GE VERNOVA

Asset Performance Management

APM Classic

V4.6.11.0.0

Getting Started

Contents

Copyright Digital, part of GE Vernova

Chapter
1

APM Overview

Topics:

- [What is APM?](#)

What is APM?

Production facilities often face problems related to recurring equipment failures, including:

- Unplanned downtime.
- The inability to maintain planned production rates.
- High costs of fixing problems that result from equipment failures.
- Threats to employee and environmental safety.

Data related to equipment failures and the impact that they have on a facility can be recorded using a data collection tool. Collecting failure data alone, however, cannot prevent the same problems from occurring in the future. What production facilities need is a tool that will analyze the failure data to help decrease the number of equipment failures, which will in turn increase profit margins.

The APM system fulfills this need.

You can use APM tools to analyze and process data that is collected in and transferred from an external system (e.g., SAP). After the data exists in APM, it can be analyzed to determine the state of your equipment and the reliability, trends, potential risks, and probability of failures associated with that equipment. Based on the gathered data and associated analyses, you can map out the impact of projected changes and then make recommendations and suggest strategies for future equipment maintenance.

Chapter
2

APM Access

Topics:

Access APM via a Web Browser

Procedure

1. Depending on the type of user, go to the following URLs via a Web browser:
   - If your user account is manually created: `http://<GEDigitalAPMServerAddress>/meridium/index.html?isadmin`
   - If you want to sign in to an SSO-enabled environment: `https://<GEDigitalAPMServerAddress>/meridium/index.html`
   - If you want to sign in to a non SSO-enabled environment, if your account is not created manually, and if you want to be authenticated via an active directory: `http://<GEDigitalAPMServerAddress>/meridium/index.html`
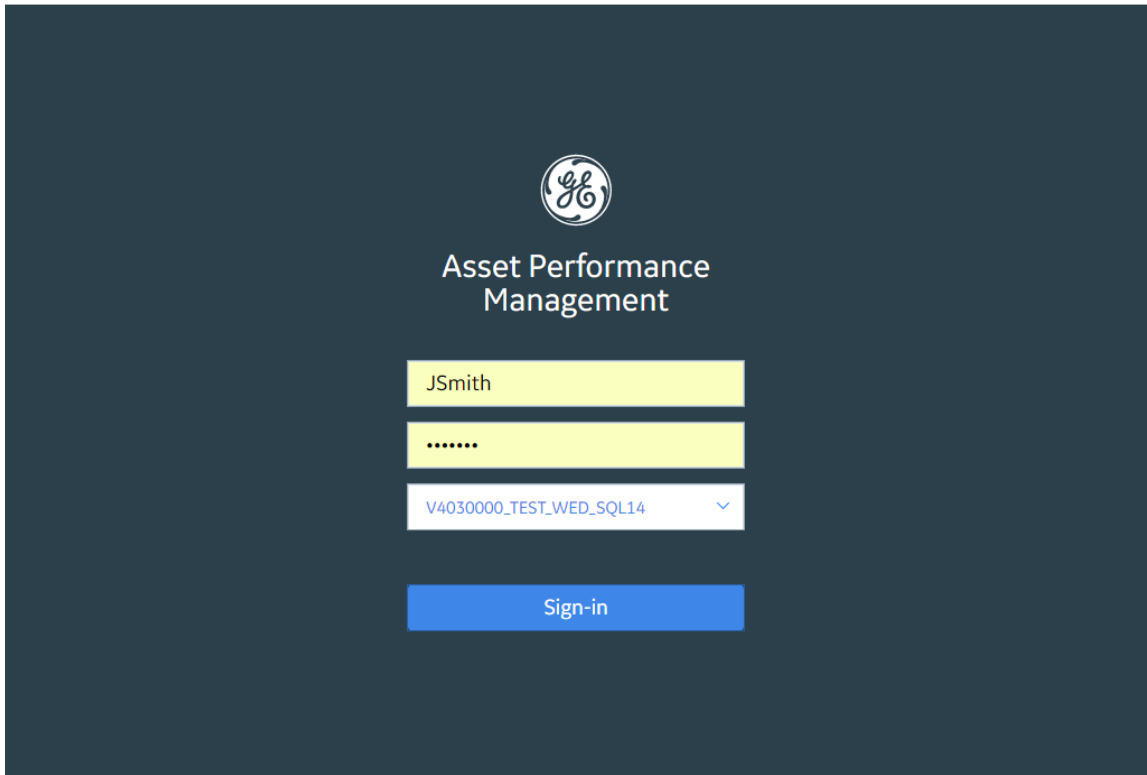
   where, `<GEDigitalAPMServerAddress>` is the address of the APM Application Server to which you want to connect.

   Examples:
   - `http://myserver.mycompany.com/meridium/index.html`
   - `http://myserver/meridium/index.html`
   - `http://172.16.254.1/meridium/index.html`

   Note: If your system uses Data Guardian from Koingo Software and you use the Google Chrome browser, you may have to use the browser in Incognito mode to successfully access APM.

   The login page appears.

2. In the **Username** box, enter your APM User ID.
3. In the **Password** box, enter your password. Passwords are case sensitive.
4. In the list that appears, select the data source to which you want to log in.
5. Select **Sign-in**.

   You are connected to the APM database, and the APM default dashboard page appears.

   Note: When logging in to APM, a notification may appear, asking if you want to allow your machine to be used for additional local storage. This local storage is used to store log in information and preferences. Allowing this local storage is optional.

