GE VERNOVA

Asset Performance Management

APM Classic

V4.6.11.0.0

APM Module Deployment and Upgrade

Contents

Copyright Digital, part of GE Vernova

Overview

About APM Deployment and Upgrade

The APM Module Deployment and Upgrade document provides information on how to configure various APM modules for the first time or upgrade existing module version to a newer version. These instructions assume that you have completed the steps for deploying or upgrading the basic APM system architecture. For more information, refer to the module-specific information using the left navigation.

Action Management

Deploy Recommended Actions for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Assign Security Users to one or more of the Recommended Actions Security Groups and Roles.	This step is required.
2	Review the Recommended Actions data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.

Upgrade or Update Recommended Actions to V4.6.11.0.0

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.0.0.0 through V4.0.1.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.1 through V3.5.1.12.3

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

Recommended Actions Security Groups

The following table lists the baseline Security Groups available for users within this module, as well as the baseline Roles to which those Security Groups are assigned.

Important: Assigning a Security User to a Role grants that user the privileges associated with all of the Security Groups that are assigned to that Role. To avoid granting a Security User unintended privileges, before assigning a Security User to a Role, be sure to review all of the privileges associated with the Security Groups assigned to that Role. Also, be aware that additional Roles, as well as Security Groups assigned to existing Roles, can be added via Security Manager.

The baseline family-level privileges that exist for these Security Groups are summarized in the following table.

Security Group	Roles
MI Recommendation Management User	MI Foundation Admin MI Foundation Power MI Foundation User

Family	MI Recommendation Management User
Entity Families	
Action	View
Equipment	View
Hazards Analysis Consequence	View
Instrumented Function	View
Protective Instrument Loop	View
RCA Analysis	View
RCA Team Member	View
RCM FMEA Analysis	View
Recommendation	View, Update, Insert, Delete
SIS Proof Test	View
SIS Proof Test Template	View
Relationship Families	
Has Asset Strategy	View, Update, Insert, Delete
Has Associated Recommendation	View, Update, Insert, Delete
Has Consolidated Recommendations	View, Update, Insert, Delete
Has Driving Recommendation	View, Update, Insert, Delete
Has Recommendations	View, Update, Insert, Delete
Has RCM FMEA Recommendation	View, Update, Insert, Delete
Has Strategy	View, Update, Insert, Delete
Has Superseded Recommendations	View, Update, Insert, Delete
Is RCM FMEA Asset	View, Update, Insert, Delete
Production Event Has RCA Analysis	View
RCA Analysis Relationships	View

Family	MI Recommendation Management User
Entity Families	
Action	View
Equipment	View
Hazards Analysis Consequence	View
Instrumented Function	View
Protective Instrument Loop	View
RCA Analysis	View
RCA Team Member	View
RCM FMEA Analysis	View
Recommendation	View, Update, Insert, Delete
SIS Proof Test	View
SIS Proof Test Template	View
Relationship Families	
Has Asset Strategy	View, Update, Insert, Delete
Has Associated Recommendation	View, Update, Insert, Delete
Has Consolidated Recommendations	View, Update, Insert, Delete
Has Driving Recommendation	View, Update, Insert, Delete
Has Recommendations	View, Update, Insert, Delete
Has RCM FMEA Recommendation	View, Update, Insert, Delete
Has Strategy	View, Update, Insert, Delete
Has Superseded Recommendations	View, Update, Insert, Delete
Is RCM FMEA Asset	View, Update, Insert, Delete
Production Event Has RCA Analysis	View
RCA Analysis Relationships	View

APM System Monitoring

Deploy APM System Monitoring for the First Time

About This Task

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Step	Task	Notes
1	On the machine that will serve as the APM System Monitoring Server, download and install the latest version of MongoDB Community Edition.	This step is required. The latest version of MongoDB Community Edition, as well as instructions about how to install it, can be found on the official MongoDB, Inc. website. Note that instructions for configuring a Windows Service for MongoDB Community Edition are provided in the next step.
2	Configure a Windows Service for MongoDB Community Edition.	This step is required.
3	On the machine that will serve as the APM System Monitoring controller, install APM System Monitoring.	This step is required.
4	On each machine that will serve as an APM System Monitoring agent, install APM System Monitoring.	This step is required.
5	On the machine that will serve as the APM System Monitoring admin, install APM System Monitoring.	This step is required.
6	Complete additional configuration steps related to APM System Monitoring.	This step is required.
7	As needed, modify APM System Monitoring settings via the Performance Monitoring feature.	This step is optional.

Upgrade or Update APM System Monitoring to V4.6.11.0.0

About This Task

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

  To upgrade APM System Monitoring, you should uninstall all of your existing APM System Monitoring components, and then follow the first-time deployment workflow.

Configure a Windows Service for MongoDB

Before You Begin

- On the machine that will serve as the APM System Monitoring Server, download and install the latest version of MongoDB Community Edition.

Procedure

1. On the machine on which you installed MongoDB Community Edition, select the Windows Start button, then navigate to and right-click **Command Prompt**, and then select **Run as administrator**.
   A command prompt window appears.
2. On the command prompt window, enter the following:
   - `mkdir c:\data\db`
   - `mkdir c:\data\log`

   Two directories that will be used by APM System Monitoring are created.

3. Create a configuration (.cfg) file. The file must set systemLog.path. Include additional configuration options as needed. For example, to create a file at `C:\data\mongod.cfg` that specifies both systemLog.path and storage.dbPath, the file would contain the following text:

```
systemLog:
destination: file
path: c:\data\log\mongod.log
storage:
dbPath: c:\data\db
```

   Note: In the configuration file, each tab indentation seen in the preceding text should be replaced with two spaces.
4. On the command prompt window, enter the following:
   `"C:\Program Files\MongoDB\Server\3.2\bin\mongod.exe" --config "C:\data\mongod.cfg" --install`

   Note: To use an alternate dbpath, specify the path in the configuration file (e.g., `C:\data\mongod.cfg`) or on the command line with the --dbpath option.

   The MongoDB service is installed.
5. On the command prompt window, enter the following:
   `net start MongoDB`

   The MongoDB service is started, and the Windows service is configured.

Next Steps

- Return to the APM System Monitoring first-time deployment workflow.

Install APM System Monitoring

Before You Begin

- Complete all previous steps in the APM System Monitoring first-time deployment workflow.

Procedure

1. On the machine on which you want to install APM System Monitoring, access the APM distribution package, and then navigate to the folder `Setup\APMSystemMonitor`.
2. Open the file `Setup.exe`.
   The Meridium APM System Monitor installer appears.
3. Select **Next**.
   The **License Agreement** screen appears.
4. Read the License Agreement and, if you agree, select the **I accept the terms of the license agreement** check box. Then, select **Next**.
   The **Select Installation Location** screen appears.
5. Select **Next** to accept the default location.
   The Select the features you want to install screen appears.

6. If this is a machine that will serve as an APM System Monitoring agent, then select the **APM System Monitor Agent** check box.

   Note: A single server machine could be the APM System Monitoring administrator, the APM System Monitoring controller, and an APM System Monitoring agent. Alternatively, you can distribute this deployment as needed. For a given server machine, select the check boxes for each APM System Monitoring feature that you want to deploy.
7. If this is the machine that will serve as the APM System Monitoring administrator, then select the **APM System Monitor Administrator** check box.

   Note: Only one machine will serve as the APM System Monitoring administrator.
8. If this is the machine that will serve as the APM System Monitoring controller, then select the **APM System Monitor Server** check box.

   Note: Only one machine will serve as the APM System Monitoring controller.
9. Select **Next**.
   The **Complete the Installation** screen appears.
10. Select **Install**.
    The **Setup Status** screen appears, displaying a progress bar. When the installation is complete, the **Installation is Complete** screen appears.
11. Select **Finish**.
    The Meridium APM System Monitor installer closes.
12. If the machine will serve as the APM System Monitoring controller or an APM System Monitoring agent, navigate to `C:\Program Files\Meridium\APMSystemMonitor`, and then open the file `Meridium.System.Monitor.ServiceManager.exe`. If the machine will serve only as the APM System Monitoring administrator, skip this step and proceed directly to step 18.
    The **Meridium APM System Monitor Service Manager** window appears.
13. If the machine will serve as the APM System Monitoring controller, then, in the **Controller** section, select **Configure**. Otherwise, skip this step.
    The **Controller Configuration** window appears.
14. In the **Mongo URL** box, enter the URL for the MongoDB database, and then select **Save and Restart**.
    The machine is configured as the APM System Monitoring controller.
15. If the machine will serve as an APM System Monitoring agent, then, in the **Agent** section, select **Configure**. Otherwise, skip this step.
    The **Agent Configuration** window appears.
16. Ensure that the values in the **Controller Server** and **Discovery Port** boxes match the values specified for the APM System Monitoring controller, and then select **Save and Restart**.
    The machine is configured as an APM System Monitoring agent.
17. Close the **Meridium APM System Monitor Service Manager** window.
    APM System Monitoring is installed on the machine.
18. If the machine will serve as the APM System Monitoring administrator, navigate to `C:\Program Files\Meridium\APMSystemMonitor\Admin`, and then open the file `Meridium.SystemMonitor.Admin.exe`. Otherwise, skip the remaining steps and return to the first-time deployment workflow.
    The **Meridium System Monitor Admin** window appears.
19. Perform the folllowing steps in the **Meridium System Monitor Admin** window:

a) In the **Location** box, enter the location of the APM System Monitor controller, and then select **Update Location.**
The connection status displayed in the lower-left corner of the window changes to Connected.
b) Select **Config**, and then select **Settings**.
The **System Monitor Settings** window appears.
c) In the **Controller Location** box, enter the location of the APM System Monitor controller.
d) Enter values in the **API Key**, **Customer Key**, and **User Name** boxes. You should have received these values from GE Global Support.
e) If you did not install MongoDB in the default location, modify the value in the **Database URL** box as needed.
f) If you want to disallow discovery, clear the **Allow Discovery** check box.

Note: Disallowing discovery is not recommended, but may be necessary, depending on your firewall settings. A firewall may prevent automatic discovery by APM System Monitoring.
g) If needed, modify the values in the **Announcement Port** and **Proxy Port** boxes.
h) Select **Update**.
The **System Monitor Settings** window closes.
i) On the **Meridium System Monitor Admin** window, select **Config**, and then select **General**.
The **General Config** window appears.
j) In the **Log Level To Store** and **Log Level to Output** sections, select the check box for each log level that you want to monitor.

Tip: We recommend that you select only the **Error** check boxes. If additional check boxes are selected, the log files produced may be very large.
k) In the **Days In Storage** box, select the number of days logs should be stored in the system before deletion.
l) In the **Days In Outputs** box, select the number of days worth of information that should be used to populate APM dashboards.
m) Enter values in the **Email Server**, **From Address**, and **To** boxes, and then select **Update**.

Tip: If you want to configure emails to be sent to multiple recipients, you can enter a list of comma separated values in the **To** box.

The **General Config** window closes.
n) On the **Meridium System Monitor Admin** window, select **Config**, and then select **Agents**.
The **Agents** window appears.

Next Steps

- Return to the APM System Monitoring first-time deployment or upgrade workflow.

Configure APM System Monitoring

Procedure

1. On the machine serving as the APM System Monitoring administrator, navigate to `C:\Program Files\Meridium\APMSystemMonitor\Admin`, and then open the file `Meridium.SystemMonitor.Admin.exe`.
   The **Meridium System Monitor Admin** window appears.
2. On the **Meridium System Monitor Admin** window, select **Config**, and then select **Agents**.
   The **Agents** window appears.
3. As needed, modify the configuration of the agents, and then close the **Agents** window.

   Note: If you have allowed discovery (i.e., the **Allow Discovery?** check box on the **System Monitor Settings** window is selected), the **Delete** and **New Agent** buttons on the **Agents** window are disabled.
4. On the **Meridium System Monitor Admin** window, select **Config**, and then select **Alerts**.
   The **Alerts** window appears.
5. As needed, modify the configuration of the alerts, and then close the **Alerts** window.
6. On the **Meridium System Monitor Admin** window, select **Config**, and then select **APM**.
   The **Configure APM Output** window appears.
7. If you want to access APM System Monitoring information within APM, enter values in the available fields, and then close the window.

   Note: If you do not configure the settings on this window, you can still access APM System Monitoring information via the **Charts** menu on the **Meridium System Monitor Admin** window. If you configure these settings, you will also be able to access APM System Monitoring information via the **APM System Monitoring** page in APM.
8. To create a new task, on the **Meridium System Monitor Admin** window, select **Tasks**, and then select the type of task that you want to create or modify.
   The **Tasks** window appears, displaying the information related to the selected task. The following image displays an example of the window for tasks of the type ServerCpuUsage.
9. As needed, create new tasks and modify existing tasks, and then close the **Tasks** window.
   The configuration of APM System Monitoring has been updated.

Next Steps

- Return to the APM System Monitoring first-time deployment or upgrade workflow.

Asset Criticality Analysis

Deploy ACA for the First Time

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Assign Security Users to one or more of the ACA Security Groups and Roles.	This step is required.
2	Review the ACA data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
3	Optional: Configure Criticality Definition records to use a Checklist as the Criticality Assessment method instead of the Risk Matrix.	To configure to use a Checklist, select the Use Checklist field and select the desired family from the Checklist Family field. To associate a Criticality Definition record with a Site, link the Criticality Definition record to a Site Reference record. The Criticality Checklist family datasheet and Before Insert Family Policy can be configured to implement the desired assessment input fields and criticality value calculation logic.

Upgrade or Update ACA to V4.6.11.0.0

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

Step	Task	Notes
1	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.
2	Create Criticality Mapping records and link them to corresponding Risk Threshold records.	This step is required only if you want to update your SAP system to reflect the criticality value that is determined in ACA.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.
2	Create Criticality Mapping records and link them to corresponding Risk Threshold records.	This step is required only if you want to update your SAP system to reflect the criticality value that is determined in ACA.

- Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.
2	Create Criticality Mapping records and link them to corresponding Risk Threshold records.	This step is required only if you want to update your SAP system to reflect the criticality value that is determined in ACA.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

Step	Task	Notes
1	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.
2	Create Criticality Mapping records and link them to corresponding Risk Threshold records.	This step is required only if you want to update your SAP system to reflect the criticality value that is determined in ACA.

- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

Step	Task	Notes
1	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.
2	Create Criticality Mapping records and link them to corresponding Risk Threshold records.	This step is required only if you want to update your SAP system to reflect the criticality value that is determined in ACA.

- Upgrade from any version V3.5.1 through V3.5.1.12.3

Step	Task	Notes
1	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.
2	Create Criticality Mapping records and link them to corresponding Risk Threshold records.	This step is required only if you want to update your SAP system to reflect the criticality value that is determined in ACA.

- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

Step	Task	Notes
1	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.
2	Create Criticality Mapping records and link them to corresponding Risk Threshold records.	This step is required only if you want to update your SAP system to reflect the criticality value that is determined in ACA.

- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.
2	Create Criticality Mapping records and link them to corresponding Risk Threshold records.	This step is required only if you want to update your SAP system to reflect the criticality value that is determined in ACA.

- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.
2	Create Criticality Mapping records and link them to corresponding Risk Threshold records.	This step is required only if you want to update your SAP system to reflect the criticality value that is determined in ACA.

- When upgrading to 4.3.0.7.0, all existing Asset Criticality Analysis Systems are now displayed in the list of Asset Criticality Analyses.
- When upgrading to 4.3.0.7.0, the Team Members and Reference Documents of existing Asset Criticality Analysis records will be transferred to the associated records in the Asset Criticality Analysis System family.
- When upgrading to 4.3.0.7.0, the State of existing Asset Criticality Analysis records will be transferred to the child records in the Asset Criticality Analysis System family. The States for Asset Criticality Analyses will be upgraded from:
  - Complete to Approved
  - Pending Approval to Pending Approval
  - All other States will be upgraded to In Progress
- When upgrading to 4.3.0.7.0, State Management roles need to be configured for the Asset Criticality Analysis System family.
- When upgrading to 4.3.0.7.0, corresponding Criticality Definition and Criticality Threshold records will be created from existing Risk Matrix records.

ACA Security Groups

The following table lists the baseline Security Groups available for users within this module, as well as the baseline Roles to which those Security Groups are assigned.

Important: Assigning a Security User to a Role grants that user the privileges associated with all of the Security Groups that are assigned to that Role. To avoid granting a Security User unintended privileges, before assigning a Security User to a Role, be sure to review all of the privileges associated with the Security Groups assigned to that Role. Also, be aware that additional Roles, as well as Security Groups assigned to existing Roles, can be added via Security Manager.

Security Group	Roles
MI ACA Administrator	MI Foundation Admin
MI ACA Member	MI Foundation Admin MI Foundation Power MI Foundation User MI APM Viewer
MI ACA Owner	MI Foundation Admin MI Foundation Power

The baseline family-level privileges that exist for these Security Groups are summarized in the following table.

Family	MI ACA Administrator	MI ACA Member	MI ACA Owner
Entity			
Asset Criticality Analysis	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Asset Criticality Analysis Has System	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Asset Criticality Analysis System	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Consequence	View, Update, Insert, Delete	View	View
Consequence Modifier	View, Update, Insert, Delete	View	View
Criticality Mapping	View	View	View
Equipment	View	View	View
Functional Location	View	View	View
Analysis Has Human Resource	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Human Resource	View, Update, Insert, Delete	None	View, Update, Insert, Delete
General Recommendation	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Mitigates Risk	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Notification	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Probability	View, Update, Insert, Delete	View	View
Protection Level	View	View	View
RCM FMEA Analysis	View	None	None
Reference Document	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Risk	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Risk Assessment	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Risk Category	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Risk Matrix	View, Update, Insert, Delete	View	View, Update, Insert, Delete

Family	MI ACA Administrator	MI ACA Member	MI ACA Owner
Risk Threshold	View, Update, Insert, Delete	View	View
Safety Analysis Has Equipment	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Site Reference	View	View	View
System Strategy	View	None	None
Relationship			
Equipment Has Equipment	View	View	View
Functional Location Has Equipment	View	View	View
Functional Location Has Functional Location	View	View	View
Has Criticality Mapping	View	View	View
Has Functional Location	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Has RCM FMEA Analysis	View	None	None
Has Recommendations	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Has Reference Documents	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Has Reference Values	View, Update, Insert, Delete	View	View
Has Risk	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Has Risk Category	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Has Risk Matrix	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Has Site Reference	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Has Strategy	View	None	None

Asset Health Manager

Asset Health Manager Deployment

Deploy AHM for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Assign Security Users to one or more of the Asset Health Manager Security Groups and Roles.	This step is required.
2	Start or restart the Meridium Asset Health Indicator (AHI) service.	This step is required. When you start the service, the Health Indicator records are automatically created or updated based on the health indicator and the data in the source records. You may review the log files for this service at `C:\ProgramData\Meridium\Logs`.
3	Review the AHM data model to determine which relationship definitions you will need to modify to include your custom asset families.	This step is required only if you store asset information in families other than the baseline Equipment and Functional Location families.
4	Determine the equipment or location whose overall health you want to evaluate, and make sure that an asset record exists in the database for this equipment or location and is included in the Asset Hierarchy configuration.	This step is required. If you are using custom asset families and relationships (see Step 5), make sure that the equivalent records and links exist in the database.
5	Configure Health Indicator Mapping records for each family that you want to use as a health indicator source, for which a baseline Health Indicator Mapping record does not already exist.	This step is required. Baseline Health Indicator Mapping records exist for the following health indicator source families: • Measurement Location • KPI • Content Map • Health Indicator

Step	Task	Notes
6	Link each asset record to the record(s) that you want to use as a health indicator source records.	This step is required.
7	For any specific records in a health indicator source family for which you do not want health indicators to be created, exclude these records from the automatic health indicator creation.	This step is optional.
8	Review the baseline event mappings and modify or create new mappings as necessary to customize the information that is displayed in the **Events** section in Asset Health Manager.	This step is optional. Refer to the Asset Health Manager end user help for more information about events.

About the Asset Health Services

When you deploy the Asset Health Manager, OT Connect, and Policy Designer modules together, the services used by each module interact with each other in various ways. This topic summarizes those services and describes a standard system architecture containing the components used by all three modules.

For a list of tasks that you must complete to deploy each module, refer to the deployment topics in the following areas:

- Asset Health Manager (AHM)
- Policy Designer
- OT Connect

Services Summary

The following services are used by the Asset Health Manager, OT Connect, and Policy Designer modules:

- **Asset Health Indicator Service:** Automatically updates the following field values in a Health Indicator record when reading values related to the health indicator source record (for example, a Content Map or Measurement Location record) change:
  - Alert Level
  - Last Reading Date
  - Last Char Reading Value (for records that accept character values)
  - Last Numeric Reading Value (for records that accept numeric values)

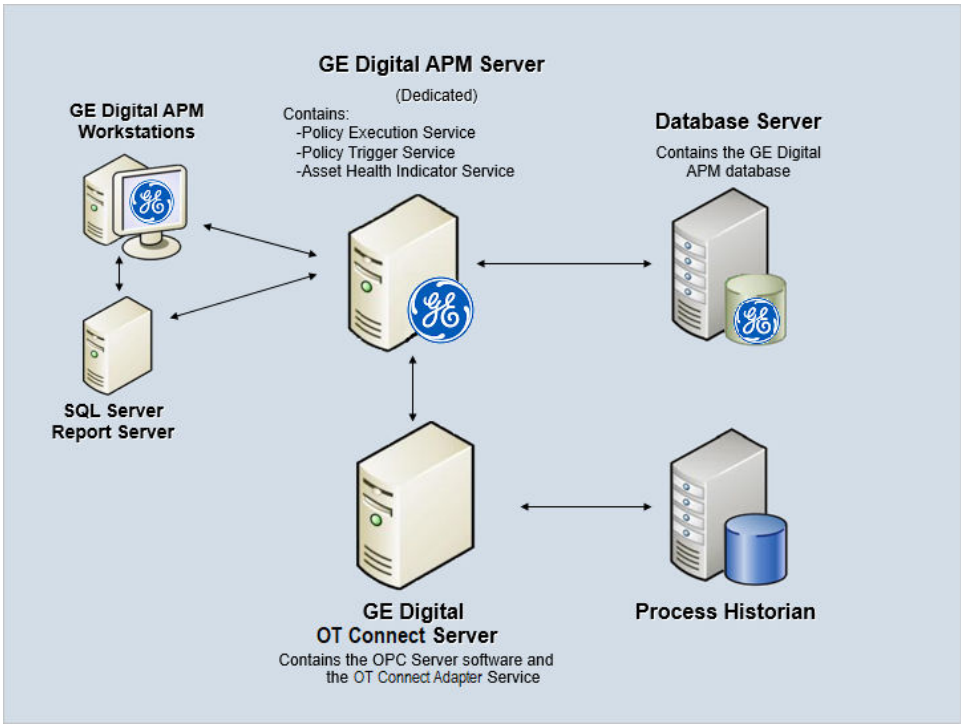
  This service also facilitates the automatic creation of Health Indicator records for configured sources.
- **Policy Trigger Service**: When an input to a policy (i.e., an associated record in the APM database or reading value in the process historian) changes or when a policy schedule is due, a message is added to the policy trigger queue.
- **Policy Execution Service:** The Meridium Policy Execution Service handles the execution of policies. Specifically, the Policy Execution Service monitors a corresponding policy execution queue and executes the policy instances that are added to it.

- **OT Connect:** Monitors the subscribed tags (tags that are used in policies and health indicators or tags for which readings are being stored in the APM database) and, when data changes occur on these tags, adds messages to the appropriate queues. This service also facilitates the automatic import and synchronization of tags from a configured process historian.

Standard System Architecture Configuration

The following diagram illustrates the machines in the APM system architecture when the Policy Designer, OT Connect, and Asset Health Manager (AHM) modules are used together. This image depicts the standard configuration, where the OPC Server software and OT Connect software are on the same machine.

Note: In this example configuration, only one machine of each type is illustrated. Your specific architecture may include multiple APM Servers, multiple OPC Servers, or multiple APM Servers used for policy executions.



The following table summarizes the machines illustrated in this diagram and the software and services that you will install when you complete the first-time deployment steps for Asset Health Manager, OT Connect, and Policy Designer.

Note: For detailed information on OT Connect, refer to the OT Connect System Architecture section.

Machine	Software Installed	Asset Health Service Installed Automatically with Service Software
APM Server	APM Server software	Asset Health Indicator Service
		Policy Trigger Service
		Policy Execution Service
OT Connect Process Data Server, which also acts as the OPC Server	OT Connect software	OT Connect Adapter Service
	OPC Server software	N/A
Process Historian	Process historian software	N/A

Upgrade or Update Asset Health Manager

Upgrade or Update Asset Health Manager to V4.6.11.0.0

About This Task

The following steps must be completed to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

Upgrade or update OT Connect.

Note: This step is required only if you are using Content Map records as health indicator sources.

Upgrade from Any Version V4.0.0.0 or Later

About This Task

The following steps must be completed to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

1. Upgrade or update OT Connect.

   Note: This step is required only if you are using Content Map records as health indicators sources.
2. **Optional:** Resync Health Indicators

   Depending on the status of potential health indicator sources in your database, the resync will result in one or both of the following scenarios:

   - If health indicators do not already exist for sources that are included as health indicators, the resync creates health indicators for those sources.
   - If health indicators exist for sources that are excluded as health indicators, the resync deletes health indicators for those sources.
     Additionally, if the exclusion table contains extraneous entries, the resync removes those entries.

Upgrade from Any Version V3.4.5 through V3.6.1.7.4

About This Task

The following steps must be completed to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

1. Review the potential health indicator source records in your database and specify whether the health indicators should be created automatically. During the database upgrade process, any valid health indicator source records that are linked to an asset and not linked to a Health Indicator record will be excluded from the automatic health indicator creation by default.

   Note:

   Alternatively, prior to upgrading to the APM, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records. Removing the exclusions after upgrading will cause the APM system to generate health indicators automatically.

2. If you previously used the Hierarchy Item Definition family to create a custom hierarchy for Asset Health Manager, ensure that the relevant asset families are included in the application-wide .
3. If you are using custom , specify values in the Type Field and Type Value fields to ensure that the mappings are used for the appropriate reading type.
4. Upgrade or update OT Connect.

   Note: This step is required only if you are using Content Map records as health indicators sources.
5. **Optional:**

   Depending on the status of potential health indicator sources in your database, the resync will result in one or both of the following scenarios:

   - If health indicators do not already exist for sources that are included as health indicators, the resync creates health indicators for those sources.
   - If health indicators exist for sources that are excluded as health indicators, the resync deletes health indicators for those sources.
     Additionally, if the exclusion table contains extraneous entries, the resync removes those entries.

Asset Strategy Implementation

Deploy Asset Strategy Implementation (ASI) for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Install the ASI for SAP ABAP add-on on your SAP System.	This step is required.
2	Verify ASI ABAP Add-On.	This step is required.
3	Review the ASI data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	Required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
4	Assign Security Users to one or more of the ASI Security Groups and Roles.	This step is required.
5	Configure SAP for external numbering. Configure SAP for external numbering.	This step is required.
6	Configure SAP permissions.	This step is required.
7	via the ASI Application Settings.	This step is required only if you want to use Work Management Item Definition records beyond those provided with the baseline database.

Upgrade or Update Asset Strategy Implementation (ASI) to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

Step	Task	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	This step is required.

- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

Step	Task	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	This step is required.

- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

Step	Task	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	This step is required.

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

Step	Task	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	This step is required.

- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

Step	Task	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	This step is required.
2	Remove rule projects that inherit MeasurementLocation_AM or MeasurementLocation_EM rule projects.	This step is required only if you have customized the baseline rule projects MeasurementLocation_AM and MeasurementLocation_EM. The baseline rules for the MeasurementLocation_AM and MeasurementLocation_EM rule projects have been removed. Therefore, the customized rule projects that inherit these rule projects do not run.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	This step is required.
2	Remove rule projects that inherit MeasurementLocation_AM or MeasurementLocation_EM rule projects.	This step is required only if you have customized the baseline rule projects MeasurementLocation_AM and MeasurementLocation_EM. The baseline rules for the MeasurementLocation_AM and MeasurementLocation_EM rule projects have been removed. Therefore, the customized rule projects that inherit these rule projects do not run.

- Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	This step is required.
2	Remove rule projects that inherit MeasurementLocation_AM or MeasurementLocation_EM rule projects.	This step is required only if you have customized the baseline rule projects MeasurementLocation_AM and MeasurementLocation_EM. The baseline rules for the MeasurementLocation_AM and MeasurementLocation_EM rule projects have been removed. Therefore, the customized rule projects that inherit these rule projects do not run.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

Step	Task	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	This step is required.
2	Remove rule projects that inherit MeasurementLocation_AM or MeasurementLocation_EM rule projects.	This step is required only if you have customized the baseline rule projects MeasurementLocation_AM and MeasurementLocation_EM. The baseline rules for the MeasurementLocation_AM and MeasurementLocation_EM rule projects have been removed. Therefore, the customized rule projects that inherit these rule projects do not run.

- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

Step	Task	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	This step is required.
2	Remove rule projects that inherit MeasurementLocation_AM or MeasurementLocation_EM rule projects.	This step is required only if you have customized the baseline rule projects MeasurementLocation_AM and MeasurementLocation_EM. The baseline rules for the MeasurementLocation_AM and MeasurementLocation_EM rule projects have been removed. Therefore, the customized rule projects that inherit these rule projects do not run.

- Upgrade from any version V3.5.1 through V3.5.1.12.3

Step	Task	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	This step is required.
2	Remove rule projects that inherit MeasurementLocation_AM or MeasurementLocation_EM rule projects.	This step is required only if you have customized the baseline rule projects MeasurementLocation_AM and MeasurementLocation_EM. The baseline rules for the MeasurementLocation_AM and MeasurementLocation_EM rule projects have been removed. Therefore, the customized rule projects that inherit these rule projects do not run.

- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

Step	Task	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	This step is required.
2	Remove rule projects that inherit MeasurementLocation_AM or MeasurementLocation_EM rule projects.	This step is required only if you have customized the baseline rule projects MeasurementLocation_AM and MeasurementLocation_EM. The baseline rules for the MeasurementLocation_AM and MeasurementLocation_EM rule projects have been removed. Therefore, the customized rule projects that inherit these rule projects do not run.

- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	This step is required.
2	Remove rule projects that inherit MeasurementLocation_AM or MeasurementLocation_EM rule projects.	This step is required only if you have customized the baseline rule projects MeasurementLocation_AM and MeasurementLocation_EM. The baseline rules for the MeasurementLocation_AM and MeasurementLocation_EM rule projects have been removed. Therefore, the customized rule projects that inherit these rule projects do not run.

- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	This step is required.
2	Remove rule projects that inherit MeasurementLocation_AM or MeasurementLocation_EM rule projects.	This step is required only if you have customized the baseline rule projects MeasurementLocation_AM and MeasurementLocation_EM. The baseline rules for the MeasurementLocation_AM and MeasurementLocation_EM rule projects have been removed. Therefore, the customized rule projects that inherit these rule projects do not run.

Asset Strategy Implementation (ASI) Security Groups and Roles

The following table lists the baseline Security Groups available for users within this module, as well as the baseline Roles to which those Security Groups are assigned.

Important: Assigning a Security User to a Role grants that user the privileges associated with all of the Security Groups that are assigned to that Role. To avoid granting a Security User

unintended privileges, before assigning a Security User to a Role, be sure to review all of the privileges associated with the Security Groups assigned to that Role. Also, be aware that additional Roles, as well as Security Groups assigned to existing Roles, can be added via Security Manager.

Security Group	Roles
MI ASI Administrator	MI Strategy Admin
MI ASI User	MI Strategy Admin MI Strategy Power MI Strategy User
MI ASI Viewer	MI APM Viewer MI Strategy Admin MI Strategy Power MI Strategy User

The baseline family-level privileges that exist for these Security Groups are summarized in the following table.

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
Entity Families			
Action	None	View, Update	View
Action Mapping	View, Update, Insert, Delete	View	View
Active Strategy	None	View	View
Asset Strategy	None	View	View
Calibration Task	None	View, Update, Insert, Delete	View
Consequence	None	View	View
Cycle	None	View, Update, Insert, Delete	View
Equipment	View, Update, Insert, Delete	View, Update, Insert	View
Execution Mapping	View, Update, Insert, Delete	View	View
Functional Location	View, Update, Insert, Delete	View, Update, Insert	View
Health Indicator	None	View	View
Health Indicator Mapping	None	View	View

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
Hierarchy Item Child Definition	None	View	View
Hierarchy Item Definition	None	View	View
Implementation Authorization	View, Update, Insert, Delete	View	View
Implementation Package	None	View, Update, Insert, Delete	View
Inspection Task	None	View, Update, Insert, Delete	View
KPI	None	View	View
KPI Measurement	None	View	View
Maintenance Item	None	View, Update, Insert, Delete	View
Maintenance Package	None	View, Update, Insert, Delete	View
Maintenance Plan	None	View, Update, Insert, Delete	View
Material	None	View, Update, Insert, Delete	View
Measurement Location	None	View, Update, Insert, Delete	View
Measurement Location Group	None	View, Update, Insert, Delete	View
Measurement Location Template	View, Update, Insert, Delete	View, Update, Insert	View
Notification	None	View, Update, Insert, Delete	View
Object List Item	None	View, Update, Insert, Delete	View
Operation	None	View, Update, Insert, Delete	View
Operator Rounds Allowable Values	None	View	View
Probability	None	View	View
Proposed Strategy	None	View	View
Protection Level	None	View	View

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
PRT	None	View, Update, Insert, Delete	View
PRT Template	View, Update, Insert, Delete	View	View
RCM FMEA Asset	None	View	View
RCM FMEA Recommendation	None	View	View
Risk	None	View	View
Risk Assessment	None	View	View
Risk Category	None	View	View
Risk Matrix	None	View	View
Risk Rank	None	View	View
Risk Threshold	None	View	View
SAP System	View, Update, Insert, Delete	View	View
Site Reference	View	View	View
System Strategy	None	View	View
Task List	None	View, Update, Insert, Delete	View
Task Types	None	View	View
Thickness Monitoring Task	None	View, Update, Insert, Delete	View
Unit Strategy	None	View	View
Work Management Item Child Definition	View, Update, Insert, Delete	View	View
Work Management Item Definition	View, Update, Insert, Delete	View	View
Work Management Item Definition Configuration	View, Update, Insert, Delete	View	View
Relationship Families			
Authorized to Implement	View, Update, Insert, Delete	View	View
Documents Action	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
Has Actions	None	View	View
Has Action Mapping	View, Update, Insert, Delete	View	View
Has Action Revisions	None	View	View
Has Active Strategy	None	View	View
Has Asset Strategy	None	View	View
Has Associated Recommendation	None	View	View
Has Checkpoint	None	View, Insert	View
Has Child Hierarchy Item	None	View	View
Has Child Work Management Item	View, Update, Insert, Delete	View	View
Has Cycles	None	View, Update, Insert, Delete	View
Has Driving Recommendation	None	View	View
Has Execution Mapping	View, Update, Insert, Delete	View	View
Has Health Indicators	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has KPI Measurement	None	View	View
Has Maintenance Item	None	View, Update, Insert, Delete	View
Has Maintenance Package	None	View, Update, Insert, Delete	View
Has Material	None	View, Update, Insert, Delete	View
Has Measurement Location Group	None	View, Update, Insert, Delete	View
Has Mitigation Revisions	None	View	View
Has Object List Item	None	View, Update, Insert, Delete	View
Has Operation	None	View, Update, Insert, Delete	View
Has Proposed Strategy	None	View	View

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
Has PRT	None	View, Update, Insert, Delete	View
Has Reference Values	None	View	View
Has Risk	None	View	View
Has Risk Category	None	View	View
Has Risk Revisions	None	View	View
Has SAP System	None	View, Update, Insert, Delete	View
Has Strategy	None	View	View
Has Strategy Revision	None	View	View
Has System Strategy	None	View	View
Has Tasks	None	View, Update, Insert, Delete	View
Has Task List	None	View, Update, Insert, Delete	View
Has Task Revision	None	View, Update, Insert, Delete	View
Has Work Management Item	None	View, Update, Insert, Delete	View
Has Work Management Item Definition Configuration	View, Update, Insert, Delete	View	View
Health Indicator Has Mapping	None	View, Update, Insert	View
Health Indicator Has Source	None	View, Update, Insert, Delete	View
Implements Action	None	View, Update, Insert, Delete	View
Implements Strategy	None	View, Update, Insert, Delete	View
Implements Secondary Strategy	None	View, Update, Insert, Delete	View
Is Mitigated	None	View	View
Master Template Has Asset Strategy	None	View	View
Mitigates Risk	None	View	View

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
Was Applied to Asset Strategy	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Was Applied to PRT	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Security Group	Roles
MI ASI Administrator	MI Strategy Admin
MI ASI User	MI Strategy Admin MI Strategy Power MI Strategy User
MI ASI Viewer	MI APM Viewer MI Strategy Admin MI Strategy Power MI Strategy User

The baseline family-level privileges that exist for these Security Groups are summarized in the following table.

