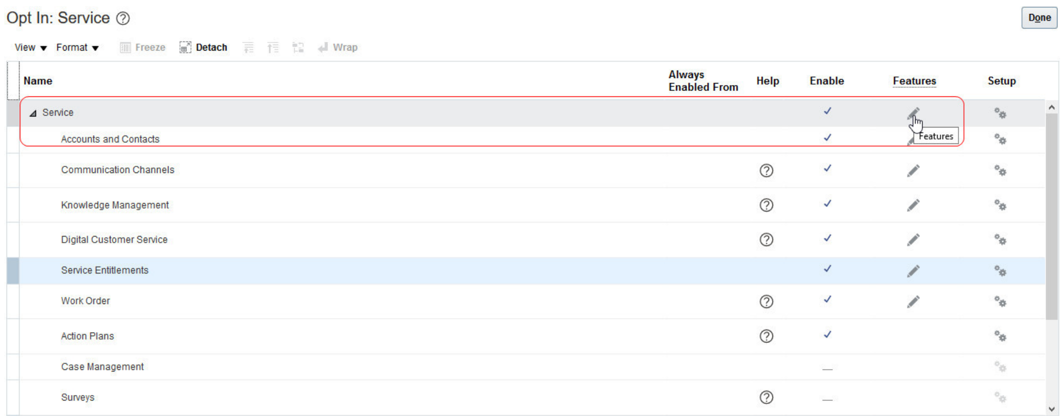
The **Manage Assets Using Common Asset Model** setting lets Oracle B2B Service use the installed base assets from Oracle SCM Cloud. These assets are automatically synced with your Oracle Service Monitoring for Connected Assets instance if the **Manage Asset Maintenance Parameters** setting is configured.

1. In Oracle B2B Service, click **Menu** ☰, and then click **Setup and Maintenance**.

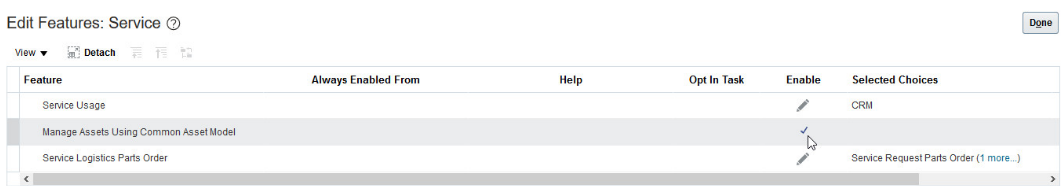
   You may find **Setup and Maintenance** under the **My Enterprise** or **Others** item.
2. Under **Setup**, select **Service**.



3. In the Functional Areas section, click the **Change Feature Opt In** link.
4. Click **Edit** under **Features** for the Service row.



5. Select the **Enable** option for **Manage Assets Using Common Asset Model**.



6. Click **Done**.

Automatically Sync New Assets and Asset Attribute Updates

Set up Oracle B2B Service to automatically sync new installed base assets with your Oracle Service Monitoring for Connected Assets instance. Updates to asset attributes in Oracle B2B Service are also pushed to Oracle Service Monitoring for Connected Assets.

You need to add your Oracle Service Monitoring for Connected Assets information in Oracle B2B Service.

1. In Oracle B2B Service, click **Menu** ≡, and then click **Setup and Maintenance**.

   You may find **Setup and Maintenance** under the **My Enterprise** or **Others** item.

2. Click **Tasks** and click **Search**.
3. Search for the following string: `Manage Asset Maintenance Parameters`.
4. Click **Manage Asset Maintenance Parameters** in the search results.

   The user must have the privilege to manage asset maintenance parameters (`MNT_MANAGE_ASSET_MAINTENANCE_PARAMETERS`).

5. Click **Enable IoT** and specify the connection details for your Oracle Service Monitoring for Connected Assets instance.
   - **URL**: Use the following format:

     `https://hostname/assetMonitoring`

     Here, *hostname* is the host name of your Oracle Service Monitoring for Connected Assets instance.

- **User Name**: Specify the user name for connecting to your Oracle Service Monitoring for Connected Assets instance.
- **Password**: Specify the password for connecting to your Oracle Service Monitoring for Connected Assets instance.

> **Note:**
>
> If you change the password for connecting to your Oracle Service Monitoring for Connected Assets instance in future, then you must update the password in Oracle B2B Service.

6. Click **Save and Close**.

Manage Service to IoT Cloud Integration

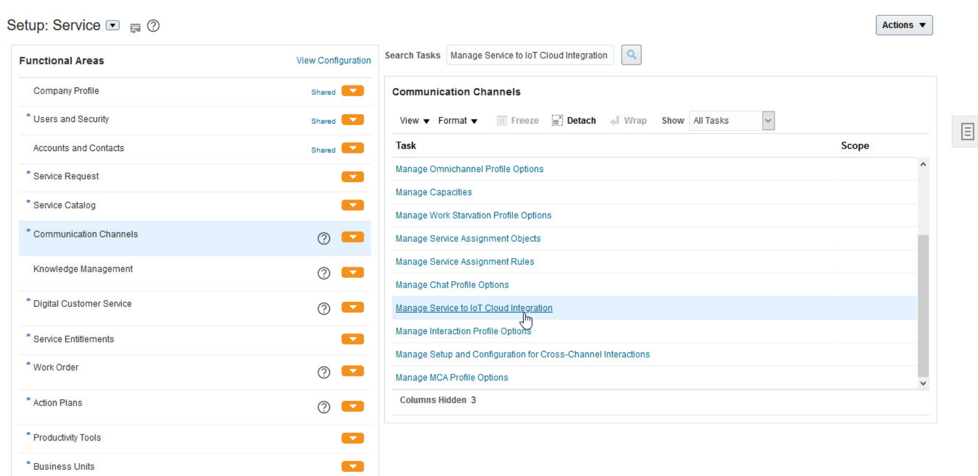
The **Manage Service to IoT Cloud Integration** is a one-time setting that you need to configure in Oracle B2B Service. This lets Oracle B2B Service fetch asset details for the Service Request page.

