Getting Started with OPM Cloud

Contents

Copyright GE Digital

© 2020 General Electric Company.

GE, the GE Monogram, and Predix are either registered trademarks or trademarks of General Electric Company. All other trademarks are the property of their respective owners.

This document may contain Confidential/Proprietary information of General Electric Company and/or its suppliers or vendors. Distribution or reproduction is prohibited without permission.

THIS DOCUMENT AND ITS CONTENTS ARE PROVIDED "AS IS," WITH NO REPRESENTATION OR WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF DESIGN, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. ALL OTHER LIABILITY ARISING FROM RELIANCE UPON ANY INFORMATION CONTAINED HEREIN IS EXPRESSLY DISCLAIMED.

Access to and use of the software described in this document is conditioned on acceptance of the End User License Agreement and compliance with its terms.

About OPM

About the Operations Performance Management Solution

Operations Performance Management (OPM) is a complete control-to-cloud optimization solution. Using OPM, you can optimize the performance and throughput of your plants, sites, and portfolio by stabilizing your operation and optimizing yield, quality, and efficiency. You can thus increase the revenue and margin of the organization.

Advantages of OPM:

- OPM provides a cloud-based distributed computation framework to define and run key performance indicator (KPI) calculations. The framework provides services and applications to build different types of KPIs to serve purposes such as tracking and analyzing manufacturing processes, or monitoring the health of industrial assets.
- It supports operational decision-making so that you can rapidly respond to changing conditions. It provides accurate, clear, and complete situational awareness to help you maximize outcomes.
- It provides access to critical production and operations data anytime and anywhere.
- You can deploy OPM on-premises and in the could on GE's Predix platform. Predix enables industrial-scale analytics and brings the right data to bear, at the right time, to drive better operating decisions.

Using Operations Performance Management (OPM), you can build web-based analytics dashboards with reusable KPI charts and templates.

The framework provides services that can be extended to perform the following tasks:

- Support multiple tenants instances and manage them separately.
- Create analytic computation artifacts to upload to the APM common analytic framework's catalog.
- Build the analytic template.
- Create analytic deployments.
- Deploy KPI jobs to run on one or many assets and run jobs in Spark runtime.
- Batch load data and run analytics.
- Stream data for generating KPIs in near real-time.
- Generate forecasted data using the forecast widget services and app.
- Audit and log KPI catalog management activities for adherence to compliance requirements. The audit logs provide a chronological record of user activities associated with creating, updating, and deleting KPI templates and with deployment and scheduling KPIs within KPI Management.

When to Use OPM Cloud

There are certain scenarios where OPM Cloud based analytics are particularly recommended.

The three main optimization focus areas of the framework are as follows.

Operational Intelligence

Operational intelligence is to proactively respond to business KPIs and enable centralized benchmarking for increased efficiency. The following are examples of possible applications in this area:

- Throughput and Margin KPIs - Accelerate time to value for Plant Managers and Process Engineers through a KPI catalog giving complex performance and financial KPI calculations including revenue, process efficiency, and process performance.
- Benchmarking - Compare KPIs between multiple sites and the ability to drill-down on contributing factors.

- Audit Logs - Provide audit functionality to track user interactions with system (who, what, when) and changes. The audit logs provide a chronological record of user activities associated with creating, updating, and deleting KPI templates and with deployment and scheduling KPIs within KPI Management.

Forecast

Scenario analysis and planning to ensure confidence to execute best business outcome. The following are examples of possible applications in this area:

- Forecasting - Provide forecasted outcomes (e.g. power output and efficiency calculations) so that managers can evaluate future output against targets and take action to further optimize.

Optimization

Optimize processes and people balancing revenue, costs, and emissions for sites and fleet. The following are examples of possible applications in this area:

- Emissions Optimization - Utilize emissions constraints to ensure that recommended optimized operations do not violate the emissions limits.
- Financial Optimization - Define financial goals (revenue vs. profit) to drive the optimization calculations. Ensure plant operations achieve financial goals.
- Schedule Optimization - Match tasks, tools, and people to ensure an optimized work schedule achieves maximum output.
- Process Optimization - Run the optimization routines on-site and coordinate with the cloud to ensure the models utilized are the latest.