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
Entity Families			
Action	None	View, Update	View
Action Mapping	View, Update, Insert, Delete	View	View
Active Strategy	None	View	View
Asset Strategy	None	View	View
Calibration Task	None	View, Update, Insert, Delete	View
Consequence	None	View	View
Cycle	None	View, Update, Insert, Delete	View
Equipment	View, Update, Insert, Delete	View, Update, Insert	View
Execution Mapping	View, Update, Insert, Delete	View	View
Functional Location	View, Update, Insert, Delete	View, Update, Insert	View

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
Health Indicator	None	View	View
Health Indicator Mapping	None	View	View
Hierarchy Item Child Definition	None	View	View
Hierarchy Item Definition	None	View	View
Implementation Authorization	View, Update, Insert, Delete	View	View
Implementation Package	None	View, Update, Insert, Delete	View
Inspection Task	None	View, Update, Insert, Delete	View
KPI	None	View	View
KPI Measurement	None	View	View
Maintenance Item	None	View, Update, Insert, Delete	View
Maintenance Package	None	View, Update, Insert, Delete	View
Maintenance Plan	None	View, Update, Insert, Delete	View
Material	None	View, Update, Insert, Delete	View
Measurement Location	None	View, Update, Insert, Delete	View
Measurement Location Group	None	View, Update, Insert, Delete	View
Measurement Location Template	View, Update, Insert, Delete	View, Update, Insert	View
Notification	None	View, Update, Insert, Delete	View
Object List Item	None	View, Update, Insert, Delete	View
Operation	None	View, Update, Insert, Delete	View
Operator Rounds Allowable Values	None	View	View
Probability	None	View	View

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
Proposed Strategy	None	View	View
Protection Level	None	View	View
PRT	None	View, Update, Insert, Delete	View
PRT Template	View, Update, Insert, Delete	View	View
RCM FMEA Asset	None	View	View
RCM FMEA Recommendation	None	View	View
Risk	None	View	View
Risk Assessment	None	View	View
Risk Category	None	View	View
Risk Matrix	None	View	View
Risk Rank	None	View	View
Risk Threshold	None	View	View
SAP System	View, Update, Insert, Delete	View	View
Site Reference	View	View	View
System Strategy	None	View	View
Task List	None	View, Update, Insert, Delete	View
Task Types	None	View	View
Thickness Monitoring Task	None	View, Update, Insert, Delete	View
Unit Strategy	None	View	View
Work Management Item Child Definition	View, Update, Insert, Delete	View	View
Work Management Item Definition	View, Update, Insert, Delete	View	View
Work Management Item Definition Configuration	View, Update, Insert, Delete	View	View
Relationship Families			
Authorized to Implement	View, Update, Insert, Delete	View	View

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
Documents Action	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Actions	None	View	View
Has Action Mapping	View, Update, Insert, Delete	View	View
Has Action Revisions	None	View	View
Has Active Strategy	None	View	View
Has Asset Strategy	None	View	View
Has Associated Recommendation	None	View	View
Has Checkpoint	None	View, Insert	View
Has Child Hierarchy Item	None	View	View
Has Child Work Management Item	View, Update, Insert, Delete	View	View
Has Cycles	None	View, Update, Insert, Delete	View
Has Driving Recommendation	None	View	View
Has Execution Mapping	View, Update, Insert, Delete	View	View
Has Health Indicators	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has KPI Measurement	None	View	View
Has Maintenance Item	None	View, Update, Insert, Delete	View
Has Maintenance Package	None	View, Update, Insert, Delete	View
Has Material	None	View, Update, Insert, Delete	View
Has Measurement Location Group	None	View, Update, Insert, Delete	View
Has Mitigation Revisions	None	View	View
Has Object List Item	None	View, Update, Insert, Delete	View
Has Operation	None	View, Update, Insert, Delete	View

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
Has Proposed Strategy	None	View	View
Has PRT	None	View, Update, Insert, Delete	View
Has Reference Values	None	View	View
Has Risk	None	View	View
Has Risk Category	None	View	View
Has Risk Revisions	None	View	View
Has SAP System	None	View, Update, Insert, Delete	View
Has Strategy	None	View	View
Has Strategy Revision	None	View	View
Has System Strategy	None	View	View
Has Tasks	None	View, Update, Insert, Delete	View
Has Task List	None	View, Update, Insert, Delete	View
Has Task Revision	None	View, Update, Insert, Delete	View
Has Work Management Item	None	View, Update, Insert, Delete	View
Has Work Management Item Definition Configuration	View, Update, Insert, Delete	View	View
Health Indicator Has Mapping	None	View, Update, Insert	View
Health Indicator Has Source	None	View, Update, Insert, Delete	View
Implements Action	None	View, Update, Insert, Delete	View
Implements Strategy	None	View, Update, Insert, Delete	View
Implements Secondary Strategy	None	View, Update, Insert, Delete	View
Is Mitigated	None	View	View
Master Template Has Asset Strategy	None	View	View

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
Mitigates Risk	None	View	View
Was Applied to Asset Strategy	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Was Applied to PRT	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Install or Upgrade the ASI ABAP Add-On on the SAP System

Before You Begin

Determine the release and level of your current ABAP installation by completing the steps to verify the ABAP installation.

Procedure

1. On a machine from which you can access the SAP Server, access your ASI ABAP installation package.
2. Determine how to proceed based on your ABAP release and level and type of SAP system.
   - For ECC6, if your currently installed ABAP release is 700_600 and the level is 0000 and above, proceed directly to step17. Otherwise, proceed to the next step.
   - For S/4 Hana, if your currently installed ABAPrelease is 700_750 and the level is 0000 and above, proceed directly to Step17. Otherwise, proceed to the next step.
3. Navigate to the folder `\\SAP ASI ABAP Add-On\Service Pack Files\ECC6` or `\\SAP ASI ABAP Add-On\Service Pack Files\S/4 Hana`, and then select one of the following folders:
   - **Exchange Upgrade**: To upgrade the ASI ABAP Add-on when upgrading to a new SAP version.
   - **Installation**: To install the ASI ABAP Add-on for the first time.
   - **Upgrade**: To upgrade the ASI ABAP Add-on.
4. Copy the .pat file(s). The file names begin with either D07 or H4S.
5. On the SAP Server, paste the copied file(s) into the folder **usr\sap\trans\eps\in**.
6. Log in to the SAP system as a user with:
   - SCTSIMPSGL and S_CTS_ADMIN authorizations.

     -or-
   - SAP_ALL authorization
7. Run the following transaction: SAINT

   The **Add-On Installation Tool** screen appears.
8. In the upper-left corner of the page, select **Installation Package**, then select **Load Packages**, and then select **From Application Server**.

   A message appears, asking if you want to upload OCS packages from the ECS inbox.
9. Select **Yes**.

   The **SAINT: Uploading Packages from the File System** screen appears.

Note: In an S/4 Hana environment, 2 files are uploaded and are displayed in the **SAINT: Uploading Packages from the File System** screen.

In the **Message Text** column, on the row corresponding the uploaded .pat file, the message Uploaded successfully is displayed.

10. At the top of the screen, select .

    The **Add-On Installation Tool** screen appears again.

11. Select **Start**.

    A new grid appears. MIAPM appears in the list of add-on packages that can be installed.

12. Select the row containing the text MIAPM in the first column, and then select **Continue**.

    The **Support Package selection** tab appears.

13. Select **Continue**, and then select **Continue** again.

    Note:

    During the installation, if the **Add Modification Adjustment Transports to the Queue** dialog box appears, select **No**.

    During the installation, if the **Open data extraction requests** dialog box appears, select **Skip**, and then select **Yes**.

    At the bottom of the screen, an indicator appears, displaying the progress of the installation.

14. When the indicator disappears, a message appears, indicating that the add-on package will be installed.

15. Select .

    The status is updated to indicate that the add-on package will now be imported, and the installation process continues. When the installation process is complete, the status is updated to indicate that the add-on package was imported successfully.

16. Select **Finish**.

    The MIAPM add-on package appears in the list of installed add-on packages on the Add-On Installation Tool screen.

17. In the installation package, navigate to the folder `\\SAP ASI ABAP Add-On\Support Package\`.

    Depending on your SAP system, navigate to either the `ECC6` folder or navigate to the `S/4 Hana` folder.

18. If your APBP release was 420_600 and level was 0000, navigate to the folder **\V4.2.0**.

    -or-

    If your ABAP release was any other version, navigate to the folder **\V4.6.0**.

19. Copy the .pat file(s).

20. On the SAP Server, paste the copied file(s) into the folder `\\usr\sap\trans\eps\in`.

21. Log in to the SAP system.

22. Run the following transaction: SPAM.

    The **Support Package Manager** screen appears.

23. Select **Menu**, then select **Support Package**, select **Load Packages**, and then select **From Application Server**.

    A message appears, asking if you want to upload the package.

24. Select **Yes**.

A summary screen appears, indicating that the package was uploaded successfully.

25. Select **Back**.
26. Select **Display/define**.

    The **Component Selection** dialog box appears.
27. Select MIAPM.
28. When prompted, confirm that the patch will be imported into the queue, and then select .
29. Select **Menu**, then select **Support Package**, and then select .
30. On the **SPAM: Import: Queue** dialog box, select .

    The import process begins. When the import is complete, a message appears, indicating that the import process was successful.
31. Select **Continue**.

    Another message appears, indicating that the import process was successful.
32. Select .
33. Select Menu, then select **Support Package**, and then select .

    The installation is complete.

Next Steps

- Configure SAP for External Numbering

Verify ASI ABAP Add-On

Procedure

1. In SAP, select **Menu**, then select **System**, and then select **Status...**.
   The System: Status window appears.
2. In the SAP System data subsection, select .
   The System: Component information window appears.
3. If you have deployed the ABAP Add-On package for the SAP Adapter, scroll down until you see the Software Component MIAPM.
   If you see the following values in the following columns, the Add-On was applied successfully:
   - **Release:**
     - ECC6: 700_600 depending on the version of SAP that you have installed.
     - S/4 Hana: 700_750
   - **Level:**
     - ECC6: 0002 (**APM Asset Strategy SP 7 - SP1**)
     - S/4 Hana: 0002

   Note: If the level does not match, go back to step 17 on page 40 of Install or Upgrade the ASI ABAP Add-On on the SAP System and rerun the installation steps.

Next Steps

Return to the workflow for the next step in the deployment process.

Uninstall the ASI ABAP Base Service Pack Add-On

Before You Begin

- Verify the release and level of your ASI ABAP installation.

Procedure

1. Log in to the SAP server as a user with either SCTSIMPSGL and S_CTS_ADMIN authorizations or SAP_ALL authorization.
2. Enter SAINT.
   The **Add-On Installation Tool** screen appears.
3. Select the **Uninstallable components** tab.
   MIAPM appears in the list of add-on packages that can be uninstalled.
4. Select **MIAPM**, and then select **Continue**.
   The **Start options** dialog box appears.
5. Select **Default options**.
6. Select .
   The status is updated to indicate that the add-on package will now be imported and the uninstallation process continues. When the process completes, the status is updated to show that the add-on package was removed successfully.
7. Select **Finish**.

Results

The MIAPM add-on package is removed from the list of installed add-on packages in the **Add-On Installation Tool** screen.

Configure SAP for External Numbering

About This Task

When you implement an Implementation Package in ASI, APM generates unique numbers for SAP Maintenance Plans, Maintenance Items, and General Maintenance Task Lists. For APM to assign these external numbers, your SAP system must be configured to allow External Numbering.

Procedure

Define the following External Number Ranges using the SAP documentation:

Object Type	From Number	To Number
Maintenance Plan **Note:** As a baseline, you must assign the number range to the PM group.	M00000000001	M99999999999
Maintenance Item	M000000000000001	M999999999999999
General Maintenance Task List	M0000001	M9999999

Next Steps

Configure SAP Permissions

Configure SAP Permissions

Before You Begin

Complete the steps described in Create APM Connect User Profile.

Procedure

Configure the following security permissions:

- Access to execute RFCs as described in SAP note 460089.
- Access to execute the functions contained in the /MIAPM/ASM function group.
- Authorizations defined in the SAP_PM_DATATRANSFER role.

  Note: For details on configuring SAP security, see the documentation for your SAP system.

Asset Strategy Management

Deploy ASM for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Review the ASM data module to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager,modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to one or more of the ASM Security Groups and Roles.	This step is required.

Upgrade or Update ASM to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

Step	Task	Notes
1	Prior to upgrading your database, review any Action records that are linked to HI Sources and link the HI Sources to Health Indicator records if necessary.	This step is optional. As of V4.3.0.6.0, actions are implemented by health indicators rather than by HI Sources. When you upgrade to the current version, if an action was previously implemented as an HI Source, if that HI Source has a related health indicator, the action will be linked to that health indicator during the upgrade. Similarly, if the action has multiple health indicators, one of them will be selected to implement the action. However, if the HI Source does not have a related health indicator, the action will no longer be implemented after the upgrade. Therefore, you should complete this step if you want to ensure your actions in these scenarios have an implementation after the upgrade (i.e., be linked to a Health Indicator record). This change does not impact Measurement Locations.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	Prior to upgrading your database, review any Action records that are linked to HI Sources and link the HI Sources to Health Indicator records if necessary.	This step is optional. As of V4.3.0.6.0, actions are implemented by health indicators rather than by HI Sources. When you upgrade to the current version, if an action was previously implemented as an HI Source, if that HI Source has a related health indicator, the action will be linked to that health indicator during the upgrade. Similarly, if the action has multiple health indicators, one of them will be selected to implement the action. However, if the HI Source does not have a related health indicator, the action will no longer be implemented after the upgrade. Therefore, you should complete this step if you want to ensure your actions in these scenarios have an implementation after the upgrade (i.e., be linked to a Health Indicator record). This change does not impact Measurement Locations.

- Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	Prior to upgrading your database, review any Action records that are linked to HI Sources and link the HI Sources to Health Indicator records if necessary.	This step is optional. As of V4.3.6.0.0, actions are implemented by health indicators rather than by HI Sources. When you upgrade to the current version, if an action was previously implemented as an HI Source, if that HI Source has a related health indicator, the action will be linked to that health indicator during the upgrade. Similarly, if the action has multiple health indicators, one of them will be selected to implement the action. However, if the HI Source does not have a related health indicator, the action will no longer be implemented after the upgrade. Therefore, you should complete this step if you want to ensure your actions in these scenarios have an implementation after the upgrade (i.e., be linked to a Health Indicator record). This change does not impact Measurement Locations.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.

- Upgrade from any version V3.5.1 through V3.5.1.12.3

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

Step	Task	Notes
1	Move to the Asset Strategy family any custom rules that are defined for the following families and configured to be executed during the Asset Strategy activation process: Action, Risk, Risk Assessment, Risk Rank, Action Revision, Risk Revision, Risk Assessment Revision, and Strategy Revision.	This step is required.
2	Move to the Asset Strategy Template family any custom rules that are defined for the following families and configured to be executed when a new Asset Strategy Template is saved after being created from an existing Asset Strategy Template or Asset Strategy: Action, Risk, Risk Assessment, Risk Rank, and Has Risk Category.	This step is required.
3	Move to the Asset Strategy or Asset Strategy Template family (as appropriate) any custom rules that are defined for any other family and are configured to be executed when an Asset Strategy or Asset Strategy Template is deleted.	This step is required.

- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Move to the Asset Strategy family any custom rules that are defined for the following families and configured to be executed during the Asset Strategy activation process: Action, Risk, Risk Assessment, Risk Rank, Action Revision, Risk Revision, Risk Assessment Revision, and Strategy Revision.	This step is required.
2	Move to the Asset Strategy Template family any custom rules that are defined for the following families and configured to be executed when a new Asset Strategy Template is saved after being created from an existing Asset Strategy Template or Asset Strategy: Action, Risk, Risk Assessment, Risk Rank, and Has Risk Category.	This step is required.
3	Move to the Asset Strategy or Asset Strategy Template family (as appropriate) any custom rules that are defined for any other family and are configured to be executed when an Asset Strategy or Asset Strategy Template is deleted.	This step is required.

- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Move to the Asset Strategy family any custom rules that are defined for the following families and configured to be executed during the Asset Strategy activation process: Action, Risk, Risk Assessment, Risk Rank, Action Revision, Risk Revision, Risk Assessment Revision, and Strategy Revision.	This step is required.
2	Move to the Asset Strategy Template family any custom rules that are defined for the following families and configured to be executed when a new Asset Strategy Template is saved after being created from an existing Asset Strategy Template or Asset Strategy: Action, Risk, Risk Assessment, Risk Rank, and Has Risk Category.	This step is required.
3	Move to the Asset Strategy or Asset Strategy Template family (as appropriate) any custom rules that are defined for any other family and are configured to be executed when an Asset Strategy or Asset Strategy Template is deleted.	This step is required.

ASM Security Groups

The following table lists the baseline Security Groups available for users within this module, as well as the baseline Roles to which those Security Groups are assigned.

Important: Assigning a Security User to a Role grants that user the privileges associated with all of the Security Groups that are assigned to that Role. To avoid granting a Security User unintended privileges, before assigning a Security User to a Role, be sure to review all of the privileges associated with the Security Groups assigned to that Role. Also, be aware that additional Roles, as well as Security Groups assigned to existing Roles, can be added via Security Manager.

Security Group	Roles
MI ASM Administrator	MI Strategy Admin
MI ASM Analyst	MI Strategy Admin MI Strategy Power MI Strategy User MI Mechanical Integrity Power
MI ASM Reviewer	MI Strategy Admin MI Strategy Power MI Strategy User
MI ASM Viewer	MI APM Viewer MI Strategy Admin MI Strategy Power MI Strategy User

The baseline family-level privileges that exist for these Security Groups are summarized in the following table.

Family	MI ASM Analyst	MI ASM Administrator	MI ASM Reviewer	MI ASM Viewer
Entity Families				
Action	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Action Mapping	View	None	None	None
Active Strategy	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Analysis Link	View	View	View	View
Asset Criticality Analysis	View	View	View	View

Family	MI ASM Analyst	MI ASM Administrator	MI ASM Reviewer	MI ASM Viewer
Asset Criticality Analysis System	View	View	View	View
Asset Strategy	View, Update, Insert, Delete	View	View, Update	View
Calibration Task	View	None	View	None
Checkpoint Task	View, Update, Insert	View, Update, Insert	View, Update, Insert	View
Consequence	View	View, Update, Insert, Delete	View	View
Distribution	View, Update, Insert, Delete	View	View	View
Execution Mapping	View	None	None	None
Growth Model	View	View	View	View
Health Indicator	View, Update, Insert, Delete	None	View, Update	View
Health Indicator Mapping	View	View, Update, Insert, Delete	View	View
Hierarchy Item Child Definition	View	View, Update, Insert, Delete	View	View
Hierarchy Item Definition	View	View, Update, Insert, Delete	View	View
Implementation Package	View, Insert	None	None	None
Inspection Task	View	None	View	View
KPI	View	View	View	View
KPI Measurement	View	View	View	View
Measurement Location	View	View	View	View
Measurement Location Group	View, Update, Insert	None	None	None
Measurement Location Template	View	View	View	View
Operator Rounds Allowable Values	View	View	View	View
Probability	View	View, Update, Insert, Delete	View	View

Family	MI ASM Analyst	MI ASM Administrator	MI ASM Reviewer	MI ASM Viewer
Proposed Strategy	View, Update, Insert, Delete	View	View, Update	View
Protection Level	View	View	View	View
RBI Degradation Mechanisms	View, Update	None	None	None
RBI Recommendation	View, Update	None	None	None
RCM FMEA Asset	View, Update, Insert, Delete	View	View	View
Reading	View	View	View	View
Reliability Distribution	View	View	View	View
Reliability Growth	View	View	View	View
Risk Assessment	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Risk Category	View	View, Update, Insert, Delete	View	View
Risk Matrix	View	View, Update, Insert, Delete	View	View
Risk Rank	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Risk Threshold	View	Insert, View, Update, Delete	View	View
Site Reference	View	View	View	View
System Action	View, Update, Insert, Delete	View	View	View
System Action Mapping	View	View, Update, Insert, Delete	View	View
System Action Optimization	View, Update, Insert, Delete	View	View	View
System Action Result	View, Update, Insert, Delete	View	View	View
System Analysis	View, Update, Insert, Delete	View	View	View
System Element	View, Update, Insert, Delete	View	View	View

Family	MI ASM Analyst	MI ASM Administrator	MI ASM Reviewer	MI ASM Viewer
System Element Result	View, Update, Insert, Delete	View	View	View
System Global Event	View, Update, Insert, Delete	View	View	View
System Resource	View, Update, Insert, Delete	View	View	View
System Resource Result	View, Update, Insert, Delete	View	View	View
System Resource Usage	View, Update, Insert, Delete	View	View	View
System Risk Assessment	View, Update, Insert, Delete	View	View	View
System Scenario	View, Update, Insert, Delete	View	View	View
System Sensor	View, Update, Insert, Delete	View	View	View
System Strategy	View, Update, Insert, Delete	View	View, Update	View
Work Management Item Child Definition	View	None	None	None
Work Management Item Definition	View	None	None	None
Work Management Item Definition Configuration	View	None	None	None
Relationship Families				
Asset Criticality Analysis Has System	View	View	View	View
Has Action Driver	View, Update, Insert, Delete	None	None	None
Has Action Mapping	View	None	None	None
Has Action Revisions	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Has Actions	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Has Active Strategy	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View

Family	MI ASM Analyst	MI ASM Administrator	MI ASM Reviewer	MI ASM Viewer
Has Asset Strategy	View, Update, Insert, Delete	View	View	View
Has Associated Recommendation	View, Update, Insert, Delete	View	View	View
Has Associated Strategy	View, Update, Insert, Delete	View	View	View
Has Checkpoint	View	None	None	None
Has Child Hierarchy Item	View	View, Update, Insert, Delete	View	View
Has Child Work Management Item	View	None	None	None
Has Driving Recommendation	View, Update, Insert, Delete	View	View, Delete	View
Has Execution Mapping	View	None	None	None
Has Functional Location	View	None	View	None
Has Global Events	View, Update, Insert, Delete	View	View	View
Has Health Indicators	View, Update, Insert, Delete	View	View	View
Has Measurement Location Group	View, Update, Insert, Delete	None	None	None
Has Mitigated TTF Distribution	View, Update, Insert, Delete	View	View	View
Has Mitigation Revisions	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Has Planned Resource Usages	View, Update, Insert, Delete	View	View	View
Has Proposed Strategy	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Has Readings	View	View	View	View
Has Recommendations	View, Update, Insert, Delete	None	None	N/A
Has Reference Values	View	View, Update, Insert, Delete	View	View

Family	MI ASM Analyst	MI ASM Administrator	MI ASM Reviewer	MI ASM Viewer
Has Resource Usages	View, Update, Insert, Delete	View	View	View
Has Risk	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Has Risk Assessments	View, Update, Insert, Delete	View	View	View
Has Risk Category	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Risk Matrix	View	None	None	None
Has Risk Revisions	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Has Root System	View, Update, Insert, Delete	View	View	View
Has Scenarios	View, Update, Insert, Delete	View	View	View
Has Strategy	View, Update, Insert, Delete	View	View	View
Has Strategy Revision	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Has System Actions	View, Update, Insert, Delete	View	View	View
Has System Elements	View, Update, Insert, Delete	View	View	View
Has System Optimization	View, Update, Insert, Delete	View	View	View
Has System Resources	View, Update, Insert, Delete	View	View	View
Has System Results	View, Update, Insert, Delete	View	View	View
Has System Risks	View, Update, Insert, Delete	View	View	View
Has System Strategy	View, Update, Insert, Delete	View	View	View
Has TTF Distribution	View, Update, Insert, Delete	View	View	View
Has TTR Distribution	View, Update, Insert, Delete	View	View	View

Family	MI ASM Analyst	MI ASM Administrator	MI ASM Reviewer	MI ASM Viewer
Has Unplanned Resource Usages	View, Update, Insert, Delete	View	View	View
Has Work Management Item	View, Update, Insert	None	None	None
Has Work Management Item Definition Configuration	View	None	None	None
Health Indicator Has Mapping	View, Update, Insert, Delete	View	View	View
Health Indicator Has Source	View, Update, Insert, Delete	View	View	View
Implements Action	View, Update, Insert	None	View	View
Implements Secondary Strategy	View	None	None	None
Implements Strategy	View, Insert	None	None	None
Is Based on RBI Degradation Mechanism	None	None	View, Delete	None
Is Based on RCM FMEA Failure Effect	View, Update, Insert, Delete	None	None	None
Is Basis for Asset Strategy Template	View, Update, Insert, Delete	View	View, Update	View
Is Mitigated	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Master Template Has Asset Strategy	View, Update, Insert, Delete	View	View, Update	View
Mitigates Risk	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Safety Analysis Has Equipment	View	N/A	View	N/A
Was Applied to Asset Strategy	View, Update, Insert, Delete	View	View, Update	View
Was Promoted to ASM Element	View	None	View	View

Associating a Strategy with a Specific Site

Some companies that use the GE Vernova software have facilities at multiple sites or locations around the world. Each site contains unique locations and equipment.

If needed, you can define these sites and associate equipment and locations with the site to which they belong. When you create an Asset Strategy record and link it to an Equipment or Functional Location record, the Site Reference field will be populated automatically with the Record ID of the Site Reference record to which the Equipment or Functional Location record is linked. To help streamline the strategy-building process, the GE Vernova system will allow you to add multiple Asset Strategies to System Strategies only if all the underlying equipment and locations belong to the same site.

Asset Strategy Optimization

Deploy ASO for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Assign Security Users to one or more of the ASO Security Groups and Roles.	This step is required.

Upgrade or Update ASO to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.0.0.0 through V4.0.1.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.1 through V3.5.1.12.3

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

Step	Task	Notes
1	Move to the Asset Strategy family any custom rules that are defined for the following families and configured to be executed during the Asset Strategy activation process: Action, Risk, Risk Assessment, Risk Rank, Action Revision, Risk Revision, Risk Assessment Revision, and Strategy Revision.	This step is required.
2	Move to the Asset Strategy Template family any custom rules that are defined for the following families and configured to be executed when a new Asset Strategy Template is saved after being created from an existing Asset Strategy Template or Asset Strategy: Action, Risk, Risk Assessment, Risk Rank, and Has Risk Category.	This step is required.
3	Move to the Asset Strategy or Asset Strategy Template family (as appropriate) any custom rules that are defined for any other family and are configured to be executed when an Asset Strategy or Asset Strategy Template is deleted.	This step is required.

- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Move to the Asset Strategy family any custom rules that are defined for the following families and configured to be executed during the Asset Strategy activation process: Action, Risk, Risk Assessment, Risk Rank, Action Revision, Risk Revision, Risk Assessment Revision, and Strategy Revision.	This step is required.
2	Move to the Asset Strategy Template family any custom rules that are defined for the following families and configured to be executed when a new Asset Strategy Template is saved after being created from an existing Asset Strategy Template or Asset Strategy: Action, Risk, Risk Assessment, Risk Rank, and Has Risk Category.	This step is required.
3	Move to the Asset Strategy or Asset Strategy Template family (as appropriate) any custom rules that are defined for any other family and are configured to be executed when an Asset Strategy or Asset Strategy Template is deleted.	This step is required.

- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Move to the Asset Strategy family any custom rules that are defined for the following families and configured to be executed during the Asset Strategy activation process: Action, Risk, Risk Assessment, Risk Rank, Action Revision, Risk Revision, Risk Assessment Revision, and Strategy Revision.	This step is required.
2	Move to the Asset Strategy Template family any custom rules that are defined for the following families and configured to be executed when a new Asset Strategy Template is saved after being created from an existing Asset Strategy Template or Asset Strategy: Action, Risk, Risk Assessment, Risk Rank, and Has Risk Category.	This step is required.
3	Move to the Asset Strategy or Asset Strategy Template family (as appropriate) any custom rules that are defined for any other family and are configured to be executed when an Asset Strategy or Asset Strategy Template is deleted.	This step is required.

ASO Security Groups

The APM Asset Strategy Optimization module leverages the baseline APM Asset Strategy Management Security Groups. To use ASO, a user must be a member of one of the following Security Groups:

- MI ASM Administrator
- MI ASM Analyst
- MI ASM Reviewer
- MI ASM Viewer

Calibration Management

Deploy Calibration Management for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Review the Calibration Management data model to determine which relationship definitions you will need to modify to include your custom families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to one or more of the Calibration Management Security Groups and Roles.	This step is required.
3	Configure the Has Standard Gas relationship family to include the desired Instrument families as predecessors to the Standard Gas Cylinder family in Configuration Manager.	This step is required only if you will use one or more standard gas cylinders to calibrate an asset.
4	Define alternate search queries.	This step is required only if you do not want to use the baseline search queries.
5	Configure default values for Calibration Template and Calibration Event Records by accessing the Calibration Setup Defaults family in Application Settings.	This step is required.
6	Install the Meridium Device Service on all of the machines that will connect to devices that will be used with Calibration Management.	This step is required only if you are performing an automated calibration.

Upgrade or Update Calibration Management to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

Step	Task	Notes
1	Uninstall the previous version of the Meridium Device Service, and install the latest version on all the machines that you will connect to a device used for automated calibration. **Important:** If, however, you use HTTPS to connect to APM, then you must follow the instructions in KBA 000059233.	This step is required only if you want to use a device to perform automated calibration.
2	Using the command prompt, navigate to the <APM `installation folder>/Upgrade` folder, and then run the following command: `Meridium.DbUtility.CalibDeviceMappingsUpgradeUtility.exe <datasource ID> <username> <password>` Where, ◦ <datasource ID> is the identification of your data source. ◦ <username> is the APM username. ◦ <password> is the APM password.	This step is required only if you want to use the Fluke documenting process calibrator. This will replace the old Calibration Device Mappings for the device with the new ones. It will also update the existing templates to use the new Calibrator Device Mappings. After you complete this step, a log file is generated containing information about the upgrade process.

- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

Step	Task	Notes
1	Uninstall the previous version of the Meridium Device Service, and install the latest version on all the machines that you will connect to a device used for automated calibration. **Important:** If, however, you use HTTPS to connect to APM, then you must follow the instructions in KBA 000059233.	This step is required only if you want to use a device to perform automated calibration.
2	Using the command prompt, navigate to the <APM `installation folder>/Upgrade` folder, and then run the following command: `Meridium.DbUtility.CalibDeviceMappingsUpgradeUtility.exe <datasource ID> <username> <password>` Where, ◦ <datasource ID> is the identification of your data source. ◦ <username> is the APM username. ◦ <password> is the APM password.	This step is required only if you want to use the Fluke documenting process calibrator. This will replace the old Calibration Device Mappings for the device with the new ones. It will also update the existing templates to use the new Calibrator Device Mappings. After you complete this step, a log file is generated containing information about the upgrade process.

- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

Step	Task	Notes
1	Uninstall the previous version of the Meridium Device Service, and install the latest version on all the machines that you will connect to a device used for automated calibration. **Important:** If, however, you use HTTPS to connect to APM, then you must follow the instructions in KBA 000059233.	This step is required only if you want to use a device to perform automated calibration.
2	Using the command prompt, navigate to the <APM `installation folder>/Upgrade` folder, and then run the following command: `Meridium.DbUtility.CalibDeviceMappingsUpgradeUtility.exe <datasource ID> <username> <password>` Where, ◦ <datasource ID> is the identification of your data source. ◦ <username> is the APM username. ◦ <password> is the APM password.	This step is required only if you want to use the Fluke documenting process calibrator. This will replace the old Calibration Device Mappings for the device with the new ones. It will also update the existing templates to use the new Calibrator Device Mappings. After you complete this step, a log file is generated containing information about the upgrade process.

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

Step	Task	Notes
1	Uninstall the previous version of the Meridium Device Service, and install the latest version on all the machines that you will connect to a device used for automated calibration. **Important:** If, however, you use HTTPS to connect to APM, then you must follow the instructions in KBA 000059233.	This step is required only if you want to use a device to perform automated calibration.
2	Using the command prompt, navigate to the <APM `installation folder>/Upgrade` folder, and then run the following command: `Meridium.DbUtility.CalibDeviceMappingsUpgradeUtility.exe <datasource ID> <username> <password>` Where, ◦ <datasource ID> is the identification of your data source. ◦ <username> is the APM username. ◦ <password> is the APM password.	This step is required only if you want to use the Fluke documenting process calibrator. This will replace the old Calibration Device Mappings for the device with the new ones. It will also update the existing templates to use the new Calibrator Device Mappings. After you complete this step, a log file is generated containing information about the upgrade process.

- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

Step	Task	Notes
1	Uninstall the previous version of the Meridium Device Service, and install the latest version on all the machines that you will connect to a device used for automated calibration. **Important:** If, however, you use HTTPS to connect to APM, then you must follow the instructions in KBA 000059233.	This step is required only if you want to use a device to perform automated calibration.
2	Using the command prompt, navigate to the <APM `installation folder>/Upgrade` folder, and then run the following command: `Meridium.DbUtility.CalibDeviceMappingsUpgradeUtility.exe <datasource ID> <username> <password>` Where, ◦ <datasource ID> is the identification of your data source. ◦ <username> is the APM username. ◦ <password> is the APM password.	This step is required only if you want to use the Fluke documenting process calibrator. This will replace the old Calibration Device Mappings for the device with the new ones. It will also update the existing templates to use the new Calibrator Device Mappings. After you complete this step, a log file is generated containing information about the upgrade process.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	Uninstall the previous version of the Meridium Device Service, and install the latest version on all the machines that you will connect to a device used for automated calibration. **Important:** If, however, you use HTTPS to connect to APM, then you must follow the instructions in KBA 000059233.	This step is required only if you want to use a device to perform automated calibration.
2	Using the command prompt, navigate to the <APM `installation folder>/Upgrade` folder, and then run the following command: `Meridium.DbUtility.CalibDeviceMappingsUpgradeUtility.exe <datasource ID> <username> <password>` Where, ◦ <datasource ID> is the identification of your data source. ◦ <username> is the APM username. ◦ <password> is the APM password.	This step is required only if you want to use the Fluke documenting process calibrator. This will replace the old Calibration Device Mappings for the device with the new ones. It will also update the existing templates to use the new Calibrator Device Mappings. After you complete this step, a log file is generated containing information about the upgrade process.

- Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	Uninstall the previous version of the Meridium Device Service, and install the latest version on all the machines that you will connect to a device used for automated calibration. **Important:** If, however, you use HTTPS to connect to APM, then you must follow the instructions in KBA 000059233.	This step is required only if you want to use a device to perform automated calibration.
2	Using the command prompt, navigate to the <APM `installation folder>/Upgrade` folder, and then run the following command: `Meridium.DbUtility.CalibDeviceMappingsUpgradeUtility.exe <datasource ID> <username> <password>` Where, ◦ <datasource ID> is the identification of your data source. ◦ <username> is the APM username. ◦ <password> is the APM password.	This step is required only if you want to use the Fluke documenting process calibrator. This will replace the old Calibration Device Mappings for the device with the new ones. It will also update the existing templates to use the new Calibrator Device Mappings. After you complete this step, a log file is generated containing information about the upgrade process.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

Step	Task	Notes
1	Using the command prompt, navigate to the <APM `installation folder>/Upgrade` folder, and then run the following command: `Meridium.DbUtility.CalibDeviceMappingsUpgradeUtility.exe <datasource ID> <username> <password>` Where, ◦ <datasource ID> is the identification of your data source. ◦ <username> is the APM username. ◦ <password> is the APM password.	This step is required only if you want to use the Fluke documenting process calibrator. This will replace the old Calibration Device Mappings for the device with the new ones. It will also update the existing templates to use the new Calibrator Device Mappings. After you complete this step, a log file is generated containing information about the upgrade process.

- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

  When you upgrade:

- For each applied template, a Calibration Profile is created.
- The Calibration Profile is linked to the applied template and the associated asset.
- You will not be able to link additional assets to the Calibration Profile.
- For each Calibration record whose **Calibration Closed** check box is selected, the state is changed to Approved.
- The Calibration Strategy and Device Type fields in the Calibration Profile will be blank.

Step	Task	Notes
1	Using the command prompt, navigate to the <APM `installation folder>/Upgrade` folder, and then run the following command: `Meridium.DbUtility.CalibDeviceMappingsUpgradeUtility.exe <datasource ID> <username> <password>` Where, ◦ <datasource ID> is the identification of your data source. ◦ <username> is the APM username. ◦ <password> is the APM password.	This step is required only if you want to use the Fluke documenting process calibrator. This will replace the old Calibration Device Mappings for the device with the new ones. It will also update the existing templates to use the new Calibrator Device Mappings. After you complete this step, a log file is generated containing information about the upgrade process.

- Upgrade from any version V3.5.1 through V3.5.1.12.3

Step	Task	Notes
1	Using the command prompt, navigate to the <APM `installation folder>/Upgrade` folder, and then run the following command: `Meridium.DbUtility.CalibDeviceMappingsUpgradeUtility.exe <datasource ID> <username> <password>` Where, ◦ <datasource ID> is the identification of your data source. ◦ <username> is the APM username. ◦ <password> is the APM password.	This step is required only if you want to use the Fluke documenting process calibrator. This will replace the old Calibration Device Mappings for the device with the new ones. It will also update the existing templates to use the new Calibrator Device Mappings. After you complete this step, a log file is generated containing information about the upgrade process.

- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

Step	Task	Notes
1	Using the command prompt, navigate to the <APM `installation folder>/Upgrade` folder, and then run the following command: `Meridium.DbUtility.CalibDeviceMappingsUpgradeUtility.exe <datasource ID> <username> <password>` Where, ◦ <datasource ID> is the identification of your data source. ◦ <username> is the APM username. ◦ <password> is the APM password.	This step is required only if you want to use the Fluke documenting process calibrator. This will replace the old Calibration Device Mappings for the device with the new ones. It will also update the existing templates to use the new Calibrator Device Mappings. After you complete this step, a log file is generated containing information about the upgrade process.

- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Using the command prompt, navigate to the <APM `installation folder>/Upgrade` folder, and then run the following command: `Meridium.DbUtility.CalibDeviceMappingsUpgradeUtility.exe <datasource ID> <username> <password>` Where, ◦ <datasource ID> is the identification of your data source. ◦ <username> is the APM username. ◦ <password> is the APM password.	This step is required only if you want to use the Fluke documenting process calibrator. This will replace the old Calibration Device Mappings for the device with the new ones. It will also update the existing templates to use the new Calibrator Device Mappings. After you complete this step, a log file is generated containing information about the upgrade process.

- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Using the command prompt, navigate to the <APM `installation folder>/Upgrade` folder, and then run the following command: `Meridium.DbUtility.CalibDeviceMappingsUpgradeUtility.exe <datasource ID> <username> <password>` Where, ◦ <datasource ID> is the identification of your data source. ◦ <username> is the APM username. ◦ <password> is the APM password.	This step is required only if you want to use the Fluke documenting process calibrator. This will replace the old Calibration Device Mappings for the device with the new ones. It will also update the existing templates to use the new Calibrator Device Mappings. After you complete this step, a log file is generated containing information about the upgrade process.

Install the Meridium Device Service

About This Task

Important: You must repeat this procedure on each machine to which you will connect a calibrator.

The Meridium Device Service can be installed as part of the workflow when you try to send data to calibrator or verify the settings of the calibrator.

Procedure

1. Access the **Calibration Management Overview** page.

   Note: A calibrator does not need to be connected.
2. Select the **Calibration Tools** tab.

   The **Calibration Tools** section appears, displaying a list of test equipment and standard gas cylinders.
3. In the upper-right corner of the page, select **Calibrator Settings**.

   The **Calibrator Settings** window appears.
4. In the **Select Device** box, select the required device.
5. If you selected the CMX Calibration Management software, enter values in the following fields:
   - If you want to test the connection of the CMX Calibration Management software, select the **Perform Connection Test** check box.
   - In the **Device Service Settings Service Port** box, enter the value of the service port number that you have configured. The default value in the **Device Service Settings Service Port** box is 2014.

   If you selected a Fluke documenting process calibrator, enter values in the following fields:

- In the **COM Port** box, select the communication port number to which the calibrator is connected.

  Important: APM supports port numbers in the range of COM1 through COM4. If the communication port number of the calibrator does not fall within this range, you must change the value in the Device Manager, or connect the calibrator to a different port.
- If you want to test the connection of the Fluke documenting process calibrator, select the **Perform Connection Test** check box.

  Note: The **Baud Rate** box contains the value 9600. You cannot change this value.
- In the **Device Service Settings Service Port** box, enter the value of the service port number that you have configured. The default value in the **Device Service Settings Service Port** box is 2014.

If you selected a GE Druck documenting process calibrator, enter values in the following fields:

- If you want to test the connection of the GE Druck documenting process calibrator, select the **Perform Connection Test** check box.
- In the **Device Service Settings Service Port** box, enter the value of the service port number that you have configured. The default value in the **Device Service Settings Service Port** box is 2014.

6. Select **Done**.

   The **Calibrator Settings** window appears, indicating that the Meridium Device Service is not installed.

7. Select **Download**.

   The file **MeridiumDevices.exe** is downloaded.

8. Run `MeridiumDevices.exe`, and then follow the instructions in the installer.

   The Meridium Device Service is installed.

Compliance Management

Deploy Compliance Management

The checklists in this section of the documentation contain all the steps necessary for deploying and configuring this module whether you are deploying the module for the first time or upgrading from a previous version.

Important: You must have an active license in Compliance Management, Inspection Management, and Policy Designer to use this module.

Deploy Compliance Management for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Review the Compliance Management data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign users to the MI Inspection Security Group to provide privileges to the Compliance Management families.	This step is required.
3	Assign Security Users to one or more of the Security Roles used in Compliance Management.	This step is required. Security Users will need permissions to the Compliance Management families before they can use the Compliance Management features.
4	Create Inspection Strategy records using Record Manager.	This step is required. You should create Compliance Strategy records that adhere to the compliance standards of a regulatory body that requires inspections.

5	Design a policy to use for a Compliance Strategy Template.	This step is required. You can create this policy using the Policy Designer.
6	Create a query that will return the assets that you want to link to the Compliance Strategy Template.	This step is optional. You can also add assets to the Compliance Strategy Template by individual asset.
7	Create a Compliance Strategy Template using the administrative features of Compliance Management.	This step is required.
8	Link assets to the Compliance Strategy Template.	This step is required.
9	Map the Policy to the Compliance Strategy Template that you created.	This step is required.

Upgrade or Update Compliance Management to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

After you upgrade to the latest version of APM, following updates are automatically available:

- The MI Compliance Approver security role caption will be updated to MI Inspection Plan Approver.
- All security users who belong to the MI RBI Analyst security group will belong to the MI Inspection Plan Approver security role.
- The MI Inspection Plan Approver security role will have the MI ASM Analyst security group assigned.
- Compliance Recommendation Revision family will be renamed to Recommendation Revision. The datasheet for this family will be renamed to Recommendation Revision.
- The query Compliance Recommendation by Plan for Compliance will be renamed to Recommendation by Plan.
- The relationship family caption Has Compliance Recommendation will be updated to Inspection Plan Has Recommendation.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

Step	Task	Notes
1	Revert the following Compliance Management query to baseline: `Public/Meridium/Modules/Inspection/Compliance/Queries/Recommended Actions by Selected Plans`	This step is required if you want to use the RBI Inspection Grouping functionality.
2	Revert the following Compliance Management query to baseline: ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/Active Recommendations of Plan for Unit` ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/All Inspection Plans for Unit` ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/Assets with Inspection Plans` ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/Compliance Superseded Recommendations`	This step is required only if you have modified the following queries: ◦ Active Recommendations of Plan for Unit ◦ All Inspection Plans for Unit ◦ Assets with Inspection Plans ◦ Compliance Superseded Recommendations (Caption: Linked Recommendations)

- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

Step	Task	Notes
1	Revert the following Compliance Management query to baseline: `Public/Meridium/Modules/Inspection/Compliance/Queries/Recommended Actions by Selected Plans`	This step is required if you want to use the RBI Inspection Grouping functionality.
2	Revert the following Compliance Management query to baseline: ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/Active Recommendations of Plan for Unit` ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/All Inspection Plans for Unit` ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/Assets with Inspection Plans` ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/Compliance Superseded Recommendations`	This step is required only if you have modified the following queries: ◦ Active Recommendations of Plan for Unit ◦ All Inspection Plans for Unit ◦ Assets with Inspection Plans ◦ Compliance Superseded Recommendations (Caption: Linked Recommendations)

- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

Step	Task	Notes
1	Revert the following Compliance Management query to baseline: `Public/Meridium/Modules/Inspection/Compliance/Queries/Recommended Actions by Selected Plans`	This step is required if you want to use the RBI Inspection Grouping functionality.
2	Revert the following Compliance Management query to baseline: ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/Active Recommendations of Plan for Unit` ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/All Inspection Plans for Unit` ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/Assets with Inspection Plans` ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/Compliance Superseded Recommendations`	This step is required only if you have modified the following queries: ◦ Active Recommendations of Plan for Unit ◦ All Inspection Plans for Unit ◦ Assets with Inspection Plans ◦ Compliance Superseded Recommendations (Caption: Linked Recommendations)

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11.

<table>
<tr><th>Step</th><th>Task</th><th>Notes</th></tr>
<tr><td>1</td><td>Execute the Revert to Baseline utility to update State Machine for Compliance Recommendation.

Following new states and operations have been added:

<table><tr><th>State ID</th><th>Caption</th></tr><tr><td>MI_ACCEPTED</td><td>Approved</td></tr></table>
<table><tr><th>Operation ID</th><th>Caption</th><th>Predecessor</th><th>Successor</th></tr><tr><td>MI_PROMOTE</td><td>Approve</td><td>Proposed</td><td>Approved</td></tr><tr><td>MI_IMPLEMENT</td><td>Implement</td><td>Approved</td><td>Implemented</td></tr><tr><td>MI_UNIMPLEMENT</td><td>Unimplement</td><td>Implemented</td><td>Approved</td></tr></table></td><td>This step is required only if:

◦ You have previously used Compliance Management and have created Compliance Recommendation records, or
◦ You have previously modified the state management for the Compliance Recommendation family.</td></tr>
<tr><td>2</td><td>Execute the database script to update the state for all Compliance Recommendations related to an Inspection Plan to the Approved state.</td><td>To complete this step, follow the instructions in KBA 000041450.</td></tr>
<tr><td>3</td><td>To facilitate workflows in Compliance Management in the latest version of APM, several queries have been modified. If you have made any modifications to these queries, you may need to review the respective query in the Baseline folder to determine if any change to the Public query is required.

Alternatively, you may also execute the Revert to Baseline utility to acquire the changes to queries in the latest version of APM.</td><td>This step is required if you have modified any of the following queries:

◦ Public\Meridium\Modules\Inspection\Compliance\Queries
  ◦ Compliance Recommendations by Plan
  ◦ Compliance Recommendations to Supersede
  ◦ Compliance Superseded Recommendation Counts
  ◦ Compliance Superseded Recommendations
  ◦ Assets with Inspection Plans
  ◦ Compliance Recommendation Revisions for Inspection Plan
  ◦ Inspection Tasks Available to Implement
◦ Public\Meridium\Modules\Asset Strategy\Queries
  ◦ Inspection Task Link Existing Query</td></tr>
<tr><td>4</td><td>Update the datasheet for the Compliance Strategy Template family and replace the Policy field to Policy Name field.</td><td>If you have customized the default datasheet for the Compliance Strategy Template family, then you must do one of the following:

◦ Using Family Management, edit the default datasheet for Compliance Strategy Template family. Next,replace the Policy field to Policy Name field in the datasheet.
◦ Run Revert to Baseline for each family</td></tr>
</table>

Step	Task	Notes
5	Update the datasheet for the Compliance Recommendation family and add the Chamber and Certification fields.	If you have customized the default datasheet for the Compliance Recommendation family, and you want to view Certification and Chamber-related data, then do one of the following: ◦ Using Family Management, edit the default datasheet for Compliance Recommendation family. Next, add the Certification and Chamber fields in the datasheet. ◦ Run Revert to Baseline for each family
7	Revert the following Compliance Management query to baseline: ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/Active Recommendations of Plan for Unit` ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/All Inspection Plans for Unit` ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/Assets with Inspection Plans` ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/Compliance Superseded Recommendations`	This step is required only if you have modified the following queries: ◦ Active Recommendations of Plan for Unit ◦ All Inspection Plans for Unit ◦ Assets with Inspection Plans ◦ Compliance Superseded Recommendations (Caption: Linked Recommendations)

Revert the Compliance Management Query to Baseline

This action is required only if you want to use the RBI Inspection Grouping functionality.

About This Task

If you have modified the Recommended Actions by Selected Plans query, perform the following steps to revert the query to baseline:

Procedure

1. Access the Catalog page.
2. Navigate to the following Public folder:
   `Public/Meridium/Modules/Inspection/Compliance/Queries/`
3. Select the check box next to the Recommended Actions by Selected Plans query, and then select  .

The **Confirm Delete** window appears, asking you to confirm if you want to delete the selected query.

4. Select **OK**.
   The selected query is deleted.
5. Navigate to the following Baseline folder.
   `Baseline/Meridium/Modules/Inspection/Compliance/Queries/`
6. Select the check box next to the Recommended Actions by Selected Plans query, and then select  .
   The **Catalog Folder Browser** window appears.
7. Navigate to the Public folder containing the query that you deleted in step 3.
8. Select **OK**.
   A success message appears indicating that the selected item has been copied successfully.

Compliance Strategy Template Datasheet - Revert to Baseline

About This Task

The default datasheet for Compliance Strategy Template family has been updated. The field Policy Name is included and the deprecated field Policy Key is removed from the datasheet.

Family	Family ID	Datasheet Updated (Default)
Compliance Strategy Template	MI_COMP_STRAT_TEMP	Compliance Strategy Template

If you have customized the default datasheet for Compliance Strategy Template family, then you must do one of the following:

- Using Family Management, edit the default datasheet for the Compliance Strategy Template family. Replace the Policy field to Policy Name field in the datasheet.
- Run Revert to Baseline for each family.

Important: Running this utility overwrites your current datasheet and replaces it with the baseline version. You must be a super user in APM to run the Revert to Baseline utility.

Procedure

1. Log in to the server where APM is installed.
2. Navigate to *<Installation Directory>*`\Meridium\Upgrade\DBUpgrade`.
3. Run the `RevertToBaselineApp.exe` file as administrator.
   The **Revert To Baseline Login** window appears.
4. In the **Meridium Data Source** box, enter the data source name that you want to access.
5. Enter your login credentials, and then select **Next**.
   The available families that can be reverted to baseline appear.
6. Select the Compliance Strategy Template family, and then select **Revert to Baseline**.
   The **Various Options For Revert** window appears.
7. Select **Datasheets**.
   Select the Default Datasheet from the drop-down list, and then select **Ok**.

Compliance Recommendation - Revert to Baseline

About This Task

The default datasheet for Compliance Recommendation family has been updated and it includes the Certification and the Chamber fields.

Family	Family ID	Datasheet Updated (Default)
Compliance Recommendation	MI_COMP_RECOMM	Compliance Recommendation

If you have customized the default datasheet for the Compliance Recommendation family, and want to view Certification and Chamber-related data, then you must do one of the following:

- Using Family Management, edit the default datasheet for the Compliance Recommendation family. Next, add the Certification, Chamber, and Applicable Regulation fields in the datasheet.
- Run Revert to Baseline for each family.

Important: Running this utility overwrites your current datasheet and replaces it with the baseline version. You must be a super user in APM to run the Revert to Baseline utility.

Procedure

1. Log in to the server where APM is installed.
2. Navigate to *<Installation Directory>*`\Meridium\Upgrade\DBUpgrade`.
3. Run the `RevertToBaselineApp.exe` file as administrator.
   The **Revert To Baseline Login** window appears.
4. In the **Meridium Data Source** box, enter the data source name that you want to access.
5. Enter your login credentials, and then select **Next**.
   The available families that can be reverted to baseline appear.
6. Select the Compliance Recommendation family, and then select **Revert to Baseline**.
   The **Various Options For Revert** window appears.
7. Select **Datasheets**.
   Select the Default Datasheet from the drop-down list, and then select **Ok**.

Compliance Management Security Groups and Roles

The following table lists the baseline Security Groups available for users within this module, as well as the baseline Roles to which those Security Groups are assigned.

Important: Assigning a Security User to a Role grants that user the privileges associated with all of the Security Groups that are assigned to that Role. To avoid granting a Security User unintended privileges, before assigning a Security User to a Role, be sure to review all of the privileges associated with the Security Groups assigned to that Role. Also, be aware that additional Roles, as well as Security Groups assigned to existing Roles, can be added via Security Manager.

Security Groups

The following families adhere to the security groups listed in the table below:

- Asset Has Compliance Template
- Asset Has Inspection Plan
- Compliance Recommendation
- Recommendation Revision
- Compliance Policy Mapping
- Compliance Strategy
- Compliance Strategy Template
- Compliance Template Has Mapping
- Inspection Plan Has Recommendations
- Has Inspection Plan Revision
- Implements Compliance Recommendation
- Inspection Plan
- Inspection Plan Revision
- Suggested Compliance Templates

Security Group	Permissions
MI Inspection	• View • Insert • Update • Delete
MI Inspection Viewer	View
MI RBI Administrator	View
MI RBI Analyst	View
MI RBI Viewer	View
MI Thickness Monitoring Administrator	View
MI Thickness Monitoring Inspector	View
MI Thickness Monitoring User	View
MI Thickness Monitoring Viewer	View

Security Roles

Compliance Management security roles can perform the following tasks:

Task	Description
Approve	Change the state of an Inspection Plan to Approved.
Apply Templates	Apply suggested Compliance Strategy Templates to assets in the **Assets without Templates** section of the **Compliance Management Overview** page.
Create	Create an Inspection Plan or Compliance Strategy Template.

Task	Description
Modify	Modify Inspection Plans and Compliance Recommendations by changing States, deleting Compliance Recommendations, and implementing Compliance Recommendations as Inspection Tasks.
Suggest Templates	Suggest Compliance Strategy Templates to be linked to assets in the **Assets without Templates** section of the **Compliance Management Overview** page.
View	Access a Compliance Recommendation, Inspection Plan, or Compliance Strategy Template.

The following security roles are available in Compliance Management:

Security Role	Inspection Plan Privileges	Compliance Strategy Template Privileges	Assigned Security Group
MI Compliance Administrator	View	• Apply Templates • Create • Modify • Suggest Templates	
MI Compliance Analyst	• Create • Modify	• Apply Templates • Suggest Templates • View	
MI Inspection Plan Approver	• Create • Modify • Approve	• Apply Templates • Suggest Templates • View	• MI ASM Analyst

eLog

Deploy eLog for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Note
1	If needed, create a subfamily for the eLog Entry family to store the information that you want to record. The subfamily inherits the fields from the eLog Entry family. You can add fields as needed. **Important:** Fields inherited from the eLog Entry family should not be modified. **Note:** If you want the data related to the additional fields (that is, the fields you may have added) to appear in the **Shift Log** workspace in the **Shift Summary** page, modify the Get All Log Entries query such that the data appears in the Log Text field of the log entry.	This step is required only if the baseline eLog Entry family does not contain the information that you want to record.
2	Review the eLog data model to determine which relationship definitions you will need to include the custom families or subfamilies. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if: • You store equipment and location information in families other than the baseline Equipment and Functional Location families. or • You have created families or subfamilies.
3	Assign Security Users to one or more of the eLog Security Groups or Roles.	This step is required.

Upgrade or Update eLog to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

Failure Modes and Effects Analysis

Deploy FMEA for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Step	Task	Notes
1	Assign Security Users to one or more of the FMEA Security Groups and Roles.	This step is required.
2	Review the FMEA data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.

Upgrade or Update FMEA to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

Step	Task	Notes
1	Prior to upgrading your database, review any FMEA Analysis records that are linked to virtual assets. If you want any of those analyses to remain an analysis, link the associated virtual assets to the Asset Hierarchy prior to upgrading. In addition, for any analyses that are linked to both real and virtual assets, link all the virtual assets in the analysis to the Asset Hierarchy prior to upgrading.	This step is required only if your database has virtual assets linked to an RCM analysis, and you do not want the analysis to be converted to an analysis template on upgrading.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.0.0.0 through V4.0.1.0

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.1 through V3.5.1.12.3

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Assign Security Users to the MI RCM Viewer Security Group.	This step is required.
2	Add values to the Recommended Resource System Code Table.	This step is required. This System Code Table is used to populate the Recommended Resource field in RCM FMEA Recommendation records.

Generation Availability Analysis

Deploy GAA for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Review the Generation Availability Analysis data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to one or more of the GAA Security Groups and Roles.	This step is required. Users must have permissions to the GAA families to use the GAA functionality.
3	Specify additional system codes for families available in GAA.	By default, APM provides a set of system codes for the families available in GAA. You can modify these default system codes or you can add new system codes.

Step	Task	Notes
4	Add a GAA Company.	This step is required. You must define the GAA Company to represent the functional location that you want to use in GAA. You must add a GAA Company at the highest level in the functional location, followed by GAA Plant and GAA Unit at the next subsequent levels. You must define GAA Company, GAA Plant, and GAA Unit before you can start recording event data. GAA Company is stored in a GAA Company record. You will need to repeat this step whenever you want to record data about any company that has not yet been identified within your system. Each GAA Company, however, can be associated with only one Hierarchy Level and vice-versa.
5	Add a GAA Plant.	This step is required. You must define the GAA Plant to represent the functional location that you want to use in GAA. You must add a GAA Plant at the level next to GAA Company in the functional location, followed by GAA Unit at the next subsequent levels. You must define a GAA Company before defining a GAA Plant, and a GAA Plant before defining a GAA Unit. GAA Plant is stored in a GAA Plant record. You will need to repeat this step whenever you want to record data about any plant that has not yet been identified within your system. Each GAA Plant, however, can be associated with only one Hierarchy Level and vice-versa.

Step	Task	Notes
6	Add a GAA Unit.	This step is required. You must define the GAA Unit to represent the functional location that you want to use in GAA. You must add a GAA Unit at the level next to GAA Plant in the functional location. You must define a GAA Unit after defining a GAA Company and a GAA Plant. GAA Unit is stored in a GAA Unit record. You will need to repeat this step whenever you want to record data about any unit that has not yet been identified within your system. Each GAA Unit, however, can be associated with only one functional location and vice-versa.
7	Verify GAA Unit Capacity.	This step is required. When you add a GAA Unit record, a Unit Capacity record is automatically created with the values defined in the capacity related fields in the GAA Unit record. You must verify these values. As needed, you can modify the values in the available fields.
8	Configure GAA Reports.	This step is required. You must configure the reports that you want to appear for a GAA Unit.

Upgrade or Update GAA to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

Migrate from Generation Management (GM) to GAA

About This Task

The following table outlines the steps that you must complete to migrate to this module. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

Results

Step	Task	Notes
1	Using the file **Meridium.DbUtility.GAAUpgradeUtility.exe** stored in the installation folder (e.g., **C:\Program Files\Meridium\Upgrade**), set the following information: • User ID in the userId field. • Password in the password field. • Database name in the datasourceId field. • Regulatory organization (NERC, CEA) in the fuelReportingOrganization field.	This step is required.
2	In the Generation Company family: • In the Enterprise 1 Code (MI_GMCOMPNY_ERP_01_CD_C) field, enter the Asset ID. **Note:** The Asset ID is the Entity ID of the functional location. • In the Enterprise 1 Description (MI_GMCOMPNY_ERP_01_DESC_C) field, for the Primary Regulatory Organization, enter the value NERC or CEA. **Note:** If the Primary Regulatory Organization information has not been set, an exception error will occur. • In the Enterprise 3 Code (MI_GMCOMPNY_ERP_03_CD_C) field, enter the Country ID. **Note:** In APM V4.3.0.0.0, the Country field is required.	This step is required. The GAA Company will receive the site key from the associated functional location.

Step	Task	Notes
3	In the Generation Plant family: • In the Enterprise 1 Code (MI_GM_PLANT_ERP_01_CD_C) field, enter the Asset ID. **Note:** The Asset ID is the Entity ID of the functional location. • In the Enterprise 1 Description (MI_GM_PLANT_ERP_01_DESC_C) field, for the Primary Regulatory Organization, enter the value NERC or CEA. **Note:** If the Primary Regulatory Organization information has not been set, an exception error will occur. • In the Enterprise 4 Code (MI_GM_PLANT_ERP_04_CD_C) field, enter the time zone for the Plant. **Note:** If the time zone information is invalid, an exception error will occur.	This step is required. The GAA Plant will receive the site key from the associated functional location.

<table>
<tr><th>Step</th><th>Task</th><th>Notes</th></tr>
<tr><td>4</td><td>In the Generation Unit family:
In the Enterprise 1 Code (MI_GM_UNIT0_ERP_01_CD_C) field, enter the Asset ID.

Note: The Asset ID is the Entity ID of the functional location.
In the Enterprise 1 Description (MI_GM_UNIT0_ERP_01_DESC_C) field, for the Primary Regulatory Organization, enter the value NERC or CEA.

Note: If the Primary Regulatory Organization information has not been set, an exception error will occur.</td><td>This step is required.

The GAA Unit will receive the site key from the associated functional location.

The Primary Event and the Contributing Event will receive the site key from the GAA Unit.

The values in the Generation Unit records will be mapped to the corresponding fields in Unit Capacity records as shown in the following table:

<table><tr><th>Fields in Generation Unit record</th><th>Fields in Unit Capacity record</th></tr><tr><td>Gross Maximum Capacity</td><td>Nameplate Gross Maximum Capacity</td></tr><tr><td>Net Maximum Capacity</td><td>Nameplate Net Maximum Capacity</td></tr><tr><td>Gross Dependable Capacity</td><td>Nameplate Gross Dependable Capacity</td></tr><tr><td>Net Dependable Capacity</td><td>Nameplate Net Dependable Capacity</td></tr></table>
By default, the Unit Capacity record will be created for all the units with the value in Start Date field set to 01/01/1900 and the value in End Date field set to null.</td></tr>
</table>

Step	Task	Notes
5	**Important:** R server must be configured and running before you run the **GAAUpgradeUtility.exe**. Run the file **GAAUpgradeUtility.exe**.	This step is required. During the upgrade: • The states in the Incident Reporting Status field for Primary Events and the states in the Reporting Status field for Performance records will be updated to the new State Management. • The queries in V3.6.0.0.0 will be replaced by the queries in V4.3.0.0.0. • The Is Default field will be set to True for all records in the GAA Configuration family. • The upgrade will map the existing fields in the Events and Performance data to the fields in the new families. • The Event Details for all the Units will be generated. After you complete this step, a log file is generated containing detailed information about the upgrade process.

Query Mapping

When you upgrade this module from V3.6.0.0.0 through V4.0.0.0.0, the following queries in V3.6.0.0.0 will be replaced by the queries in V4.3.0.0.0:

Query in V3.6.0.0.0	Query in V4.3.0.0.0
Public\Meridium\Modules\Generation Management \Queries\NERC Queries\NERC GADS Event Report 07	Public\Meridium\Modules\Generation Management \Queries\NERC Queries\NERC Event Report 07
Public\Meridium\Modules\Generation Management \Queries\NERC Queries\NERC GADS Performance Report 05	Public\Meridium\Modules\Generation Management \Queries\NERC Queries\NERC Performance Report 05

State Management Mapping

When you upgrade this module from V3.6.0.0.0 through V4.0.0.0.0, the state in the Incident Reporting Status field for Primary Events and the state in the Reporting Status field for Performance Records will be updated to the new State Management as shown in the following table:

States in V3.6.0.0.0	States in V4.3.0.0.0
Created	In Progress
Unit Level Approval	Unit Approved
Corporate Approval	Approved

The values from the Incident Reporting Status field (MI_GMCAPINC_INC_REPOR_STATU_C) for a Primary Event and the values from the Reporting Status field (MI_GMCAPHST_REPOR_STATU_C) for a Performance Record in V3.6.0.0.0, will be mapped to the new State Management field (MI_SM_STATE_ID_C) for a Primary Event and Performance Record in V4.3.0.0.0.

Field Mapping

When you upgrade this module from V3.6.0.0.0 through V4.0.0.0.0, the calculations will be performed for the net and gross values. The policies that are provided as part of the baseline data during the upgrade will be associated with all the GAA Units.

Note: During the upgrade, for the GAA Performance Indexes family, one record each will be created for the Net Maximum Capacity (NMC) and Gross Maximum Capacity (GMC) weightage type fields. Also, in the GAA Performance Fuel family, one record each will be created for the primary and secondary Fuel Source.

The upgrade will map the Events and Performance data from the fields in the existing Capacity History family to the corresponding fields in the GAA Performance Fuel, GAA Performance Index, and GAA Performance Summary families as follows.

Fields in V3.6.0.0.0	Fields in V4.3.0.0.0
Capacity History	GAA Performance Fuel
Common Fuel Code 1 (MI_GMCAPHST_COMMO_FUEL_CD_1_C)	Common Fuel Code (MI_PERF_FUEL_COMM_FUEL_CODE_C)
Heat Rate (G) (MI_GMCAPHST_G_HEAT_RATE_N)	Heat Rate (MI_PERF_FUEL_HEAT_RATE_N)
Primary Ash Softening Temp (MI_GMCAPHST_PRI_ASH_SOFTE_TE_N)	Ash Softening Temperature (MI_PERF_FUEL_ASH_SOFT_TEMP_N)
Primary Average Heat Content (MI_GMCAPHST_PRI_AVG_HEAT_C_N)	Average Heat Content (MI_PERF_FUEL_AVER_HEAT_CONT_N)
Primary Fuel BTUs - Contract (MI_GMCAPHST_PRI_FUEL_BTUS_CO_N)	Fuel BTUs - Contract (MI_PERF_FUEL_BTUS_CONT_N)
Primary Fuel BTUs - Electrical Generation (MI_GMCAPHST_PRI_FUEL_BTUS_EL_N)	Fuel BTUs - Electrical Generation (MI_PERF_FUEL_BTUS_ELEC_GEN_N)
Primary Fuel BTUs - Plant Heat and Cooling (MI_GMCAPHST_PRI_FUEL_BTUS_HC_N)	Fuel BTUs - Plant Heat and Cooling (MI_PERF_FUEL_BTUS_PL_HEAT_CL_N)
Primary Fuel BTUs - Process Steam (MI_GMCAPHST_PRI_FUEL_BTUS_PS_N)	Fuel BTUs - Process Steam (MI_PERF_FUEL_BTUS_PROC_STEA_N)
Primary Fuel BTUs Total (MI_GMCAPHST_PRI_FUEL_BTUS_N)	Fuel BTUs - Total (MI_PERF_FUEL_BTUS_TOTA_N)

Fields in V3.6.0.0.0	Fields in V4.3.0.0.0
Primary Fuel Code (MI_GMCAPHST_PRI_FUEL_CODE_C)	Fuel Code (MI_PERF_FUEL_FUEL_CODE_C)
Primary Grindability Index (MI_GMCAPHST_PRI_GRIND_INDEX_N)	Grindability Index (MI_PERF_FUEL_GRIN_INDE_NBR)
Primary Percent Alkalines (MI_GMCAPHST_PRI_PERCE_ALKAL_N)	Percent Alkalines (MI_PERF_FUEL_PERC_ALKA_N)
Primary Percent Ash (MI_GMCAPHST_PRI_PERCE_ASH_N)	Percent Ash (MI_PERF_FUEL_PERC_ASH_N)
Primary Percent Moisture (MI_GMCAPHST_PRI_PERCE_MOIST_N)	Percent Moisture (MI_PERF_FUEL_PERC_MOIS_N)
Primary Percent Sulfur (MI_GMCAPHST_PRI_PERCE_SULFU_N)	Percent Sulfur (MI_PERF_FUEL_PERC_SULF_N)
Primary Quantity Burned (MI_GMCAPHST_PRI_QUANT_BURNE_N)	Quantity Burned (MI_PERF_FUEL_QUAN_BURN_N)
Primary Quantity Burned Unit of Measure (MI_GMCAPHST_PRIM_BURN_UOM_C)	Quantity Burned Unit of Measure (MI_PERF_FUEL_QTY_BRN_UNITMES_C)
Secondary Ash Softening Temp (MI_GMCAPHST_SEC_ASH_SOFTE_TE_N)	Ash Softening Temperature (MI_PERF_FUEL_ASH_SOFT_TEMP_N)
Secondary Average Heat Content (MI_GMCAPHST_SEC_AVG_HEAT_N)	Average Heat Content (MI_PERF_FUEL_AVER_HEAT_CONT_N)
Secondary Fuel Code (MI_GMCAPHST_SEC_FUEL_CODE_C)	Fuel Code (MI_PERF_FUEL_FUEL_CODE_C)
Secondary Grindability Index (MI_GMCAPHST_SEC_GRIND_INDEX_N)	Grindability Index (MI_PERF_FUEL_GRIN_INDE_NBR)
Secondary Percent Alkalines (MI_GMCAPHST_SEC_PERCE_ALKAL_N)	Percent Alkalines (MI_PERF_FUEL_PERC_ALKA_N)
Secondary Percent Ash (MI_GMCAPHST_SEC_PERCE_ASH_N)	Percent Ash (MI_PERF_FUEL_PERC_ASH_N)
Secondary Percent Moisture (MI_GMCAPHST_SEC_PERCE_MOIST_N)	Percent Moisture (MI_PERF_FUEL_PERC_MOIS_N)
Secondary Percent Sulfur (MI_GMCAPHST_SEC_PERCE_SULFU_N)	Percent Sulfur (MI_PERF_FUEL_PERC_SULF_N)
Secondary Quantity Burned (MI_GMCAPHST_SEC_QUANT_BURNE_N)	Quantity Burned (MI_PERF_FUEL_QUAN_BURN_N)
Secondary Quantity Burned Unit of Measure (MI_GMCAPHST_SECND_BURN_UOM_C)	Quantity Burned Unit of Measure (MI_PERF_FUEL_QTY_BRN_UNITMES_C)
Sum of Fuel BTUs (MI_GMCAPHST_SUM_OF_FUEL_BTUS_N)	Sum of Fuel BTUs (MI_PERF_FUEL_SUM_OF_BTUS_N)
Capacity History (Net)	GAA Performance Indexes
Capacity Factor (N) (MI_GMCAPHST_N_CAPAC_FAC_N)	Capacity Factor (MI_PERF_INDX_CAPA_FACT_N)