1. In Oracle B2B Service, click **Menu**, and then click **Setup and Maintenance**.

   You may find **Setup and Maintenance** under the **My Enterprise** or **Others** item.

2. Click **Tasks** and click **Search**.

   Alternatively, you can also select **Service** under **Setup**, and find the setting under **Communication Channels**.



3. Search for the following string: `Manage Service to IoT Cloud Integration`.
4. Click **Manage Service to IoT Cloud Integration** in the search results.
5. Under Integration Configuration, specify the connection details for your Oracle Service Monitoring for Connected Assets instance.
   - **IOT API Base URL**: Use the following format:

     `https://`*`hostname`*

Here, *hostname* is the host name of your Oracle Service Monitoring for Connected Assets instance.

- **User Name**: Specify the user name for connecting to your Oracle Service Monitoring for Connected Assets instance.
- **Password**: Specify the password for connecting to your Oracle Service Monitoring for Connected Assets instance.

6. Click **Verify Connection** to test your connection.
7. Click **Save**.

Enable Connected Asset Tab for Service Requests

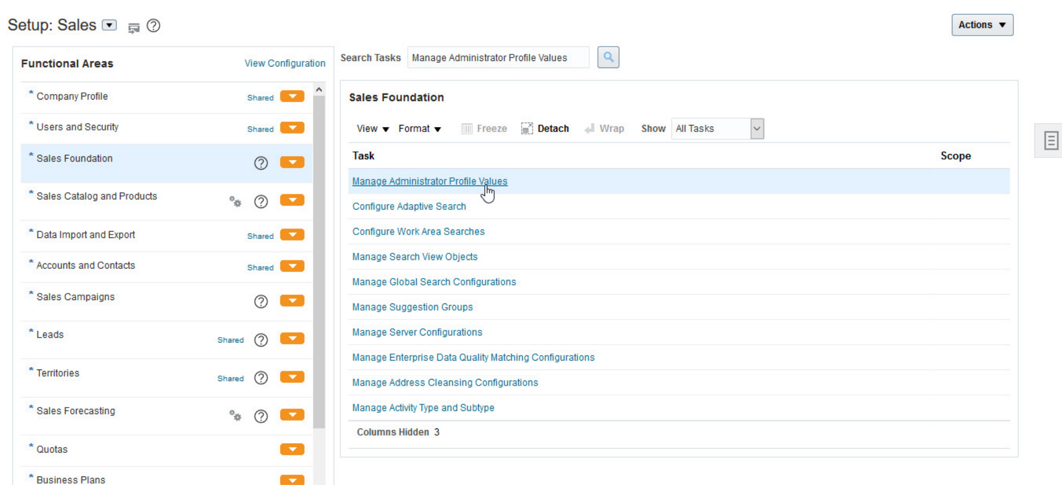
The **Enable Connected Asset Tab for Service Requests** enables the IoT **Connected Asset** tab for the Service Request page in Oracle B2B Service.

1. In Oracle B2B Service, click **Menu**, and then click **Setup and Maintenance**.

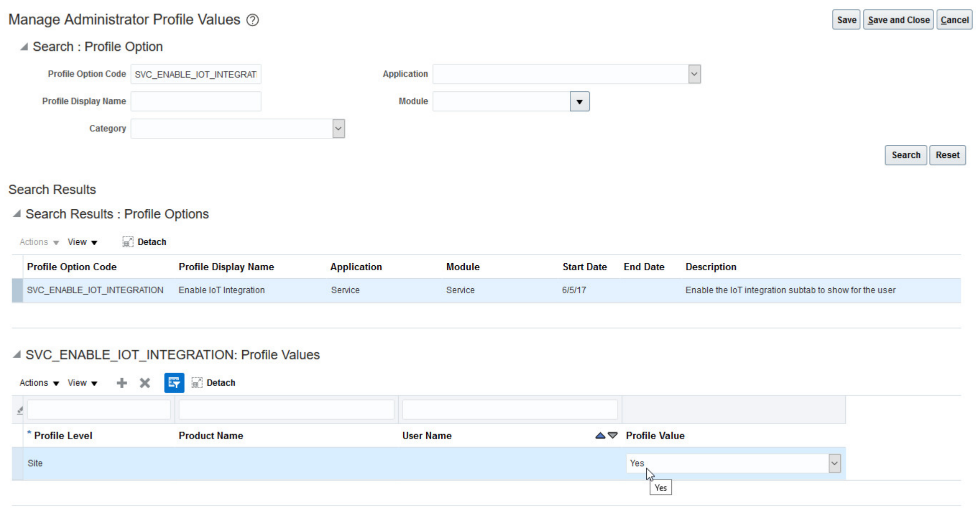
   You may find **Setup and Maintenance** under the **My Enterprise** or **Others** item.

2. Click **Tasks** and click **Search**.

   Alternatively, you can also select **Sales** under **Setup**, and find the setting under **Sales Foundation**.



3. Search for the following string: `Manage Administrator Profile Values`.
4. Click **Manage Administrator Profile Values** in the search results.
5. Under **Profile Option Code**, search for `SVC_ENABLE_IOT_INTEGRATION`.



6. Under **Profile Value** for SVC_ENABLE_IOT_INTEGRATION, select **Yes**.
7. Click **Save and Close**.

Configure Rules to Generate Automatic Service Requests

Configure rules to automatically create service requests in Oracle B2B Service 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 B2B Service.