About Navigating APM via the Asset Hierarchy

APM is built on the premise, within your company, there are multiple functional locations that can be organized in a hierarchy to represent the fact that some locations belong to other locations. These relationships create the Asset Hierarchy.

Navigating the Asset Hierarchy

The Asset Hierarchy allows you to browse your assets from the top-level functional location.

- Company (MRD ~ Meridium, Inc.)
- Sites (MRD-ROA ~ Meridium Roanoke)
- Areas (MRD-ROA-REFN ~ Meridium Roanoke Chemicals)
- Units (MRD-ROA-CHEM-CM101 ~ Meridium Roanoke Chemicals Unit CM101)
- Functional Locations (MRD-ROA-CHEM-CM101-FT101A ~ REACTOR COOLANT FLOW)
- Equipment (G0022-065 ~ 000000000001034757 ~ PUMP)
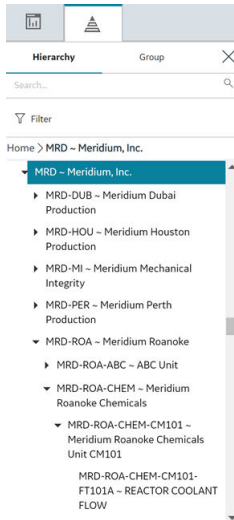
Tip:

- To navigate to a parent-level or child-level equipment or functional location of an asset that is selected in the hierarchy, select the corresponding breadcrumb link in the breadcrumb path.

- To expand or collapse the Asset Hierarchy panel, select ⛭ or ✕, respectively.

- To resize the Asset Hierarchy panel, drag the border of the panel to the required width.

Note:

- As a standard practice, we assume that your equipment is installed in locations that exist on the lowest level of your location hierarchy.

- The Asset Hierarchy displays:

  ○ A maximum of 500 top-level records in the hierarchy.

  ○ A maximum of 500 child equipment or functional locations for a parent functional location.

The <Asset Name> Page

As you navigate through the Asset Hierarchy, at each level, information about the Risk, Strategy, and Performance of that level is displayed on the <Asset Name> page. The <Asset Name> page provides a snapshot of all the data in APM related to the asset selected in the Asset Hierarchy. For each Risk, Strategy, and Performance item, there is a hyperlink displaying the number and type of analysis performed against that asset. The hyperlinks, once selected, open the analyses or inspections on a new page while maintaining the selection in the Asset Hierarchy.

> Example: View An Asset Criticality Analysis from an Asset in the Asset Hierarchy.
>
> 1. In the Asset Hierarchy, navigate to **Meridium Roanoke Refining**.
>
>   Meridium Roanoke Refining is selected in the Asset Hierarchy, and the **Meridium Roanoke Refining** page is displayed, and the **Risk** tab is selected. From this page, you can view the Risk snapshot (e.g. there are 11 ACAs, 8 FMEAs, 12 RCMs, etc.) against the asset, as shown in the following image.
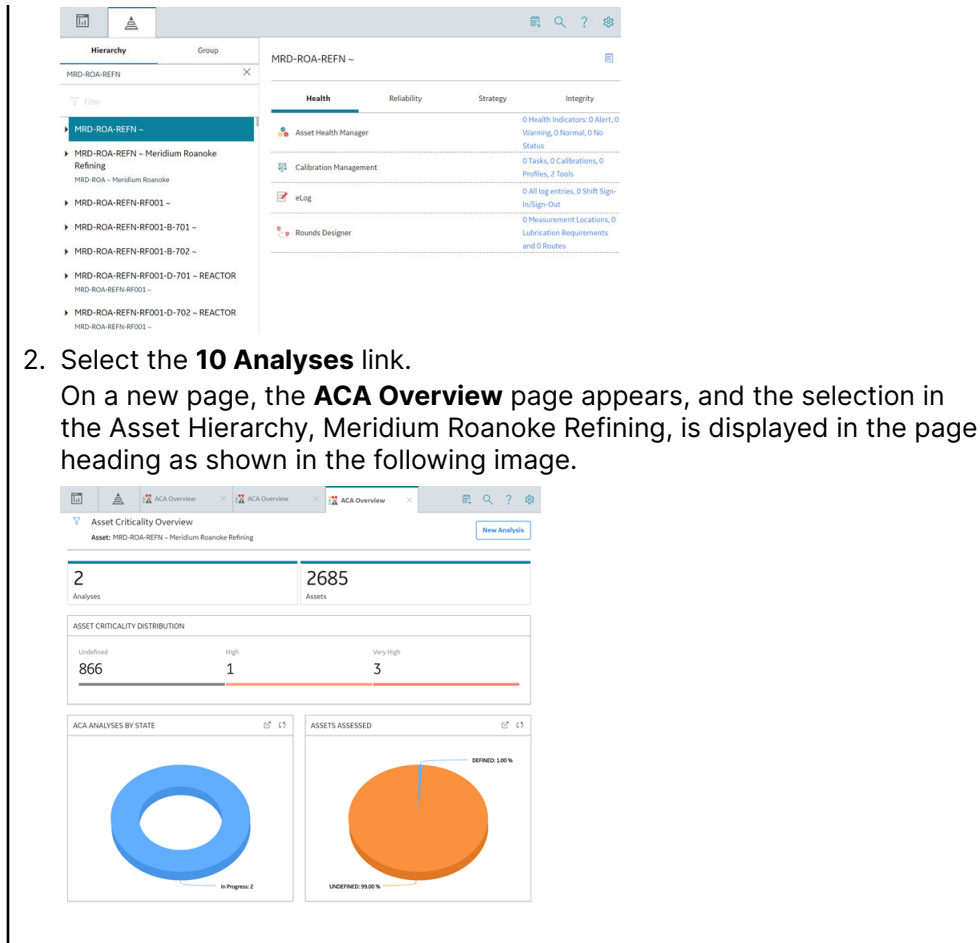
2. Select the **10 Analyses** link.