Fields in V3.6.0.0.0	Fields in V4.3.0.0.0
D1 Eqv Upl Derate Hrs (N) (MI_GMCAPHST_D1_HRS_N)	D1 Equivalent Unplanned Derate Hours (MI_PERF_INDX_D1_EQ_UPL_DR_HR_N)
D1 Eqv Upl Derate MWh (N) (MI_GMCAPHST_D1_EQV_UPL_DRT_N)	D1 Equivalent Unplanned Derate MWH (MI_PERF_INDX_D1_EQ_UPL_DR_MW_N)
D2 Eqv Upl Derate Hrs (N) (MI_GMCAPHST_D2_HRS_N)	D2 Equivalent Unplanned Derate Hours (MI_PERF_INDX_D2_EQ_UPL_DR_HR_N)
D2 Eqv Upl Derate MWh (N) (MI_GMCAPHST_D2_EQV_UPL_DRT_N)	D2 Equivalent Unplanned Derate MWH (MI_PERF_INDX_D2_EQ_UPL_DR_MW_N)
D3 Eqv Upl Derate Hrs (N) (MI_GMCAPHST_D3_HRS_N)	D3 Equivalent Unplanned Derate Hours (MI_PERF_INDX_D3_EQ_UPL_DR_HR_N)
D3 Eqv Upl Derate MWh (N) (MI_GMCAPHST_D3_EQV_UPL_DRT_C)	D3 Equivalent Unplanned Derate MWH (MI_PERF_INDX_D3_EQ_UPL_DR_MW_N)
D4 Eqv Maint Derate Hrs (N) (MI_GMCAPHST_MNT_DRT_HRS_D4_N)	D4 Equivalent Maintenance Derating Hours (MI_PERF_INDX_D4_EQ_MN_DR_HRS_N)
D4 Eqv Maint Derate MWh (N) (MI_GMCAPHST_D4_EQV_MNT_DRT_N)	D4 Equivalent Maintenance Derate MWH (MI_PERF_INDX_D4_EQ_MN_DR_MW_N)
Eqv Avail Factor (N) (MI_GMCAPHST_EQV_AVAIL_FAC_NE_N)	Equivalent Availability Factor (MI_PERF_INDX_EQ_AVAI_FACT_N)
Eqv Derate Ext (N) (MI_GMCAPHST_EQV_DRT_EXT_N_N)	Equivalent Derate Extension (MI_PERF_INDX_EQ_DR_EXT_N)
Eqv Forced Derate Hrs (N) (MI_GMCAPHST_FORCE_DRT_HRS_D1_N)	Equivalent Forced Derated Hours (MI_PERF_INDX_EQ_FORC_DR_HRS_N)
Eqv Forced Outage Factor (N) (MI_GMCAPHST_EQV_FRC_OU_FAC_N_N)	Equivalent Forced Outage Factor (MI_PERF_INDX_EQ_FORC_OUT_FAC_N)
Eqv Forced Outage Rate (N) (MI_GMCAPHST_EQV_FRC_OUT_RA_N_N)	Equivalent Forced Outage Rate (MI_PERF_INDX_EQ_FOR_OUT_RATE_N)
Eqv Forced Outage Rate Dmd (N) (MI_GMCAPHST_EQV_FRC_ORT_DE_N_N)	Equivalent Forced Outage Rate Demand (MI_PERF_INDX_EQ_FOR_OT_RTDEM_N)
Eqv Maint Derate Hrs (N) (MI_GMCAPHST_EMDH_N_N)	Equivalent Maintenance Derated Hours (MI_PERF_INDX_EQ_MN_DR_HRS_N)
Eqv Maint Derate Hrs RS (N) (MI_GMCAPHST_EMDHRS_HRS_N_N)	Equivalent Maintenance Derated Hours During Reserve Shutdown (MI_PERF_INDX_EQ_MN_DR_HR_RS_N)
Eqv Maint Outage Factor (N) (MI_GMCAPHST_EQV_MN_OU_FAC_N_N)	Equivalent Maintenance Outage Factor (MI_PERF_INDX_EQ_MN_OUT_FAC_N)
Eqv Maintenance Outage Rate (N) (MI_GMCAPHST_EQV_MN_OU_RA_N_N)	Equivalent Maintenance Outage Rate (MI_PERF_INDX_EQ_MN_OUT_RAT_N)
Eqv Planned Derate Hrs (N) (MI_GMCAPHST_PL_DRT_HRS_PD_N)	Equivalent Planned Derated Hours (MI_PERF_INDX_EQ_PLN_DR_HRS_N)
Eqv Planned Derate Hrs RS (N) (MI_GMCAPHST_EPDHRS_HRS_N_N)	Equivalent Planned Derated Hours During Reserve Shutdown (MI_PERF_INDX_EQ_PL_DR_HR_RS_N)

Fields in V3.6.0.0.0	Fields in V4.3.0.0.0
Eqv Planned Derate MWh (N) (MI_GMCAPHST_PD_EQV_PL_DRT_M_N)	Equivalent Planned Derate MWH (MI_PERF_INDX_EQ_PLN_DR_MWH_N)
Eqv Planned Outage Factor (N) (MI_GMCAPHST_EQV_PL_OU_FAC_N_N)	Equivalent Planned Outage Factor (MI_PERF_INDX_EQ_PLN_OUT_FAC_N)
Eqv Planned Outage Rate (N) (MI_GMCAPHST_EQV_PLAN_OU_RA_N_N)	Equivalent Planned Outage Rate (MI_PERF_INDX_EQ_PLN_OUT_RATE_N)
Eqv Sched Derate Hrs (N) (MI_GMCAPHST_ESDH_N_N)	Equivalent Scheduled Derated Hours (MI_PERF_INDX_EQ_SCH_DR_HRS_N)
Eqv Sched Outage Factor (N) (MI_GMCAPHST_EQV_SCH_OU_FAC_N_N)	Equivalent Scheduled Outage Factor (MI_PERF_INDX_EQ_SCH_OUT_FAC_N)
Eqv Sched Outage Factor (N) (MI_GMCAPHST_EQV_SEA_DRT_HO_N_N)	Equivalent Seasonal Derated Hours (MI_PERF_INDX_EQ_SEAS_DR_HRS_N)
Eqv Seasonal Derate MWh (N) (MI_GMCAPHST_EQV_SEA_DRT_MW_N_N)	Equivalent Seasonal Derate MWH (MI_PERF_INDX_EQ_SEAS_DR_MWH_N)
Eqv Unavail Factor (N) (MI_GMCAPHST_EQV_UNAV_FAC_NE_N)	Equivalent Unavailability Factor (MI_PERF_INDX_EQ_UNAV_FAC_N)
Eqv Unplanned Outage Rate (N) (MI_GMCAPHST_EQV_UNPL_OU_RA_N_N)	Equivalent Unplanned Outage Rate (MI_PERF_INDX_EQ_UNPL_OUT_RAT_N)
Eqv Upl Derate Hrs (N) (MI_GMCAPHST_EUDH_N)	Equivalent Unplanned Derated Hours (MI_PERF_INDX_EQ_UNPL_DR_HRS_N)
Eqv Upl Derate Hrs RS (N) (MI_GMCAPHST_EUDHRS_HRS_N_N)	Equivalent Unplanned Derated Hours During Reserve Shutdown (MI_PERF_INDX_EQ_UNPL_DR_HR_S_N)
Eqv Upl Frcd Derate Hrs RS (N) (MI_GMCAPHST_EUFDH_HRS_N_N)	Equivalent Unplanned Forced Derate Hours (MI_PERF_INDX_EQ_UPLFRC_DR_HR_N)
Eqv Upl Frcd Derate MWh RS (N) (MI_GMCAPHST_EUFDH_MWH_N_N)	Equivalent Unplanned Forced Derate MWH (MI_PERF_INDX_EQ_UPLFRC_DR_MW_N)
Eqv Uplanned Outage Factor (N) (MI_GMCAPHST_EQV_UPL_OU_FAC_N_N)	Equivalent Unplanned Outage Factor (MI_PERF_INDX_EQ_UNPL_OUT_FAC_N)
Ext Maint Derate Eqv Hrs (N) (MI_GMCAPHST_EXT_MNT_DRTEQVHR_N)	Extension of Maintenance Derating Equivalent Hours (MI_PERF_INDX_EXT_MN_DR_EQ_HR_N)
Ext Maint Derate Eqv MWh (N) (MI_GMCAPHST_EXT_OF_MNT_D_MW_N)	Extended Maintenance Derate Equivalent MWH (MI_PERF_INDX_EXT_MN_DR_EQ_MW_N)
Ext Pln Derate Eqv Hrs (N) (MI_GMCAPHST_EXT_PL_DRT_EQV_H_N)	Extension of Planned Derating Equivalent Hours (MI_PERF_INDX_EXT_PL_DR_EQ_HR_N)
Ext Pln Derate Eqv MWh (N) (MI_GMCAPHST_EXT_PL_DRT_EQU_N)	Extended Planned Derate Equivalent MWH (MI_PERF_INDX_EXT_PL_DR_EQ_MW_N)
Forced Outage MWh (N) (MI_GMCAPHST_FORCE_OUT_MWH_N)	Forced Outage MWH (MI_PERF_INDX_FORC_OUT_MWH_N)
Maint Outage MWh (N) (MI_GMCAPHST_MNT_OUT_MWH_N)	Maintenance Outage MWH (MI_PERF_INDX_MAIN_OUT_MWH_N)

Fields in V3.6.0.0.0	Fields in V4.3.0.0.0
Maint Outage Sched Ext MWh (N) (MI_GMCAPHST_MNT_OUT_SCHD_EXT_N)	Maintenance Outage Scheduled Extension MWH (MI_PERF_INDX_MN_OT_SCHEXT_MW_N)
Maint and Ext Outage MWh (N) (MI_GMCAPHST_MNT_EXT_OUTMWH_N)	Maintenance and Extension Outage MWH (MI_PERF_INDX_MN_ND_EXT_OT_MW_N)
NonCurtailing Event MWh (N) (MI_GMCAPHST_NC_NONCU_EVT_MWH_N)	Non Curtailing Event MWH (MI_PERF_INDX_NON_CURT_EVT_MW_N)
Output Factor (N) (MI_GMCAPHST_N_OUTPU_FAC_N)	Output Factor (N) (MI_GAA_PERF_OUTPUT_FACT_NET_N)
Planned Outage MWh (N) (MI_GMCAPHST_PL_OUT_MWH_N)	Planned Outage MWH (MI_PERF_INDX_PLN_OUT_MW_N)
Planned and Ext Outage MWh (N) (MI_GMCAPHST_PL_EXT_OUTMWH_N)	Planned and Extension Outage MWH (MI_PERF_INDX_PLN_EXT_OT_MW_N)
Pln Outage Sched Ext MWh (N) (MI_GMCAPHST_PLN_OUT_SCHD_EXT_N)	Planned Outage Scheduled Extension MWH (MI_PERF_INDX_PL_OT_SC_EXT_MW_N)
Reserve Shutdown MWh (N) (MI_GMCAPHST_RESER_SHUTD_MWH_N)	Reserve Shutdown MWH (MI_PERF_INDX_RSRV_SHUT_MW_N)
Seasonal Derate Factor (N) (MI_GMCAPHST_SEA_DRT_FAC_NE_N)	Seasonal Derating Factor (MI_PERF_INDX_SEAS_DR_FAC_N)
Startup Failure MWh (N) (MI_GMCAPHST_SF_STRT_FAIL_MWH_N)	Startup Failure MWH (MI_PERF_INDX_STAR_FAIL_MW_N)
Total Eqv Derate Hrs (N) (MI_GMCAPHST_TOTAL_DRT_HRS_N)	Total Equivalent Derate Hours (MI_PERF_INDX_TOTA_EQ_DR_HR_N)
Total Eqv Derate MWh (N) (MI_GMCAPHST_TOTAL_EQV_DRT_MW_N)	Total Equivalent Derate MWH (MI_PERF_INDX_TOTA_EQ_DR_MW_N)
U1 Unplanned Outage MWh (N) (MI_GMCAPHST_U1_UPL_OUT_MWH_N)	U1 Unplanned Outage MWH (MI_PERF_INDX_U1_UNPL_OUT_MW_N)
U2 Unplanned Outage MWh (N) (MI_GMCAPHST_U2_UPL_OUT_MWH_N)	U2 Unplanned Outage MWH (MI_PERF_INDX_U2_UNPL_OUT_MW_N)
U3 Unplanned Outage MWh (N) (MI_GMCAPHST_U3_UPL_OUT_MWH_N)	U3 Unplanned Outage MWH (MI_PERF_INDX_U3_UNPL_OUT_MW_N)
Unit Derating Factor (N) (MI_GMCAPHST_UNIT_DRT_FAC_NE_N)	Unit Derating Factor (MI_PERF_INDX_UNIT_DR_FAC_N)
Weightage Type	Weightage Type (MI_PERF_INDX_WEIG_TYPE_C)
Performance Summary Key	Performance Summary Key (MI_PERF_INDX_PERF_SUMM_KEY_N)
Capacity History (Gross)	GAA Performance Indexes
Capacity Factor (G) (MI_GMCAPHST_G_CAPAC_FAC_N)	Capacity Factor (MI_PERF_INDX_CAPA_FACT_N)
D1 Eqv Upl Derate Hrs (G) (MI_GMCAPHST_D1_EQV_UPL_G_DRT_N)	D1 Equivalent Unplanned Derate Hours (MI_PERF_INDX_D1_EQ_UPL_DR_HR_N)

Fields in V3.6.0.0.0	Fields in V4.3.0.0.0
D1 Eqv Upl Derate MWh (G) (MI_GMCAPHST_D1_EQV_UPL_DRTG_N)	D1 Equivalent Unplanned Derate MWH (MI_PERF_INDX_D1_EQ_UPL_DR_MW_N)
D2 Eqv Upl Derate Hrs (G) (MI_GMCAPHST_D2_EQV_UPL_G_DRT_N)	D2 Equivalent Unplanned Derate Hours (MI_PERF_INDX_D2_EQ_UPL_DR_HR_N)
D2 Eqv Upl Derate MWh (G) (MI_GMCAPHST_D2_EQV_UPL_DRTG_N)	D2 Equivalent Unplanned Derate MWH (MI_PERF_INDX_D2_EQ_UPL_DR_MW_N)
D3 Eqv Upl Derate Hrs (G) (MI_GMCAPHST_D3_EQV_UPL_G_DRT_N)	D3 Equivalent Unplanned Derate Hours (MI_PERF_INDX_D3_EQ_UPL_DR_HR_N)
D3 Eqv Upl Derate MWh (G) (MI_GMCAPHST_D3_EQV_UPL_DRTG_N)	D3 Equivalent Unplanned Derate MWH (MI_PERF_INDX_D3_EQ_UPL_DR_MW_N)
D4 Eqv Maint Derate Hrs (G) (MI_GMCAPHST_D4_EQV_MNT_G_DRT_N)	D4 Equivalent Maintenance Derating Hours (MI_PERF_INDX_D4_EQ_MN_DR_HRS_N)
D4 Eqv Maint Derate MWh (G) (MI_GMCAPHST_D4_EQV_MNT_DRTG_N)	D4 Equivalent Maintenance Derate MWH (MI_PERF_INDX_D4_EQ_MN_DR_MW_N)
Eqv Avail Factor (G) (MI_GMCAPHST_EQV_AVAIL_FAC_N)	Equivalent Availability Factor (MI_PERF_INDX_EQ_AVAI_FACT_N)
Eqv Derate Ext (G) (MI_GMCAPHST_EQV_DRT_EXT_G_N)	Equivalent Derate Extension (MI_PERF_INDX_EQ_DR_EXT_N)
Eqv Forced Derate Hrs (G) (MI_GMCAPHST_FRC_DRT_HRS_D1_G_N)	Equivalent Forced Derated Hours (MI_PERF_INDX_EQ_FORC_DR_HRS_N)
Eqv Forced Outage Factor (G) (MI_GMCAPHST_EQV_FRC_OU_FAC_G_N)	Equivalent Forced Outage Factor (MI_PERF_INDX_EQ_FORC_OUT_FAC_N)
Eqv Forced Outage Rate (G) (MI_GMCAPHST_EQV_FORCE_OUT_N)	Equivalent Forced Outage Rate (MI_PERF_INDX_EQ_FOR_OUT_RATE_N)
Eqv Forced Outage Rate Dmd (G) (MI_GMCAPHST_EQV_FRC_ORT_DE_G_N)	Equivalent Forced Outage Rate Demand (MI_PERF_INDX_EQ_FOR_OT_RTDEM_N)
Eqv Maint Derate Hrs (G) (MI_GMCAPHST_EMDH_G_N)	Equivalent Maintenance Derated Hours (MI_PERF_INDX_EQ_MN_DR_HRS_N)
Eqv Maint Outage Factor (G) (MI_GMCAPHST_EQV_MN_OU_FAC_G_N)	Equivalent Maintenance Outage Factor (MI_PERF_INDX_EQ_MN_OUT_FAC_N)
Eqv Maintenance Outage Rate (G) (MI_GMCAPHST_EQV_MN_OU_RA_G_N)	Equivalent Maintenance Outage Rate (MI_PERF_INDX_EQ_MN_OUT_RAT_N)
Eqv Planned Derate Hrs (G) (MI_GMCAPHST_PD_EQV_PL_G_DRT_N)	Equivalent Planned Derated Hours (MI_PERF_INDX_EQ_PLN_DR_HRS_N)
Eqv Planned Derate Hrs RS (G) (MI_GMCAPHST_EPDHRS_HRS_G_N)	Equivalent Planned Derated Hours During Reserve Shutdown (MI_PERF_INDX_EQ_PL_DR_HR_RS_N)
Eqv Planned Derate MWh (G) (MI_GMCAPHST_PD_EQV_PL_DRT_MG_N)	Equivalent Planned Derate MWH (MI_PERF_INDX_EQ_PLN_DR_MWH_N)
Eqv Planned Outage Factor (G) (MI_GMCAPHST_EQV_PL_OU_FAC_G_N)	Equivalent Planned Outage Factor (MI_PERF_INDX_EQ_PLN_OUT_FAC_N)

Fields in V3.6.0.0.0	Fields in V4.3.0.0.0
Eqv Planned Outage Rate (G) (MI_GMCAPHST_EQV_PLAN_OU_RA_G_N)	Equivalent Planned Outage Rate (MI_PERF_INDX_EQ_PLN_OUT_RATE_N)
Eqv Sched Derate Hrs (G) (MI_GMCAPHST_ESDH_G_N)	Equivalent Scheduled Derated Hours (MI_PERF_INDX_EQ_SCH_DR_HRS_N)
Eqv Sched Outage Factor (G) (MI_GMCAPHST_EQV_SCH_OU_FAC_G_N)	Equivalent Scheduled Outage Factor (MI_PERF_INDX_EQ_SCH_OUT_FAC_N)
Eqv Sched Outage Factor (G) (MI_GMCAPHST_EQV_SCH_OU_FAC_G_N)	Equivalent Seasonal Derated Hours (MI_PERF_INDX_EQ_SEAS_DR_HRS_N)
Eqv Seasonal Derate MWh (G) (MI_GMCAPHST_EQV_SESO_DRT_MW_N)	Equivalent Seasonal Derate MWH (MI_PERF_INDX_EQ_SEAS_DR_MWH_N)
Eqv Unavail Factor (G) (MI_GMCAPHST_EQV_UNAVA_FAC_N)	Equivalent Unavailability Factor (MI_PERF_INDX_EQ_UNAV_FAC_N)
Eqv Unplanned Outage Rate (G) (MI_GMCAPHST_EQV_UNPL_OU_RA_G_N)	Equivalent Unplanned Outage Rate (MI_PERF_INDX_EQ_UNPL_OUT_RAT_N)
Eqv Upl Derate Hrs (G) (MI_GMCAPHST_EUDH_G_N)	Equivalent Unplanned Derated Hours (MI_PERF_INDX_EQ_UNPL_DR_HRS_N)
Eqv Upl Derate Hrs RS (G) (MI_GMCAPHST_EUDHRS_HRS_G_N)	Equivalent Unplanned Derated Hours During Reserve Shutdown (MI_PERF_INDX_EQ_UNPL_DR_HR_S_N)
Eqv Upl Frcd Derate Hrs RS (G) (MI_GMCAPHST_EUFDH_HRS_N)	Equivalent Unplanned Forced Derate Hours (MI_PERF_INDX_EQ_UPLFRC_DR_HR_N)
Eqv Upl Frcd Derate MWh RS (G) (MI_GMCAPHST_EUFDH_MWH_N)	Equivalent Unplanned Forced Derate MWH (MI_PERF_INDX_EQ_UPLFRC_DR_MW_N)
Eqv Uplanned Outage Factor (G) (MI_GMCAPHST_EQV_UPL_OU_FAC_G_N)	Equivalent Unplanned Outage Factor (MI_PERF_INDX_EQ_UNPL_OUT_FAC_N)
Ext Maint Derate Eqv Hrs (G) (MI_GMCAPHST_EXT_MNT_DRT_GEQV_N)	Extension of Maintenance Derating Equivalent Hours (MI_PERF_INDX_EXT_MN_DR_EQ_HR_N)
Ext Maint Derate Eqv MWh (G) (MI_GMCAPHST_EXT_OF_MNT_D_MWG_N)	Extended Maintenance Derate Equivalent MWH (MI_PERF_INDX_EXT_MN_DR_EQ_MW_N)
Ext Pln Derate Eqv Hrs (G) (MI_GMCAPHST_EXT_PL_DRT_G_N)	Extension of Planned Derating Equivalent Hours (MI_PERF_INDX_EXT_PL_DR_EQ_HR_N)
Ext Pln Derate Eqv MWh (G) (MI_GMCAPHST_EXT_PL_DRT_EQUG_N)	Extended Planned Derate Equivalent MWH (MI_PERF_INDX_EXT_PL_DR_EQ_MW_N)
Forced Outage MWh (G) (MI_GMCAPHST_FORCE_OUT_MWHG_N)	Forced Outage MWH (MI_PERF_INDX_FORC_OUT_MWH_N)
Maint Outage MWh (G) (MI_GMCAPHST_MNT_OUT_MWHG_N)	Maintenance Outage MWH (MI_PERF_INDX_MAIN_OUT_MWH_N)
Maint Outage Sched Ext MWh (G) (MI_GMCAPHST_MNT_OUT_SCH_EXTG_N)	Maintenance Outage Scheduled Extension MWH (MI_PERF_INDX_MN_OT_SCHEXT_MW_N)
Maint and Ext Outage MWh (G) (MI_GMCAPHST_MNT_EXT_OUTMWHG_N)	Maintenance and Extension Outage MWH (MI_PERF_INDX_MN_ND_EXT_OT_MW_N)

Fields in V3.6.0.0.0	Fields in V4.3.0.0.0
NonCurtailing Event MWh (G) (MI_GMCAPHST_NC_NC_EVT_MWHG_N)	Non Curtailing Event MWH (MI_PERF_INDX_NON_CURT_EVT_MW_N)
Output Factor (G) (MI_GMCAPHST_G_OUTPU_FAC_N)	Output Factor (G) (MI_GAA_PERF_OUTPUT_FACT_GROS_N)
Planned Outage MWh (G) (MI_GMCAPHST_PL_OUT_MWHG_N)	Planned Outage MWH (MI_PERF_INDX_PLN_OUT_MW_N)
Planned and Ext Outage MWh (G) (MI_GMCAPHST_PL_EXT_OUTMWHG_N)	Planned and Extension Outage MWH (MI_PERF_INDX_PLN_EXT_OT_MW_N)
Pln Outage Sched Ext MWh (G) (MI_GMCAPHST_PLN_OUT_SCH_EXTG_N)	Planned Outage Scheduled Extension MWH (MI_PERF_INDX_PL_OT_SC_EXT_MW_N)
Reserve Shutdown MWh (G) (MI_GMCAPHST_RESER_SHUTD_MWHG_N)	Reserve Shutdown MWH (MI_PERF_INDX_RSRV_SHUT_MW_N)
Seasonal Derate Factor (G) (MI_GMCAPHST_SEA_DRT_FAC_N)	Seasonal Derating Factor (MI_PERF_INDX_SEAS_DR_FAC_N)
Startup Failure MWh (G) (MI_GMCAPHST_SF_STR_FAIL_MWHG_N)	Startup Failure MWH (MI_PERF_INDX_STAR_FAIL_MW_N)
Total Eqv Derate Hrs (G) (MI_GMCAPHST_TOTAL_DRT_HRS_G_N)	Total Equivalent Derate Hours (MI_PERF_INDX_TOTA_EQ_DR_HR_N)
Total Eqv Derate MWh (G) (MI_GMCAPHST_TOT_EQV_DRT_MWG_N)	Total Equivalent Derate MWH (MI_PERF_INDX_TOTA_EQ_DR_MW_N)
U1 Unplanned Outage MWh (G) (MI_GMCAPHST_U1_UPL_OUT_MWHG_N)	U1 Unplanned Outage MWH (MI_PERF_INDX_U1_UNPL_OUT_MW_N)
U2 Unplanned Outage MWh (G) (MI_GMCAPHST_U2_UPL_OUT_MWHG_N)	U2 Unplanned Outage MWH (MI_PERF_INDX_U2_UNPL_OUT_MW_N)
U3 Unplanned Outage MWh (G) (MI_GMCAPHST_U3_UPL_OUT_MWHG_N)	U3 Unplanned Outage MWH (MI_PERF_INDX_U3_UNPL_OUT_MW_N)
Unit Derating Factor (G) (MI_GMCAPHST_UNIT_DRT_FAC_N)	Unit Derating Factor (MI_PERF_INDX_UNIT_DR_FAC_N)
Capacity History	GAA Performance Summary
Actual Unit Starts (MI_GMCAPHST_ACTUA_UNIT_STRT_N)	Actual Unit Starts (MI_GAA_PERF_ACT_UNIT_STAR_N)
Attempted Unit Starts (MI_GMCAPHST_ATTEM_UNIT_STRT_N)	Attempted Unit Starts (MI_GAA_PERF_ATT_UNIT_STAR_N)
Availability Factor (MI_GMCAPHST_AVAIL_FAC_N)	Availability Factor (MI_GAA_PERF_AVAI_FACT_N)
Available Hrs (MI_GMCAPHST_AVAIL_HRS_N)	Available Hours (MI_GAA_PERF_AVAI_HRS_N)
Average Run Time (MI_GMCAPHST_AVER_RUN_TIME_N)	Average Run Time (MI_GAA_PERF_AVG_RUN_TIME_N)
Demonstrated Max Capacity (N) (MI_GMCAPHST_DEMON_N_MAXIM_CP_N)	Demonstrated Max Capacity (MI_GAA_PERF_DEMO_MAX_CAPA_N)

Fields in V3.6.0.0.0	Fields in V4.3.0.0.0
Ext Sched Outages Hrs (MI_GMCAPHST_EXT_OF_SCHED_OUT_N)	Extension of Scheduled Outage Hours (MI_GAA_PERF_EXT_SCH_OUT_HRS_N)
Forced Outage Factor (MI_GMCAPHST_FORCE_OUT_FAC_N)	Forced Outage Factor (MI_GAA_PERF_FORC_OUT_FACT_N)
Forced Outage Hrs (MI_GMCAPHST_FORCE_OUT_HRS_N)	Forced Outage Hours (MI_GAA_PERF_FORC_OUT_HRS_N)
Forced Outage Rate (MI_GMCAPHST_FORCE_OUT_RATE_N_N)	Forced Outage Rate (MI_GAA_PERF_FORC_OUT_RATE_N)
Forced Outage Rate Demand (MI_GMCAPHST_FRC_OUT_RT_DM_N_N)	Forced Outage Rate Demand (MI_GAA_PERF_FORC_OUT_RAT_DEM_N)
GADS Unit Code (MI_GMCAPHST_UNIT_CODE_N)	Primary Unit Code (MI_GAA_PERF_PRIM_UNIT_CODE_N)
GADS Utility Code (MI_GMCAPHST_UTILI_CODE_N)	Primary Utility Code (MI_GAA_PERF_PRIM_UTIL_CODE_N)
Gross Actual Capacity (G) (MI_GMCAPHST_G_ACTUA_CAPAC_N)	Gross Actual Capacity (G) (MI_GAA_PERF_GROSS_ACTU_CAPA_N)
Gross Actual Generation (G) (MI_GMCAPHST_G_ACTUA_GENER_N)	Gross Actual Generation (G) (MI_GAA_PERF_GROSS_ACTU_GENE_N)
Gross Dependable Capacity (G) (MI_GMCAPHST_G_DEPEN_CAPAC_N)	Gross Dependable Capacity (G) (MI_GAA_PERF_GROSS_DEPE_CAPA_N)
Gross Max Capacity (G) (MI_GMCAPHST_G_MAXIM_CAPAC_N)	Gross Maximum Capacity (G) (MI_GAA_PERF_GROSS_MAX_CAPA_N)
Inactive Hours (MI_GMCAPHST_INACT_HRS_N)	Inactive Hours (MI_GAA_PERF_INAC_HRS_N)
MI_SM_STATE_ENTERED_D (MI_SM_STATE_ENTERED_D)	MI_SM_STATE_ENTERED_D (MI_SM_STATE_ENTERED_D)
MI_SM_STATE_ID_C (MI_SM_STATE_ID_C)	MI_SM_STATE_ID_C (MI_SM_STATE_ID_C)
MI_SM_STATE_KEY_N (MI_SM_STATE_KEY_N)	MI_SM_STATE_KEY_N (MI_SM_STATE_KEY_N)
MI_SM_STATE_OWNER_ID_C (MI_SM_STATE_OWNER_ID_C)	MI_SM_STATE_OWNER_ID_C (MI_SM_STATE_OWNER_ID_C)
Maint Outage Basic Hrs (MI_GMCAPHST_MNT_OUT_HRS_N)	Maintenance Outage Hours (MI_GAA_PERF_MAIN_OUT_HRS_N)
Maint Outage Factor (MI_GMCAPHST_MNT_OUT_FAC_N)	Maintenance Outage Factor (MI_GAA_PERF_MNT_OUT_FACT_N)
Maint Outage Sched Ext Hrs (MI_GMCAPHST_MNT_OUT_SCHD_EX_N)	Maintenance Outage Schedule Extension Hours (MI_GAA_PERF_MNTOT_SCHEXT_HR_N)
Maint and Ext Outage Hrs (MI_GMCAPHST_MNT_AND_EXT_OT_N)	Maintenance and Extenstion Outage Hours (MI_GAA_PERF_MNT_ND_EXT_OT_HR_N)
Max Generation (G) (MI_GMCAPHST_MAX_G_GENER_N)	Max Generation (G) (MI_GAA_PERF_MAX_GENE_GROSS_N)
Max Generation (N) (MI_GMCAPHST_MAX_N_GENER_N)	Max Generation (N) (MI_GAA_PERF_MAX_GENE_NET_N)

Fields in V3.6.0.0.0	Fields in V4.3.0.0.0
Mean Forced Outage Duration (MI_GMCAPHST_MN_FORC_OUT_DUR_N)	Mean Forced Outage Duration (MI_GAA_PERF_MEAN_FORC_OT_DUR_N)
Mean Maintenance Outage Duration (MI_GMCAPHST_MN_MAIN_OUT_DUR_N)	Mean Maintenance Outage Duration (MI_GAA_PERF_MEAN_MAIN_OT_DUR_N)
Mean Planned Outage Duration (MI_GMCAPHST_MN_PLAN_OUT_DUR_N)	Mean Planned Outage Duration (MI_GAA_PERF_MEAN_PLAN_OT_DUR_N)
Mean Service Time To Forced Outage (MI_GMCAPHST_MN_SER_TM_FRC_OU_N)	Mean Service Time To Forced Outage (MI_GAA_PERF_MEAN_SER_TIME_OT_N)
Mean Service Time To Maintenance Outage (MI_GMCAPHST_MN_SER_TM_MAI_OU_N)	Mean Service Time To Maintenance Outage (MI_GAA_PERF_MN_SERTIM_MNT_OT_N)
Mean Service Time To Planned Outage (MI_GMCAPHST_MN_SER_TM_PL_OU_N)	Mean Service Time To Planned Outage (MI_GAA_PERF_MN_SERTIM_PLN_OT_N)
Mean Service Time To Unplanned Outage (MI_GMCAPHST_MN_SER_TM_UPL_OU_N)	Mean Service Time To Unplanned Outage (MI_GAA_PERF_MN_SERTM_UNPL_OT_N)
Mean Unplanned Outage Duration (MI_GMCAPHST_MN_UNPL_OUT_DUR_N)	Mean Unplanned Outage Duration (MI_GAA_PERF_MEAN_UNPL_OT_DUR_N)
Net Actual Capacity (N) (MI_GMCAPHST_N_ACTUA_CAPAC_N)	Net Actual Capacity (N) (MI_GAA_PERF_NET_ACTU_CAPA_N)
Net Actual Generation (N) (MI_GMCAPHST_N_ACTUA_GENER_N)	Net Actual Generation (N) (MI_GAA_PERF_NET_ACTU_GENE_N)
Net Dependable Capacity (N) (MI_GMCAPHST_N_DEPEN_CAPAC_N)	Net Dependable Capacity (N) (MI_GAA_PERF_NET_DEPE_CAPA_N)
Net Maximum Capacity (N) (MI_GMCAPHST_N_MAXIM_CAPAC_N)	Net Maximum Capacity (N) (MI_GAA_PERF_NET_MAXI_CAPA_N)
NonCurtailing Event Hrs (MI_GMCAPHST_NONCU_EVT_HRS_NC_N)	Non Curtailing Event Hours (MI_GAA_PERF_NON_CURTEVNT_HRS_N)
Number Of Non Curtailing Events (MI_GMCAPHST_NUM_NC_EVE_N)	Number Of Non Curtailing Events (MI_GAA_PERF_NON_CURTEVNT_CNT_N)
Number of Forced Outages (MI_GMCAPHST_NUM_FRC_OUT_N)	Number of Forced Outages (MI_GAA_PERF_FORC_OUT_CNT_N)
Number of Maintenance Outages (MI_GMCAPHST_NUM_MNT_OUT_N)	Number of Maintenance Outages (MI_GAA_PERF_MAIN_OUT_CNT_N)
Number of Planned Outages (MI_GMCAPHST_NUM_PLN_OUT_N)	Number of Planned Outages (MI_GAA_PERF_PLAN_OUT_CNT_N)
Number of Unplanned Outages (MI_GMCAPHST_NUM_UPL_OUT_N)	Number of Unplanned Outages (MI_GAA_PERF_UNPL_OUT_CNT_N)
Override Reserve Shutdown Hours (MI_GMCAPHST_OV_RSRV_SHTD_HRS_F)	Override Reserve Shutdown Hours (MI_GAA_PERF_RSRVSHUT_HRS_FLG)
Period Hours (MI_GMCAPHST_PERIO_HRS_N)	Period Hours (MI_GAA_PERF_PERIOD_HRS_N)