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 Oracle B2B Service 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 Oracle B2B Service

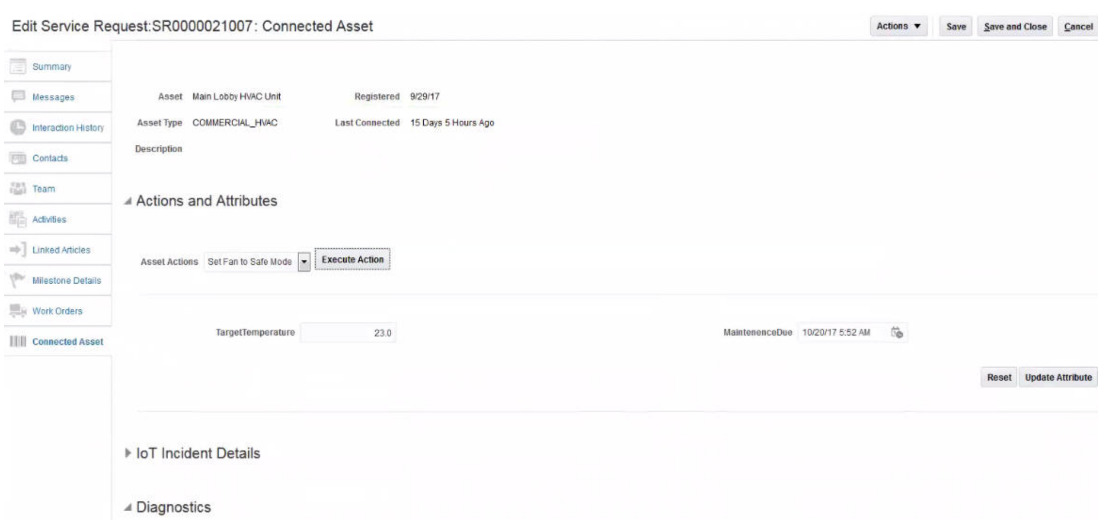
When an incident gets created for an imported asset in Oracle Service Monitoring for Connected Assets, the incident rule automatically creates a corresponding service request (SR) in Oracle B2B Service.

Oracle Service Monitoring for Connected Assets provides tight integration with Oracle B2B Service. You can not only sync incidents to Oracle B2B Service, but also take asset actions, and set asset attributes from Oracle B2B Service. Diagnostics let you see a graphical plot of your asset sensor attributes and the results of the actions that you execute from Oracle B2B Service.

Once you change the status of the SR in Oracle B2B Service, 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 Oracle B2B Service. 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 Oracle B2B Service 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 Oracle B2B Service, 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 B2C Service with Oracle Service Monitoring for Connected Assets

You can integrate Oracle B2C Service with Oracle Service Monitoring for Connected Assets to directly manage your IoT connected assets from Oracle B2C Service. When an incident gets created for an IoT asset in Oracle Service Monitoring for Connected Assets, the incident rule automatically creates a corresponding incident in Oracle B2C Service.

To export incidents, Oracle Service Monitoring for Connected Assets connects to Oracle B2C Service through Oracle Integration Cloud (Oracle Integration Service).

Once you change the status of the incident in Oracle B2C Service, the incident status automatically gets updated in Oracle Service Monitoring for Connected Assets.

The following table maps the Oracle B2C Service entities with their corresponding IoT entries:

Oracle B2C Service	IoT	Map Definition
Sales Product	Asset Type	Sales product Id
Asset	Asset	Sales product Id + SKU (serial number)
Incident	Incident	Incident Id

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.

Add an Oracle B2C Service Integration

Use the Integrations page in your IoT application to add an integration for Oracle Fusion Cloud Maintenance.

To enable integration with Oracle B2C Service:

1. In your IoT application, click **Menu** (≡), and then click **Settings**.

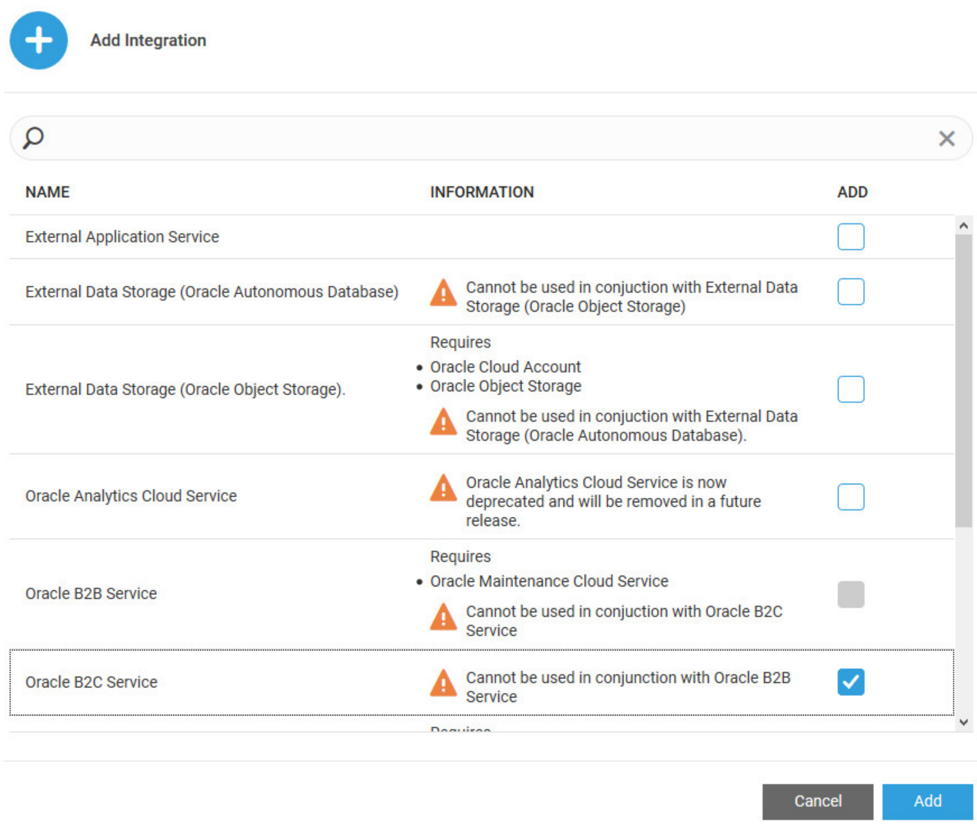
   You can access Oracle Service Monitoring for Connected Assets at the following URL:

   `https://hostname/smca`

   Here, *`hostname`* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.