Architecture and Components

The following product architecture shows the components of the framework and its dataflow:
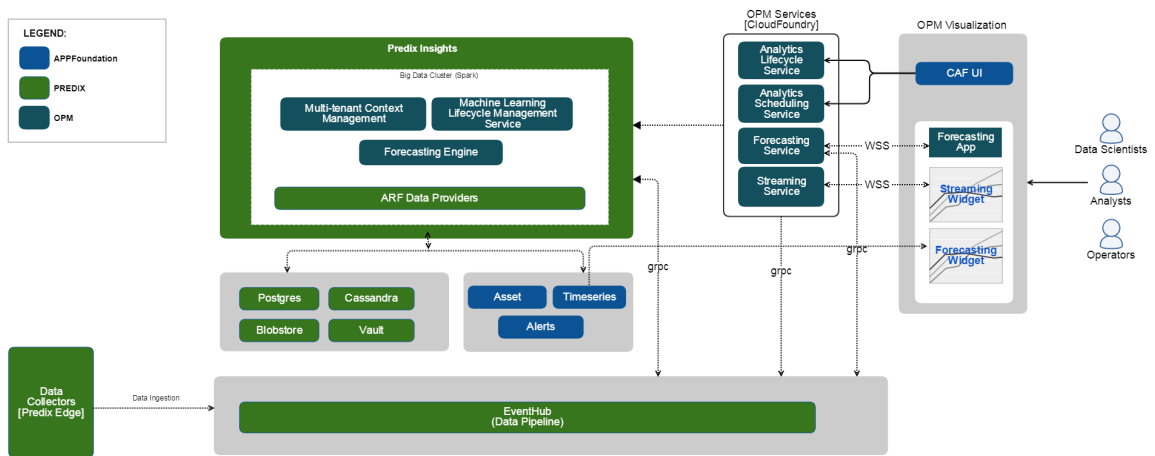
Operations Performance Management consists of the following primary components:

OPM UI Widgets and Apps

The suite of visualization apps that enable you to plot the output tags that the deployed analytic generates. OPM widgets are available in the APM widget library for access to a configured OPM tenant. These widgets are not available as part of the core APM widget library.

OPM Services

A suite of services that provide the ability to define your analytic, add and manage them in the catalog, create and deploy jobs for analytic, and run deployed jobs.

OPM Runtime

The environment for running the deployed analytic jobs. The runtime also houses the forecasting and prediction engines. Apache Spark cluster is the default deployment and runtime environment for the deploying the created analytic.

Operations Performance Management User Workflow

The following diagram provides a workflow overview for the Operations Performance Management users in the system.
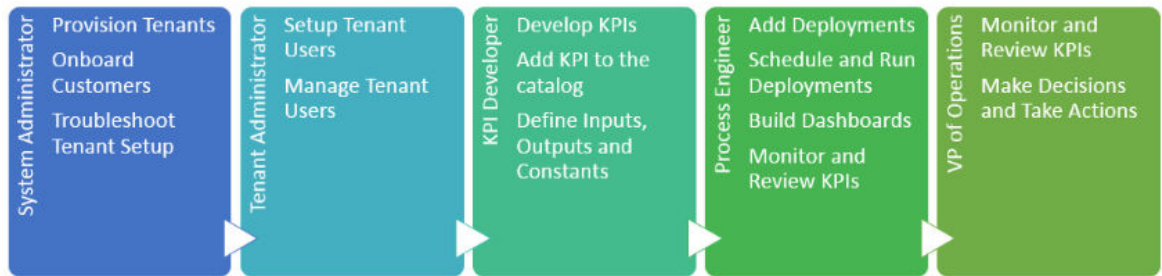

Figure 1: User Workflow

Documentation Scope

The documentation in the **Manage OPM** section covers the concepts and tasks related to the following persona- KPI developers, process engineers, and VP of operations. The system administrator and tenant administrator tasks are not covered here.

OPM Users

The following users may directly or indirectly interact with OPM framework and features:

System Administrator

System administrators need to create customer tenancy and connect their data sources to OPM. They also train customers on how to add their own analytics to the catalog. System administrators use the framework to perform the following tasks

• Provision tenants for customers.
• Set up new customers.
• Provide customer support for using OPM.

Tenant Administrator

Tenanat administrators manage users within a tenant. They can perform the following tasks:

• Set up users within a tenant.
• Manage users within a tenant.
• Manage access to assets and features for users within a tenant.

Analytics Developers and Data Scientists

These users employ historical data to study data patterns, draw insights and identify both asset and non-asset key performance indicators relevant to their industry needs. They have granular knowledge of data and data statistics, and use programming languages such as Java and Python to develop the analytic templates and deployment jobs. They use the framework to perform the following tasks:

- Build the analytic's computation logic.
- Test and validate the analytics.
- Add analytics to the catalog.
- Create analytic template definitions.