Fields in V3.6.0.0.0	Fields in V4.3.0.0.0
Planned Outage Basic Hrs (MI_GMCAPHST_PL_OUT_HRS_N)	Planned Outage Hours (MI_GAA_PERF_PLAN_OUT_HRS_N)
Planned Outage Factor (MI_GMCAPHST_PL_OUT_FAC_N)	Planned Outage Factor (MI_GAA_PERF_PLAN_OUT_FACT_N)
Planned and Ext Outage Hrs (MI_GMCAPHST_PL_AND_EXT_OT_N)	Planned and Extension Outage Hours (MI_GAA_PERF_PLN_EXT_OT_HRS_N)
Plant ID (MI_GMCAPHST_PLANT_ID_C)	Plant ID (MI_GAA_PERF_PLANT_ID_C)
Plant Name (MI_GMCAPHST_PLANT_NAME_C)	Plant Name (MI_GAA_PERF_PLANT_NAME_C)
Pln Outage Sched Ext Hrs (MI_GMCAPHST_PL_OUT_SCHD_EX_N)	Planned Outage Schedule Extension Hours (MI_GAA_PERF_PL_OT_SCHEXT_HRS_N)
Pumping Hrs (MI_GMCAPHST_PUMPI_HRS_N)	Pumping Hours (MI_GAA_PERF_PUMPING_HRS_N)
Report Date (MI_GMCAPHST_REPO_DATE_DT)	Report Date (MI_GAA_PERF_REPORT_DATE_DT)
Reporting Date (MI_GMCAPHST_REPOR_DATE_D)	Reporting Date (MI_GAA_PERF_REPORTING_DATE_DT)
Reporting Month (MI_GMCAPHST_REPOR_MONTH_C)	Reporting Month (MI_GAA_PERF_REPORTING_MONT_C)
Reporting Year (MI_GMCAPHST_REPOR_YEAR_C)	Reporting Year (MI_GAA_PERF_REPORTING_YEAR_C)
Reserve Shutdown Hrs (MI_GMCAPHST_RESER_SHUTD_HRS_N)	Reserve Shutdown Hours (MI_GAA_PERF_RESE_SHUT_HRS_N)
Revision (MI_GMCAPHST_REVIS_N)	Revision (MI_GAA_PERF_REVISION_N)
Sched Outage Hrs (MI_GMCAPHST_SCHED_OUTAG_HRS_N)	Scheduled Outage Hours (MI_GAA_PERF_SCH_OUT_HRS_N)
Scheduled Outage Factor (MI_GMCAPHST_SCHED_OUT_FAC_N)	Scheduled Outage Factor (MI_GAA_PERF_SCH_OUT_FACT_N)
Service Factor (MI_GMCAPHST_SERVI_FAC_N)	Service Factor (MI_GAA_PERF_SERV_FACT_N)
Service Hrs (MI_GMCAPHST_SERVI_HRS_N)	Service Hours (MI_GAA_PERF_SERV_HRS_N)
Start Reliability (MI_GMCAPHST_STRT_RELIA_N)	Start Reliability (MI_GAA_PERF_STAR_RELI_N)
Startup Failure Hrs (MI_GMCAPHST_STRT_FAIL_HRS_SF_N)	Startup Failure Hours (MI_GAA_PERF_STAR_FAIL_HRS_N)
Synchronous Condensing Hrs (MI_GMCAPHST_SYNCR_CONDE_HRS_N)	Synchronous Condensing Hours (MI_GAA_PERF_SYNC_COND_HRS_N)
Typical Unit Loading (MI_GMCAPHST_TYPIC_UNIT_LOADI_C)	Typical Unit Loading (MI_GAA_PERF_TYPI_UNIT_LOAD_C)
U1 Unplanned Outage Hrs (MI_GMCAPHST_U1_HRS_N)	U1 Unplanned Outage Hours (MI_GAA_PERF_U1_UNPL_OUT_HRS_N)
U2 Unplanned Outage Hrs (MI_GMCAPHST_U2_HRS_N)	U2 Unplanned Outage Hours (MI_GAA_PERF_U2_UNPL_OUT_HRS_N)
U3 Unplanned Outage Hrs (MI_GMCAPHST_U3_HRS_N)	U3 Unplanned Outage Hours (MI_GAA_PERF_U3_UNPL_OUT_HRS_N)

Fields in V3.6.0.0.0	Fields in V4.3.0.0.0
Unavailability Factor (MI_GMCAPHST_UNAVA_FAC_N)	Unavailability Factor (MI_GAA_PERF_UNAV_FACT_N)
Unavailable Hrs (MI_GMCAPHST_UNAVA_HRS_N)	Unavailable Hours (MI_GAA_PERF_UNAV_HRS_N)
Unit ID (MI_GMCAPHST_UNIT_ID_C)	Unit ID (MI_GAA_PERF_UNIT_ID_C)
Unit Name (MI_GMCAPHST_UNIT_NAME_C)	Unit Name (MI_GAA_PERF_UNIT_NAME_C)
Unit Type (MI_GMCAPHST_NERC_UNIT_TYPE_C)	Unit Type (MI_GAA_PERF_UNIT_TYPE_C)
Unplanned Outage Factor (MI_GMCAPHST_UPL_OUT_FAC_N)	Unplanned Outage Factor (MI_GAA_PERF_UNPL_OUT_FACT_N)
Unplanned Outage Hrs (MI_GMCAPHST_UPL_OUT_HUR_UO_N)	Unplanned Outage Hours (MI_GAA_PERF_UNPL_OUT_HRS_N)
Verbal Description (MI_GMCAPHST_DESCR_C)	Verbal Description (MI_GAA_PERF_VERB_DESC_C)
YTD Actual Unit Starts (MI_GMCAPHST_YTD_CUM_ACT_STRT_N)	YTD Actual Unit Starts (MI_GAA_PERF_YTD_ACTUNIT_STAR_N)
YTD Attempted Unit Starts (MI_GMCAPHST_YTD_CUM_ATT_STRT_N)	YTD Attempted Unit Starts (MI_GAA_PERF_YTD_ATTUNIT_STAR_N)
YTD Start Reliability (MI_GMCAPHST_YTD_STRT_RELIA_N)	YTD Start Reliability (MI_GAA_PERF_YTD_STAR_RELI_N)
Zone (MI_GMCAPHST_ZONE_C)	Zone (MI_GAA_PERF_ZONE_C)

Generation Availability Analysis Wind

Deploy GAA Wind for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Review the GAA Wind data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to one or more of the GAA Wind Security Groups and Roles.	This step is required.
3	Specify additional system code tables for the GAA Wind families.	By default, APM provides a set of system code tables for the GAA Wind families. You can modify these default system code tables or add new system code tables.
4	Configure the GAA Wind Report Configuration records.	This step is required.
5	Using the GAA Wind Asset Hierarchy Data Loader, create the following records in the GAA Wind Asset Hierarchy: • GAA Company • GAA Wind Plant • GAA Wind Group • GAA Wind Sub Group • GAA Wind Unit	This step is required.
6	Using the GAA Wind Sub Group Capacity Data Loader, create the GAA Wind Sub Group Capacity record.	This step is required.

Upgrade or Update GAA Wind to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

Hazards Analysis

Deploy Hazards Analysis for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Define alternate search queries .	This step is required only if you do not want to use the baseline search queries.
2	Manage the types of Deviations in a HAZOP Analysis. To do so, add a code to the MI_HAZOP_DECIATIONS system code table. For more information, refer to the System Codes and Tables section of the documentation.	This step is required only if you want to add another value to the list of default values in the Deviation/ Guideword list in the HAZOP Deviation datasheet.
3	Activate the SIS Management license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
4	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. **Tip:** For more information, refer to the Security Group topic for this module.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

Step	Task	Notes
5	Review the Hazards Analysis data model to determine which relationship definitions you will need to modify to include your custom equipment or location families. Modify any relationship definitions as needed via the Configuration Manager application.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
6	Assign Security Users to one or more of the Hazards Analysis Security Groups and Roles.	This step is required.

Upgrade or Update Hazards Analysis to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

Step	Task	Notes
1	Activate the SIS Management license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. **Tip:** For more information, refer to the Security Group topic for this module.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

Step	Task	Notes
1	Activate the SIS Management license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. **Tip:** For more information, refer to the Security Group topic for this module.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

Step	Task	Notes
1	Activate the SIS Management license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. **Tip:** For more information, refer to the Security Group topic for this module.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

Step	Task	Notes
1	Activate the SIS Management license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. **Tip:** For more information, refer to the Security Group topic for this module.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

Step	Task	Notes
1	Activate the SIS Management license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. **Tip:** For more information, refer to the Security Group topic for this module.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
3	Access the Safeguards and verify the mapping of IPL Checklist records to the existing Safeguards after upgrade.	This step is optional. In V4.3.0.0.0, IPL Checklist records are used to store your selection for the criteria that are used to determine if a Safeguard is an IPL. When you upgrade to V4.3.0.0.0, for each of the previously existing Safeguards, IPL Checklist records are created and associated with the corresponding Safeguard.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	Activate the SIS Management license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. **Tip:** For more information, refer to the Security Group topic for this module.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	Activate the SIS Management license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. **Tip:** For more information, refer to the Security Group topic for this module.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

Step	Task	Notes
1	Activate the SIS Management license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. **Tip:** For more information, refer to the Security Group topic for this module.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

Step	Task	Notes
1	Activate the SIS Management license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. **Tip:** For more information, refer to the Security Group topic for this module.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V3.5.1 through V3.5.1.12.3

Step	Task	Notes
1	Activate the SIS Management license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. **Tip:** For more information, refer to the Security Group topic for this module.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

Step	Task	Notes
1	Activate the SIS Management license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. **Tip:** For more information, refer to the Security Group topic for this module.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Activate the SIS Management license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. **Tip:** For more information, refer to the Security Group topic for this module.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Activate the SIS Management license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. **Tip:** For more information, refer to the Security Group topic for this module.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

Inspection Management

Deploy Inspection Management

The checklists in this section of the documentation contain all the steps necessary for deploying and configuring this module whether you are deploying the module for the first time or upgrading from a previous version.

Deploy Inspection Management for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Review the Inspection Management data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Configure APM to create Task Revision records.	This step is required only if you want Task Revision records to be created every time you create or update a task. These records are used to track historical data related to a task.
3	Assign Security Users to one or more of the Security Roles used in IM.	This step is required. Security Users will need permissions to the Inspection Management families before they can use the Inspection Management features.
4	Assign Resource Roles to users.	This step is required to define the users who can perform Inspection workflows as Inspectors, supervisors, administrators, contract inspectors, and risk analysts in Inspection Management.

5	Modify baseline Application Configuration settings.	This step is required only if you want to modify Application Configurations. The following Application Configurations are defined in the baseline database: Asset Query Path; Associated Relationship Family; Published Query Path; Summary Query Path; Alerts Query Path; Asset Is Successor; Profile Configuration; Method Configuration; Strategy Rule Configuration.
6	Define the Inspection Profile for each piece of equipment that you will inspect.	This step is required only if you plan to create Inspection records in baseline families other than the Checklists subfamilies.
7	Modify the baseline Asset query.	This step is required only if you want Inspection records to be linked to records in a family other than the Equipment family.
8	Define Event Configurations for any new Inspection families that you have created.	This step is required only if you have created custom Inspection families that you want to use within Inspection Management.
9	for custom inspections.	This step is optional.
10	Define Taxonomy Configurations for Inspection Families and Checklist Configurations.	This step is required only if you want to link Inspection Families and Checklist Configurations to assets using equipment taxonomy.
11	Assign certifications to users.	This step is optional.
12	Group inspection work into Work Packs.	This step is optional.

Upgrade or Update Inspection Management to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Note: If you are using Inspection Field Data Collection for Offline Inspections, please follow the upgrade steps to install the latest app on mobile devices used for Inspection Field Data Collection.

After you upgrade:

A new Human Resource role, Contract Inspector (ID: CONTRACT INSPECTOR) is now available in MI_RESOURCE_ROLE system code table. This is to facilitate the enhancement where a Contract Inspector can now update the Status field in Inspection records to Pending Approval without being the user defined in the Inspection Report Owner field if they are also a Team Member in the associated Inspection record.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

Step	Task	Notes
1	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset with Inspection Grouping` ◦ `Public\Meridium\Modules\Inspection\Work Pack Queries\All Inspections in a Work Pack` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit and Below` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\My Open Inspections` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Open Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections (Including Team Members)` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections`	This step is required only if you have modified the following queries: ◦ All Inspections for Asset. ◦ All Inspections for Asset with Inspection Grouping. ◦ All Inspections in a Work Pack. ◦ All Inspections for Unit ◦ All Inspections for Unit and Below ◦ My Open Inspections ◦ Open Inspections for Unit ◦ Users Open Inspections (Including Team Members) ◦ Users Open Inspections

Step	Task	Notes
2	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Report Queries\Checklist Report Query`	This step is required only if you want to use the baseline Checklist Inspection Report/ Blank Checklist Inspection Report and modified the following query: ◦ Checklist Report Query **Note:** Inspection ID details are added in the Checklist Report Query to display the Inspection ID in the baseline Checklist Inspection Report.

- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

Step	Task	Notes
1	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset with Inspection Grouping` ◦ `Public\Meridium\Modules\Inspection\Work Pack Queries\All Inspections in a Work Pack` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit and Below` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\My Open Inspections` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Open Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections (Including Team Members)` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections`	This step is required only if you have modified the following queries: ◦ All Inspections for Asset. ◦ All Inspections for Asset with Inspection Grouping. ◦ All Inspections in a Work Pack. ◦ All Inspections for Unit ◦ All Inspections for Unit and Below ◦ My Open Inspections ◦ Open Inspections for Unit ◦ Users Open Inspections (Including Team Members) ◦ Users Open Inspections

Step	Task	Notes
2	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Report Queries\Checklist Report Query`	This step is required only if you want to use the baseline Checklist Inspection Report/ Blank Checklist Inspection Report and modified the following query: ◦ Checklist Report Query **Note:** Inspection ID details are added in the Checklist Report Query to display the Inspection ID in the baseline Checklist Inspection Report.

- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

Step	Task	Notes
1	Revert the following Inspection Management queries to baseline: ◦ `Public/Meridium/Modules/Inspection/Overview Queries/All Inspection Assets with Inspection Or Task for Unit` ◦ `Public/Meridium/Modules/Inspection/Overview Queries/All Inspections for Asset` ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/Active Recommendations of Plan for Unit` ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/All Inspection Plans for Unit` ◦ `Public/Meridium/Modules/Inspection/Compliance/Queries/Assets with Inspection Plans` ◦ `Public/Meridium/Modules/Inspection/Report Queries/MI_INSPHIST_ASSETDTL`	This step is required only if you have modified the following queries: ◦ All Inspection Assets with Inspection Or Task for Unit ◦ All Inspections for Asset ◦ Active Recommendations of Plan for Unit ◦ All Inspection Plans for Unit ◦ Assets with Inspection Plans ◦ MI_INSPHIST_ASSETDTL

Step	Task	Notes
2	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset with Inspection Grouping` ◦ `Public\Meridium\Modules\Inspection\Work Pack Queries\All Inspections in a Work Pack` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit and Below` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\My Open Inspections` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Open Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections (Including Team Members)` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections`	This step is required only if you have modified the following queries: ◦ All Inspections for Asset. ◦ All Inspections for Asset with Inspection Grouping. ◦ All Inspections in a Work Pack. ◦ All Inspections for Unit ◦ All Inspections for Unit and Below ◦ My Open Inspections ◦ Open Inspections for Unit ◦ Users Open Inspections (Including Team Members) ◦ Users Open Inspections

Step	Task	Notes
3	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Report Queries\Checklist Report Query`	This step is required only if you want to use the baseline Checklist Inspection Report/ Blank Checklist Inspection Report and modified the following query: ◦ Checklist Report Query **Note:** Inspection ID details are added in the Checklist Report Query to display the Inspection ID in the baseline Checklist Inspection Report.

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

Step	Task	Notes
1	Update the approval work process of Inspection Recommendations to use the new state management.	A new state configuration has been developed for the Inspection Recommendation approval work process. This state configuration includes some new states and the existing states are updated. This step is required only if: ◦ You are using customized state configuration for the approval workflow and want to use the new state configuration. ◦ You have a customized state configuration for the approval workflow, but using the recommendation status for the approval workflow, and want to use the new state configuration. In both the cases, you must run the Revert to Baseline utility to map the existing states to the new states.
2	Add WHERE criteria to the following queries to accommodate date filters: ◦ The Underlying Inspection Tasks query: ◦ Public\Meridium\Modules\Inspection\Overview Queries\All Tasks for Unit ◦ The Underlying Recommendations query: ◦ Public\Meridium\Modules\Inspection\Overview Queries\Open Inspection Recommendations for Unit ◦ The Overdue Inspection Recommendations query: ◦ Public\Meridium\Modules\Inspection\Overview Queries\Overdue Inspection Recommendations for Unit	This step is required only if you have previously modified the queries. You can add the WHERE criteria by following the instructions in KBA 000044807. If you have not modified your queries, you do not need to follow this step. This step will be completed automatically when you upgrade the components in the basic APM system architecture.

Step	Task	Notes
3	Update the datasheets for Inspection families supported in Inspection Field Data Collection: ◦ Full Inspection ◦ General Inspection ◦ API 510 External Checklist ◦ API 510 Internal Checklist ◦ API 510 Internal Exchanger Checklist ◦ API 570 External Checklist ◦ API 653 External Checklist ◦ API 653 Internal Checklist ◦ External PRD Checklist ◦ PRD Pop Test Checklist ◦ Checklist Inspection Template	If you have customized the default datasheet for any of these families and want to see the download data for Inspection Field Data Collection, you must do one of the following: ◦ Using Family Management, edit the default datasheet of each family. Add a new section, Download Information with the following fields: ◦ Downloaded ◦ Last Downloaded By ◦ Last Downloaded Date ◦ Last Synced Back By ◦ Last Synced Date ◦ Run Revert to Baseline for each family.

Step	Task	Notes
4	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset with Inspection Grouping` ◦ `Public\Meridium\Modules\Inspection\Work Pack Queries\All Inspections in a Work Pack` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit and Below` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\My Open Inspections` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Open Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections (Including Team Members)` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections`	This step is required only if you have modified the following queries: ◦ All Inspections for Asset. ◦ All Inspections for Asset with Inspection Grouping. ◦ All Inspections in a Work Pack. ◦ All Inspections for Unit ◦ All Inspections for Unit and Below ◦ My Open Inspections ◦ Open Inspections for Unit ◦ Users Open Inspections (Including Team Members) ◦ Users Open Inspections

Step	Task	Notes
5	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Report Queries\Checklist Report Query`	This step is required only if you want to use the baseline Checklist Inspection Report/ Blank Checklist Inspection Report and modified the following query: ◦ Checklist Report Query **Note:** Inspection ID details are added in the Checklist Report Query to display the Inspection ID in the baseline Checklist Inspection Report.

- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

Step	Task	Notes
1	Revert the My Open Inspections Query to baseline.	This step is required only if you have modified the My Open Inspections query. If you have, you will not have the ability to download inspections from the **My Open Inspections** section of the **Inspections** page until you revert the My Open Inspections query to baseline for the offline functionality to be enabled. **Note:** If you want to modify this query, you must have both the Inspection Lock and the Entity Key fields as selected fields in the customized query.

Step	Task	Notes
2	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset with Inspection Grouping` ◦ `Public\Meridium\Modules\Inspection\Work Pack Queries\All Inspections in a Work Pack` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit and Below` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\My Open Inspections` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Open Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections (Including Team Members)` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections`	This step is required only if you have modified the following queries: ◦ All Inspections for Asset. ◦ All Inspections for Asset with Inspection Grouping. ◦ All Inspections in a Work Pack. ◦ All Inspections for Unit ◦ All Inspections for Unit and Below ◦ My Open Inspections ◦ Open Inspections for Unit ◦ Users Open Inspections (Including Team Members) ◦ Users Open Inspections

Step	Task	Notes
3	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Report Queries\Checklist Report Query`	This step is required only if you want to use the baseline Checklist Inspection Report/ Blank Checklist Inspection Report and modified the following query: ◦ Checklist Report Query **Note:** Inspection ID details are added in the Checklist Report Query to display the Inspection ID in the baseline Checklist Inspection Report.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium \Modules\Inspection \Overview Queries \All Inspections for Asset` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \All Inspections for Asset with Inspection Grouping` ◦ `Public\Meridium \Modules\Inspection \Work Pack Queries \All Inspections in a Work Pack` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \All Inspections for Unit` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \All Inspections for Unit and Below` ◦ `Public\Meridium \Modules\Inspection \Overview Queries\My Open Inspections` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \Open Inspections for Unit` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \Users Open Inspections (Including Team Members)` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \Users Open Inspections`	This step is required only if you have modified the following queries: ◦ All Inspections for Asset. ◦ All Inspections for Asset with Inspection Grouping. ◦ All Inspections in a Work Pack. ◦ All Inspections for Unit ◦ All Inspections for Unit and Below ◦ My Open Inspections ◦ Open Inspections for Unit ◦ Users Open Inspections (Including Team Members) ◦ Users Open Inspections

Step	Task	Notes
2	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Report Queries\Checklist Report Query`	This step is required only if you want to use the baseline Checklist Inspection Report/ Blank Checklist Inspection Report and modified the following query: ◦ Checklist Report Query **Note:** Inspection ID details are added in the Checklist Report Query to display the Inspection ID in the baseline Checklist Inspection Report.

- Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset with Inspection Grouping` ◦ `Public\Meridium\Modules\Inspection\Work Pack Queries\All Inspections in a Work Pack` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit and Below` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\My Open Inspections` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Open Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections (Including Team Members)` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections`	This step is required only if you have modified the following queries: ◦ All Inspections for Asset. ◦ All Inspections for Asset with Inspection Grouping. ◦ All Inspections in a Work Pack. ◦ All Inspections for Unit ◦ All Inspections for Unit and Below ◦ My Open Inspections ◦ Open Inspections for Unit ◦ Users Open Inspections (Including Team Members) ◦ Users Open Inspections

Step	Task	Notes
2	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Report Queries\Checklist Report Query`	This step is required only if you want to use the baseline Checklist Inspection Report/ Blank Checklist Inspection Report and modified the following query: ◦ Checklist Report Query **Note:** Inspection ID details are added in the Checklist Report Query to display the Inspection ID in the baseline Checklist Inspection Report.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

Step	Task	Notes
1	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset with Inspection Grouping` ◦ `Public\Meridium\Modules\Inspection\Work Pack Queries\All Inspections in a Work Pack` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit and Below` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\My Open Inspections` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Open Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections (Including Team Members)` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections`	This step is required only if you have modified the following queries: ◦ All Inspections for Asset. ◦ All Inspections for Asset with Inspection Grouping. ◦ All Inspections in a Work Pack. ◦ All Inspections for Unit ◦ All Inspections for Unit and Below ◦ My Open Inspections ◦ Open Inspections for Unit ◦ Users Open Inspections (Including Team Members) ◦ Users Open Inspections

Step	Task	Notes
2	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Report Queries\Checklist Report Query`	This step is required only if you want to use the baseline Checklist Inspection Report/ Blank Checklist Inspection Report and modified the following query: ◦ Checklist Report Query **Note:** Inspection ID details are added in the Checklist Report Query to display the Inspection ID in the baseline Checklist Inspection Report.

- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

Step	Task	Notes
1	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset with Inspection Grouping` ◦ `Public\Meridium\Modules\Inspection\Work Pack Queries\All Inspections in a Work Pack` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit and Below` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\My Open Inspections` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Open Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections (Including Team Members)` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections`	This step is required only if you have modified the following queries: ◦ All Inspections for Asset. ◦ All Inspections for Asset with Inspection Grouping. ◦ All Inspections in a Work Pack. ◦ All Inspections for Unit ◦ All Inspections for Unit and Below ◦ My Open Inspections ◦ Open Inspections for Unit ◦ Users Open Inspections (Including Team Members) ◦ Users Open Inspections

Step	Task	Notes
2	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Report Queries\Checklist Report Query`	This step is required only if you want to use the baseline Checklist Inspection Report/ Blank Checklist Inspection Report and modified the following query: ◦ Checklist Report Query **Note:** Inspection ID details are added in the Checklist Report Query to display the Inspection ID in the baseline Checklist Inspection Report.

- Upgrade from any version V3.5.1 through V3.5.1.12.3

Step	Task	Notes
1	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset with Inspection Grouping` ◦ `Public\Meridium\Modules\Inspection\Work Pack Queries\All Inspections in a Work Pack` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit and Below` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\My Open Inspections` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Open Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections (Including Team Members)` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections`	This step is required only if you have modified the following queries: ◦ All Inspections for Asset. ◦ All Inspections for Asset with Inspection Grouping. ◦ All Inspections in a Work Pack. ◦ All Inspections for Unit ◦ All Inspections for Unit and Below ◦ My Open Inspections ◦ Open Inspections for Unit ◦ Users Open Inspections (Including Team Members) ◦ Users Open Inspections

Step	Task	Notes
2	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Report Queries\Checklist Report Query`	This step is required only if you want to use the baseline Checklist Inspection Report/ Blank Checklist Inspection Report and modified the following query: ◦ Checklist Report Query **Note:** Inspection ID details are added in the Checklist Report Query to display the Inspection ID in the baseline Checklist Inspection Report.

- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

Step	Task	Notes
1	Define Time-Based Inspection settings.	This step is optional.
2	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium \Modules\Inspection \Overview Queries \All Inspections for Asset` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \All Inspections for Asset with Inspection Grouping` ◦ `Public\Meridium \Modules\Inspection \Work Pack Queries \All Inspections in a Work Pack` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \All Inspections for Unit` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \All Inspections for Unit and Below` ◦ `Public\Meridium \Modules\Inspection \Overview Queries\My Open Inspections` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \Open Inspections for Unit` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \Users Open Inspections (Including Team Members)` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \Users Open Inspections`	This step is required only if you have modified the following queries: ◦ All Inspections for Asset. ◦ All Inspections for Asset with Inspection Grouping. ◦ All Inspections in a Work Pack. ◦ All Inspections for Unit ◦ All Inspections for Unit and Below ◦ My Open Inspections ◦ Open Inspections for Unit ◦ Users Open Inspections (Including Team Members) ◦ Users Open Inspections

Step	Task	Notes
3	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Report Queries\Checklist Report Query`	This step is required only if you want to use the baseline Checklist Inspection Report/ Blank Checklist Inspection Report and modified the following query: ◦ Checklist Report Query **Note:** Inspection ID details are added in the Checklist Report Query to display the Inspection ID in the baseline Checklist Inspection Report.

- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Define Time-Based Inspection settings.	This step is optional.
2	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium \Modules\Inspection \Overview Queries \All Inspections for Asset` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \All Inspections for Asset with Inspection Grouping` ◦ `Public\Meridium \Modules\Inspection \Work Pack Queries \All Inspections in a Work Pack` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \All Inspections for Unit` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \All Inspections for Unit and Below` ◦ `Public\Meridium \Modules\Inspection \Overview Queries\My Open Inspections` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \Open Inspections for Unit` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \Users Open Inspections (Including Team Members)` ◦ `Public\Meridium \Modules\Inspection \Overview Queries \Users Open Inspections`	This step is required only if you have modified the following queries: ◦ All Inspections for Asset. ◦ All Inspections for Asset with Inspection Grouping. ◦ All Inspections in a Work Pack. ◦ All Inspections for Unit ◦ All Inspections for Unit and Below ◦ My Open Inspections ◦ Open Inspections for Unit ◦ Users Open Inspections (Including Team Members) ◦ Users Open Inspections

Step	Task	Notes
3	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Report Queries\Checklist Report Query`	This step is required only if you want to use the baseline Checklist Inspection Report/ Blank Checklist Inspection Report and modified the following query: ◦ Checklist Report Query **Note:** Inspection ID details are added in the Checklist Report Query to display the Inspection ID in the baseline Checklist Inspection Report.

- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Create Task Types records representing those task types, and then set the value in the Reference field to Inspection.	This step is required only if you have added System Codes to the MI_INSPECTION_TYPE System Code table.
2	Define Time-Based Inspection settings.	This step is optional.

Step	Task	Notes
3	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Asset with Inspection Grouping` ◦ `Public\Meridium\Modules\Inspection\Work Pack Queries\All Inspections in a Work Pack` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\All Inspections for Unit and Below` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\My Open Inspections` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Open Inspections for Unit` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections (Including Team Members)` ◦ `Public\Meridium\Modules\Inspection\Overview Queries\Users Open Inspections`	This step is required only if you have modified the following queries: ◦ All Inspections for Asset. ◦ All Inspections for Asset with Inspection Grouping. ◦ All Inspections in a Work Pack. ◦ All Inspections for Unit ◦ All Inspections for Unit and Below ◦ My Open Inspections ◦ Open Inspections for Unit ◦ Users Open Inspections (Including Team Members) ◦ Users Open Inspections

Step	Task	Notes
4	Revert the following Inspection Management queries to baseline: ◦ `Public\Meridium\Modules\Inspection\Report Queries\Checklist Report Query`	This step is required only if you want to use the baseline Checklist Inspection Report/ Blank Checklist Inspection Report and modified the following query: ◦ Checklist Report Query **Note:** Inspection ID details are added in the Checklist Report Query to display the Inspection ID in the baseline Checklist Inspection Report.

Revert Inspection Management Queries to Baseline

This action is required only if you have modified certain Inspection Management queries.

About This Task

If you have modified the following Inspection Management queries, perform the steps to revert these queries to baseline.

- All Inspection Assets with Inspection Or Task for Unit
- All Inspections for Asset
- Active Recommendations of Plan for Unit
- All Inspection Plans for Unit
- Assets with Inspection Plans
- MI_INSPHIST_ASSETDTL

Procedure

1. Access the Catalog page.
2. Navigate to the Public folder for the query that you want to revert.
   The queries that you want to revert are stored in the following sub-folders within the `Public/Meridium/Modules/Inspection/` folder.
   - `Overview Queries`
   - `Compliance/Queries`
   - `Report Queries`
3. Select the check box next to the query that you want to revert, and then select  .
   The **Confirm Delete** window appears, asking you to confirm if you want to delete the selected query.
4. Select **OK**.
   The selected query is deleted.
5. Navigate to the Baseline folder for queries.
   The baseline queries for the queries that you want to revert are stored in the following sub-folders within the `Baseline/Meridium/Modules/Inspection/` folder.
   - `Overview Queries`
   - `Compliance/Queries`
   - `Report Queries`

6. Select the check box next to the query that you want to revert, and then select  .
   The **Catalog Folder Browser** window appears.
7. Navigate to the folder containing the public query that you deleted in step 3.
8. Select **OK**.
   A success message appears indicating that the selected Item has been copied successfully.
9. Repeat Steps 2-8 for each query that you want to revert to baseline.

Inspection Datasheets - Revert to Baseline

About This Task

The default datasheets on Inspection families supported for Inspection Field Data Collection have been updated to include fields to track download information:

Family	Family ID	Datasheet Updated (Default)
Full Inspection	MI_INSPFULL	Full Visual Inspection
General Inspection	MI_INSP_GEN	General Inspection - Default
API 510 External Checklist	MI_API510EXT_CHECK	API 510 External Checklist - Default
API 510 Internal Checklist	MI_API510INT_CHECK	API 510 Internal Checklist - Default
API 510 Internal Exchanger Checklist	MI_API510IEX_CHECK	API 510 Internal Exchanger Checklist - Default
API 570 External Checklist	MI_API570EXT_CHECK	API 570 External Checklist - Default
API 653 External Checklist	MI_API653EXT_CHECK	API 653 External Checklist – Default
API 653 Internal Checklist	MI_API653INT_CHECK	API 653 Internal Checklist - Default
External PRD Checklist	MI_EXTNL_PRD_CHECK	External PRD Checklist
PRD Pop Test Checklist	MI_PRD_PT_CHECK	PRD Pop Test Checklist
Checklist Inspection Template	MI_GEN_INSP_TMP	Checklist Inspection Template

If you have customized the default datasheet for any of these families and want to see the download data for Inspection Field Data Collection must do one of the following:

- Using Family Management, edit the default datasheet of each family. Add a new section, Download Information with the following fields:
  - Downloaded
  - Last Downloaded By
  - Last Downloaded Date
  - Last Synced Back By
  - Last Synced Date
- Run Revert to Baseline for each family.

Important: Running this utility overwrites your current datasheet and replaces it with the baseline version. You must be a super user in APM to run the Revert to Baseline utility.

Procedure

1. Log in to the server where APM is installed.
2. Navigate to `<Installation Directory>\Meridium\Upgrade\DBUpgrade`.
3. Run the `RevertToBaselineApp.exe` file as administrator.
   The **Revert To Baseline Login** window appears.
4. In the **Meridium Data Source** box, enter the data source name that you want to access.
5. Enter your login credentials, and then select **Next**.
   The available families that can be reverted to baseline appear.
6. Select the Inspection family that you want to update, and then select **Revert to Baseline**.
   The **Various Options For Revert** window appears.
7. Select **Datasheets**.
   Select the Default Datasheet from the drop-down, and then select **Ok**.
8. Repeat steps 6-7 for each Inspection Family.

Inspection Recommendation State Management - Revert to Baseline

About This Task

The Inspection Recommendation state management is now available with a new state configuration for the approval workflow. This state configuration allows Inspection Recommendation approval workflow to use the State field, instead of the Status field. For more information about the new state configuration, refer to the topic. If you are using a customized state configuration for the approval workflow and want to use the functionality of the new state management without impacting the current approval workflow, you must map the existing states to the new states using the Revert to Baseline utility. You can run this utility in any of the following conditions:

- You are using customized state configuration for the approval workflow and want to use the new state configuration.
- You have a customized state configuration for the approval workflow, but using the recommendation status for the approval workflow, and want to use the new state configuration.

Important: Running this utility overwrites your current state configuration. After you transition to the new state configuration, you cannot revert to the old state configuration.

Before You Begin

- You must be a super user in APM.
- The State Configuration for Inspection Recommendation must be enabled.

Procedure

1. Log in to the server where APM is installed.
2. Navigate to `<Installation Directory>\Meridium\Upgrade\DBUpgrade`.
3. Run the `RevertToBaselineApp.exe` file as administrator.
   The **Revert To Baseline Login** window appears.
4. In the **Meridium Data Source** box, enter the data source name that you want to access.
5. Enter your login credentials, and then select **Next**.
   The available families that can be reverted to baseline appear.

6. Select the Inspection Recommendation family, and then select **Revert to Baseline**.
   The **Various Options For Revert** window appears.
7. Select **State Management**, and then select **Ok**.
   The **State Management Mapper** window appears.
8. In the **Entity Families** pane, select **Inspection Recommendation**.
   The State Management Baseline Mapping table appears and contains the following columns:
   - Custom Source: Contains all the existing states that are available for mapping to the new states.
   - Select Target: Allows you to select the new states that you want to map to the existing states.
   - Baseline Target: Displays the newly mapped states corresponding to the existing states.
9. Using the **Select Target** column, select the state that you want to map to the existing state.

   Note: You can use the **Auto Map** button to automatically map the existing states to the new states based on the state name.
10. Repeat step 9 for all the existing states.
11. Select **Save Mapping**.
12. Browse for the path where you want to save the mapping file, and then select **Save**.
    A .xml file containing the state mappings is saved.
13. Select **Revert Single Family**.
14. Select the state mapping file that you saved in step 12, and then select **OK**.
    The mapping operation starts. After the operation is successfully completed, a success message appears.
15. Select **Exit**.
    The Revert to Baseline utility is closed.

Configure APM to Create Task Revisions

About This Task

You can configure APM to create records that track changes to Task record values, so that you can keep a historical record of Task data on a given date and time. Throughout this documentation, GE Vernova refers to these revision-tracking records as Task Revision records. The family caption, however, is not necessarily Task Revision.

APM provides the following Task Revision families, but you can create your own:

- Task Revision
- Inspection Task Revision

GE Vernova assumes that you do not want a Task Revision record to be created when you create a new Task record or update an existing Task record. If, however, you want these Task Revision records to be created, you will need to perform the following step.

Procedure

Configure the Has Task Revision relationship to include the Task family as the predecessor and its Task Revision subfamily as the successor.

Results

When you create or modify a task, a Task Revision is created and linked to the task.

About Configuring the Has Task Revision Relationship

The Has Task Revision relationship family is used to link Task Revisions to Tasks. If a relationship definition exists between a Task family and its Task Revision subfamily, when you create a Task record in that family, the APM system will automatically create a Task Revision and link it to the Task. The Task Revision serves as a historical record of the Task data on a given date and time. If you later update the Task, a new Task Revision will be created.