   On a new page, the **ACA Overview** page appears, and the selection in the Asset Hierarchy, Meridium Roanoke Refining, is displayed in the page heading as shown in the following image.

Navigate APM

All pages in APM are framed by the left navigation menu and the top navigation bar.

The left navigation menu, which appears on the left side of the screen, serves as an access point for each APM module and tool.

The top navigation bar provides access to the following commonly used APM features.

Option	Description
⌂	Provides access to the main dashboard. **Note:** You can configure any General Dashboard or Metrics and Scorecards data to appear on the main dashboard page.
⛰	Provides access to the asset hierarchy and asset grouping functionality.
▤+	Displays a menu from which you can select a family to create a new record.
🔍	Displays the search menu, from which you can search APM for records and other items (e.g., Catalog items).

Option	Description
	Provides access to the APM Help system.
	Displays a menu on which you can select or clear the **Disable Network Connection** and **Compact View** check boxes. When selected, the **Disable Network Connection** check box forces APM to behave as if your device is offline. This is useful if your network connectivity is intermittent. **Note:** If you are using a small screen device, select to access the **Disable Network Connection** check box. The **Compact View** selection persists between user sessions, and can be modified at any time. When selected, this option renders compact layout for the following features of APM: • Result Grid • Datasheet • Left or Collapsible pane • Custom forms and tables

Chapter
3

Mobile Application

Topics:

About the APM Mobile Application

APM provides a mobile app that can be installed on iOS, Android, and Windows devices.

This app offers certain APM functionality designed specifically for use offline and includes the following modules:

- Inspection Management and Inspection Field Data Collection
- Mobile Proof Testing
- Rounds Data Collection
- SIS Management

Note: The Rounds Pro module provides the Rounds Pro mobile application which can be installed on hand-held devices and allows you to collect data. For more information, refer to the Rounds Pro Mobile App section of the Rounds Pro documentation.

Mobile Application Supported Operating Systems

Supported Operating Systems

Important:

- Any management policy applied to mobile devices must be set up to allow the required permissions for the APM mobile application. If restrictions are placed on iOS, Windows, or Android devices by a global policy or mobile device management system, device storage, scanning, photography, location services, and other functionality may be disabled.
- If you are using a Windows device, ensure that Windows App Store access is enabled.
- Ensure that the application is distributed to all relevant devices.

The following table lists the operating systems and corresponding versions that the APM mobile application supports.

Operating System	Version(s) Supported
iOS	12, 13, and 14
Android	7, 8, 9, 10, and 11
Windows	Windows 10 (64 bit)

Note: The method used to access Reference Documents in the GE Digital APM mobile application will vary depending on your device platform. For example, on Windows and Android devices, the first time you access Reference Documents, you will be prompted to select the application in which you want to open a file, and this selection will then become the default. Apple iOS will always prompt you to select an application. On all platforms, you will also be prompted when the platform for your device does not recognize the file type that it is attempting to download.

Install the APM Mobile Application on an iOS Device

We no longer provide unsigned .ipa files for you to sign and distribute in your organization. As per the Apple Developer Program License Agreement and Apple Developer Enterprise

Program License Agreement, you cannot bypass the App Store to distribute apps to non-employees. Starting from APM version 4.4, the GE Digital APM Mobile iOS app is distributed through Apple Business Manager only. You must submit a support request to GE Vernova to distribute the GE Digital APM mobile app through Apple Business Manager.

Before You Begin

An Apple developer's license must be purchased.

Note: This procedure is generally done by your organization's IT team.

Procedure

1. Go to GE Vernova Customer Center at APM Support Teamhttps://digitalsupport.ge.com/.
2. Submit a support request with the following details:
   - Your Apple Organization ID
   - Your Apple Organization Name
   - OnPremises GE Digital APM App Version

Results

After you submit a request, we will validate and distribute the required app version to your organization. Your organization can then view the app in your Apple Business Manager. Apple Business Manager provides multiple options to distribute the app within your organization.

Install the APM Mobile Application on an Android Device

We provide an Android application, but there are specific steps that you must perform to install the APM mobile application on Android devices.

Procedure

1. Access the application package file at `C:\Program Files\Meridium \ApplicationServer\distribution\GEDigitalAPM.apk`.

   Note: This is the default location of the application package file. The exact location at which you can obtain the application package file may differ based on your initial installation of APM.
2. **Optional:** If your organization does not use mobile device management, in the web page from which you want to distribute the application within your organization, add an anchor tag with an href pointing to the installation file, as shown in the following example:
   `<a href="my.company.com/GEDigitalAPM.apk">Install GE Digital APM</a>`

   You can use the link you configured to distribute the application within your organization.

Install the APM Mobile Application on a Windows Device

Procedure

1. Access the application package file at `C:\Program Files\Meridium \ApplicationServer\distribution\GEDigitalAPM.zip`.

Note: This is the default location of the application package file. The exact location at which you can obtain the application package file may differ based on your initial installation of APM.