Process Engineer

Process engineers monitor and analyze current processes to identify areas for improvement. They work closely with data scientists and analytic developers to define and test algorithm efficacy. Technically competent, they are also familiar with analytic users. Process engineers proactively monitor analytic ouputs to identify early risks and anomalies. They use the framework to perform the following tasks:

- Add analytic deployments.
- Schedule and run analytic deployments for published analytics.
- Build context-aware, industry-specific dashboards (contextual dashboard).
- Configure dashboards with existing analytic ouputs from the catalog.
- Monitor and review analytic ouputs.
- Report targets and risks based on KPIs.

VP of Operations

Operations executives can use customized analytics dashboards to perform the following actions:

- Monitor and review analytics at organization or group level. For example, a plant manager may be interested in viewing the yield of a product.
- Make decisions and take required actions.

OPM Tenants

About OPM Tenants

Operations Performance Management (OPM) utilizes the platform's tenancy management services to support multitenancy. A tenant is a group of users that shares a common access to a specific OPM application instance. A common set of underlying web services provides functionality to each tenant and provides secure access to customer-specific resources and data.

A system administrator creates tenants for customer access. When adding a new tenant, the system administrator assigns a primary administrator for that tenant.

After a customer is onboarded to a new tenant the following happen:

- Tenants subscribe to use OPM services and apps.
- The platform's tenant provisioning service creates a tenant-specific application instance for OPM.

In the newly configured tenant, the primary tenant administrator can log on to complete the initial setup tasks, such as setting the ingestor password, creating users, and assigning user privileges.

Set Up Your Tenant Structure

Before users can access the application (specific tenant organization), the OPM tenant or user administrator must set up the tenant structure.

The tenant administrator needs to complete the following tasks to support a tenant architecture in OPM:

- Create a permission set to enable asset ingestion and add a user with this permission set. This step is essential before ingesting assets into the tenant.
- Add other users and administrators.
- Ingest asset model, tag classification and data (including asset instances, connections, and tag associations).
- Ingest the time-series data for the input tags to be used in the analytics.
- Ingest alert templates necessary for building your analytic template.
- Add user groups and link them to the appropriate permission sets.
- Add assets to users and user groups.
- Register your tenant's Event Hub with the Alerts service on production.

Configure Tenant Display Preferences

You can configure the display preferences for all the users of the tenant.

Before You Begin

You must have tenant admin permissions to access the **Tenant Preferences** page.

Procedure

1.
   The **Tenant Preferences** page appears.
2. Select the **Display** tab.
3. As needed, enter the values in the following fields.

Field Names	Description
Asset Display Name	Displays the name of the asset based on the following options: • GE: Displays the asset name. By default, this option is selected. • Customer: Displays the alias name of the asset that you provided. This name appears on the Asset page. Select the (⦂) button to switch between GE and Customer name.
Language	Determines the display language. By default, **US English** is selected. You can select the preferred language from the following options: • Chinese (Simplified) • Dutch (Netherlands) • French (France) • German (Germany) • Italian (Italy) • Japanese • Polish • Portuguese (Brazil) • Russian • Spanish (Spain) • US English
System of Measure	Determines the system of measure. You can select your preferred system of measure in the drop-down list box. **Note:** The values in the drop-down list box appear based on the values that you configure in the **Systems of Measure Configuration** section. **None** and **Metric** are the system-provided system of measures, and by default, **None** is selected.
TimeZone	Determines the time zone of your location. You can select your preferred time zone from the drop-down list box. If you select **Site Local** as your preferred time zone, all the date or time values will be converted to the time zone of your asset. **Note:** • The selected time zone affects only this application. • Any selected time zone that observes Daylight Savings Time automatically observes the local time.

4. Select **Save**.
   A message appears, indicating that the changes will take effect after you log out and then log in to the application.
5. Select **OK**.

Next Steps

Log out of the application and then log in for the changes to take effect.

Note: The display preferences that are configured in the **Tenant Preferences** page appear as default preferences for all users of the tenant, except for the users who have set their own display preferences in the **User Preferences** page.

Configure the Module Navigation Menu Using Navigation Profiles

A navigation profile contains information about the set of menu items that should appear in the module navigation menu.

Before You Begin

• Ensure that you have the tenant admin permissions to access the **Tenant Preferences** page.