GE Vernova assumes that you do not want a Task Revision to be created when you create a new Task or update an existing Task. If, however, you do want these Task Revisions to be created, you will need to configure the Has Task Revision relationship to include the required families. No relationship definitions are configured for this family in the baseline APM database.

The following table provides an example of a relationship definition that you might configure for the Has Task Revision relationship if you are using the root Task family.

Predecessor	Successor	Cardinality
Task	Task Revision	One to Many

Inspection Task Revision

GE Vernova assumes that you do not want an Inspection Task Revision to be created when you create a new Inspection Task or update an existing Inspection Task. If, however, you do want these Inspection Task Revisions to be created, you will need to configure the Has Task Revision relationship to include the required families. No relationship definitions are configured for this family in the baseline Inspection Management product.

The following table provides an example of a relationship definition that you might configure for the Has Task Revision relationship if you are using the Inspection Task family.

Predecessor	Successor	Cardinality
Inspection Task	Inspection Task Revision	One to Many

Inspection Management Security Groups and Roles

The following table lists the baseline Security Groups available for users within this module, as well as the baseline Roles to which those Security Groups are assigned.

Important: Assigning a Security User to a Role grants that user the privileges associated with all of the Security Groups that are assigned to that Role. To avoid granting a Security User unintended privileges, before assigning a Security User to a Role, be sure to review all of the privileges associated with the Security Groups assigned to that Role. Also, be aware that additional Roles, as well as Security Groups assigned to existing Roles, can be added via Security Manager.

Security Group	Roles
MI Inspection	MI Mechanical Integrity Administrator MI Mechanical Integrity Power MI Mechanical Integrity User
MI Inspection Viewer	MI APM Viewer MI Mechanical Integrity Viewer
MI Compliance Analyst	
MI Compliance Administrator	
MI Inspection Plan Approver	

Note:

The groups MI Compliance Analyst, MI Compliance Administrator, and MI Inspection Plan Approver are in general provided as a baseline content. These groups must be used only when you implement the KBA 000041664.

The following roles can be assigned to a group or user:

- Inspector
- Inspection Supervisor
- SC Recommendations Implementer
- SC Recommendations Reviewer

These roles are used in State Management.

Family	MI Inspection	MI Inspection Viewer
Entity Families		
Alert	View, Insert, Update, Delete	View
Certification	View, Insert, Update, Delete	View
Checklist Finding	View, Insert, Update, Delete	View
Conditional Alerts	View, Insert, Update, Delete	View
Corrosion	View, Insert, Update, Delete	View
Equipment	View, Insert, Update, Delete	View
Event	View, Insert, Update, Delete	View
Finding	View, Insert, Update, Delete	View
Human Resource	View	View
Inspection Method	View, Insert, Update, Delete	View
Inspection Profile	View, Insert, Update, Delete	View
Inspection Team Member	View, Insert, Update, Delete	View
Inventory Group Configuration	View	View
Potential Degradation Mechanisms	View	View
RBI Degradation Mechanisms	View	View
RBI Inspection Auto-Selection Criteria	View	View
Recommendation	View, Insert, Update, Delete	View

Family	MI Inspection	MI Inspection Viewer
Reference Document	View, Insert, Update, Delete	View
Resource Role	View, Insert, Update, Delete	View
SAP System	View	View
Security User	View	View
Strategy	View, Update	View
Task	View, Insert, Update, Delete	View
Taxonomy References	View	View
Time Based Inspection Interval	View, Insert, Update, Delete	View
Time Based Inspection Setting	View, Insert, Update, Delete	View
Work Pack	View, Insert, Update, Delete	View
Relationship Families		
Belongs to a Unit	View, Update, Insert, Delete	View
Checklist Has Finding	View, Insert, Update, Delete	View
Has Certifications	View, Insert, Update, Delete	View
Has Degradation Mechanisms	View	View
Has Findings	View, Insert, Update, Delete	View
Has Inspection Method	View, Insert, Update, Delete	View
Has Inspection Profile	View, Insert, Update, Delete	View
Has Inspection Scope	View, Insert, Update, Delete	View
Has Inspections	View, Insert, Update, Delete	View
Has Potential Degradation Mechanisms	View	View
Has Recommendations	View, Insert, Update, Delete	View
Has Reference Documents	View, Insert, Update, Delete	View
Has Roles	View, Insert, Update, Delete	View
Has Sub-Inspections	View, Insert, Update, Delete	View
Has Tasks	View, Insert, Update, Delete	View
Has Task History	View, Insert	View
Has Task Revision	View, Insert	View
Has Team Member	View, Insert, Update, Delete	View
Has Taxonomy Hierarchy Element	View	View
Has Taxonomy Mapping	View	View
Has Time Based Inspection Interval	View, Insert, Update, Delete	View
Has Work Pack	View, Update, Insert, Delete	View
Is a User	View	View
Is Planned By	View, Insert, Update, Delete	View
Is Executed By	View, Insert, Update, Delete	View

Note: Security privileges for all modules and catalog folders can be found in the APM documentation.

Note that:

- The family-level privileges granted to the following families are also spread to all of their subfamilies:
  - Event
  - Taxonomy References
- The Has Task History relationship family is inactive in the baseline APM database.
- In addition to the families listed in the preceding table, members of the MI Inspection Security Group have View privileges to additional families to facilitate integration with the Risk Based Inspection module. Since these families are not used elsewhere in Inspection Management, they are not listed in this table.

Note: As part of implementing Inspection Management, you will decide whether you want to link Inspection records to Equipment records, Functional Location records, or both. If you want to link Inspection records to Functional Location records, you will need to grant members of the MI Inspection Security Group at least View privileges to the Functional Location family and the Functional Location Has Equipment relationship family. All new users are automatically assigned to the Everyone user group.

Layers of Protection Analysis

Deploy LOPA for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Modify existing or create additional Initiating Events.	This step is required only if you want to modify or create additional initiating event types that appear in the Initiating Event Type field, on the LOPA datasheet. **Note:** Initiating Event records also populate the CCPS Cause Type field on the Hazards Analysis Cause datasheet. Therefore, any modifications to these records will also reflect on the Hazards Analysis Cause datasheet.
2	Modify existing or create additional Consequence Adjustment Probabilities.	This step is required only if you want to modify or create additional conditional modifier types that appear in the Modifier Type field, on the Consequence Modifier datasheet.
3	Modify existing or create additional Active IPLs.	This step is required only if you want to modify or create additional active IPL types that appear in the IPL Sub Type field, on the Hazards Analysis Safeguard datasheet.
4	Modify existing or create additional Passive IPLs.	This step is required only if you want to modify or create additional passive IPL types that appear in the IPL Sub Type field, on the Hazards Analysis Safeguard datasheet.

Step	Task	Notes
5	Modify existing or create additional Human IPLs.	This step is required only if you want to modify or create additional human IPL types that appear in the IPL Sub Type field, on the Hazards Analysis Safeguard datasheet.
6	Modify the Safety Integrity Level record.	The Safety Integrity Level records contain the standard boundary values for the required probability of failure for each SIL. This step is required only if you want to modify the default boundary values for the required probability of failure for a Safety Integrity Level.
7	Review the LOPA data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
8	Assign Security Users to one or more of the LOPA Security Groups and Roles.	This step is required.

Upgrade or Update LOPA to V4.6.11.0.0

About This Task

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.

Life Cycle Cost Analysis

Deploy LCC for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Assign Security Users to one or more of the Life Cycle Cost Analysis (LCC) Security Groups and Roles.	This step is required.

Upgrade or Update LCC to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

LCC Security Groups

The following table lists the baseline Security Groups available for users within this module, as well as the baseline Roles to which those Security Groups are assigned.

Important: Assigning a Security User to a Role grants that user the privileges associated with all of the Security Groups that are assigned to that Role. To avoid granting a Security User unintended privileges, before assigning a Security User to a Role, be sure to review all of the privileges associated with the Security Groups assigned to that Role. Also, be aware that additional Roles, as well as Security Groups assigned to existing Roles, can be added via Security Manager.

Security Group	Roles
MI LCC Administrator	MI APM Viewer MI Strategy User MI Strategy Power MI Strategy Admin
MI LCC User	MI Strategy User MI Strategy Power
MI LCC Viewer	MI APM Viewer

The baseline family-level privileges that exist for these Security Groups are summarized in the following table.

Family	LCC Administrator	LCC User	LCC Viewer
Entity Families			
LCC Analysis	View, Update, Insert, Delete	View, Update, Insert, Delete	View
LCC Cost	View, Update, Insert, Delete	View, Update, Insert, Delete	View
LCC Cost Value	View, Update, Insert, Delete	View, Update, Insert, Delete	View
LCC Element	View, Update, Insert, Delete	View, Update, Insert, Delete	View
LCC Operating Profile	View, Update, Insert, Delete	View, Update, Insert, Delete	View
LCC Period	View, Update, Insert, Delete	View, Update, Insert, Delete	View
LCC Resource	View, Update, Insert, Delete	View, Update, Insert, Delete	View
LCC Scenario	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	LCC Administrator	LCC User	LCC Viewer
Relationship Families			
Has Associated LCC Element	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has LCC Member	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has LCC Cost	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has LCC Cost Value	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has LCC Element	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has LCC Operating Profile	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has LCC Period	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has LCC Scenario	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Management of Change

Deploy MoC for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Review the MOC data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to one or more of the MOC Security Groups and Roles.	This step is required.
3	In the Configuration Manager, configure the *Change Project Has Elements* relation family to include the desired families in APM as Successors to the MI MOC Change Project family.	This step is required only if you want to associate a Change Project with records from families other than Hazards Analysis, SIL Analysis, and LOPA.
4	Modify the MI_MOC_ANS_OPT System Code Table.	This step is required only if you want to add or modify the values that appear in the Answer field when you create a Question or modify Answer Options in a Question.
5	Modify the MI_Change_Project_Type System Code Table.	This step is required only if you want to add or modify the values that appear in the Change Type field, on the MI MOC Change Project datasheet.

Upgrade or Update MoC to V4.6.11.0.0

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

Metrics and Scorecards

Deploy Metrics and Scorecards for the First Time

About This Task

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Deploy SQL Server Analysis Services 2014 or SQL Server Analysis Services 2016. Ensure that the SQL Server Analysis Services machine meets the system requirements. Deploying SQL Server Analysis Services on the SQL Server Analysis Server machine includes the following steps: 1. Install SQL Server Analysis Services. 2. Deploy the Work History Analysis Services database. This Work History cube is a replacement for the *Equipment and Functional Location Work History* cubes in the Meridium_Event_Analysis database. 3. Create a Windows User on the Analysis Server or in your organization's Active Directory. The user name requires minimum privileges and will only be used by the APM Server to connect to the cubes. It is recommended that: • The password for this user should never expire. • The user should be restricted to change password. • The user should be restricted to log in to others servers (e.g., meridium_ssas_user). 4. Add the user created in Step 3 to a role on all SQL Analysis Services databases you want to access in APM software. The role should have read and drill through permissions. The Work History database already has a *View role* defined, you should add the user to this role. For more information, consult the MSDN documentation regarding Roles and Permissions for Analysis Services. 5. Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication. HTTPS is recommended with basic authentication. For more information, consult the MSDN	This step is required. This step assumes that you have read the Metrics and Scorecards hardware and software requirements and that you have obtained the SQL Server Analysis Services software installer.

Step	Task	Notes
2	Verify that your event and asset criticality data meet the standard classification requirements, and modify the Event or Asset Criticality Data for the Work History cube as needed.	This step is required.
3	Localize the event and asset criticality values in the application.	This step is optional.
4	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.
5	Assign Security Users to one or more of the Metrics and Scorecards Security Groups and Roles.	This step is required.
6	Create Analysis Services Cube records for each cube that has been defined in SQL Server Analysis Services. Since APM uses HTTP connection to connect to the cube, in addition to server address, you need to provide credentials of the user created in Step 1 Task 3.	This step is required.
7	Grant Security Users and Groups access rights to Analysis Services Cube records .	This step is required.
8	Configure privileges for KPI.	This step is required.
9	Configure privileges for Scorecards.	This step is required.
10	Configure a cube for usage metrics tracking on the SQL Server Analysis Server.	This step is required only if you use Metrics and Scorecards to view the usage metrics in a cube.

Upgrade or Update Metrics and Scorecards to V4.6.11.0.0

About This Task

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

Step	Task	Notes
1	Deploy the new Work History cube.	**Important:** Before deploying the new Work History cube, ensure that: ◦ The Security User who will run the Analysis Services Deployment Wizard has been granted View permissions to the cubes associated with the Metric Views. ◦ The cubes are active. This step is required, and the baseline work history cube must be redeployed. The baseline Work History cube was modified such that even if the event or equipment data do not meet the standard classification defined for the Work History cube, with minor modifications to the event and asset criticality data used by the cube, the cube will work with the non-standard event and equipment data.
2	If you have modified a cube that belongs to a previous version, you must manually make the same modifications to the current Work History cube.	This step is required only if you have modified a Work History cube that belongs to a previous version. If you have made modifications to the Work History cube, then you must manually make those updates again.
3	Verify that your event and asset criticality data meet the standard classification requirements, and modify the event or asset criticality data for the Work History cube as needed.	This step is required. If you are an existing user who uses the work history cube, you can map the event or asset criticality data available in your database to the standard event or asset criticality data defined for the work history cube using one of the following procedures: ◦ Modifying the corresponding views for the work history cube in the APM database. ◦ Modifying records available for the corresponding event or asset criticality data family by constructing and executing an update query.
4	Localize the event and equipment values in APM .	This step is required only if you want to localize the event and equipment values in the Work History cube.
5	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.

- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

Step	Task	Notes
1	Deploy the new Work History cube.	**Important:** Before deploying the new Work History cube, ensure that: ◦ The Security User who will run the Analysis Services Deployment Wizard has been granted View permissions to the cubes associated with the Metric Views. ◦ The cubes are active. This step is required, and the baseline work history cube must be redeployed. The baseline Work History cube was modified such that even if the event or equipment data do not meet the standard classification defined for the Work History cube, with minor modifications to the event and asset criticality data used by the cube, the cube will work with the non-standard event and equipment data.
2	If you have modified a cube that belongs to a previous version, you must manually make the same modifications to the current Work History cube.	This step is required only if you have modified a Work History cube that belongs to a previous version. If you have made modifications to the Work History cube, then you must manually make those updates again.
3	Verify that your event and asset criticality data meet the standard classification requirements, and modify the event or asset criticality data for the Work History cube as needed.	This step is required. If you are an existing user who uses the work history cube, you can map the event or asset criticality data available in your database to the standard event or asset criticality data defined for the work history cube using one of the following procedures: ◦ Modifying the corresponding views for the work history cube in the APM database. ◦ Modifying records available for the corresponding event or asset criticality data family by constructing and executing an update query.
4	Localize the event and equipment values in APM .	This step is required only if you want to localize the event and equipment values in the Work History cube.
5	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.

- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

Step	Task	Notes
1	Deploy the new Work History cube.	**Important:** Before deploying the new Work History cube, ensure that: ◦ The Security User who will run the Analysis Services Deployment Wizard has been granted View permissions to the cubes associated with the Metric Views. ◦ The cubes are active. This step is required, and the baseline work history cube must be redeployed. The baseline Work History cube was modified such that even if the event or equipment data do not meet the standard classification defined for the Work History cube, with minor modifications to the event and asset criticality data used by the cube, the cube will work with the non-standard event and equipment data.
2	If you have modified a cube that belongs to a previous version, you must manually make the same modifications to the current Work History cube.	This step is required only if you have modified a Work History cube that belongs to a previous version. If you have made modifications to the Work History cube, then you must manually make those updates again.
3	Verify that your event and asset criticality data meet the standard classification requirements, and modify the event or asset criticality data for the Work History cube as needed.	This step is required. If you are an existing user who uses the work history cube, you can map the event or asset criticality data available in your database to the standard event or asset criticality data defined for the work history cube using one of the following procedures: ◦ Modifying the corresponding views for the work history cube in the APM database. ◦ Modifying records available for the corresponding event or asset criticality data family by constructing and executing an update query.
4	Localize the event and equipment values in APM .	This step is required only if you want to localize the event and equipment values in the Work History cube.
5	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

Step	Task	Notes
1	Deploy the new Work History cube.	**Important:** Before deploying the new Work History cube, ensure that: ◦ The Security User who will run the Analysis Services Deployment Wizard has been granted View permissions to the cubes associated with the Metric Views. ◦ The cubes are active. This step is required, and the baseline work history cube must be redeployed. The baseline Work History cube was modified such that even if the event or equipment data do not meet the standard classification defined for the Work History cube, with minor modifications to the event and asset criticality data used by the cube, the cube will work with the non-standard event and equipment data.
2	If you have modified a cube that belongs to a previous version, you must manually make the same modifications to the current Work History cube.	This step is required only if you have modified a Work History cube that belongs to a previous version. If you have made modifications to the Work History cube, then you must manually make those updates again.
3	Verify that your event and asset criticality data meet the standard classification requirements, and modify the event or asset criticality data for the Work History cube as needed.	This step is required. If you are an existing user who uses the work history cube, you can map the event or asset criticality data available in your database to the standard event or asset criticality data defined for the work history cube using one of the following procedures: ◦ Modifying the corresponding views for the work history cube in the APM database. ◦ Modifying records available for the corresponding event or asset criticality data family by constructing and executing an update query.
4	Localize the event and equipment values in APM .	This step is required only if you want to localize the event and equipment values in the Work History cube.
5	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.

- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

Step	Task	Notes
1	Deploy the new Work History cube.	**Important:** Before deploying the new Work History cube, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted View permissions to the cubes associated with the Metric Views, and that the cubes are active. This step is required, and the baseline work history cube must be redeployed. The baseline Work History cube was modified such that even if the event or equipment data do not meet the standard classification defined for the Work History cube, with minor modifications to the event and asset criticality data used by the cube, the cube will work with the non-standard event and equipment data.
2	If you have made modifications in the previous version of the cube, then you must manually make the same modifications to the current Work History cube.	This step is required only if you had made any modifications to the previously provided Work History cube. If you had made any modifications to the Work History cube, then you must manually make those updates again.
3	Verify that your event and asset criticality data meet the standard classification requirements, and modify the event or asset criticality data for the Work History cube as needed.	This step is required.
4	Localize the event and equipment values in APM .	This step is required only if you want to localize the event and equipment values in the Work History cube.
5	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	Deploy the new Work History cube.	**Important:** Before deploying the new Work History cube, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted View permissions to the cubes associated with the Metric Views, and that the cubes are active. This step is required, and the baseline work history cube must be redeployed. The baseline Work History cube was modified such that even if the event or equipment data do not meet the standard classification defined for the Work History cube, with minor modifications to the event and asset criticality data used by the cube, the cube will work with the non-standard event and equipment data.
2	If you have made modifications in the previous version of the cube, then you must manually make the same modifications to the current Work History cube.	This step is required only if you had made any modifications to the previously provided Work History cube. If you had made any modifications to the Work History cube, then you must manually make those updates again.
3	Verify that your event and asset criticality data meet the standard classification requirements, and modify the event or asset criticality data for the Work History cube as needed.	This step is required.
4	Localize the event and equipment values in APM .	This step is required only if you want to localize the event and equipment values in the Work History cube.
5	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.

- Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	Deploy the new Work History cube.	**Important:** Before deploying the new Work History cube, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted View permissions to the cubes associated with the Metric Views, and that the cubes are active. This step is required, and the baseline work history cube must be redeployed. The baseline Work History cube was modified such that even if the event or equipment data do not meet the standard classification defined for the Work History cube, with minor modifications to the event and asset criticality data used by the cube, the cube will work with the non-standard event and equipment data.
2	If you have made modifications in the previous version of the cube, then you must manually make the same modifications to the current Work History cube.	This step is required only if you had made any modifications to the previously provided Work History cube. If you had made any modifications to the Work History cube, then you must manually make those updates again.
3	Verify that your event and asset criticality data meet the standard classification requirements, and modify the event or asset criticality data for the Work History cube as needed.	This step is required.
4	Localize the event and equipment values in APM .	This step is required only if you want to localize the event and equipment values in the Work History cube.
5	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

Step	Task	Notes
1	Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: ◦ 2014 ◦ 2016	This step is required only if you were previously using SQL Server Analysis Services 2008 R2.
2	Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication.	This step is required.

Step	Task	Notes
3	Deploy Work History Analysis Services database. This Work History cube is a replacement for the Equipment and Functional Location Work History cubes in the Meridium_Event_Analysis database.	**Important:** Before executing this step, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted View permissions to the cubes associated with the Metric Views, and that the cubes are active. This step is required.
4	Create a Windows User on the Analysis Server or in your organization's Active Directory. The user name requires minimum privileges and will only be used by the APM Server to connect to the cubes. It is recommended that: ◦ The password for this user should never expire. ◦ The user should be restricted to change password. ◦ The user should be restricted to log in to others servers (e.g., meridium_ssas_user).	This step is required.
5	Add the user created in Step 4 to a role on all SQL Analysis Services databases that you want to access in APM. The role should have read and drill-through permissions. If the Work History database already has a View role defined, then you should add the user to this role. For more information, consult the MSDN documentation regarding Roles and Permissions for Analysis Services.	This step is required.
6	Verify that your event and asset criticality data meet the standard classification requirements, and modify the event or asset criticality data for the Work History cube as needed.	This step is required.
7	Localize the event and equipment values in APM .	This step is required only if you want to localize the event and equipment values in the Work History cube.
8	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.
9	Update the existing Analysis Services Cube records so that APM connects to the cube using the HTTP/ HTTPS access.	This step is required.

- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

Step	Task	Notes
1	Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: ◦ 2014 ◦ 2016	This step is required only if you were previously using SQL Server Analysis Services 2008 R2.
2	Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication.	This step is required.
3	Deploy Work History Analysis Services database. This Work History cube is a replacement for the Equipment and Functional Location Work History cubes in the Meridium_Event_Analysis database.	**Important:** Before executing this step, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted View permissions to the cubes associated with the Metric Views, and that the cubes are active. This step is required.
4	Create a Windows User on the Analysis Server or in your organization's Active Directory. The user name requires minimum privileges and will only be used by the APM Server to connect to the cubes. It is recommended that: ◦ The password for this user should never expire. ◦ The user should be restricted to change password. ◦ The user should be restricted to log in to others servers (e.g., meridium_ssas_user.	This step is required.
5	Add the user created in Step 4 to a role on all SQL Analysis Services databases that you want to access in APM. The role should have read and drill-through permissions. If the Work History database already has a View role defined, then you should add the user to this role. For more information, consult the MSDN documentation regarding Roles and Permissions for Analysis Services.	This step is required.
6	Verify that your event and asset criticality data meet the standard classification requirements, and modify the event or asset criticality data for the Work History cube as needed.	This step is required.
7	Localize the event and equipment values in APM .	This step is required only if you want to localize the event and equipment values in the Work History cube.

Step	Task	Notes
8	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.
9	Update the existing Analysis Services Cube records so that APM connects to the cube using the HTTP/ HTTPS access.	This step is required.

- Upgrade from any version V3.5.1 through V3.5.1.12.3

Step	Task	Notes
1	Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: ◦ 2014 ◦ 2016	This step is required only if you were previously using SQL Server Analysis Services 2008 R2.
2	Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication.	This step is required.
3	Deploy Work History Analysis Services database. This Work History cube is a replacement for the Equipment and Functional Location Work History cubes in the Meridium_Event_Analysis database.	**Important:** Before executing this step, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted View permissions to the cubes associated with the Metric Views, and that the cubes are active. This step is required.
4	Create a Windows User on the Analysis Server or in your organization's Active Directory. The user name requires minimum privileges and will only be used by the APM Server to connect to the cubes. It is recommended that: ◦ The password for this user should never expire. ◦ The user should be restricted to change password. ◦ The user should be restricted to log in to others servers (e.g., meridium_ssas_user).	This step is required.
5	Add the user created in Step 4 to a role on all SQL Analysis Services databases that you want to access in APM. The role should have read and drill-through permissions. If the Work History database already has a View role defined, then you should add the user to this role. For more information, consult the MSDN documentation regarding Roles and Permissions for Analysis Services.	This step is required.

Step	Task	Notes
6	Verify that your event and asset criticality data meet the standard classification requirements, and modify the event or asset criticality data for the Work History cube as needed.	This step is required.
7	Localize the event and equipment values in APM .	This step is required only if you want to localize the event and equipment values in the Work History cube.
8	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.
9	Update the existing Analysis Services Cube records so that APM connects to the cube using the HTTP/ HTTPS access.	This step is required.

- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

Step	Task	Notes
1	Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: ◦ 2014 ◦ 2016	This step is required only if you were previously using SQL Server Analysis Services 2008 R2.
2	Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication.	This step is required.
3	Deploy Work History Analysis Services database. This Work History cube is a replacement for the Equipment and Functional Location Work History cubes in the Meridium_Event_Analysis database.	**Important:** Before executing this step, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted View permissions to the cubes associated with the Metric Views, and that the cubes are active. This step is required.
4	Create a Windows User on the Analysis Server or in your organization's Active Directory. The user name requires minimum privileges and will only be used by the APM Server to connect to the cubes. It is recommended that: ◦ The password for this user should never expire. ◦ The user should be restricted to change password. ◦ The user should be restricted to log in to others servers (e.g.,meridium_ssas_user).	This step is required.

Step	Task	Notes
5	Add the user created in Step 4 to a role on all SQL Analysis Services databases that you want to access in APM. The role should have read and drill-through permissions. If the Work History database already has a View role defined, then you should add the user to this role. For more information, consult the MSDN documentation regarding Roles and Permissions for Analysis Services.	This step is required.
6	Verify that your event and asset criticality data meet the standard classification requirements, and modify the event or asset criticality data for the Work History cube as needed.	This step is required.
7	Localize the event and equipment values in APM .	This step is required only if you want to localize the event and equipment values in the Work History cube.
8	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.
9	Update the existing Analysis Services Cube records so that APM connects to the cube using the HTTP/ HTTPS access.	This step is required.

- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: ◦ 2014 ◦ 2016	This step is required only if you were previously using SQL Server Analysis Services 2008 R2.
2	Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication.	This step is required.
3	Deploy Work History Analysis Services database. This Work History cube is a replacement for the Equipment and Functional Location Work History cubes in the Meridium_Event_Analysis database.	**Important:** Before executing this step, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted View permissions to the cubes associated with the Metric Views, and that the cubes are active. This step is required.

Step	Task	Notes
4	Create a Windows User on the Analysis Server or in your organization's Active Directory. The user name requires minimum privileges and will only be used by the APM Server to connect to the cubes. It is recommended that: ◦ The password for this user should never expire. ◦ The user should be restricted to change password. ◦ The user should be restricted to log in to others servers (e.g.,meridium_ssas_user).	This step is required.
5	Add the user created in Step 4 to a role on all SQL Analysis Services databases that you want to access in APM. The role should have read and drill-through permissions. If the Work History database already has a View role defined, then you should add the user to this role. For more information, consult the MSDN documentation regarding Roles and Permissions for Analysis Services.	This step is required.
6	Verify that your event and asset criticality data meet the standard classification requirements, and modify the event or asset criticality data for the Work History cube as needed.	This step is required.
7	Localize the event and equipment values in APM .	This step is required only if you want to localize the event and equipment values in the Work History cube.
8	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.
9	Update the existing Analysis Services Cube records so that APM connects to the cube using the HTTP/ HTTPS access.	This step is required.

- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: ◦ 2014 ◦ 2016	This step is required only if you were previously using SQL Server Analysis Services 2008 R2.
2	Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication.	This step is required.

Step	Task	Notes
3	Deploy Work History Analysis Services database. This Work History cube is a replacement for the Equipment and Functional Location Work History cubes in the Meridium_Event_Analysis database.	**Important:** Before executing this step, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted View permissions to the cubes associated with the Metric Views, and that the cubes are active. This step is required.
4	Create a Windows User on the Analysis Server or in your organization's Active Directory. The user name requires minimum privileges and will only be used by the APM Server to connect to the cubes. It is recommended that: ◦ The password for this user should never expire. ◦ The user should be restricted to change password. ◦ The user should be restricted to log in to others servers (e.g.,meridium_ssas_user).	This step is required.
5	Add the user created in Step 4 to a role on all SQL Analysis Services databases that you want to access in APM. The role should have read and drill-through permissions. If the Work History database already has a View role defined, then you should add the user to this role. For more information, consult the MSDN documentation regarding Roles and Permissions for Analysis Services.	This step is required.
6	Verify that your event and asset criticality data meet the standard classification requirements, and modify the event or asset criticality data for the Work History cube as needed.	This step is required.
7	Localize the event and equipment values in APM .	This step is required only if you want to localize the event and equipment values in the Work History cube.
8	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.
9	Update the existing Analysis Services Cube records so that APM connects to the cube using the HTTP/ HTTPS access.	This step is required.

About Configuring a Cube for Usage Metrics Tracking

You can track the activity of the users in your system. Usage metrics are stored in the MI_SEC_LOG_EVENTS system table. When a user logs in to APM, actions of the user are stored in batches for that session in the MI_SEC_LOG_EVENTS table.

The MI_SEC_LOG_EVENTS table records the following events:

- Successful logins
- Failed logins
- Password changes
- User account creation, activation, deactivation, modification
- Session expiry

The following table describes the columns that exist in the MI_SEC_LOG_EVENTS table:

Column ID	Description
SECL_KEY	Stores the values that identify the events in the MI_SEC_LOG_EVENTS table.
SECL_EVENT_NM	Stores the names of the events.
SECL_USER_ID	Stores the user IDs of the users who attempt to log in to APM.
SECL_ADMIN_ID	Stores the user IDs of the Administrators who create, update, and delete users.
LAST_UPDT_DT	Stores the value that identifies the date and time when a record was last updated.

Note: Usage metrics are recorded only for activities performed via APM. Usage metrics are not recorded for activities performed in the APM Administrative applications.

To view the usage metrics that have been tracked for your system, you must create a cube based upon the MI_SEC_LOG_EVENTS table. After you create the cube, you must join the MI_SEC_LOG_EVENTS and the MIV_MI_IS_A_USER tables. You must also join the MIV_MI_IS_A_USER and MIV_MI_HUMAN_RESOURCE tables.

Note: Before you use the cube in the Metrics and Scorecards module, you must enable usage metrics tracking via the **Monitoring** page in Configuration Manager .

About Scheduling Cubes for Processing

An Analysis Services cube is a combination of measures and dimensions that together determine how a set of data can be viewed and analyzed. A cube is a static object and initially represents the data that existed in Analysis Services for the selected measures and dimensions when the cube was created. To keep a cube current, it must be processed regularly, whereby the cube is updated with the most current data in Analysis Services.

To make sure that a cube always provides users with the most current data, you should schedule it for processing regularly, usually on a daily basis. One way to process cubes and shared dimensions successfully is to do so manually on the Analysis Server. Using this method, you can process shared dimensions first, and then process the related cubes. Processing cubes manually, however, is not a viable option if you have many cubes that you want to process on a daily basis.

Instead, a preferable option would be to schedule cubes for processing using Data Transformation Services (DTS). This functionality is available in the SQL Server Business Intelligence Development Studio, which is included in SQL Server Standard Edition. For details on creating a DTS package that can be used to process objects according to a custom schedule, see your SQL Server documentation.

Install SQL Server Analysis Services on the Server

SQL Server Analysis Services is the foundation for the APM Metrics and Scorecards module because it serves as a storage and management mechanism for cubes, which can then be accessed and viewed via APM. To support Metrics and Scorecards features, SQL Server Analysis Services must be installed on the machine that will serve as the Analysis Server. The Analysis Server must be set up as a machine that is separate from the APM Application Server.

Where Does This Software Need to Be Installed?

SQL Server Analysis Services must be installed on the machine that will function as the Analysis Server. You do not need to install any SQL Server components on the Application Server to support the Metrics and Scorecards functionality.

Performing the Installation

SQL Server Analysis Services can be installed using the SQL Server Standard Edition installation package, which you may have received from APM or from a third-party vendor, depending upon the licensing options you selected when you purchased the APM product. Instructions for performing the installation can be found in the documentation included in the SQL Server Standard Edition installation package.

Creating the Analysis Services Database, Data Source, and Cubes

In addition to creating the Analysis Services database, data source, and cubes, the cubes must be processed before they will be available for use in the APM system. For details on completing these tasks, consult your SQL Server documentation.

Migrate SQL Server Cubes

About This Task

If you are upgrading from a previous version of APM and you have existing Metrics and Scorecards objects (e.g., Metric Views and KPIs) that are based upon SQL Server 2005 or SQL Server 2008 R2 Analysis Services cubes, you may be able to migrate your cubes while maintaining the proper functioning of your existing APM objects.

- If you have SQL Server 2008 or SQL Server 2012 cubes, you must migrate them to one of the following SQL server versions:
  - SQL Server 2014
  - SQL Server 2016

The following workflow provides a general overview of the process for migrating cubes from an older version of SQL Server Analysis Services to a newer version of SQL Server Analysis Services. For more details, you should see your SQL Server documentation.

Important: Depending upon the complexity of your cubes, you may or may not be able to migrate them successfully. We recommend that you attempt to migrate them using the following procedure. If you review the cubes after the migration and determine that the migration was not successful, the cubes will need to be rebuilt. In that case, any KPIs and Metric Views that were based upon those cubes must also be rebuilt.

Procedure

1. On the SQL Server Analysis Services Server where the older version of SQL Server Analysis Services is installed, open the **SQL Server Management Studio** window.
2. Connect to the SQL Sever Analysis Services database that you want to upgrade.
3. In the **Object Explorer** pane, right-click **Databases**, and select **Backup**.
   The **Backup Database - <Database Name>** window appears, where <Database Name> is the name of the database that you want to upgrade.
4. To the right of the **Backup file** box, select the **Browse** button, and specify the location where the database will be backed up.
5. Specify any additional settings, and then select **OK**.
   The selected database is saved to an .ABF file in the specified location.
6. Open the **SQL Server Management Studio** window for the new version of SQL Server Analysis Services.
7. In the **Object Explorer** pane, right-click **Databases**, and select **New Database**.
   The **New Database** window appears.
8. In the **Database name** box, enter a name for the database that you are migrating to the new version of SQL Server Analysis Services.
9. Specify any additional settings, and then select **OK**.
   The specified database is created, and a corresponding node appears in the **Object Explorer** pane.
10. Right-click the node representing the new database, and then select **Restore**.
    The **Restore Database** window appears.
11. In the **Backup** file, enter the file path or select the **Browse** button and navigate to the database file that you backed up in step 5.
12. Specify an additional settings, and then select **OK**.
    Your SQL Server Analysis Services database is migrated to the new SQL Server Analysis Services version.
13. In the APM, in the Metrics and Scorecards module, modify the remaining properties of each Analysis Services Cube record, including selecting the appropriate new SQL Server Analysis Server. You can do by using the **Manage Cubes** page in the Metrics and Scorecards module.
14. View existing objects (e.g. Metric Views and KPIs) that are based upon the migrated cubes to ensure that the correct data is being displayed. If the correct data is not displayed, rebuild the cubes and the objects that are based upon them. For details on rebuilding cubes, see your SQL Server documentation.

Deploy the Work History Cube

Procedure

1. Copy the `Cubes` folder from the Release CD to the SQL Server Analysis Services server.
2. On the SQL Server Analysis Services server, in the `Cubes` folder, select the `Work History` folder.

The following files and folders appear:

- Work_History.asdatabase
- Work_History.configsettings
- Work_History.deploymentoptions
- Work_History.deploymenttargets
- Work_History.asassemblylocations
- MDXFunctions folder

3. Run the Analysis Services Deployment Wizard program.
   The **Welcome** page appears.
4. Select **Next**.
5. When the wizard prompts you to choose the database file, navigate to the `Work History` folder, and then select the `Work History.asdatabase` file.
6. Perform all steps of the wizard to deploy the Work History database to the SQL Server Analysis Services server.