2. Access the application package file at `C:\Program Files\Meridium \ApplicationServer\distribution\GEDigitalAPM.zip`.

   Note: This is the default location of the application package file. The exact location at which you can obtain the application package file may differ based on your initial installation of APM.

3. On the device on which you want to install the APM mobile application, extract the content of the application package file to a local folder.

4. In the folder into which you extracted the application package file content, right-click **Install.bat**, and then select **Run as an Administrator**.

   Note: If you are using a touch-screen device, press and hold **Install.bat**, and then select **Run as an Administrator**.

   The APM mobile application is installed on the Windows device for all current and future Windows user accounts.

5. **Optional:** To cancel future installations or uninstall the APM mobile application, in the folder into which you extracted the application package file content, right-click **Uninstall.bat**, and then select **Run as an Administrator**.
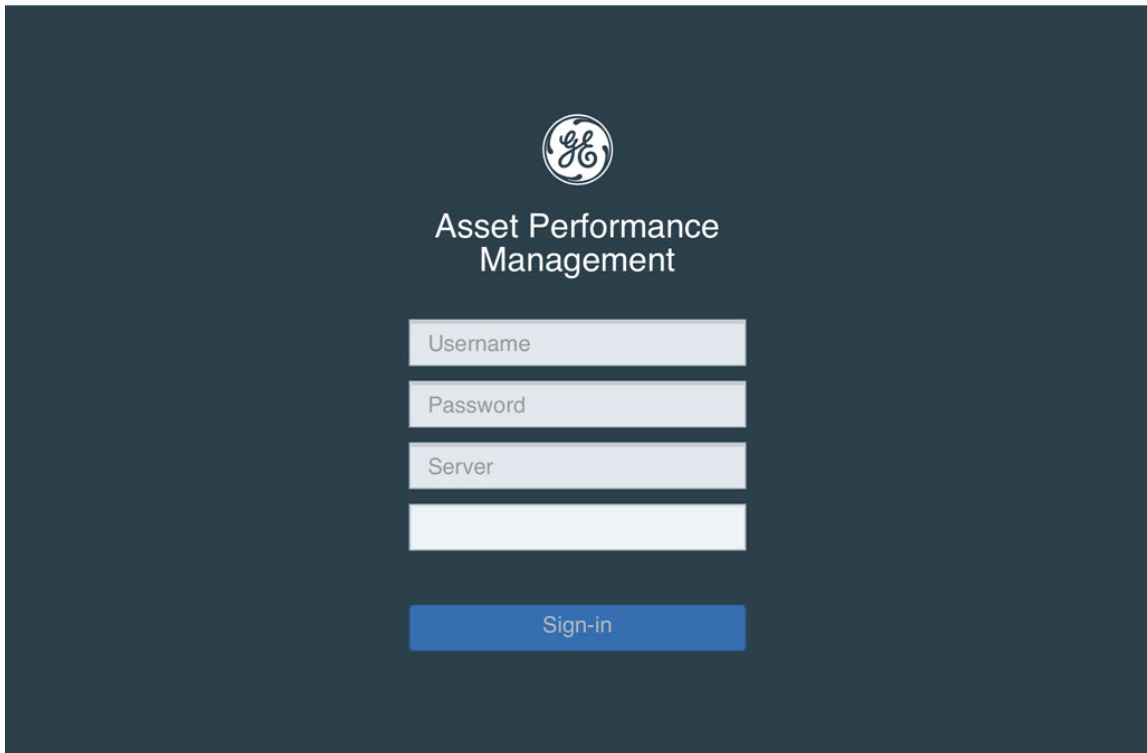
   Note: If you are using a touch-screen device, press and hold **Uninstall.bat**, and then select **Run as an Administrator**.

   The APM mobile application is uninstalled for the Windows user account that is currently logged in, and installations for future Windows user accounts are canceled.

Access APM via the Mobile Application

Procedure

1. On a mobile device, select the APM icon to launch the application.

   The login page appears.

2. In the **Server** box, enter the name or URL of the APM Server to which you want to connect.

   Important:

   If your APM Server is configured to use a secure connection, you must enter the full server URL or IP Address in one of the following formats:

   - `https://<GEDigitalAPMServer.CustomerDomain>`

     -or-
   - `https://<IP address>`

   Examples:

   - `https://myserver.mycompany.com`
   - `https://172.16.254.1`

   A list of data sources configured for the server appears.
3. Select the data source to which you want to log in.
4. In the **Username** box, enter your APM User ID.
5. In the **Password** box, enter your password. Passwords are case sensitive.
6. Select **Login**.

   You are connected to the APM database, and the APM default dashboard page appears.

   Note: When logging in to APM, a notification may appear, asking if you want to allow your machine to be used for additional local storage. This local storage is used to store log in information and preferences. Allowing this local storage is optional.

Access the APM Mobile Application Using Single Sign-On (SSO)

This topic describes how to access the APM mobile application using SSO.

Before You Begin

- Ensure that SSO is configured for APM.