About This Task

You can select a navigation profile if you want to switch to the user interface of a specific product for all the users of a tenant. For example, if you want to change the user interface to display the menu that is available for GE Digital APM, you can select the APM navigation profile. The following navigation profiles are available for you to select:

- APM
- Predix Essentials
- Predix Essentials & APM
- Predix Essentials & OPM
- Predix Essentials, APM & OPM

The following images display the different sets of menu items that appear based on the navigation profiles that you select:

- Module navigation menu that appears when you select the APM navigation profile.
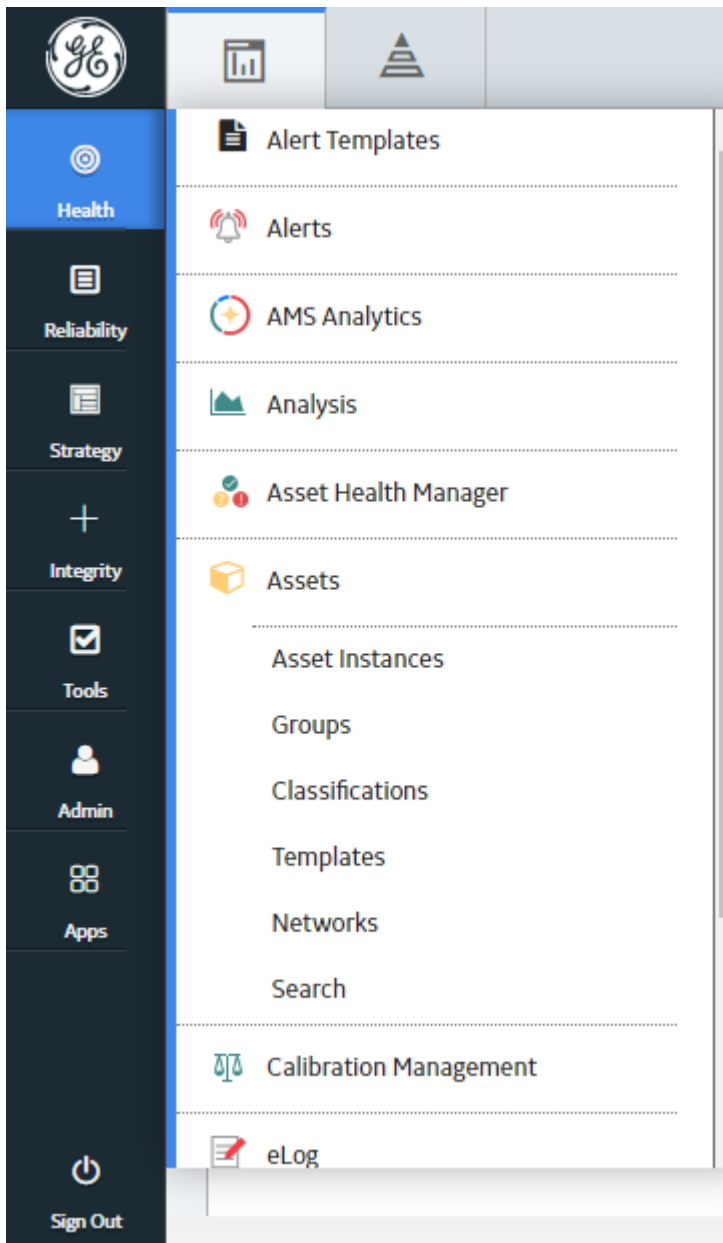
- Module navigation menu that appears when you select the Predix Essentials navigation profile.
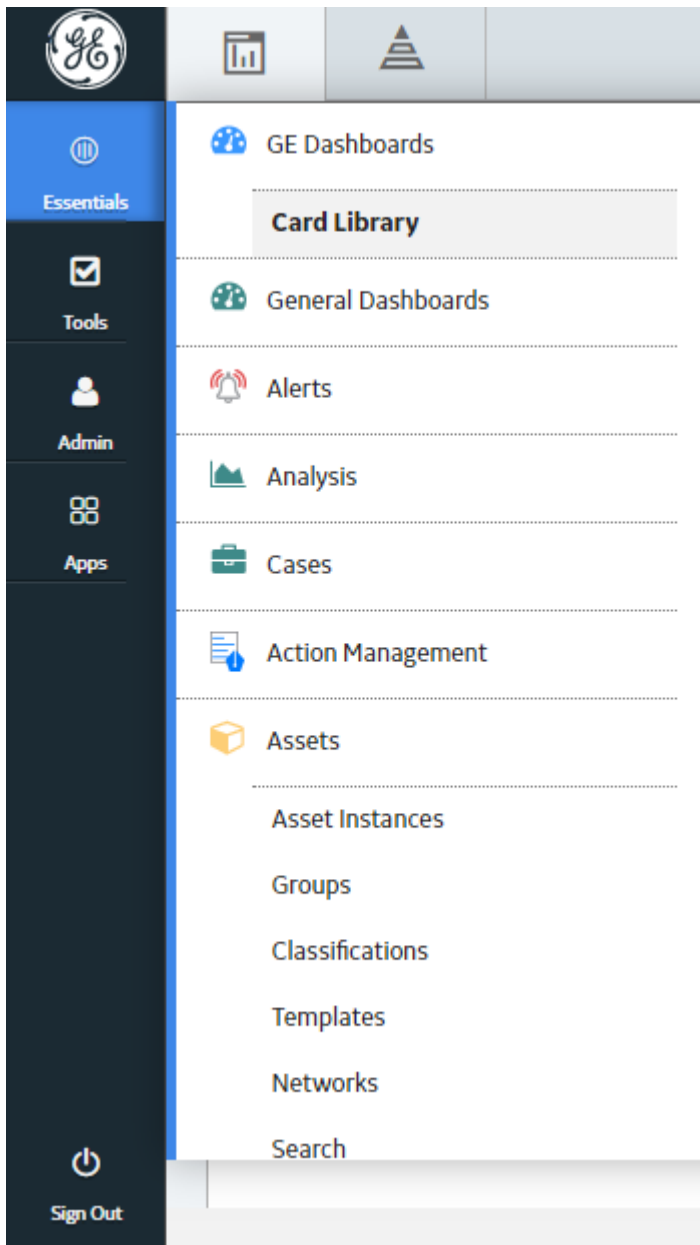
• Module navigation menu that appears when you select the Predix Essentials & OPM navigation profile.
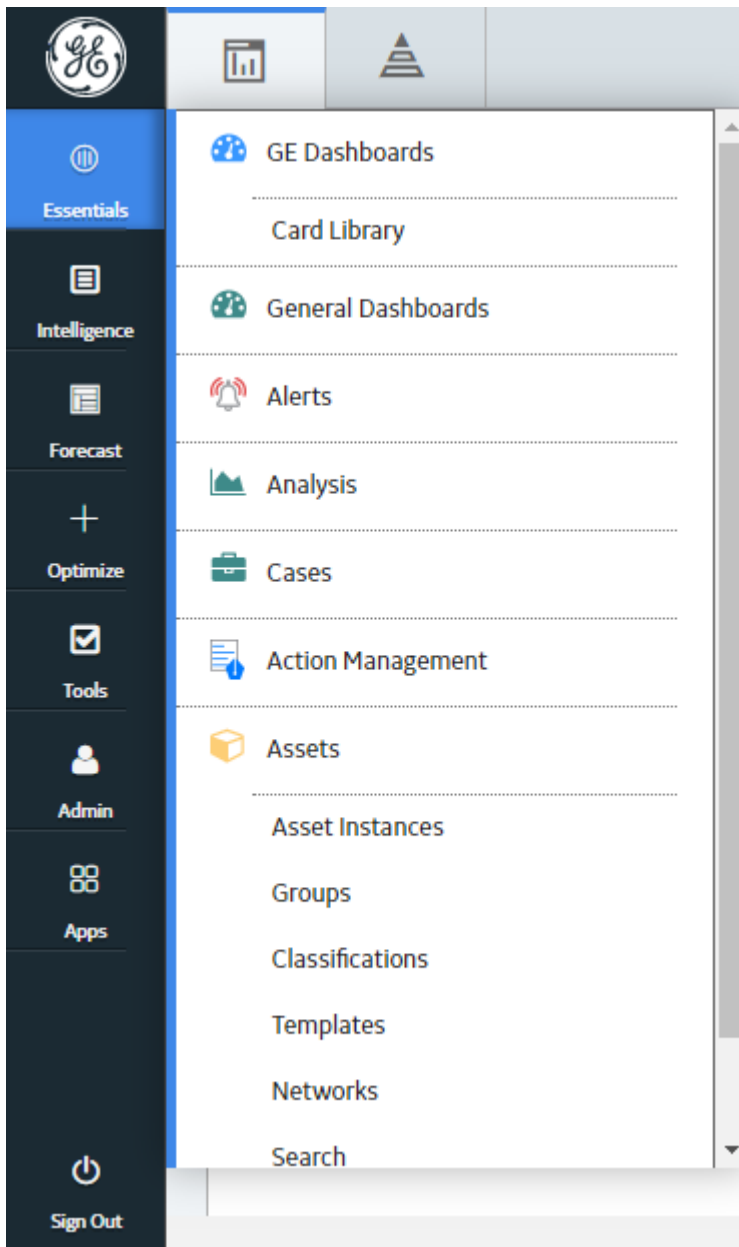
Procedure

1. In the module navigation menu, navigate to **Tenant Preferences**.
   The **Tenant Preferences** page appears.
2. Select the **Module Navigation** tab.
   The **Module Navigation** section appears.
3. In the **Select a Navigation Profile** drop-down list box, select the products that you want to appear in the module navigation menu.