   If you are in the Design Center, you need to click **Previous** (<) before you see the **Settings** option in the menu.
2. Click **Integrations**.
3. Click **Add** + to add a new integration.
4. In the Add Integration dialog, select **Oracle B2C Service** and click **Add**.

Tip: You can also search for an integration name in the list.



> **Note:**
>
> You cannot use **Oracle B2C Service** integration and **Oracle B2B Service** integration at the same time.

Oracle B2C Service integration gets added to the Integrations page.

5. On the Integrations page, under **Oracle B2C Service**, click **Connect**.
6. Specify the **Service URL** for your Oracle Integration Cloud instance.

   To export incidents, Oracle Service Monitoring for Connected Assets connects to Oracle B2C Service through the Oracle Integration Service.

   The Service URL is the URL of your Oracle Integration Cloud host.

   For example: `https://MyIntCloud.oraclecloud.com`.
7. Specify the **User Name** to connect to Oracle Integration Service.
8. Specify the **Password** to connect to Oracle Integration Service.
9. Click **Save** to save the connection settings.

Enable and Configure the Oracle B2C Service Integration

To start using Oracle B2C Service integration, enable and configure the integration for Oracle B2C Service on the Integrations page.

To export incidents, Oracle Service Monitoring for Connected Assets connects to Oracle B2C Service through the Oracle Integration Service.

To enable integration with Oracle B2C Service:

1. In your IoT application, click **Menu** (☰), and then click **Settings**.
2. Click **Integrations**.
3. Under Oracle B2C Service, click **Edit Configuration**.
4. Toggle the **Integration Status** switch to **ON**.

   This enables your Oracle B2C Service integration.
5. Under **Primary Contact for Incidents**, specify the email address of the primary contact for incidents.

   The email address typically belongs to the asset owner in Oracle B2C Service. This user can create incidents in Oracle B2C Service.
6. **Download** the ICS par file (`Iot_Svcs.par`) to configure your Oracle Integration Cloud instance to connect to Oracle B2C Service.
7. Click **Save** to save the configuration settings you specified in the Oracle B2C Service Configuration dialog.
8. Log in to Oracle Integration Service:
   a. Open a web browser, enter the URL for yourOracle Integration Service instance in the address field, and then press **Enter**.
   b. Enter your user name and password and then click **Sign In**.
9. Click **Integrations**.
10. Click the **Menu** (☰) icon next to Oracle Integration Cloud, click **Designer**, and then click **Packages**.
11. 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 6.
    c. Double-click the `Iot_Svcs.par` file.
    d. Click **Import**.
12. Click the **Menu** (☰) icon next to Oracle Integration Cloud, click **Designer**, and then click **Connections**.
13. Set up the **Iot-Svcs RightNow Connection**:
    a. Select the **Iot-Svcs RightNow Connection**.
    b. Click the **Menu** (☰) 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**.

14. Set up the **Iot-Svcs dev Connection**:
    a. Select the **Iot-Svcs dev Connection**.
    b. Click the **Menu** ( ) 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**.
15. Click the **Menu** () icon next to Oracle Integration Cloud, click **Designer**, and then click **Integrations**.
16. Select **IotSvcsIncidentGetInteg** and then click the slider to activate the integration.
17. Repeat the previous step for these integrations:
    - iotSvcsStatusTypeName
    - iotSvcsBulkIncidentQuery
    - Create SVCS INCIDENT
    - Sales-Product-To-AssetType-Integration
    - SearchContact
    - SvcS Asset Creation
    - SvcsRightNowInteg4Exp
    - UpdateIncident
18. Log out of Oracle Integration Service.

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 rotable 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

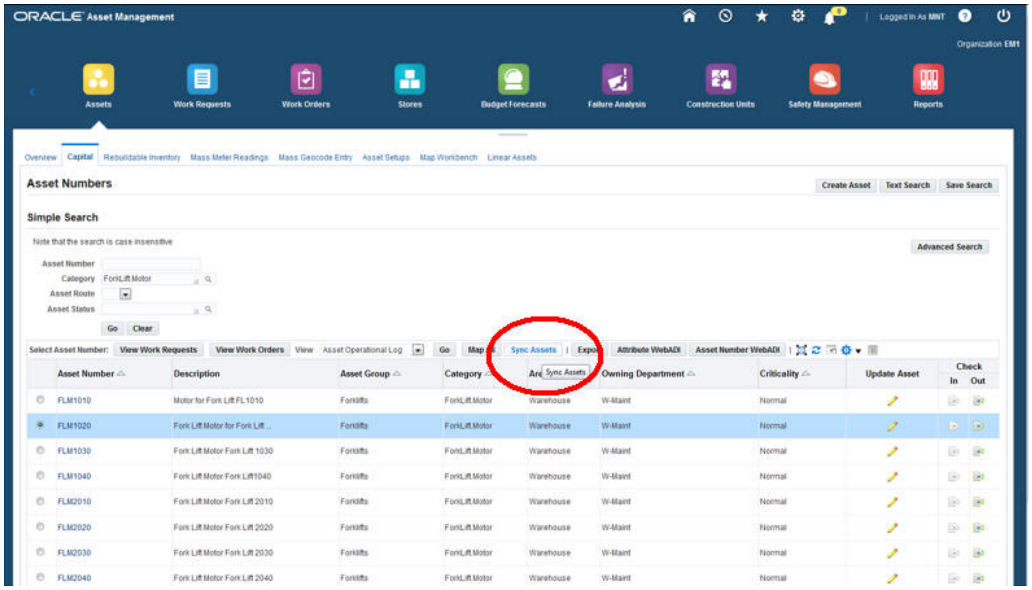
Oracle Internet of Things (IoT) Asset Monitoring Cloud Service integration is available in Oracle E-Business Suite (EBS) releases 12.1.3, 12.2.6, and above.