Procedure

1. Start the APM application.
   The APM login page appears.
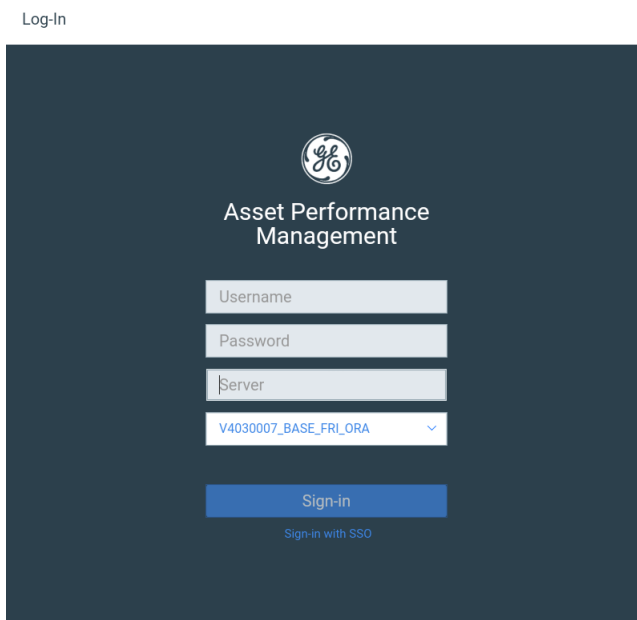
2. In the **Server** box, enter the name or URL of the APM server to which you want to connect.

   Important: If your APM server is configured to use a secure connection, you must enter the URL or IP address of the server in one of the following formats:

   - `<GEDigitalAPMServer.CustomerDomain>` (for example, `myserver.mycompany.com`)
   - <IP address> (for example, 172.16.254.1)

   A list of data sources configured for the server appears.
3. In the drop-down list box, select the data source that you want to access.
4. Select **Sign-in with SSO**.
   The SSO login page appears that is based on the IDP that is selected while configuring SSO.
5. Specify your SSO credentials, and then log in to access APM.
   You are connected to APM, and the default dashboard page appears.

   Note: If you have configured Single Logout, when you log out, you are logged out of the third-party identity provider (IDP) application as well. Therefore, when you attempt to

access the APM mobile application the next time, you are first redirected to the IDP login page where you must enter your SSO credentials again to log in.

Configure Single Logout

About This Task

This topic describes how to configure the settings of the APM mobile application and Active Directory so that after you log out, you are logged out of the third-party identity provider (IDP) application as well. As a result, when you attempt to access the APM mobile application the next time, you are first redirected to the IDP login page where you must enter your SSO credentials again to log in.

Procedure

1. Access the SAML configuration provided in Active Directory, and copy the value provided for the Logout URL parameter. This is the IDP URL to which the APM mobile application sends a SAML logout request when you log out of the APM mobile application.
2. On the machine on which you have installed the APM application server, access the `saml.json` file. By default, it is located in the `C:\Program Files\Meridium\ApplicationServer\api` folder.
3. Insert the following parameter, and assign the Logout URL value that you have copied:

```
SingleLogoutServiceUrl="<Logout URL of the identity provider (IDP)
application>"
```

```
{
    "SAML": {
        "$schema": "https://www.componentspace.com/schemas/saml-
config-schema-v1.0.json",
        "Configurations": [
            {
                "LocalServiceProviderConfiguration": {
                    "Name": "urn:componentspace:Meridium",
                    "AssertionConsumerServiceUrl": "~/core/security/
ssologinauth",
                    "LocalCertificates": [
                        {
                            "FileName": "sp.pfx",
                            "Password": "password"
                        }
                    ]
                },
                "PartnerIdentityProviderConfigurations": [
                    {
                        "Name": "http://fs.xyz.com/adfs/services/
trust",
                        "Description": "ADFS",
                        "SignAuthnRequest": true,
                        "WantSamlResponseSigned": false,
                        "UseEmbeddedCertificate": false,
                        "WantAssertionEncrypted": false,
                        "WantAssertionSigned": true,
                        "SingleSignOnServiceUrl": "https://
fs.xyz.com/adfs/ls/idpinitiatedsignon.aspx",
                        "SingleLogoutServiceUrl": "",
```

```
                         "PartnerCertificates": [
                             {
                                 "FileName": "idp.cer"
                             }
                         ]
                     }
                 ]
             }
         ]
     }
 }
```

4. Access Active Directory, and then under **Basic SAML Configuration**, in the **Logout URL** box, enter a value in the following format:

```
https://<APM Application Server Name>/Meridium/api/core/security/
singlelogout
```

The Logout URL is the APM application URL to which the IDP service sends the SAML logout response after you log out.

After you log out of APM mobile application, when you attempt to log in again, you are prompted to enter your SSO credentials.

Chapter
4

APM Product Workflows

Topics:

APM Product Workflow

The following diagram outlines the integration between the different modules that make up APM.
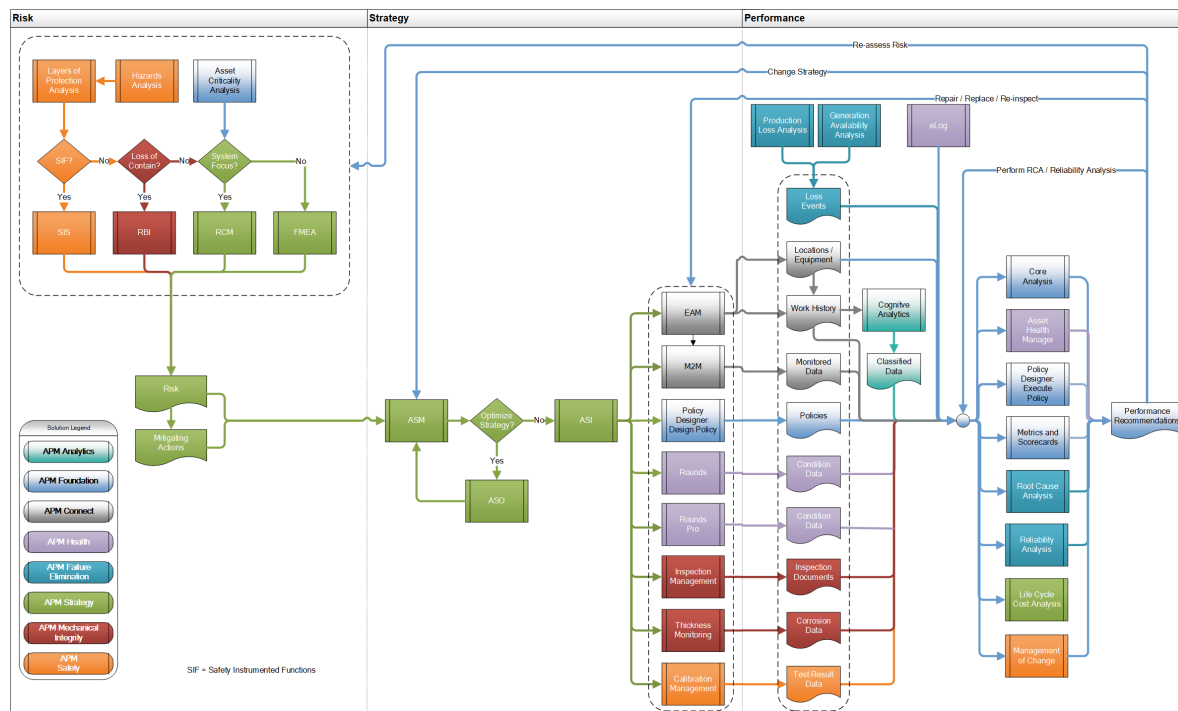
Module-Level Workflows

Each solution within APM consists of multiple modules, each of which is composed of one or more workflows that describe the various capabilities of the module. You can find details about each of these product workflows in the respective module user help.

Tip: Refer to the APM Product Workflow for a visualization of how these modules interact within APM.

APM Analytics

Module	Workflows
Cognitive Analytics	Manage Classifiers
	Manage Cognitions

APM Connect

Module	Workflows
Data Loaders	General Data Import

EAM Extraction and Notification	Asset Management
	Event Management
	Notification Creation
EAM Work Management	Task and Confirmation Generation
	Work Order Generation
M2M Integration	Integrate with M2M Data Source

APM Failure Elimination

Module	Workflows
Generation Availability Analysis	GAA Administration
	GAA Event Management
	GAA Performance
	GAA Reporting
Production Loss Analysis	Production Loss Analysis
Reliability Analytics	Automation Rule
	Production Analysis
	Reliability and Probability Distribution
	Reliability Growth Analysis
	Spares Analysis
	System Reliability Analysis
Root Cause Analysis	Root Cause Analysis

APM Foundation

Module	Workflows
Asset Criticality Analysis	Perform Asset Criticality Analysis
Core Analysis	Asset Event Analysis
	Graph Analysis
	Query Analysis
	Report Analysis
	Geospatial Analysis
Metrics and Scorecards	Manage SSAS Cubes
	Manage Metric Views
	Manage KPIs
	Manage Scorecards

Performance Recommendations	Manage Performance Recommendations
	Execute Recommendations
Policy Designer	Design Policy
	Execute Policy

APM Mechanical Integrity

Module	Workflows
Inspection Management	Inspection Planning
	Inspection Assessment
Risk Based Inspection	Define Components
	Perform RBI Analysis
	Recommendation Management
	Recommendation Implementation
Thickness Monitoring	TM Planning
	Thickness Assessment

APM Health

Module	Workflows
AMS Analytics	AMS Analytics
Asset Health Manager	Assess Asset Health
	Manage Health Indicators
	Manage Health Indicator Sources
eLog	eLog
GE Analytics	GE Analytics
Rounds	Manage Rounds Routes
	Manage Rounds Templates
	Collect Rounds Data
	Monitor Rounds Compliance
Rounds Pro	Rounds Designer
	Rounds Data Collection

APM Safety

Module	Workflows
Calibration Management	Calibration Planning
	Calibration Administration
	Calibration Assessment
	Calibration Assessment CMX
Hazards Analysis	HAZOP Analysis
	What If Analysis
Layers of Protection Analysis (LOPA)	LOPA Workflow
Management of Change (MOC)	MoC Administration
	MoC Change Project
SIS Management	SIL Assessment
	LOPA
	SIL Verification
	SIL Validation
	Trip Reporting
	Custom Device
	SRS

APM Strategy
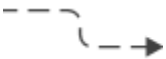
Module	Workflows
Reliability Centered Maintenance (RCM)	RCM and FMEA
Failure Modes and Effects Analysis (FMEA)	RCM and FMEA
Asset Strategy Management (ASM)	Asset Strategy Management
Asset Strategy Optimization (ASO)	Asset Strategy Optimization
Asset Strategy Implementation (ASI)	ASI for SAP
Life Cycle Cost Analysis (LCC)	Life Cycle Cost Analysis

Interpreting the Workflow Diagrams

The Product Workflow section of the APM documentation is designed to illustrate the basic functions of APM.

In each diagram, blue text in a shape indicates that a description is provided for that step in the workflow.

The following table summarizes the conventions used to represent the various activities in each workflow process.

Shape	Description
	The starting or ending point of a workflow.
	Another workflow within APM.
	Another workflow outside of APM.
	A user action or an automated process.
	A data output, such as a document or record.
	A decision.
	The primary process flow.
	An item referenced by part of the process flow.
A3	A reference number that accompanies some shapes in the workflow diagrams. These numbers are for identification purposes only and do not indicate the order of the workflows.