   Note: If you select a navigation profile other than the default navigation profile, only the module navigation menu configured for that profile appears. You cannot access custom applications using the menu.

   or

Select **Reset Module Navigation Settings to Default**.

Note: This setting shows menu items that are based on your permissions.

A message appears, stating that your changes are saved. This configuration is applied to all the users of the tenant.

Note: You can access only the menu items for which you have permission to access.

Next Steps

Sign out of the application, and then sign in to access the module navigation menu that you have configured.

Set or Change the Ingestor Password

Before You Begin

You must have an tenant available. You must also have tenant administrator credentials to perform the initial tenant setup.

About This Task

During tenant setup, you must provide the ingestor password used by asset and alert ingestion services to ingest assets, alerts, and time series data into your current tenant. This password is unique to each tenant, as the asset model and instances are exclusive to that tenant. Provide a complex password that complies with your enterprise policies for password safekeeping.

When setting or changing a password, use the following guidelines:

- The password is case-sensitive and should be at least *eight* characters long.
- You must use a combination of alphanumeric characters.
- You can use special characters.
- You cannot use consecutive characters such as `123` or `abc`.
- You cannot repeat characters more than two times consecutively; for example, `looop` or `777`.

The following are examples of *invalid* passwords:

```
Aaaron777
b!rthday20009
@bc1xyz
rapper123
```

After setup, you can also change the ingestor password at any time.

Procedure

1. Sign in to your tenant with your administrator credentials.
2.
3. Depending on whether you are setting up a new password or changing the password, one of the following applies:
   - If you are setting up the password for the first time, you will be presented with a password setup page.
   - If you are changing an existing password, click **Change Ingestor Password**.
4. Enter a new password, and then re-enter the password to confirm.
5. Select **Submit** to save your changes.

Next Steps

Once the password is set, you can ingest data into .

Obtain the Authorization Token for Data Ingestion

Before You Begin

You need the following:

- The token request URL.
- Get the following information from the Setup section:
  ◦ Token Request URL
  ◦ Client ID
  ◦ Username
- The ingestion password that you set up during first-time tenant access as an administrator.
- Access to a REST client such as Postman or Advanced REST client, or curl CLI.

About This Task

Use this procedure to obtain an authorization bearer token before ingesting data (assets, alerts, or time series) into a specific tenant. Tokens are client-specific and usually expire within a set time period. You must obtain a new token every time your token expires.

Procedure

1. Access your REST client.
2. Enter the token request URL in the **HOST value** field.

   Note: This URL is used to authenticate the token before connecting to the respective ingestion service. You can obtain this from the **Setup** section.
3. Select the POST method.
4. In the request authorization: enter or select the following:

   a) Select `Basic Auth`.
   b) In the **Username** field, enter the Client ID obtained from the Setup section.
   c) Leave the password blank.

   The authorization headers auto populate in the request.
5. In the request body, select **x-www-form-urlencoded**.
6. Enter the following query parameters (key-value pairs):

   Note: You can obtain the values from the **Setup** section.

Option	
grant_type	Grant type for ingestion. The default value is `password`.
username	Ingestion account username (for example, `07F28C049E0F4F29B8E85E4A6C916D7F_ingestor`).
password	Ingestion account password created during the initial tenant setup.
7. Select **Send**.

Results

On successful ingestion, you receive the authorization bearer token as a JSON response; copy this information into a temporary file. Also, make note of the `expires_in` field in the JSON response, as it gives the expiration time in seconds.