   Note: For more information, refer to the MSDN documentation regarding Analysis Services Deployment Wizard.

About Modifying the Work History Cube

The baseline Work History cube provided with the Metrics and Scorecards module uses the following standard classifications for event and asset criticality data. If the event or asset criticality data in your database cannot be classified as one of following the standard IDs, the data, by default, will be classified as *Unknown*.

- Event Type
  - Standard Event Types
    - ID: Miscellaneous; Caption: Miscellaneous
    - ID: PM/PdM; Caption: PM/PdM
    - ID: Repair; Caption: Repair
    - ID: Unknown; Caption: Unknown
- Event Breakdown Indicator
  - Standard Event Breakdown Indicators
    - ID: N, Caption: N
    - ID: Y, Caption: Y
    - ID: Unknown, Caption: Unknown
- Event Priority
  - Standard Event Priorities
    - ID: 1, Caption: Very Low
    - ID: 2, Caption: Low
    - ID: 3, Caption: Medium
    - ID: 4, Caption: High
    - ID: 5, Caption: Emergency
    - ID: Unknown, Caption: Unknown
- Event Detection Method
  - Standard Event Detection Methods
    - ID: 0001, Caption: Continuous Condition Monitoring

    - ID: 0002, Caption: Corrective Maintenance
    - ID: 0003, Caption: Formal Inspection
    - ID: 0004, Caption: Operator Routine Observation
    - ID: 0005, Caption: Periodic Condition Monitoring
    - ID: 0006, Caption: Preventive Maintenance
    - ID: 0007, Caption: Production Interference
    - ID: 0008, Caption: Radar Operator Observation
    - ID: Unknown, Caption: Unknown
- Asset Criticality Data
    - Standard Asset Criticality Data
        - ID: A, Caption: High
        - ID: B, Caption: Medium
        - ID: C, Caption: Low
        - ID: Unknown, Caption: Unknown

Modify the Event or Asset Criticality Data for Work History Cube

If the event or asset criticality data in your database does not match with the standard IDs used for the work history cube, then you have to modify the corresponding views on the server or map the event or asset criticality data to the standard event or asset criticality data using the corresponding families.

Modify the Non-Standard Event Type Data Using the View

Before You Begin

- Log in to SQL Server Management Studio and connect to the database.
- Verify the standard classification defined for event or asset criticality data.

Procedure

1. In the **Views**, select MIV_MI_FAC_WORK_HSTY view, and then run the following query to check if the Event Type data matches the standard classification defined.

   SELECT distinct MI_EVENT_TYP_CHR from MI_EVENT
2. Verify if the results match the standard event type IDs defined by the Work History cube.
3. If the results do not match, then modify the case statement CASE MI_EVENT_TYP_CHR in the view to display the standard event type IDs.

Example

Suppose the distinct Event Types returned by the query run in Step 1 are *Miscellaneous*, *Repair* ,*PM/PdM*, and *Inspection* and if *Inspection* event in your data should be *PM/PdM* event, then modify the CASE statement in the View as follows:

```
CASE MI_EVENT_TYP_CHR

 WHEN 'Miscellaneous' THEN 'Miscellaneous'
```

```
 WHEN 'PM/PdM' THEN 'PM/PdM'
 WHEN 'Repair' THEN 'Repair'
 WHEN 'Inspection' THEN 'PM/PdM'
 ELSE 'Unknown'
END AS EventType
```

Modify the Non-Standard Event Priority Data Using the View

Before You Begin

- Log in to SQL Server Management Studio and connect to the database.
- Verify the standard classification defined for event or asset criticality data.

Procedure

1. In the **Views**, select MIV_MI_FAC_WORK_HSTY view, and then run the following queries to check if the Event priority data matches the standard classification defined.

   SELECT distinct MI_EVWKHIST_ORDR_PRTY_C from MI_EVWKHIST

   SELECT distinct MI_EVWKHIST_RQST_PRTY_C from MI_EVWKHIST
2. Verify if the results match the standard event priority IDs defined by the Work History cube.
3. If the results do not match, then modify the case statement CASE ISNULL(MI_EVWKHIST_ORDR_PRTY_C, MI_EVWKHIST_RQST_PRTY_C) in the view to display the standard event priority IDs.

Example

Suppose the distinct Event Priorities returned by the query are *1*, *2*,*3*, *4*,*5*, and *M* and if *M* in your data should be event priority *3*, then you should modify the CASE statement in View as:

```
CASE ISNULL(MI_EVWKHIST_ORDR_PRTY_C,
MI_EVWKHIST_RQST_PRTY_C)
WHEN 'Very Low' THEN '1'
WHEN 'Low' THEN '2'
WHEN 'Medium' THEN '3'
WHEN 'High' THEN '4'
WHEN 'Emergency' THEN '5'
WHEN '1' THEN '1'
WHEN '2' THEN '2'
WHEN '3' THEN '3'
```

```
WHEN '4' THEN '4'

WHEN '5' THEN '5'

WHEN 'M' THEN '3'

ELSE 'Unknown'

END AS Priority
```

Modify the Non-Standard Event Detection Method Data Using the View

Before You Begin

- Log in to SQL Server Management Studio and connect to the database.
- Verify the standard classification defined for event or asset criticality data.

Procedure

1. In the **Views**, select MIV_MI_FAC_WORK_HSTY view, and then run the following queries to check if the Event detection method data matches the standard classification defined.

   SELECT distinct MI_EVWKHIST_DETCT_MTHD_CD_C from MI_EVWKHIST
2. Verify if the results match the standard event detection method IDs defined by the Work History cube.
3. If the results do not match, then modify the case statement CASE MI_EVWKHIST_DETCT_MTHD_CD_C in the view to display standard event detection method IDs.

Example

Suppose distinct Event Detection Methods returned by the query are *0001*, *0002*,*0003*, *0004*,*0005*,*0006*,*0007*,*0008*, and *0009* and if *0009* in your data should be *0001* event detection method, then you should modify the CASE statement in View as:

```
CASE MI_EVWKHIST_DETCT_MTHD_CD_C

WHEN 'Continous Condition Monitoring' THEN '0001'

WHEN 'Corrective Maintenance' THEN '0002'

WHEN 'Formal Inspection' THEN '0003'

WHEN 'Operator Routine Observation' THEN '0004'

WHEN 'Periodic Condition Monitoring' THEN '0005'

WHEN 'Preventive Maintenance' THEN '0006'

WHEN 'Production Interference' THEN '0007'

WHEN 'Radar operator Observation' THEN '0008'
```

```
WHEN '0001' THEN '0001'
WHEN '0002' THEN '0002'
WHEN '0003' THEN '0003'
WHEN '0004' THEN '0004'
WHEN '0005' THEN '0005'
WHEN '0006' THEN '0006'
WHEN '0007' THEN '0007'
WHEN '0008' THEN '0008'
WHEN '0009' THEN '0001'
ELSE 'Unknown'
END AS DetectionMethod
```

Modify the Non-Standard Event Breakdown Data Using the View

Before You Begin

- Log in to SQL Server Management Studio and connect to the database.
- Verify the standard classification defined for event or asset criticality data.

Procedure

1. In the **Views**, select MIV_MI_FAC_WORK_HSTY view and then run the following query to check if the Event Breakdown data matches the standard classification defined.

   SELECT distinct MI_EVWKHIST_BRKDN_IND_F from MI_EVWKHIST
2. Verify if the results match the standard event breakdown IDs defined by the Work History cube.
3. If the results do not match, then modify the case statement CASE MI_EVWKHIST_BRKDN_IND_F in the view to display the standard event breakdown IDs.

Example

Suppose the distinct Event Breakdown returned by the query is *Y*, *N*, and *No* and if *No* in your data is should be *N* event breakdown, then you should modify the CASE statement in View as:

```
CASE MI_EVWKHIST_BRKDN_IND_F
 WHEN 'Y' THEN 'Y'
 WHEN 'N' THEN 'N'
 WHEN 'No' THEN 'N'
 ELSE 'Unknown'
```

```
END AS Breakdown
```

Modify the Non-Standard Equipment Criticality Data Using the View

Before You Begin

- Log in to SQL Server Management Studio and connect to the database.
- Verify the standard classification defined for event or asset criticality data.

Procedure

1. In the **Views**, select MIV_MI_FAC_EQUIPMENT view, and then run the following queries to check if the Equipment Criticality data matches the standard classification defined.

   SELECT distinct MI_EQUIP000_CRITI_MTHD_IND_C from MI_EQUIP000
2. Verify if the results match the standard equipment criticality IDs defined by the Work History cube.
3. If the results do not match, then modify the case statement CASE MI_EQUIP000_CRITI_IND_C in the view to display standard equipment criticality IDs.

Example

Suppose distinct Equipment Criticality returned by the query in Step 1 is *A*, *B*, *C*, and *H* and if *H* in your data is actually *A* equipment criticality ID, then you should modify the CASE statement in the View as:

```
CASE MI_EQUIP000_CRITI_IND_C

WHEN 'HIGH' THEN 'A'

WHEN 'Medium' THEN 'B'

WHEN 'Low' THEN 'C'

WHEN 'A' THEN 'A'

WHEN 'B' THEN 'B'

WHEN 'C' THEN 'C'

WHEN 'H' THEN 'A'

ELSE 'Unknown'

END AS EquipmentCriticality
```

Modify the Non-Standard Functional Location Criticality Data Using the View

Before You Begin

- Log in to SQL Server Management Studio and connect to the database.
- Verify the standard classification defined for event or asset criticality data.

Procedure

1. In the **Views**, select MIV_MI_FAC_FNC_LOC view, and then run the following queries to check if the Functional Location Criticality data matches the standard classification defined.

   SELECT distinct MI_FNCLOC00_CRTCAL_IND_C from MI_FNCLOC00
2. Verify if the results match the standard functional location criticality IDs defined by the Work History cube.
3. If the results do not match, then modify the case statement CASE A.MI_FNCLOC00_CRTCAL_IND_C in the view to display standard functional location criticality IDs.

Example

Suppose the distinct functional location criticality returned by the query in Step 1 is *A*, *B*,*C*, and *M* and if *M* in your data should be *B* functional location criticality ID, then you should modify the CASE statement in the View as:

```
CASE A.MI_FNCLOC00_CRTCAL_IND_C

WHEN 'HIGH' THEN 'A'

WHEN 'Medium' THEN 'B'

WHEN 'Low' THEN 'C'

WHEN 'A' THEN 'A'

WHEN 'B' THEN 'B'

WHEN 'C' THEN 'C'

WHEN 'M' THEN 'B'

ELSE 'Unknown'

END AS FunctionalLocationCriticality
```

Map the Non-Standard Event Type Data to Standard Event Type IDs Using Queries for Event Type Dimension Family

This topic describes how to map the event type data available in your database to the standard event type data defined for a work history cube.

Procedure

1. In the module navigation menu, select **Tools**, and then select **Queries**.
   The **Query** page appears.
2. Select **Create New**.
   The **Select a Family or Query** window appears.
3. Search for the Event Type Dimension family, and then select **Add**.
   The **Design** workspace appears.
4. Select the **SQL** tab.
   The **SQL** workspace appears.
5. Run the query `SELECT [MI_DIM_EVENT_TYPE].[EventType] "EventType", [MI_DIM_EVENT_TYPE].[EventTypeCaption] "EventTypeCaption" FROM [MI_DIM_EVENT_TYPE].`
   The standard event type data available in APM appears in the query results.
6. Run the query `SELECT distinct MI_EVENT_TYP_CHR from MI_EVENT.`
   The event type data available in your database appears in the query results.
7. Verify if the event type data returned by the query in Step 6 matches the standard event type IDs returned by the query in Step 5.
8. If the results do not match, perform the following steps to map the event type data available in your database with the standard event type ID available in APM:

   a) In the **SQL** workspace, enter the following update query:
   ```
   UPDATE [MI_DIM_EVENT_TYPE] SET [MI_DIM_EVENT_TYPE].[EventTypeCaption] = '<New Data>' WHERE [MI_DIM_EVENT_TYPE].[EventTypeCaption] = '<Standard Data Caption>'
   ```

   Note: In this query:

   - <New Data> denotes the event type data that you want to map to the standard event type ID available in APM.
   - <Standard Data Caption> denotes the captions corresponding to the standard event type data available in APM.

   b) Replace <New Data> with a value that you want to map with the standard event type data available in APM.
   c) Replace <Standard Data Caption> with the caption available for the corresponding event type ID to which the new event type data will be mapped.
   d) Run the query.
   The **Execute Query** window appears.
   e) Select **Yes**.
   The event type data is mapped to the standard event type ID defined for the work history cube.

   Map an Event Type to a Standard Event Type ID

   The following standard event type data is returned by the query run in Step 5.

EventType	EventTypeCaption
Miscellaneous	Miscellaneous
PM/PdM	PM/PdM
Repair	Repair
Unknown	Unknown

The following event type data is returned by the query run in Step 6:

- INSPECTION
- PM/PdM
- Reading
- Repair

If you want to map the event type INSPECTION to the standard event type ID Miscellaneous:

- Run the query `UPDATE [MI_DIM_EVENT_TYPE] SET [MI_DIM_EVENT_TYPE].[EventTypeCaption] = 'INSPECTION' WHERE [MI_DIM_EVENT_TYPE].[EventTypeCaption] = 'Miscellaneous'.`

  The event type INSPECTION is mapped to the standard event type ID Miscellaneous.

Map the Non-Standard Event Priority Data to Standard Event Priority IDs Using Queries for Event Priority Dimension Family

This topic describes how to map the event priority data available in your database to the standard event priority data defined for a work history cube.

Procedure

1. In the module navigation menu, select **Tools**, and then select **Queries**.
   The **Query** page appears.
2. Select **Create New**.
   The **Select a Family or Query** window appears.
3. Search for the Event Priority Dimension family, and then select **Add**.
   The **Design** workspace appears.
4. Select the **SQL** tab.
   The **SQL** workspace appears.
5. Run the query `SELECT [MI_DIM_EVENT_PRIORITY].[Priority] "Priority", [MI_DIM_EVENT_PRIORITY].[PriorityCaption] "PriorityCaption" FROM [MI_DIM_EVENT_PRIORITY].`
   The standard event priority data available in APM appears in the query results.
6. Run the following queries:
   - `SELECT distinct MI_EVWKHIST_BRKDN_IND_F from MI_EVWKHIST`
   - `SELECT distinct MI_EVWKHIST_RQST_PRTY_C from MI_EVWKHIST`

   The event priority data available in your database appears in the query results.
7. Verify if the event priority data returned by the query in Step 6 matches the standard event priority IDs returned by the query in Step 5.

8. If the results do not match, perform the following steps to map the event priority data available in your database with the standard event priority ID available in APM:

   a) In the **SQL** workspace, enter the following update query:

   ```
   UPDATE [MI_DIM_EVENT_PRIORITY] SET [MI_DIM_EVENT_PRIORITY].
   [PriorityCaption] = '<New Data>' WHERE [MI_DIM_EVENT_PRIORITY].
   [PriorityCaption] = '<Standard Data Caption>'
   ```

   Note: In this query:

   - <New Data> denotes the event priority data that you want to map to the standard event priority ID available in APM.
   - <Standard Data Caption> denotes the captions corresponding to the standard event priority data available in APM.

   b) Replace <New Data> with a value that you want to map with the standard event priority data available in APM.

   c) Replace <Standard Data Caption> with the caption available for the corresponding event priority ID to which the new event priority data will be mapped.

   d) Run the query.
   The **Execute Query** window appears.

   e) Select **Yes**.
   The event priority data is mapped to the standard event priority ID defined for the work history cube.

Map Event Priority Data to a Standard Event Priority ID

The following standard event priority data is returned by the query run in Step 5.

Priority	PriorityCaption
1	Very Low
2	Low
3	Medium
4	High
5	Emergency
Unknown	Unknown

The following event priority data is returned by the query run in Step 6:

- 1
- 2
- 3
- 4

If you want to map the event priority data 1 to the standard event priority ID 5:

- Run the query `UPDATE [MI_DIM_EVENT_PRIORITY] SET [MI_DIM_EVENT_PRIORITY].[PriorityCaption] = '1' WHERE [MI_DIM_EVENT_PRIORITY].[PriorityCaption] = 'Emergency'`.
  The event priority data 1 is mapped to the standard event priority ID 5.

Map the Non-Standard Event Detection Methods to Standard Event Detection Method IDs Using Queries for Event Detection Method Dimension Family

This topic describes how to map the event detection methods available in your database to the standard event detection methods defined for a work history cube.

Procedure

1. In the module navigation menu, select **Tools**, and then select **Queries**.
   The **Query** page appears.
2. Select **Create New**.
   The **Select a Family or Query** window appears.
3. Search for the Event Detection Method Dimension family, and then select **Add**.
   The **Design** workspace appears.
4. Select the **SQL** tab.
   The **SQL** workspace appears.
5. Run the query `SELECT [MI_DIM_EVENT_DETECTION].[DetectionMethod] "DetectionMethod", [MI_DIM_EVENT_DETECTION].[DetectionMethodCaption] "DetectionMethodCaption" FROM [MI_DIM_EVENT_DETECTION].`
   The standard event detection methods available in APM appears in the query results.
6. Run the query `SELECT distinct MI_EVWKHIST_DETCT_MTHD_CD_C from MI_EVWKHIST`.
   The event detection methods available in your database appears in the query results.
7. Verify if the event detection methods returned by the query in Step 6 match the standard event detection method IDs returned by the query in Step 5.
8. If the results do not match, perform the following steps to map the event detection methods available in your database with the standard event detection method ID available in APM:
   a) In the **SQL** workspace, enter the following update query:
   ```
   UPDATE [MI_DIM_EVENT_DETECTION] SET [MI_DIM_EVENT_DETECTION].
   [DetectionMethod] = '<New Data>' WHERE [MI_DIM_EVENT_DETECTION].
   [DetectionMethod] = '<Standard Data Caption>'
   ```
   Note: In this query:
   - <New Data> denotes the event detection method that you want to map to the standard event detection method ID available in APM.
   - <Standard Data Caption> denotes the captions corresponding to the standard event detection method available in APM.

   b) Replace <New Data> with a value that you want to map with the standard event detection method available in APM.
   c) Replace <Standard Data Caption> with the caption available for the corresponding event detection method ID to which the new event detection method will be mapped.
   d) Run the query.
   The **Execute Query** window appears.
   e) Select **Yes**.
   The event detection method is mapped to the standard event detection method ID defined for the work history cube.

Map an Event Detection Method to a Standard Event Detection Method ID

The following standard event detection methods are returned by the query run in Step 5.

DetectionMethod	DetectionMethodCaption
0001	Continuous Condition Monitoring
0002	Corrective Maintenance
0003	Formal Inspection
0004	Operator Routine Observation
0005	Periodic Condition Monitoring
0006	Preventive Maintenance
0007	Production Interference
0008	Radar Operator observation

The following event detection methods are returned by the query run in Step 6:

- Inspection
- Observation
- Preventive Maintenance
- Production Interference

If you want to map the event detection method Inspection to the standard event detection method ID 0001:

- Run the query `UPDATE [MI_DIM_EVENT_DETECTION] SET [MI_DIM_EVENT_DETECTION].[DetectionMethod] = 'Inspection' WHERE [MI_DIM_EVENT_DETECTION].[DetectionMethod] = '0001'.`
  The event detection method Inspection is mapped to the standard event detection method ID 0001.

Map the Non-Standard Event Breakdown Data to Standard Event Breakdown IDs Using Queries for Event Breakdown Dimension Family

This topic describes how to map the event breakdown data available in your database to the standard event breakdown data defined for a work history cube.

Procedure

1. In the module navigation menu, select **Tools**, and then select **Queries**.
   The **Query** page appears.
2. Select **Create New**.
   The **Select a Family or Query** window appears.
3. Search for the Event Breakdown Dimension family, and then select **Add**.
   The **Design** workspace appears.
4. Select the **SQL** tab.

The **SQL** workspace appears.

5. Run the query `SELECT [MI_DIM_EVENT_BREAKDOWN].[Breakdown] "Breakdown", [MI_DIM_EVENT_BREAKDOWN].[BreakdownCaption] "BreakdownCaption" FROM [MI_DIM_EVENT_BREAKDOWN].`
   The standard event breakdown data available in APM appears in the query results.
6. Run the query `SELECT distinct MI_EVWKHIST_BRKDN_IND_F from MI_EVWKHIST.`
   The event breakdown data available in your database appears in the query results.
7. Verify if the event breakdown data returned by the query in Step 6 matches the standard event breakdown IDs returned by the query in Step 5.
8. If the results do not match, perform the following steps to map the event breakdown data available in your database with the standard event breakdown ID available in APM:
   a) In the **SQL** workspace, enter the following update query:
   ```
   UPDATE [MI_DIM_EVENT_BREAKDOWN] SET [MI_DIM_EVENT_BREAKDOWN].
   [BreakdownCaption] = '<New Data>' WHERE [MI_DIM_EVENT_BREAKDOWN].
   [BreakdownCaption] = '<Standard Data Caption>'
   ```
   Note: In this query:
   - <New Data> denotes the event breakdown data that you want to map to the standard event breakdown ID available in APM.
   - <Standard Data Caption> denotes the captions corresponding to the standard event breakdown data available in APM.

   b) Replace <New Data> with a value that you want to map with the standard event breakdown data available in APM.
   c) Replace <Standard Data Caption> with the caption available for the corresponding event breakdown ID to which the new event breakdown data will be mapped.
   d) Run the query.
   The **Execute Query** window appears.
   e) Select **Yes**.
   The event breakdown data is mapped to the standard event breakdown ID defined for the work history cube.

Map an Event Breakdown Indicator to a Standard Event Breakdown ID

The following standard event breakdown data is returned by the query run in Step 5.

Breakdown	BreakdownCaption
N	N
Unknown	Unknown
Y	Y

The following event breakdown data is returned by the query run in Step 6:

- No
- Yes
- Unknown

If you want to map the event breakdown indicator Yes to the standard event breakdown ID Y:

- Run the query `UPDATE [MI_DIM_EVENT_BREAKDOWN] SET [MI_DIM_EVENT_BREAKDOWN].[BreakdownCaption] = 'Yes' WHERE [MI_DIM_EVENT_BREAKDOWN].[BreakdownCaption] = 'Y'.`
  The event breakdown indicator Yes is mapped to the standard event breakdown ID Y.

Map the Non-Standard Asset Criticality Data to Standard Asset Criticality IDs Using Queries for Asset Criticality Dimension Family

This topic describes how to map the asset criticality data available in your database to the standard asset criticality IDs defined for a work history cube.

Procedure

1. In the module navigation menu, select **Tools**, and then select **Queries**.
   The **Query** page appears.
2. Select **Create New**.
   The **Select a Family or Query** window appears.
3. Search for the Asset Criticality Dimension family, and then select **Add**.
   The **Design** workspace appears.
4. Select the **SQL** tab.
   The **SQL** workspace appears.
5. Run the query `SELECT [MI_DIM_ASSET_CRITICALITY].[Criticality] "Criticality", [MI_DIM_ASSET_CRITICALITY].[CriticalityCaption] "CriticalityCaption" FROM [MI_DIM_ASSET_CRITICALITY].`
   The standard asset criticality data available in APM appears in the query results.
6. Run the following queries:
   - For equipment criticality data, run the query `SELECT distinct MI_EQUIP000_CRITI_MTHD_IND_C from MI_EQUIP000.`
     The equipment criticality data available in your database appears in the query results.
   - For functional location criticality data, run the query `SELECT distinct MI_FNCLOC00_CRTCAL_IND_C from MI_FNCLOC00.`
     The functional location criticality data available in your database appears in the query results.
7. Verify if the asset criticality data returned by the query in Step 6 matches the standard asset criticality IDs returned by the query in Step 5.
8. If the results do not match, perform the following steps to map the asset criticality data available in your database with the standard asset criticality ID available in APM:
   a) In the **SQL** workspace, enter the following update query:
   ```
   UPDATE [MI_DIM_ASSET_CRITICALITY] SET [MI_DIM_ASSET_CRITICALITY].
   [CriticalityCaption] = '<New Data>' WHERE [MI_DIM_ASSET_CRITICALITY].
   [CriticalityCaption] = '<Standard Data Caption>'
   ```
   Note: In this query:
   - <New Data> denotes the asset criticality data that you want to map to the standard asset criticality ID available in APM.
   - <Standard Data Caption> denotes the captions corresponding to the standard asset criticality data available in APM.

b) Replace <New Data> with a value that you want to map with the standard asset criticality data available in APM.
c) Replace <Standard Data Caption> with the caption available for the corresponding asset criticality ID to which the new asset criticality data will be mapped.
d) Run the query.
The **Execute Query** window appears.
e) Select **Yes**.
The asset criticality data is mapped to the standard asset criticality ID defined for the work history cube.

Map Asset Criticality Data to a Standard Asset Criticality ID

The following standard asset criticality data are returned by the query run in Step 5.

Criticality	CriticalityCaption
A	High
B	Medium
C	Low
Unknown	Unknown

The following asset criticality data are returned by the query run in Step 6:

- X
- Y
- Z
- H

If you want to map the asset criticality data X to the standard asset criticality ID A:

- Run the query `UPDATE [MI_DIM_ASSET_CRITICALITY] SET [MI_DIM_ASSET_CRITICALITY].[CriticalityCaption] = 'X' WHERE [MI_DIM_ASSET_CRITICALITY].[CriticalityCaption] = 'High'`.
  The asset criticality data X is mapped to the standard asset criticality ID A.

Localize the Event or Asset Criticality Values

By default, the Meridium Work History cube displays the event and asset criticality data in English. However, you can modify the event or asset criticality values to other languages supported by APM. The examples in this topic explain how to modify event and asset criticality values, and how you can verify, in APM, that those modifications have been implemented.

Before You Begin

- Log in to SQL Server Management Studio and connect to the database.

Example: Localize the Event Type Values

Procedure

1. In the **Tables**, select the table MI_DIM_EVENT_TYPE.
   The table values appear, displaying the event type ID and the event caption.
2. In the **EventTypeCaption** column, select the cell for the event type that you want to localize, and then manually modify the caption.
3. Save the modification, and then process the cube.
4. Log in to APM.
5. Access the **Metrics and Scorecards** page and create a new Metric View.
   The design page for the Metric View appears.
6. In the Metric Views design page, in the **Rows/X-Axis** subsection, select +.
   The **Add to Rows** window appears.
7. In the **Event Type**, select **Event Type-Breakdown**, and then select **Event Type**.
   The caption for the event breakdown values appears in the language to which you have modified.

Example: Localize the Event Breakdown Values

Procedure

1. In the **Tables**, select the table MI_DIM_EVENT_BREAKDOWN.
   The table values appear, displaying the breakdown ID and the breakdown caption.
2. In the **BreakdownCaption** column, select the cell for the breakdown that you want to localize, and then manually modify the caption.
3. Save the modification, and then process the cube.
4. Log in to APM.
5. Access the **Metrics and Scorecards** page and create a new Metric View.
   The design page for the Metric View appears.
6. In the Metric Views design page, in the **Rows/X-Axis** subsection, select +.
   The **Add to Rows** window appears.
7. In the **Event Type**, select **Event Type-Breakdown**, and then select **Breakdown**.
   The caption for the event type values appears in the language to which you have modified.

Example: Localize the Event Priority Values

Procedure

1. In the **Tables**, select the table MI_DIM_EVENT_PRIORITY.
   The table values appear, displaying the Priority ID and the Priority caption.
2. In the **PriorityCaption** column, select the cell for the priority caption that you want to localize, and then manually modify the caption.
3. Save the modification, and then process the cube.
4. Log in to APM.
5. Access the **Metrics and Scorecards** page and create a new Metric View.
   The design page for the Metric View appears.
6. In the Metric Views design page, in the **Rows/X-Axis** subsection, select +.

The **Add to Rows** window appears.

7. In the **Event Priority**, select **Priority**, and then select **Priority**.
   The caption for the priorities appears in the language to which you have modified.

Example: Localize Event Detection Method Values

Procedure

1. In the **Tables**, select the table MI_DIM_EVENT_DETECTION_METHOD.
   The table values appear, displaying the event type ID and the event caption.
2. In the **DetectionMethodCaption** column, select the cell for the detection method that you want to localize, and then manually modify the caption.
3. Save the modification, and then process the cube.
4. Log in to APM.
5. Access the **Metrics and Scorecards** page and create a new Metric View.
   The design page for the Metric View appears.
6. In the Metric Views design page, in the **Rows/X-Axis** subsection, select +.
   The **Add to Rows** window appears.
7. In the **Event Detection**, select **Detection**, and then select **Detection Method**.
   The caption of the Detection Method values appear in the language to which it was modified.

Example: Localize Equipment Criticality Values

Procedure

1. In the **Tables**, select the table MI_DIM_ASSET_CRITICALITY.
   The table values appear, displaying the Criticality ID and the Criticality caption.
2. In the **CriticalityCaption** column, select the cell for the caption that you want to localize, and then manually modify the caption.
3. Save the modification, and then process the cube.
4. Log in to APM.
5. Access the **Metrics and Scorecards** page and create a new Metric View.
   The design page for the Metric View appears.
6. In the Metric Views design page, in the **Rows/X-Axis** subsection, select +.
   The **Add to Rows** window appears.
7. In the **Equipment**, select **Criticality**, and then select **Criticality**.
   The caption of the criticality values appear in the language to which it was modified.

Example: Localize Functional Location Criticality Values

Procedure

1. In the **Tables**, select the table MI_DIM_ASSET_CRITICALITY.
   The table values appear, displaying the criticality ID and the criticality caption.
2. In the **CriticalityCaption** column, select the cell for the caption that you want to localize, and then manually modify the caption.
3. Save the modification, and then process the cube.

4. Log in to APM.
5. Access the **Metrics and Scorecards** page and create a new Metric View.
   The design page for the Metric View appears.
6. In the Metric Views design page, in the **Rows/X-Axis** subsection, select  .
   The **Add to Rows** window appears.
7. In the **Functional Location**, select **Criticality**, and then select **Criticality**.
   The caption of the functional location criticality values appear in the language to which it was modified.

Policy Designer

Deploy Policy Designer

The checklists in this section of the documentation contain all the steps necessary for deploying and configuring this module whether you are deploying the module for the first time or upgrading from a previous module.

Deploy Policy Designer for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Important: The Policy Execution Service uses the MIJOB user account. MIJOB should be a Super User, should have its time zone set to UTC, and must not be locked out of any data source configured on the GE Vernova server. Any modifications to the security privileges of the MIJOB user account may lead to failure of the Policy Execution Service.

Note: If your system uses an Oracle schema, you must modify the Policy Overview dashboard to use the Oracle version of the graph.

Table 1: Procedure

Step	Task	Notes
1	Assign Security Users to one or more of the Policy Designer Security Groups and Roles.	This step is required.
2	Review the Policy Designer data model to determine which relationship definitions you will need to modify to include your custom equipment and location families, and as needed, modify the relationship definitions using Configuration Manager.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
3	Configure settings for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the default retries, concurrency, or duplicate trigger timeout settings.

Step	Task	Notes
4	Configure the time limit for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the policy execution time limit for the Policy Execution Service. By default, the policy execution time limit is 15 minutes per policy instance.
5	Configure the time limit for the execution of the Math node.	This step is optional. You can perform this step if you want to modify the Math node execution time limit for the Policy Execution Service. By default, the Math node execution time limit is 5 minutes.
6	Configure the default Historical Readings time range for the OT Connect Tag node.	This step is optional. You can perform this step to modify the default time range of retrieving Historical Readings for the OT Connect Tag node if a specific time range cannot be determined. By default, the OT Connect tag node will retrieve two years of HDA data.
7	On the APM Server, stop and restart the Meridium Policy Execution service.	This step is required. If your system architecture contains more than one APM Server, you must complete this step for every server that you want to use for policy execution.
8	Configure the queue settings for the Policy Trigger Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
9	On the APM Server, stop and restart the Meridium Policy Trigger service.	This step is required.
10	On the APM Server, reset IIS.	This step is required only if you have modified the time out value for the Math node execution or Policy Execution in the `appSettings.json` configuration file.

Upgrade or Update Policy Designer to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

Step	Task	Notes
1	Configure the time limit for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the policy execution time limit for the Policy Execution Service. By default, the policy execution time limit is 15 minutes per policy instance.
2	Configure the time limit for the execution of the Math node.	This step is optional. You can perform this step if you want to modify the Math node execution time limit for the Policy Execution Service. By default, the Math node execution time limit is 5 minutes.
3	Delete duplicate policies from the APM database.	You must perform this step only if an error message appears during the upgrade, indicating that a unique index could not be created because of duplicate family policies in the database.
4	Configure the alternative query for the **Policy Designer Overview** page.	This step is optional. You can perform this step if you are facing performance issues with the **Policy Designer Overview** page.
5	Configure the settings for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the default retries, concurrency, or duplicate trigger timeout settings.
6	On the APM Server, stop and restart the Meridium Policy Execution service.	This step is required. If your system architecture contains more than one APM Server, you must complete this step for every server that you want to use for policy execution.
7	Configure the settings for the Policy Trigger Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
8	On the APM Server, stop and restart the Meridium Policy Trigger service.	This step is required. If your system architecture contains more than one APM Server, you must start the Policy Trigger Service on at least one APM Server.
9	On the APM Server, reset IIS.	This step is required only if you have modified the time out value for the Math node execution or Policy Execution in the `appSettings.json` configuration file.

- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

Step	Task	Notes
1	Configure the time limit for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the policy execution time limit for the Policy Execution Service. By default, the policy execution time limit is 15 minutes per policy instance.
2	Configure the time limit for the execution of the Math node.	This step is optional. You can perform this step if you want to modify the Math node execution time limit for the Policy Execution Service. By default, the Math node execution time limit is 5 minutes.
3	Delete duplicate policies from the APM database.	You must perform this step only if an error message appears during the upgrade, indicating that a unique index could not be created because of duplicate family policies in the database.
4	Configure the alternative query for the **Policy Designer Overview** page.	This step is optional. You can perform this step if you are facing performance issues with the **Policy Designer Overview** page.
5	Configure the settings for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the default retries, concurrency, or duplicate trigger timeout settings.
6	On the APM Server, stop and restart the Meridium Policy Execution service.	This step is required. If your system architecture contains more than one APM Server, you must complete this step for every server that you want to use for policy execution.
7	Configure the settings for the Policy Trigger Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
8	On the APM Server, stop and restart the Meridium Policy Trigger service.	This step is required. If your system architecture contains more than one APM Server, you must start the Policy Trigger Service on at least one APM Server.
9	On the APM Server, reset IIS.	This step is required only if you have modified the time out value for the Math node execution or Policy Execution in the `appSettings.json` configuration file.

- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

Step	Task	Notes
1	Configure the time limit for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the policy execution time limit for the Policy Execution Service. By default, the policy execution time limit is 15 minutes per policy instance.
2	Configure the time limit for the execution of the Math node.	This step is optional. You can perform this step if you want to modify the Math node execution time limit for the Policy Execution Service. By default, the Math node execution time limit is 5 minutes.
3	Delete duplicate policies from the APM database.	You must perform this step only if an error message appears during the upgrade, indicating that a unique index could not be created because of duplicate family policies in the database.
4	Configure the alternative query for the **Policy Designer Overview** page.	This step is optional. You can perform this step if you are facing performance issues with the **Policy Designer Overview** page.
5	Configure the settings for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the default retries, concurrency, or duplicate trigger timeout settings.
6	On the APM Server, stop and restart the Meridium Policy Execution service.	This step is required. If your system architecture contains more than one APM Server, you must complete this step for every server that you want to use for policy execution.
7	Configure the settings for the Policy Trigger Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
8	On the APM Server, stop and restart the Meridium Policy Trigger service.	This step is required. If your system architecture contains more than one APM Server, you must start the Policy Trigger Service on at least one APM Server.
9	On the APM Server, reset IIS.	This step is required only if you have modified the time out value for the Math node execution or Policy Execution in the `appSettings.json` configuration file.