APM Analytics Personas

The workflows for this solution are completed by the following user personas.

Persona	Description	Applicable APM Roles	Notes
Analyst	The Analyst is responsible for prioritizing the areas where efforts should be directed to drive improvements that directly affect productivity and profitability. The Analyst monitors and evaluates historical and condition data. Based on evaluation, the Analyst will make recommendations to take action on current conditions or propose changes to existing strategies.	MI Analytics Power MI Analytics Administrator	None

APM Connect Personas

The workflows for this solution are completed by the following user personas.

Data Loader Personas

Persona	Description	Applicable APM Roles	Notes
Analyst	The Analyst is responsible for prioritizing the areas where efforts should be directed to drive improvements that directly affect productivity and profitability. The Analyst monitors and evaluates historical and condition data. Based on evaluation, the Analyst will make recommendations to take action on current conditions or propose changes to existing strategies.	MI Data Loader User MI Foundation Power MI Strategy Power	The Data Loader Analyst is responsible for the data that is imported via the data loaders from the external source. Analysts have the authorization and responsibility to assure that the data is collected, cleansed, and loaded completely and correctly. Traits of the Analyst: • Manipulates data • Applies standard processes and methodologies for analysis • Is a high-level APM User
Technician	The Technician is responsible for executing and documenting inspection activities to maintain both asset integrity and compliance with the overall inspection program. The Technician does the following: • Performs inspections, calibrations, or proof tests. • Records results. • Initiates recommendations.	MI Data Loader User MI Foundation Power MI Mechanical Integrity Power MI Strategy User	Depending on the module into which you are loading data, the Data Loader Technician can be responsible for numerous APM modules including: FMEA, RCM, Inspection Management, or Thickness Monitoring.

EAM Personas

Persona	Description	Applicable APM Roles	Notes
System Administrator	The System Administrator is responsible for installing and implementing APM. The System Administrator maintains backups of the APM system and ensures that the data flowing to and from APM is safe, secure, and performing well.	MI Data Loader Admin MI Foundation Admin	In addition to the applicable roles the System Administrator needs access to the following Security Groups: MI SAP Interface Administrator
Solution Administrator (EAM)	The Solution Administrator (EAM) may or may not have access to APM but is responsible for managing and maintaining master data in their EAM system solution.	N/A	None
APM	The APM persona represents automated processes performed by the APM system.	N/A	In the EAM Workflow the APM persona represents an automated process performed by APM Connect based on context files and triggers.
Analyst (EAM)	The Analyst is responsible for prioritizing the areas where efforts should be directed to drive improvements that directly affect productivity and profitability. The Analyst monitors and evaluates historical and condition data. Based on evaluation, the Analyst will make recommendations to take action on current conditions or propose changes to existing strategies.	N/A	The EAM Analyst may or may not have access to APM but is responsible for planning and scheduling work in the EAM system.

Analyst	The Analyst is responsible for prioritizing the areas where efforts should be directed to drive improvements that directly affect productivity and profitability. The Analyst monitors and evaluates historical and condition data. Based on evaluation, the Analyst will make recommendations to take action on current conditions or propose changes to existing strategies.	MI Data Loader User MI Foundation User MI Strategy Power	In addition to the applicable roles the Analyst needs access to the following Security Groups: MI SAP Interface User.
Technician	The Technician is responsible for executing and documenting inspection activities to maintain both asset integrity and compliance with the overall inspection program. The Technician does the following: • Performs inspections, calibrations, or proof tests. • Records results. • Initiates recommendations.	MI Data Loader User MI Foundation User MI Mechanical Integrity Power MI Strategy User	In addition to the applicable roles the Technician needs access to the following Security Groups: MI SAP Interface User and MI Configuration Role.

M2M Personas

Persona	Description	Applicable APM Roles	Notes
Solution Administrator	The Solution Administrator is responsible for managing advanced features of a APM solution. Some examples are managing health indicators, managing M2M interfaces, and managing SSAS cubes.	MI Health Power MI Foundation Power MI Data Loader Admin	In addition to the applicable roles the Solution Administrator needs access to the following Security Groups: MI AMS Suite Administrator and MI Configuration Role.

APM Failure Elimination Personas

The workflows for this solution are completed by the following user personas.

Persona	Description	Applicable APM Roles	Notes
Analyst	The Analyst is responsible for prioritizing the areas where efforts should be directed to drive improvements that directly affect productivity and profitability. The Analyst monitors and evaluates historical and condition data. Based on evaluation, the Analyst will make recommendations to take action on current conditions or propose changes to existing strategies.	MI FE Power User MI FE User MI Foundation User	None
Operator	The Operator is responsible for day-to-day operation of one or more GAA Units. The operator enters events that affect power generation in a GAA Unit.	MI Foundation User MI FE User	None
Solution Administrator	The Solution Administrator is responsible for managing advanced features of a APM solution. Some examples are managing health indicators, managing M2M interfaces, and managing SSAS cubes.	MI FE Admin MI Foundation User	None
Supervisor	The Supervisor has line authority over subordinates. The responsibilities of the Supervisor include asset integrity and program compliance as determined by company standards, the approval of recommendation proposals, and the review and approval of asset strategies.	MI Foundation User MI FE User	None

APM Foundation Personas

The workflows for this solution are completed by the following user personas.