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:

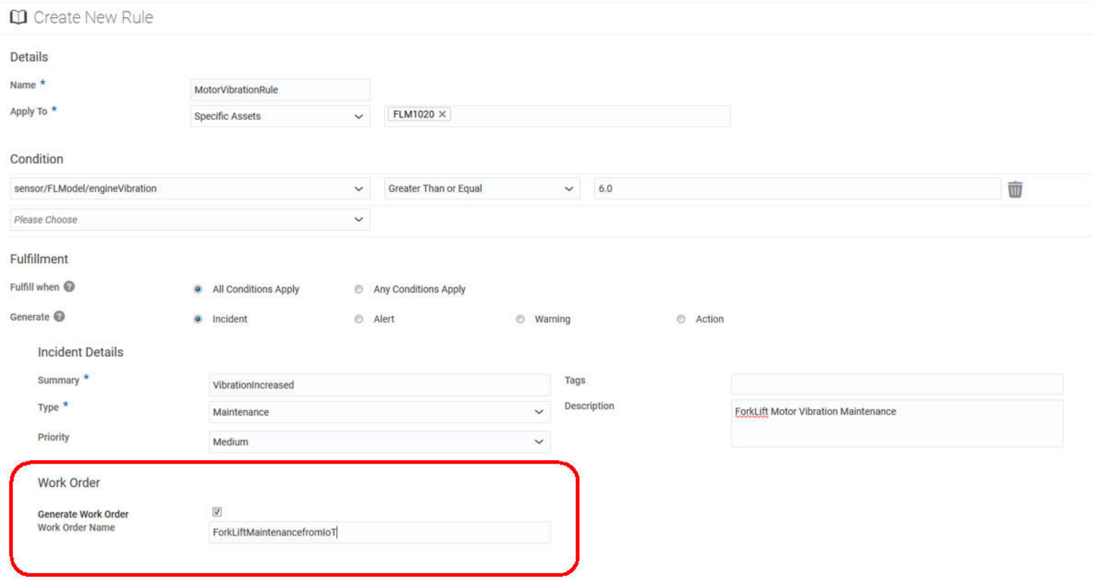
1. Edit the asset type to add the required device model. See Edit an Asset Type for more information on editing asset types.
2. Edit the assets to add the sensor devices. See Edit Asset Details for more information on editing assets.

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:**
>
> Oracle Analytics Cloud integration is now deprecated and will be removed in a future release.

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.

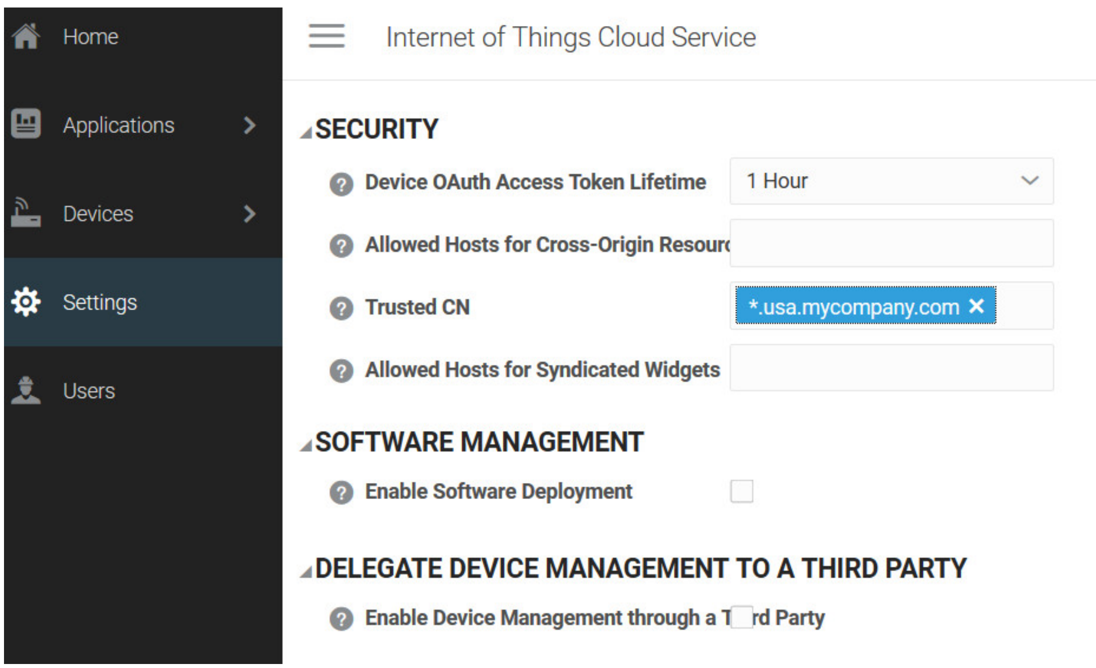
For detailed information on Analytics Cloud, refer to the Oracle Analytics Cloud Help Center Resources.

Add an Oracle Analytics Cloud Integration

Use the Integrations page in Oracle Internet of Things (IoT) Asset Monitoring Cloud Service to add an integration for Oracle Analytics Cloud.

Before you configure Oracle Analytics Cloud integration, make sure your Oracle Analytics Cloud host is trusted by your Oracle Internet of Things Intelligent Applications Cloud domain.

Host names with `.oraclecloud.com` and `.oraclecloudapps.com` suffixes are always allowed. If your Oracle Analytics Cloud domain name is different, then add the domain as a trusted CN in the Oracle Internet of Things Intelligent Applications Cloud management console. To do this, add `*.`*`YourDomain`*`.com` under **Trusted CN** in the Settings page.



You can access your Oracle Internet of Things Intelligent Applications Cloud management console at the following URL:

https://*hostname*/ui

Here, *hostname* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.