Example

The following code sample shows a JSON response :

```
{
  "access_token":
"eyJhbGciOiJSUzI1NiJ9.eyJqdGkiOiI1ZTJjOTBlYS05ZWRkLTRkYTE
tODBjOC00YTBkNjdmNzdlZjMiLCJzdWIiOiI2YWY0YjBlNi1mZmY4LTRm
OWEtYTdhNC1mYzI5Nzg4ZTY5YzAiLCJzY29wZSI6WyJvcGVuaWQiXSwiY
2xpZW50X2lkIjoiaW5nZXN0b3IuREU2QjcxODQyODI0NENGMkE0MDlGM0
YwRUU1OTBBNzQiLCJjaWQiOiJpbmdlc3Rvci5ERTZCNzE4NDI4MjQ0Q0Y
yQTQwOUYzRjBFRTU5MEE3NCIsImF6cCI6ImluZ2VzdG9yLkRFNkI3MTg0
MjgyNDRDRjJBNDA5RjNGMEVFNTkwQTc0IiwiZ3JhbnRfdHlwZSI6InBhc
3N3b3JkIiwidXNlcl9pZCI6IjZhZjRiMGU2LWZmZjgtNGY5YS1hN2E0LW
ZjMjk3ODhlNjljMCIsIm9yaWdpbiI6InVhYSIsInVzZXJfbmFtZSI6Ijl
CMjY0QUU3MDk2NzQ3QzM4MEM2QjA5OUU2NkQ3NTddBX2luZ2VzdG9yIiwi
ZW1haWwiOiI5QjI2NEFFNzA5Njc0N0MzODBDNkIwOTlFNjZENzU3QV9pb
mdlc3RvckBhcG0tYXBwbGljYXRpb24tYWNjZXB0YW5jZS5ncmMtYXBwcy
5zdmMuaWNlLmdlLmNvbSIsImF1dGhfdGltZSI6MTQ0OTE2NTQyNywicmV
2X3NpZyI6ImJiNjI3MzU0IiwiaWF0IjoxNDQ5MTY1NDI3LCJleHAiOjE0
NDkyNTE4MjcsImlzcyI6Imh0dHBzOi8vMDRiOGM4OTEtZWRlYS00NGQ0L
WI3YmEtYmIzMGQ3MDA2ZDU5LnByZWRpeC11YWEtc3lzaW50LmdyYy1hcH
BzLnN2Yy5pY2UuZ2UuY29tL29hdXRoL3Rva2VuIiwiemlkIjoiMDRiOGM
4OTEtZWRlYS00NGQ0LWI3YmEtYmIzMGQ3MDA2ZDU5IiwiYXVkIjpbImlu
Z2VzdG9yLkRFNkI3MTg0MjgyNDRDRjJBNDA5RjNGMEVFNTkwQTc0Iiwib
3BlbmlkIl19.dtcD0uYyahB0ocp6I7xPoefwAxPBiXx0yqVxrmPHxagXE
wuK9a1SswiG9-
dIByf6ty2PMPDau4UeMwxzZg29DE6qxfEWXEOP4J7Uy_H2AiM9V9WqJg7
Q2NbVoEYwlKfnH8RIScz20nDLP1IEqFH1d1Kf7MhXwxhcLVed250Z0I7q
mMlB1axqjcWqeBv2BdLUlgja1o5YOa9A9xq46rwZ81TyGyAu9_UavibYO
6H9l4cYQYJkU5TwFJdY4D83hvxRtXpUownDC7wHVWDHUP1DXpu44F3uMk
BB40K8FqbzQQmhujOmSbV5hdVaSF_QBu71a59KI78knEyclDa0BK5GHA"
,
  "token_type": "bearer",
  "refresh_token":
"eyJhbGciOiJSUzI1NiJ9.eyJqdGkiOiIzZTU0NTgzZS0xZjIwLTQ0ZjU
tODk2NC0zMTQxNDcyYzhiMzUtciciIsInN1YiI6IjZhZjRiMGU2LWZmZjgt
NGY5YS1hN2E0LWZjMjk3ODhlNjljMCIsInNjb3BlIjpbIm9wZW5pZCJdL
CJpYXQiOjE0NDkxNjU0MjcsImV4cCI6MTQ0OTc3MDIyNywiY2lkIjoiaW
5nZXN0b3IuREU2QjcxODQyODI0NENGMkE0MDlGM0YwRUU1OTBBNzQiLCJ
jbGllbnRfaWQiOiJpbmdlc3Rvci5ERTZCNzE4NDI4MjQ0Q0YyQTQwOUYz
RjBFRTU5MEE3NCIsImlzcyI6Imh0dHBzOi8vMDRiOGM4OTEtZWRlYS00N
GQ0LWI3YmEtYmIzMGQ3MDA2ZDU5LnByZWRpeC11YWEtc3lzaW50LmdyYy
1hcHBzLnN2Yy5pY2UuZ2UuY29tL29hdXRoL3Rva2VuIiwiemlkIjoiMDR
iOGM4OTEtZWRlYS00NGQ0LWI3YmEtYmIzMGQ3MDA2ZDU5IiwiZ3JhbnRf
dHlwZSI6InBhc3N3b3JkIiwidXNlcl9uYW1lIjoiOUIyNjRBRTcwOTY3N
DdDMzgwQzZCMDk5RTY2RDc1N0FfaW5nZXN0b3IiLCJvcmlnaW4iOiJ1YW
EiLCJ1c2VyX2lkIjoiNmFmNGIwZTYtZmZmOC00ZjlhLWE3YTQtZmMyOTc
4OGU2OWMwIiwicmV2X3NpZyI6ImJiNjI3MzU0IiwiYXVkIjpbImluZ2Vz
dG9yLkRFNkI3MTg0MjgyNDRDRjJBNDA5RjNGMEVFNTkwQTc0Iiwib3Blb
mlkIl19.Kc4PioQAOeHNeGacFwfePhLSogh06RR8c4zQPPr46rD_S49UH
egOq1Uv3cWnP6sttL25GaPeidTnYyFLADFF-
GyORkdmKUjx4CiAdQucoKusidjoNJQmaQNhicL62B2goUNf9VYztjrBqH
```

```
GZkKt2DvdtU0RtXAkgc-
qFUo2ToMQj86hqc80OhiIb_2mnXOOWZswrrfxPizgk9zL22-
i6a00LGsptJZ2ErCDSmpGBka6h6H-
N8vVWTsOhx_nnp7jUHKGZOZQjcsqSIWwRosIE_G6kgGMpL2L_bLgDVpZi
Q3Ri19K5J7co1y4TqjMF3kvXb0rOdIJsDO1PCfMztAazlw",
   "expires_in": 86399,
   "scope": "openid",
   "jti": "5e2c90ea-9edd-4da1-80c8-4a0d67f77ef3"
}
```