Persona	Description	Applicable APM Roles	Notes
Analyst	The Analyst is responsible for prioritizing the areas where efforts should be directed to drive improvements that directly affect productivity and profitability. The Analyst monitors and evaluates historical and condition data. Based on evaluation, the Analyst will make recommendations to take action on current conditions or propose changes to existing strategies.	MI Foundation User MI Health Power	Any APM Security User can perform core analysis on entities for which permission to access has been granted. In Metrics and Scorecards, the Analyst designs and manages Metric Views, KPIs and Scorecards and has privileges to schedule KPIs or publish the results to the other users.
APM	The APM persona represents automated processes performed by the APM system.	MI Foundation User	None
Solution Administrator	The Solution Administrator is responsible for managing advanced features of a APM solution. Some examples are managing health indicators, managing M2M interfaces, and managing SSAS cubes.	MI Foundation Admin MI Health Power	In Metrics and Scorecards, the Solution Administrator sets the connection to SQL Server Analysis Services (SSAS), registers cubes to APM, and manages cube access privileges.

Supervisor	The Supervisor has line authority over subordinates. The responsibilities of the Supervisor include asset integrity and program compliance as determined by company standards, the approval of recommendation proposals, and the review and approval of asset strategies.	MI Foundation Admin	None
Technician	The Technician is responsible for executing and documenting inspection activities to maintain both asset integrity and compliance with the overall inspection program. The Technician does the following: • Performs inspections, calibrations, or proof tests. • Records results. • Initiates recommendations.	MI Foundation Admin	None

APM Mechanical Integrity Personas

The workflows for this solution are completed by the following user personas.

Persona	Description	Applicable APM Roles	Notes
Analyst	The Analyst is responsible for prioritizing the areas where efforts should be directed to drive improvements that directly affect productivity and profitability. The Analyst monitors and evaluates historical and condition data. Based on evaluation, the Analyst will make recommendations to take action on current conditions or propose changes to existing strategies.	MI Mechanical Integrity Power MI Mechanical Integrity Admin	None
Supervisor	The Supervisor has line authority over subordinates. The responsibilities of the Supervisor include asset integrity and program compliance as determined by company standards, the approval of recommendation proposals, and the review and approval of asset strategies.	MI Mechanical Integrity Power MI Mechanical Integrity Admin	None
Technician	The Technician is responsible for executing and documenting inspection activities to maintain both asset integrity and compliance with the overall inspection program. The Technician does the following: • Performs inspections, calibrations, or proof tests. • Records results. • Initiates recommendations.	MI Mechanical Integrity Power MI Mechanical Integrity Admin	None

APM Health Personas

The workflows for this solution are completed by the following user personas.

Persona	Description	Applicable APM Roles	Notes
Analyst	The Analyst is responsible for prioritizing the areas where efforts should be directed to drive improvements that directly affect productivity and profitability. The Analyst monitors and evaluates historical and condition data. Based on evaluation, the Analyst will make recommendations to take action on current conditions or propose changes to existing strategies.	MI Health User MI Health Power MI Health Admin MI Strategy User MI Strategy Power MI Strategy Admin	None
APM	The APM persona represents automated processes performed by the APM system.	None	None

Persona	Description	Applicable APM Roles	Notes
Solution Administrator	The Solution Administrator is responsible for managing advanced features of a APM solution. Some examples are managing health indicators, managing M2M interfaces, and managing SSAS cubes.	MI Health Admin	None
Technician	The Technician is responsible for executing and documenting inspection activities to maintain both asset integrity and compliance with the overall inspection program. The Technician does the following: • Performs inspections, calibrations, or proof tests. • Records results. • Initiates recommendations.	MI Health User	None

APM Safety Personas

The workflows for this solution are completed by the following user personas.

Persona	Description	Applicable APM Roles	Notes
Analyst	The Analyst is responsible for prioritizing the areas where efforts should be directed to drive improvements that directly affect productivity and profitability. The Analyst monitors and evaluates historical and condition data. Based on evaluation, the Analyst will make recommendations to take action on current conditions or propose changes to existing strategies.	MI Safety Admin MI Safety Power	• Responsible for setting up the standards, creating templates, approving recommendations, assigning tasks, and reviewing the calibration or proof test results • Responsible for performing SIL assessment, SIL verification, and SIL validation. • Responsible for creating Change Projects, adding Checklists to the projects, managing Exceptions and Tasks, and finalizing the Change Project.
Solution Administrator	The Solution Administrator is responsible for creating the Exceptions, Questions, and Checklists that can be used in the Change Project.	MI Safety Admin	None
Technician	The Technician is responsible for executing and documenting inspection activities to maintain both asset integrity and compliance with the overall inspection program. The Technician does the following: • Performs inspections, calibrations, or proof tests. • Records results. • Initiates recommendations.	MI Safety User	Responsible for performing calibrations or proof tests based on the tasks that are assigned.

APM Strategy Personas

The workflows for this solution are completed by the following user personas.

Persona	Description	Applicable APM Roles	Notes
Analyst	The Analyst is responsible for prioritizing the areas where efforts should be directed to drive improvements that directly affect productivity and profitability. The Analyst monitors and evaluates historical and condition data. Based on evaluation, the Analyst will make recommendations to take action on current conditions or propose changes to existing strategies.	Strategy User Strategy Power Strategy Admin	None
Supervisor	The Supervisor has line authority over subordinates. The responsibilities of the Supervisor include asset integrity and program compliance as determined by company standards, the approval of recommendation proposals, and the review and approval of asset strategies.	Strategy User Strategy Power	None