To enable integration with Oracle Analytics Cloud:

1. In Oracle IoT Asset Monitoring Cloud Service, click **Menu** (☰), and then click **Settings**.

   You can access Oracle IoT Asset Monitoring Cloud Service at the following URL:

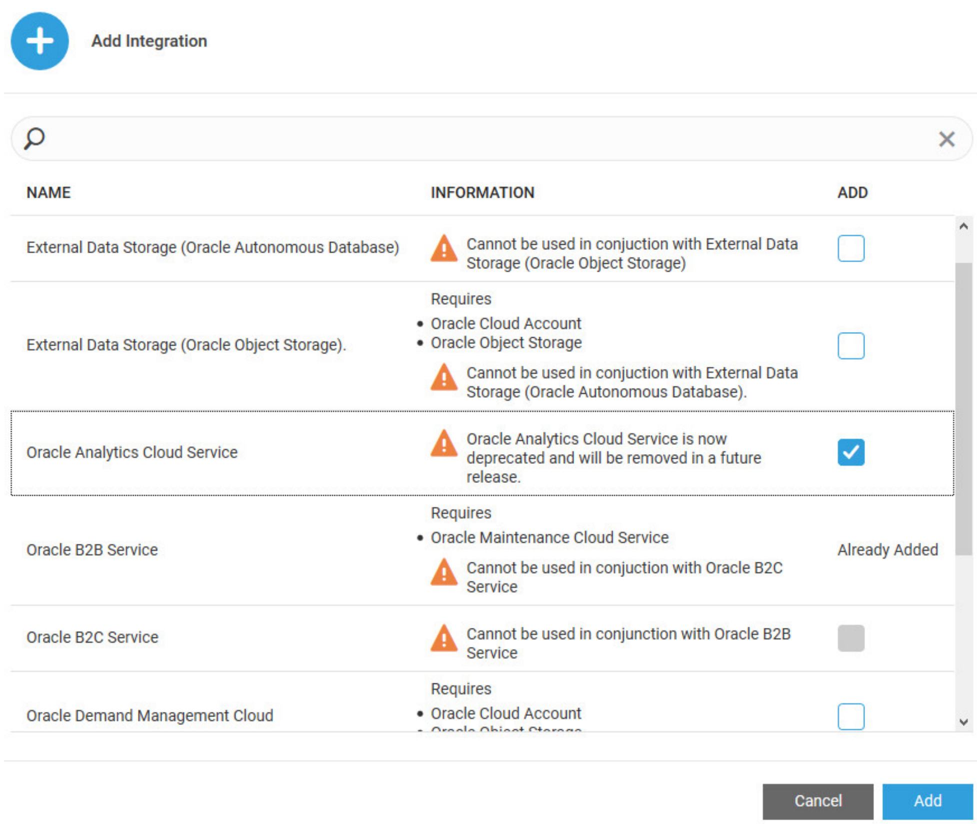
   https://*hostname*/am

   Here, *hostname* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.

   If you are in the Design Center, you need to click **Previous** ( ) before you see the **Settings** option in the menu.

2. Click **Integrations**.
3. Click **Add** + to add a new integration.
4. In the Add Integration dialog, select **Oracle Analytics Cloud Service** and click **Add**.

   Tip: You can also search for an integration name in the list.



Oracle Analytics Cloud Service integration gets added to the Integrations page.

Enable and Configure the Oracle Analytics Cloud Integration

To start using Oracle Analytics Cloud integration, enable and configure the integration for **Oracle Analytics Cloud Service** on the Integrations page.

1. In Oracle IoT Asset Monitoring Cloud Service, click **Menu** (☰), and then click **Settings**.
2. Click **Integrations**.
3. Under **Oracle Analytics Cloud Service**, select **Oracle Analytics Cloud Enabled**.
4. 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.

5. Click **Sync Data to OAC** to sync the asset, metric, and incident data with your Analytics Cloud instance.

   The **Sync Report** shows details on the status of the sync process.

   The default sync interval between Oracle IoT Asset Monitoring Cloud Service and Oracle Analytics Cloud is 24 hours. However, you can manually sync the data at any time.

6. (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.

7. (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 Integrations page of Oracle IoT Asset Monitoring Cloud Service.

   Under Download OAC Project, click **Download**. See Enable and Configure the Oracle Analytics Cloud Integration for more information.

2. In Oracle Analytics Cloud, click **Page Menu** in the Projects page.

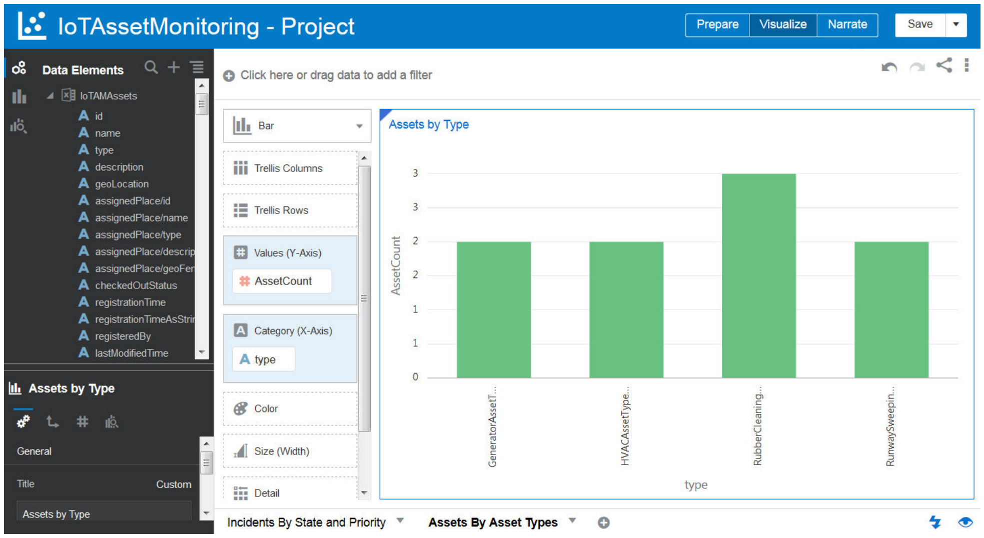
3. Click **Import.**

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.

Integrate with Oracle Supply Chain Planning Cloud

Use advanced analytics in Oracle IoT Asset Monitoring Cloud Service to forecast product demand for new products in Supply Chain Planning (SCP) Demand Management. Oracle IoT Asset Monitoring Cloud Service employs feature-based machine learning on historical product sales data to come up with insights and forecast recommendations for new products.