Next Steps

You can perform data ingestion.

Register your OPM Tenant with Alert Service

As a tenant administrator, you must register your production ready OPM tenant specific Event Hub instance with the Alert Service in production.

Before You Begin

You need the following:

- Oauth token to register with the Alert service Event Hub instance for your tenant.

  Important: Make sure you have a valid, unexpired token. Tokens are client specific and usually expire within a set time. Look for the token expiration in the JSON response.
- On the **Setup** section, get the following information:
  - Client ID
  - Alert service URL
  - Username
- Tenant specific event hub zoneId
- Tenant specific username and password (for example, analytics.user.<tenant alias>)
- Ingestion Password that was created during initial tenant setup.
- Access to a REST client such as Postman or Advanced REST client.

About This Task

Procedure

1. Access your REST client.
2. Enter the Alert service URL in the **HOST value** field, for example, `https://apm-event-ingestor-alerts-svc-prod.app-api.aws-usw02-pr.predix.io/v1/addConfig`.
3. Select the **POST** method.
4. In the **Body** tab, enter the following key-value pairs:

Table 1: Service Headers

Parameter	Description
Authorization	Enter the token_type followed by a space, then the access_token from the response you previously obtained, for example, `bearer eyJhbGciOiJSUzI1NiJ9.A...` The following code sample includes a bearer token: ```{ "access_token": "eyJhbGciOiJSUzI1NiJ9.A...", "token_type": "bearer", "refresh_token": "eyJhbGciOiJSUzI1NiJ9.e..", "expires_in": 86399, "scope": "openid", "jti": "5e2c90ea-9edd-4da1-80c8-4a0d67f77ef3" }```
tenant	The unique ID for the tenant (for example, `07F28C049E0F4F29B8E85E4A6C916D7F`)
Content-Type	Select `application/json`

5. In the body enter the payload. The example payload shows variables within angular brackets <> replace them with the appropriate values.

```
{
"scopePrefix":"predix-event-hub.zones",
"eventHubUri":"event-hub-aws-usw02.data-services.predix.io",
"eventhubPort":443,
"apmAuthUrl":"https://d1e53858-2903-4c21-86c0-95edc7a5cef2.predix-
uaa.run.aws-usw02-pr.ice.predix.io/oauth/token",
"authUrl":"https://d1e53858-2903-4c21-86c0-95edc7a5cef2.predix-
uaa.run.aws-usw02-pr.ice.predix.io/oauth/token",
"tenant":"<tenant uuid>",
"ingestorUser":"analytics.user.<tenant alias>",
"password":<"<analytics.user.<tenant alias> password>",
"clientId":"<stuff client id>",
"clientSecret":"<stuff client secret>",
"zoneId":"<eventhub zoneId>",
"ingestorClientId":"<ingestor client id>:"
}
```

Note:

ingestorClientId value requires a terminating colon :

6. Select **Send**.

Results

On successful acceptance, you will receive a 200 OK with the message: `Added configuration for zone: <eventhub zoneId>`