Demand Management provides the required input data through Oracle Object Storage using BICC (Oracle Business Intelligence Cloud Connector). Oracle IoT Asset Monitoring Cloud Service creates training models on the ingested data and performs scoring to create on-demand forecasts for Demand Management.

For detailed information on this feature, including prerequisites, configuration steps, and usage, please refer to the *Using Demand Management* guide:

- *Using Demand Management*: Feature-Based Forecasting
- Other Resources
  - Demo Video
  - Optimize New Product Introduction Using Recommendations from Planning Advisor Readiness Training

Add a Demand Management Integration

Use the Integrations page in Oracle Internet of Things (IoT) Asset Monitoring Cloud Service to add an integration for Demand Management.

Before you can add and configure the Demand Management integration, make sure you have configured your Cloud Account and enabled Oracle Object Storage. The following sections provide more information:

1. Add an Oracle Cloud Account
2. Connect to an OCI Object Storage Instance

Use the Demand Management documentation and resources to configure the integration in Oracle Supply Chain Planning (SCP) Cloud:

- Optimize New Product Introduction Using Recommendations from Planning Advisor
- *Using Demand Management*: Feature-Based Forecasting

This section covers the steps to add the integration in Oracle IoT Asset Monitoring Cloud Service.

1. In Oracle IoT Asset Monitoring Cloud Service, click **Menu** (≡), and then click **Settings**.

   You can access Oracle IoT Asset Monitoring Cloud Service at the following URL:

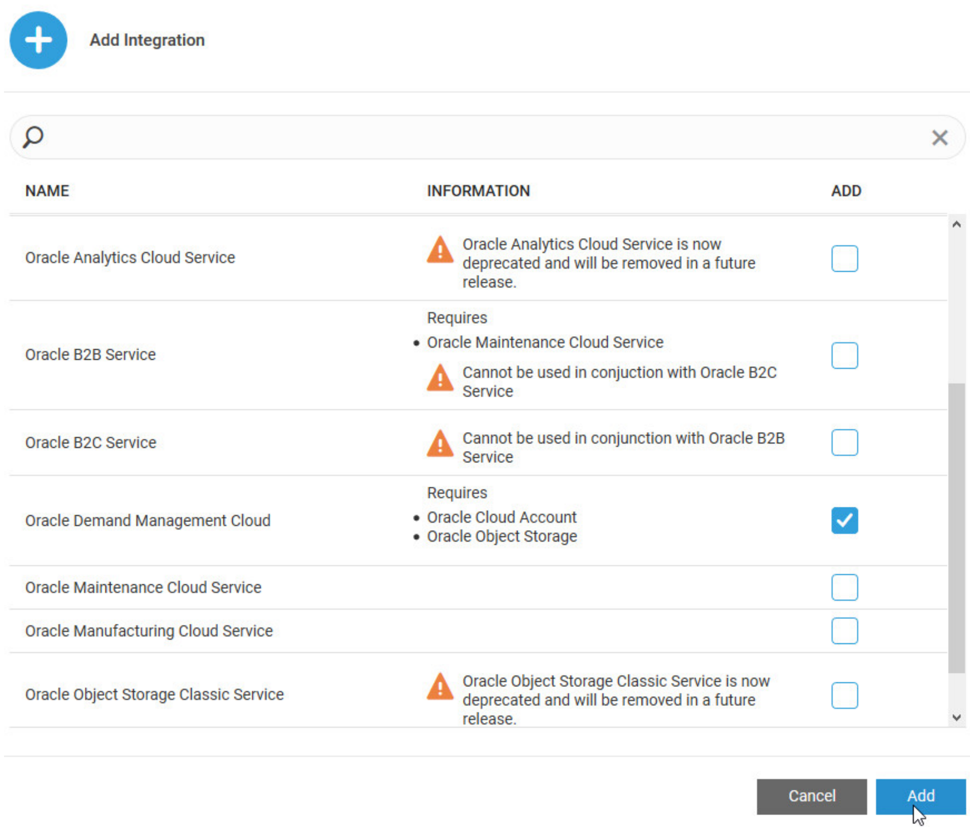
   `https://`*`hostname`*`/am`

Here, *hostname* is the host name of your Oracle Internet of Things Intelligent Applications Cloud instance.

If you are in the Design Center, you need to click **Previous** ( ) before you see the **Settings** option in the menu.

2. Click **Integrations**.
3. Click **Add** to add a new integration.
4. In the Add Integration dialog, select **Oracle Demand Management Cloud** and click **Add**.

   Tip: You can also search for an integration name in the list.



   Oracle Demand Management Cloud Service integration gets added to the Integrations page.

Enable and Configure the Integration with Demand Management

To start using the Demand Management integration, enable and configure the integration for **Oracle Demand Management Cloud Service** on the Integrations page.

1. In Oracle IoT Asset Monitoring Cloud Service, click **Menu** ( ), and then click **Settings**.
2. Click **Integrations**.
3. Under **Oracle Demand Management Cloud Service**, click **Connect**.

The Oracle Demand Management Cloud Service Connection dialog appears.

4. Select the **Object Storage Integration** to use.
5. Under **Object Storage Container**, enter the name of the bucket in OCI Object Storage that stores the data extracted by the Business Intelligence Cloud Connector (BICC) from Demand Management.
6. Click **Save**.
7. Under **Oracle Demand Management Cloud Service**, click **Edit Configuration**.
8. Toggle the **Integration Status** switch to **ON** and click **Save**.

   This enables your Demand Management integration.

After you enable the integration, Demand Management ingests product item and sales history data into OCI Object Storage, as batches of compressed `csv` files `(.gz)`. Demand Management uses REST APIs to request and communicate with Oracle IoT Asset Monitoring Cloud Service.

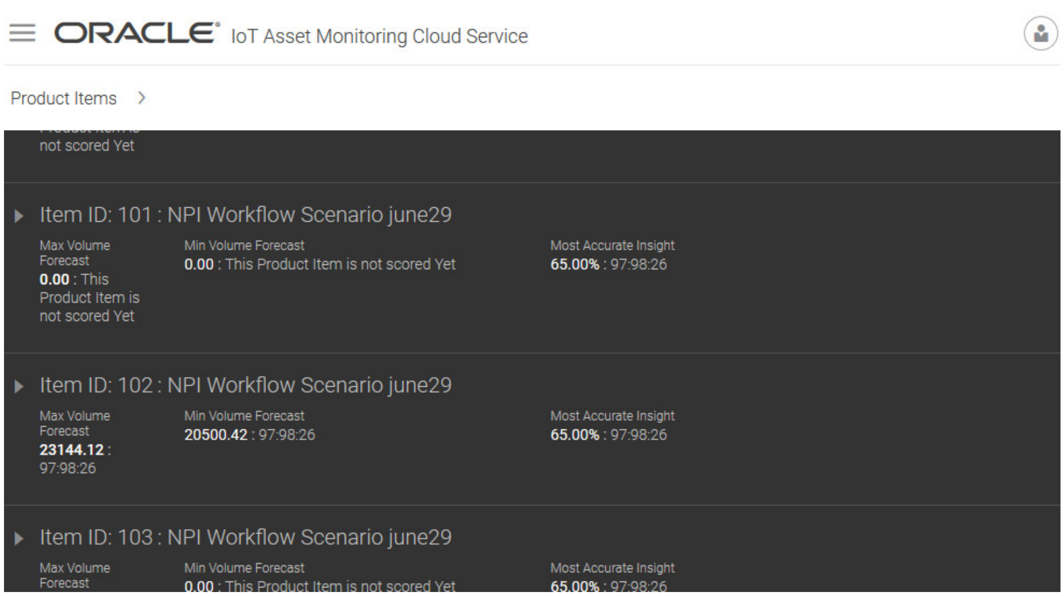
Demand Management then triggers a training request to Oracle IoT Asset Monitoring Cloud Service to gain insights into the data provided. Once the training is completed, Demand Management triggers scoring requests for forecasts. Demand Management retrieves the results and forecast recommendations from Oracle IoT Asset Monitoring Cloud Service.

View Product Items, Scenarios, Insights, and Forecasts

After you enable integration with Demand Management, the Product Items page becomes available in Oracle IoT Asset Monitoring Cloud Service.

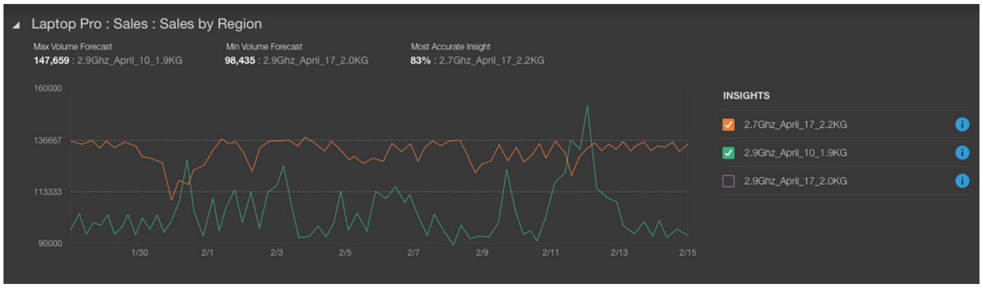
1. Click **Menu** (≡), and then click **Product Items**.

   The Product Items page appears only if Demand Management integration is enabled.

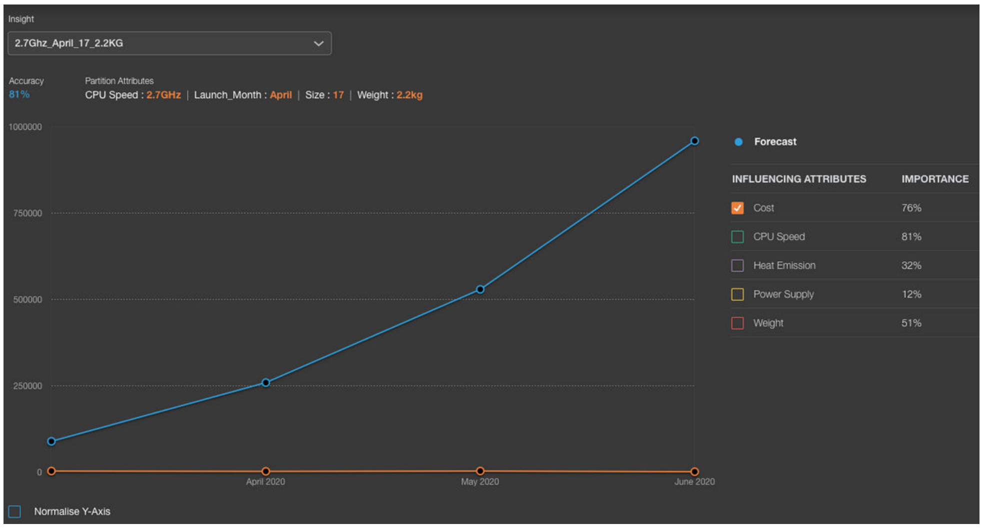


The product items are listed along with the scenarios. The most recent scenarios are shown first. The forecast values associated with the product items, if already scored, are also shown. The insight accuracy shows the accuracy percentage for the most accurate insight.

2. Click on a product item scenario row to see the forecast chart.



3. Click an Insight information icon to see more details on an insight.



Demand Management links also take you to the Insight page.

Use Asset Monitoring Widgets in Your Application

Oracle IoT Asset Monitoring Cloud Serviceprovides 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:

   ```
   <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.

8 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

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** () 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 Intelligent Applications Cloud.

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** ( ) icon.
4. Tap the **Set Location** ( ) icon.
5. Drag the map until the **Target** ( ) 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** (≡) icon, and then tap the **Search** ( ) 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 (<) 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** (≡) icon, and then tap the **Information** ( ) 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** (≡) icon, and then tap the**Information** ( ) icon.
2. Tap **Logout**.