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

Step	Task	Notes
1	Configure the time limit for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the policy execution time limit for the Policy Execution Service. By default, the policy execution time limit is 15 minutes per policy instance.
2	Configure the time limit for the execution of the Math node.	This step is optional. You can perform this step if you want to modify the Math node execution time limit for the Policy Execution Service. By default, the Math node execution time limit is 5 minutes.
3	Delete duplicate policies from the APM database.	You must perform this step only if an error message appears during the upgrade, indicating that a unique index could not be created because of duplicate family policies in the database.
4	Configure the alternative query for the **Policy Designer Overview** page.	This step is optional. You can perform this step if you are facing performance issues with the **Policy Designer Overview** page.
5	Configure the settings for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the default retries, concurrency, or duplicate trigger timeout settings.
6	On the APM Server, stop and restart the Meridium Policy Execution service.	This step is required. If your system architecture contains more than one APM Server, you must complete this step for every server that you want to use for policy execution.
7	Configure the settings for the Policy Trigger Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
8	On the APM Server, stop and restart the Meridium Policy Trigger service.	This step is required. If your system architecture contains more than one APM Server, you must start the Policy Trigger Service on at least one APM Server.
9	On the APM Server, reset IIS.	This step is required only if you have modified the time out value for the Math node execution or Policy Execution in the `appSettings.json` configuration file.

- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

Step	Task	Notes
1	Configure the time limit for the Policy Execution Service.	This step is optional. You can perform this step if you want modify the policy execution time limit for the Policy Execution Service. By default, the policy execution time limit is 15 minutes per policy instance.
2	Configure the time limit for the execution of the Math node.	This step is optional. You can perform this step if you want to modify the Math node execution time limit for the Policy Execution Service. By default, the Math node execution time limit is 5 minutes.
3	Delete duplicate policies from the APM database.	You must perform this step only if an error message appears during the upgrade, indicating that a unique index could not be created because of duplicate family policies in the database.
4	Configure the alternative query for the **Policy Designer Overview** page.	This step is optional. You can perform this step if you are facing performance issues with the **Policy Designer Overview** page.
5	Configure the settings for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the default retries, concurrency, or duplicate trigger timeout settings.
6	On the APM Server, stop and restart the Meridium Policy Execution service.	This step is required. If your system architecture contains more than one APM Server, you must complete this step for every server that you want to use for policy execution.
7	Configure the settings for the Policy Trigger Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
8	On the APM Server, stop and restart the Meridium Policy Trigger service.	This step is required. If your system architecture contains more than one APM Server, you must start the Policy Trigger Service on at least one APM Server.
9	On the APM Server, reset IIS.	This step is required only if you have modified the time out value for the Math node execution or policy execution in the `appSettings.json` configuration file.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	Configure the time limit for the Policy Execution Service.	This step is optional. You can perform this step if you want modify the policy execution time limit for the Policy Execution Service. By default, the policy execution time limit is 15 minutes per policy instance.
2	Configure the time limit for the execution of the Math node.	This step is optional. You can perform this step if you want to modify the Math node execution time limit for the Policy Execution Service. By default, the Math node execution time limit is 5 minutes.
3	Delete duplicate policies from the APM database.	You must perform this step only if an error message appears during the upgrade, indicating that a unique index could not be created because of duplicate family policies in the database.
4	Configure the alternative query for the **Policy Designer Overview** page.	This step is optional. You can perform this step if you are facing performance issues with the **Policy Designer Overview** page.
5	Configure the settings for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the default retries, concurrency, or duplicate trigger timeout settings.
6	On the APM Server, stop and restart the Meridium Policy Execution service.	This step is required. If your system architecture contains more than one APM Server, you must complete this step for every server that you want to use for policy execution.
7	Configure the settings for the Policy Trigger Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
8	On the APM Server, stop and restart the Meridium Policy Trigger service.	This step is required. If your system architecture contains more than one APM Server, you must start the Policy Trigger Service on at least one APM Server.

<table>
<tr><th>Step</th><th>Task</th><th>Notes</th></tr>
<tr><td>9</td><td>On the APM Server, reset IIS.</td><td>This step is required only if you have modified the time out value for the Math node execution or policy execution in the <code>appSettings.json</code> configuration file.</td></tr>
<tr><td>10</td><td>If you are upgrading from V4.1.5.x and you used Policy Recommendations for the first time in V4.1.5.x, after you upgrade your database, use the State Management option in the Revert to Baseline feature to apply the correct State Configuration for the Policy Recommendation Family.

When you do so, you will need to provide mappings from the incorrect states to the corresponding correct states, as shown in the following table:

<table><tr><th>Custom (incorrect)</th><th>Baseline (correct)</th></tr><tr><td>Accepted by ASM</td><td>Completed</td></tr><tr><td>Closed</td><td>Completed</td></tr><tr><td>Consolidated</td><td>Superseded</td></tr><tr><td>Open</td><td>Proposed</td></tr><tr><td>Pending</td><td>Pending Approval</td></tr><tr><td>Superseded</td><td>Superseded</td></tr></table></td><td>This step is necessary because an incorrect baseline State Configuration was delivered for the Policy Recommendation family in V4.1.5.0. The baseline configuration was corrected in V4.1.6.0.

The correct baseline state configuration must be applied for various queries and lists in APM to function as expected.

You do not need to complete this step if:
You never used V4.1.5.x

-or-
You never used Policy Recommendations

-or-
You used Policy Recommendations in a version prior to V4.1.5.x</td></tr>
</table>

- Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	Configure the time limit for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the policy execution time limit for the Policy Execution Service. By default, the policy execution time limit is 15 minutes per policy instance.
2	Configure the time limit for the execution of the Math node.	This step is optional. You can perform this step if you want to modify the Math node execution time limit for the Policy Execution Service. By default, the Math node execution time limit is 5 minutes.
3	Delete duplicate policies from the APM database.	You must perform this step only if an error message appears during the upgrade, indicating that a unique index could not be created because of duplicate family policies in the database.

Step	Task	Notes
4	Configure the alternative query for the **Policy Designer Overview** page.	This step is optional. You can perform this step if you are facing performance issues with the **Policy Designer Overview** page.
5	Configure the settings for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the default retries, concurrency, or duplicate trigger timeout settings.
6	On the APM Server, stop and restart the Meridium Policy Execution service.	This step is required. If your system architecture contains more than one APM Server, you must complete this step for every server that you want to use for policy execution.
7	Configure the settings for the Policy Trigger Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
8	On the APM Server, stop and restart the Meridium Policy Trigger service.	This step is required. If your system architecture contains more than one APM Server, you must start the Policy Trigger Service on at least one APM Server.
9	On the APM Server, reset IIS.	This step is required only if you have modified the time out value for the Math node execution or Policy Execution in the `appSettings.json` configuration file.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

Step	Task	Notes
1	Configure the time limit for the Policy Execution Service.	This step is optional. You can perform this step if you want modify the policy execution time limit for the Policy Execution Service. By default, the policy execution time limit is 15 minutes per policy instance.
2	Configure the time limit for the execution of the Math node.	This step is optional. You can perform this step if you want to modify the Math node execution time limit for the Policy Execution Service. By default, the Math node execution time limit is 5 minutes.
3	Configure the alternative query for the **Policy Designer Overview** page.	This step is optional. You can perform this step if you are facing performance issues with the **Policy Designer Overview** page.
4	Configure the settings for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the default retries, concurrency, or duplicate trigger timeout settings.

Step	Task	Notes
5	On the APM Server, stop and restart the Meridium Policy Execution service.	This step is required. If your system architecture contains more than one APM Server, you must complete this step for every server that you want to use for policy execution.
6	Configure the settings for the Policy Trigger Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
7	On the APM Server, stop and restart the Meridium Policy Trigger service.	This step is required. If your system architecture contains more than one APM Server, you must start the Policy Trigger Service on at least one APM Server.
8	On the APM Server, reset IIS.	This step is required only if you have modified the time out value for the Math node execution or Policy Execution in the `appSettings.json` configuration file.
9		This step is required. If your database contained policies with execution schedules containing invalid times for the most recent Next Date or Last Date (for example, between 2:00 A.M. and 3:00 A.M. on the morning of daylight savings time), these fields were left blank during the upgrade. To ensure that your scheduled policies execute as expected, review the log, and update policy schedules in Policy Designer as needed.

- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

Step	Task	Notes
1	Configure the time limit for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the policy execution time limit for the Policy Execution Service. By default, the policy execution time limit is 15 minutes per policy instance.
2	Configure the time limit for the execution of the Math node.	This step is optional. You can perform this step if you want to modify the Math node execution time limit for the Policy Execution Service. By default, the Math node execution time limit is 5 minutes.
3	Configure the alternative query for the **Policy Designer Overview** page.	This step is optional. You can perform this step if you are facing performance issues with the **Policy Designer Overview** page.

Step	Task	Notes
4	Configure the settings for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the default retries, concurrency, or duplicate trigger timeout settings.
5	On the APM Server, stop and restart the Meridium Policy Execution service.	This step is required. If your system architecture contains more than one APM Server, you must complete this step for every server that you want to use for policy execution.
6	Configure the settings for the Policy Trigger Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
7	On the APM Server, stop and restart the Meridium Policy Trigger service.	This step is required. If your system architecture contains more than one APM Server, you must start the Policy Trigger Service on at least one APM Server.
8	On the APM Server, reset IIS.	This step is required only if you have modified the time out value for the Math node execution or Policy Execution in the `appSettings.json` configuration file.
9		This step is required. If your database contained policies with execution schedules containing invalid times for the most recent Next Date or Last Date (for example, between 2:00 A.M. and 3:00 A.M. on the morning of daylight savings time), these fields were left blank during the upgrade. To ensure that your scheduled policies execute as expected, review the log, and update policy schedules in Policy Designer as needed.

- Upgrade from any version V3.5.1 through V3.5.1.12.3

Step	Task	Notes
1	Configure the time limit for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the policy execution time limit for the Policy Execution Service. By default, the policy execution time limit is 15 minutes per policy instance.
2	Configure the time limit for the execution of the Math node.	This step is optional. You can perform this step if you want to modify the Math node execution time limit for the Policy Execution Service. By default, the Math node execution time limit is 5 minutes.

Step	Task	Notes
3	Configure the alternative query for the **Policy Designer Overview** page.	This step is optional. You can perform this step if you are facing performance issues with the **Policy Designer Overview** page.
4	Configure the settings for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the default retries, concurrency, or duplicate trigger timeout settings.
5	On the APM Server, stop and restart the Meridium Policy Execution service.	This step is required. If your system architecture contains more than one APM Server, you must complete this step for every server that you want to use for policy execution.
6	Configure the settings for the Policy Trigger Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
7	On the APM Server, stop and restart the Meridium Policy Trigger service.	This step is required. If your system architecture contains more than one APM Server, you must start the Policy Trigger Service on at least one APM Server.
8	On the APM Server, reset IIS.	This step is required only if you have modified the time out value for the Math node execution or Policy Execution in the `appSettings.json` configuration file.
9		This step is required. If your database contained policies with execution schedules containing invalid times for the most recent Next Date or Last Date (for example, between 2:00 A.M. and 3:00 A.M. on the morning of daylight savings time), these fields were left blank during the upgrade. To ensure that your scheduled policies execute as expected, review the log, and update policy schedules in Policy Designer as needed.

- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

  Note: For a Policy created in V3.5.0 with a node using built-in filter fields is opened in policy designer and saved, the fields will be removed from the policy model. You can modify the affected policies to use Collection Filter nodes to re-implement the desired time range.

Step	Task	Notes
1	Configure the time limit for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the policy execution time limit for the Policy Execution Service. By default, the policy execution time limit is 15 minutes per policy instance.
2	Configure the time limit for the execution of the Math node.	This step is optional. You can perform this step if you want to modify the Math node execution time limit for the Policy Execution Service. By default, the Math node execution time limit is 5 minutes.
3	Configure the alternative query for the **Policy Designer Overview** page.	This step is optional. You can perform this step if you are facing performance issues with the **Policy Designer Overview** page.
4	Configure the settings for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the default retries, concurrency, or duplicate trigger timeout settings.
5	On the APM Server, stop and restart the Meridium Policy Execution service.	This step is required. If your system architecture contains more than one APM Server, you must complete this step for every server that you want to use for policy execution.
6	Configure the settings for the Policy Trigger Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
7	On the APM Server, stop and restart the Meridium Policy Trigger service.	This step is required. If your system architecture contains more than one APM Server, you must start the Policy Trigger Service on at least one APM Server.
8	On the APM Server, reset IIS.	This step is required only if you have modified the time out value for the Math node execution or Policy Execution in the `appSettings.json` configuration file.
9		This step is required. If your database contained policies with execution schedules containing invalid times for the most recent Next Date or Last Date (for example, between 2:00 A.M. and 3:00 A.M. on the morning of daylight savings time), these fields were left blank during the upgrade. To ensure that your scheduled policies execute as expected, review the log, and update policy schedules in Policy Designer as needed.

- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Configure the time limit for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the policy execution time limit for the Policy Execution Service. By default, the policy execution time limit is 15 minutes per policy instance.
2	Configure the time limit for the execution of the Math node.	This step is optional. You can perform this step if you want to modify the Math node execution time limit for the Policy Execution Service. By default, the Math node execution time limit is 5 minutes.
3	Configure the alternative query for the **Policy Designer Overview** page.	This step is optional. You can perform this step if you are facing performance issues with the **Policy Designer Overview** page.
4	Configure the settings for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the default retries, concurrency, or duplicate trigger timeout settings.
5	On the APM Server, stop and restart the Meridium Policy Execution service.	This step is required. If your system architecture contains more than one APM Server, you must complete this step for every server that you want to use for policy execution.
6	Configure the settings for the Policy Trigger Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
7	On the APM Server, stop and restart the Meridium Policy Trigger service.	This step is required. If your system architecture contains more than one APM Server, you must start the Policy Trigger Service on at least one APM Server.

Step	Task	Notes
8	On the APM Server, reset IIS.	This step is required only if you have modified the time out value for the Math node execution or Policy Execution in the `appSettings.json` configuration file.
9		This step is required. If your database contained policies with execution schedules containing invalid times for the most recent Next Date or Last Date (for example, between 2:00 A.M. and 3:00 A.M. on the morning of daylight savings time), these fields were left blank during the upgrade. To ensure that your scheduled policies execute as expected, review the log, and update policy schedules in Policy Designer as needed.

- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Configure the time limit for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the policy execution time limit for the Policy Execution Service. By default, the policy execution time limit is 15 minutes per policy instance.
2	Configure the time limit for the execution of the Math node.	This step is optional. You can perform this step if you want to modify the Math node execution time limit for the Policy Execution Service. By default, the Math node execution time limit is 5 minutes.
3	Configure the alternative query for the **Policy Designer Overview** page.	This step is optional. You can perform this step if you are facing performance issues with the **Policy Designer Overview** page.
4	Configure the settings for the Policy Execution Service.	This step is optional. You can perform this step if you want to modify the default retries, concurrency, or duplicate trigger timeout settings.
5	On the APM Server, stop and restart the Meridium Policy Execution service.	This step is required. If your system architecture contains more than one APM Server, you must complete this step for every server that you want to use for policy execution.
6	Configure the settings for the Policy Trigger Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.

Step	Task	Notes
7	On the APM Server, stop and restart the Meridium Policy Trigger service.	This step is required. If your system architecture contains more than one APM Server, you must start the Policy Trigger Service on at least one APM Server.
8	On the APM Server, reset IIS.	This step is required only if you have modified the time out value for the Math node execution or Policy Execution in the `appSettings.json` configuration file.
9		This step is required. If your database contained policies with execution schedules containing invalid times for the most recent Next Date or Last Date (for example, between 2:00 A.M. and 3:00 A.M. on the morning of daylight savings time), these fields were left blank during the upgrade. To ensure that your scheduled policies execute as expected, review the log, and update policy schedules in Policy Designer as needed.

About the Asset Health Services

When you deploy the Asset Health Manager, OT Connect, and Policy Designer modules together, the services used by each module interact with each other in various ways. This topic summarizes those services and describes a standard system architecture containing the components used by all three modules.

Services Summary

The following services are used by the Asset Health Manager, OT Connect, and Policy Designer modules:

- Asset Health Indicator Service: Automatically updates the following field values in a Health Indicator record when reading values related to the health indicator source record (for example, an OT Source Tag or Measurement Location record) change:
  - Alert Level
  - Last Reading Date
  - Last Char Reading Value (for records that accept character values)
  - Last Numeric Reading Value (for records that accept numeric values)

  This service also facilitates the automatic creation of Health Indicator records for configured sources.
- Policy Trigger Service: When an input to a policy (that is, an associated record in the APM database or reading value in the process historian) changes, when a policy schedule is due, or a user submits an Execute Now request, a message is added to the policy trigger queue. The Policy Trigger Service monitors the trigger queue. When it receives a message, it determines which policy instances should be executed for the message, and then it

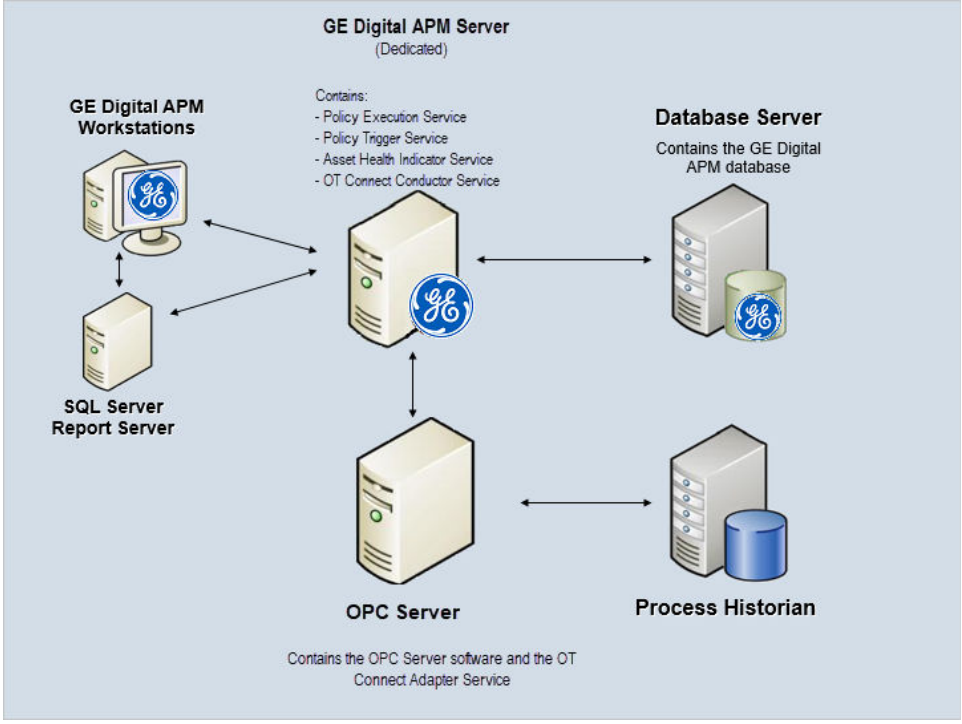
sends corresponding messages to the policy execution queue. Even if your APM system is configured with multiple Policy Execution servers, only one policy execution queue is used.

- Policy Execution Service: The Policy Execution Service handles the execution of policies. Specifically, the Policy Execution Service monitors the policy execution queue and executes the policy instances that are added to it. If the APM system is configured with multiple Policy Execution servers, when each Policy Execution Service completes the execution of a policy instance, it will execute the next instance from the shared policy execution queue. In this way, the policy execution load is automatically balanced across all available Policy Execution Services.
- OT Connect Service: Monitors the subscribed tags (that is, tags that are used in policies and health indicators) and when data changes occur on these tags adds messages to the appropriate queues. This service also facilitates the automatic import and synchronization of tags from a configured OT Source. For more information, refer to the OT Connect section of the documentation.

Standard System Architecture Configuration

The following diagram illustrates the machines in the APM system architecture when the Policy Designer, OT Connect, and Asset Health Manager (AHM) modules are used together. This image depicts the standard configuration, where the OPC Server software and the OT Connect Adapter Service are on the same machine.

Note: In this example configuration, only one machine of each type is illustrated. Your specific architecture may include multiple APM Servers, multiple OPC Servers, or multiple APM Servers used for policy executions.



The following table summarizes the machines illustrated in this diagram and the software and services that you will install when you complete the first-time deployment steps for Asset Health Manager, OT Connect, and Policy Designer.

Machine	Software Installed	Service Installed with APM Software
APM Server	APM Server software	Asset Health Indicator Service
		Policy Trigger Service
		Policy Execution Service
		OT Connect Conductor Service
OPC Server	GE Vernova OT Connect Adapter software	OT Connect Adapter Service
	OPC Server software	N/A
Process Historian	Process historian software	N/A

About Policy Execution

Policy designers can configure a policy to be executed on a schedule or automatically when records or reading values associated with the policy are updated. Policies may also be executed on demand. This topic describes the ways that the items configured in the first-time deployment workflow facilitate each type of policy execution.

Note: Only the active instances of active policies are executed.

Automatic Execution

When any record or reading value is updated by the APM Server, or when a reading value for a tag associated with one or more policies is updated on the process historian, a message is added to the policy trigger queue. The Policy Trigger Service monitors the trigger queue. When it receives a message, it determines which policy instances should be executed for the message, if any. Only active policy instances associated with the record or reading update will be executed. The Policy Trigger Service then sends corresponding messages to the policy execution queue for each relevant policy instance. Finally, a Policy Execution Service executes each policy instance that was added to the policy execution queue in turn.

Scheduled Execution

When a scheduled policy is due, a scheduled job adds a message to the policy trigger queue. The Policy Trigger Service monitors the trigger queue and sends messages to the policy

execution queue for each active instance of the policy. Finally, a Policy Execution Service executes each active instance that was added to the policy execution queue in turn.

On Demand Execution

When you request a policy or policy instance execution from the Policy Designer user interface, or select a hyperlink configured to execute a policy or policy instance, a message is added to the policy trigger queue. The Policy Trigger Service monitors the trigger queue and sends messages to the policy execution queue for each active instance of the policy. Finally, a Policy Execution Service executes each active instance that was added to the policy execution queue in turn.

Configure Queue Settings for Policy Execution Service

About This Task

The Policy Execution Service on each APM Server is configured to use a single shared ActiveMQ queue service. Available queue configuration options include retries, redelivery attempts and interval, and concurrency limit.

Procedure

1. On the APM Server, access the folder that contains the Policy Execution Service files.

   Note: If you have installed APM in the default location, you can locate the folder in `C:\Program Files\Meridium\ApplicationServer\policy-execution`.
2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).
3. In the file, locate the following text:

```
"notificationMessageSettings": {
  "concurrencyLimit": 16,
  "retries": 10,
  "redeliveryAttempts": 3,
  "redeliveryMinInterval": 1,
  "redeliveryMaxInterval": 2440,
  "redeliveryDelta": 5
},
"executionMessageSettings": {
  "concurrencyLimit": 8,
  "retries": 5,
  "redeliveryAttempts": 3,
  "redeliveryMinInterval": 1,
  "redeliveryMaxInterval": 2440,
  "redeliveryDelta": 5
}
```

4. Update the key values as desired.
5. Save and close the file.
   The updated settings will be applied when the Meridium Policy Execution service is stopped and restarted.

Configure Queue Settings for Policy Trigger Service

About This Task

The Policy Trigger Service is configured to use a single shared ActiveMQ queue service. Queue configuration options include retries, redelivery attempts and interval, concurrency limit, and duplicate Measurement Location reading trigger elimination timeout.

Procedure

1. On the APM Server, access the folder that contains the Policy Trigger Service files.

   Note: If you have installed APM in the default location, you can locate the folder in `C:\Program Files\Meridium\ApplicationServer\policy-trigger`.
2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).
3. In the file, locate the following text:

```
 "DuplicateTriggerTimeout": 5000,

"notificationMessageSettings": {
  "concurrencyLimit": 16,
  "retries": 10,
  "redeliveryAttempts": 3,
  "redeliveryMinInterval": 1,
  "redeliveryMaxInterval": 2440,
  "redeliveryDelta": 5
},
"triggerMessageSettings": {
  "concurrencyLimit": 16,
  "retries": 5,
  "redeliveryAttempts": 3,
  "redeliveryMinInterval": 1,
  "redeliveryMaxInterval": 2440,
  "redeliveryDelta": 5
},
"readingMessageSettings": {
  "concurrencyLimit": 16,
  "retries": 5,
  "redeliveryAttempts": 3,
  "redeliveryMinInterval": 1,
  "redeliveryMaxInterval": 2440,
  "redeliveryDelta": 5
}
```

4. Update the key values as desired.
5. Save and close the file.
   The updated settings will be applied when the Meridium Policy Trigger service is stopped and restarted.

Configure the Time Limit for Policy Execution

About This Task

The Policy Execution Service limits the amount of time allocated to execute each policy instance. This ensures that the Policy Execution Service queue is not backlogged when a poorly designed policy takes too long to execute. If a policy execution is canceled as a result of the time limit, an error message appears in the policy execution history indicating that the time limit was exceeded. By default, the policy execution time limit is set to 15 minutes per policy instance. The minimum time limit is 1 minute, and the maximum time limit is 1 hour. This topic describes how to modify the Policy Execution Service configuration to change the time limit for policy execution.

Procedure

1. On the APM Server, access the folder that contains the Policy Execution Service files.

   Note: If you have installed APM in the default location, you can locate the folder in the following directory:

   `C:\Program Files\Meridium\ApplicationServer\policy-execution`
2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).
3. In the file, locate the following text:

   ```
   "PolicyExecutionTimeoutMs": 900000
   ```
4. Replace `900000` with the time limit value in milliseconds, that you want to apply to policy executions.

   Note: The value you enter should be between the minimum time limit of 60000 milliseconds (that is, 1 minute) and the maximum time limit of 3600000 milliseconds (that is, 1 hour).
5. Save and close the file.
   The modified settings are applied when the Policy Execution Service is restarted. If the execution time of a policy instance exceeds the time limit that you have specified, the execution is canceled, and an error message is added to the policy execution history.
6. On the APM Server, access the folder that contains the Meridium configuration files.

   Note: If you have installed APM in the default location, you can locate the folder in the following directory:

   `C:\Program Files\Meridium`
7. Go to `C:\Program Files\Meridium\ApplicationServer\api`.
8. Access the `appsettings` file in an application that can be used to modify JSON files (for example, Notepad++).
9. Repeat steps 3 through 5.
   The modified settings are applied when Meridium Policy Execution service is stopped and restarted on each policy execution server and IIS is reset on the APM Server.

Configure Execution Time Out Value for Math Node

About This Task

If the execution of a Math node in a policy takes a very long time, the execution times out after a pre-defined duration. By default, the execution times out after 1 minute. However, you can configure the interval after which the execution must time out for the Math node.

Procedure

1. On the Policy Execution Server, go to `C:\Program Files\Meridium \ApplicationServer\policy-execution`.
2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).
3. In the file, locate the following text:

   ```
   "MathNodeExecutionTimeout": 60000
   ```

4. Replace `60000` with the interval value in milliseconds at which the execution of the Math node must time out.
5. Save and close the file.
6. On the APM Server, go to `C:\Program Files\Meridium\ApplicationServer\api`.
7. Access the `appsettings` file in an application that can be used to modify JSON files (for example, Notepad++).
8. Repeat steps 3 through 5.
   The updated settings will be applied when the Policy Execution Service is stopped and restarted on the Policy Execution Server and IIS is reset on the APM Server.

Configure the Default Historical Readings Time Range for the OT Connect Tag node

About This Task

During policy execution, if a specific time range to retrieve the historical data for the OT Connect Tag node cannot be determined. For example, if there is no collection filter applied to the Historical Readings output from the node, by default, two years of data will be added. However, you can change the default time range by modifying the settings on the Policy Execution Server and APM Server.

Procedure

1. On the Policy Execution Server, go to `C:\Program Files\Meridium \ApplicationServer\policy-execution`.
2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example; Notepad++).
3. In the file, locate the following text:

   ```
   "DefaultHdaTimeRangeYrs": 2
   ```

4. Replace `2` with the number of years for which you want to retrieve the historical data of the OT Connect Tag node.
5. On the APM Server, go to `C:\Program Files\Meridium\ApplicationServer\api`.
6. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).
7. Repeat steps 3 through 5.
   The updated settings will be applied when the Policy Execution Service is restarted on the Policy Execution Server and IIS is reset on the APM Server.

Delete Duplicate Policies from the APM Database

About This Task

If you are upgrading from any version V4.0.0.0.0 through 4.3.0.7.0, the APM database may contain duplicate records of a family policy configured for the same family and trigger. You may face issues while working with the family policies because of such duplicate records. While upgrading APM to the latest version, you must identify and delete the duplicate records that exist for the same family and trigger.

Procedure

1. Run the following query on your database to identify any duplicate family policy records that exist for the same family and trigger:

```
SELECT MI_FAMPOLICY_FMLY_ID_CHR,MI_FAMPOLICY_TRIGGER_C, count(*)
FROM MI_FAMPOLICY
GROUP BY MI_FAMPOLICY_FMLY_ID_CHR,MI_FAMPOLICY_TRIGGER_C
HAVING COUNT(*) > 1;
```

2. Identify the correct records that must be retained in the database, and then delete the unwanted duplicate records.

Configure Alternative Query for the Policy Designer Overview Page

About This Task

To optimize the performance of the **Policy Designer Overview** page in the systems with a large volume of policy execution history records, the Policies tab displays a simplified view which does not display the latest policy execution results. If you want to see the latest results in the Policies list, you can configure the **Policy Designer Overview** page to use the alternative query (Policy Overview – Policies Alternate Query) that is provided in the APM Catalog.

Note: When you configure an alternative query for **Policy Designer Overview** page, you might face some performance issues.

Procedure

1. Access the APM using the super user account.
2. Access the **Catalog** page.

3. In the **Catalog** section, select **Public** > **Meridium** > **Modules** > **Policy Manager** > **Queries**.
   The **Queries** workspace appears, displaying the catalog items of the Queries folder in a table.
4. Select the check box corresponding to the Policy Overview – Policies query.
5. In the same row, select .
   The **Catalog Item Properties** window appears, displaying the properties of the Policy Overview – Policies query.
6. In the **Name** box, modify the value to rename the query.
7. Select **Done**.
   The Policy Overview – Policies query is renamed.
8. Select the check box corresponding to the alternative query (Policy Overview – Policies Alternate Query).
9. In the same row, select .
   The **Catalog Item Properties** window appears, displaying the properties of the alternative query.
10. In the **Name** box, delete the existing value, and then enter `Policy Overview – Policies`.
11. Select **Done**.
    The alternative query is configured for the **Policy Designer Overview** page.

Configure Multiple APM Servers for Policy Execution

Depending on the number of policies that you need to manage in your system, you may have multiple APM Servers to process policy executions. Based on your company preference for server load balancing, you can configure these servers using global load balancing or isolated load balancing.

Regardless of the approach you use, you must fully configure each APM Server according to the steps for deploying the basic APM system architecture. In addition, each APM Server must be configured to use the same instance of Redis and ActiveMQ.

Global Load Balancing

In global load balancing, you configure all APM Servers to process policy executions in a single load-balanced cluster. In this scenario, an increase in policy execution demand can be absorbed across all servers in your system architecture.

In this scenario, you must:

- Configure and start the Policy Trigger Service on at least one APM Server.
- Configure and start the Policy Execution Service on all APM Servers.

Isolated Load Balancing

In isolated load balancing, you configure designated APM Server(s) to process policy executions. In this scenario, the policy execution processes are isolated from other APM Server processes, therefore preventing an increase in policy execution activity from negatively impacting other processes.

In this scenario, you must:

- Configure and start the Policy Trigger service on at least one APM Server.

- Configure and start the Policy Execution Service on only the APM Servers that you want to use to process policy executions.

Production Loss Analysis

Deploy PLA for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Review the PLA data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to one or more of the Production Loss Analysis Security Groups and Roles.	This step is required. Users must have permissions to the PLA families to use the PLA functionality.
3	Change the default currency symbol.	This step is optional. By default, the currency symbol is set to $ and appears in the following places: • Default Margin field on the Production Profile datasheet. • **Production Summary** workspace.
4	Define all products.	This step is required. You must define all products whose production you plan to track using PLA. Each product is stored in a Product record.

Step	Task	Notes
5	Define Production Units.	This step is required. You must identify the Production Units that produce the products you defined in the previous task. A single product can be produced by more than one Production Unit. A single Production Unit can also produce more than one product. Each Production Unit is stored in a Production Unit record, which can be linked to an existing Functional Location record that contains detailed information about the Production Unit.
6	Define Production Profiles.	This step is required. For each Production Unit that you defined in the previous step, you must identify all the products that it produces and information about those products, such as the maximum demonstrated rate of production and the amount of profit one of those products yields. The combination of data about a product and the corresponding Production Unit is the Production Profile for that Production Unit. A Production Unit will have one Production Profile for each product it produces. Each Production Profile is stored in a Production Profile record, which is linked to the corresponding Product record and Production Unit record.

Step	Task	Notes
7	Define Production Event Codes.	The baseline APM database contains Production Event Code records that define a set of basic production event codes. Therefore, this step is required only if you do not want to use the baseline production event codes or if you want to use codes in addition to those that are provided. You must use Production Event Codes to categorize the types of events that can cause you to produce less than the maximum sustained capacity amount. Production Event Codes define the cause of lost production and answer the question: Why are we losing production? You can also group the types of events by structuring them in a hierarchy. For example, you might group event types into planned and unplanned, where planned events are events such as maintenance down days or employee holidays, and unplanned events are events such as equipment failures or natural disasters (e.g., floods or hurricanes). Each production event code will be stored in a separate Production Event Code record.
8	Define Impact Codes.	The baseline APM database contains Impact Code records that define a set of basic Impact Codes. Therefore, this step is required only if you do not want to use the baseline Impact Codes or if you want to use codes in addition to those that are provided.
9	Define OEE Codes.	The baseline APM database contains OEE Code records that define a set of basic OEE Codes. Therefore, this step is required only if you do not want to use the baseline OEE Codes or if you want to use codes in addition to those that are provided. For non-baseline codes to be included in the OEE Metric View, however, they must be children of the baseline parent codes.

Step	Task	Notes
10	Configure PLA for for OT Connect integration: 1. Deploy OT Connect. **Note:** Deploying OT Connect requires the OT Connect license. 2. Configure the PLA Service policy. 3. Link Production Profile records to Policy Instance ID records.	This step is required if you want to use the integration between PLA and the OT Connect feature where Production Data records are created automatically using the baseline PLA Service policy in Policy Designer.
11	Replace the Top 10 Bad Actors query for the **PLA Overview** page.	This step is optional. The Top 10 Bad Actors query is used by APM to populate the **Top 10 Bad Actors** graph on the **PLA Overview** page. In some databases, when viewing this graph, you may receive an error that prevents the graph from populating correctly. If this error occurs, replace the Top 10 Bad Actors query.

Upgrade or Update PLA to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

Note: A new field, RCA Needed, has been added to the Production Event family. For records created before upgrading to V4.3.0.6.0, the default value in this field is No Entry.

- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	Replace the Top 10 Bad Actors query for the **PLA Overview** page.	This step is optional. The Top 10 Bad Actors query is used by APM to populate the **Top 10 Bad Actors** graph in the **PLA Overview** page. In some databases, when accessing this graph, you may receive an error that prevents the graph from populating correctly. If this error occurs, replace the Top 10 Bad Actors query.

- Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	Replace the Top 10 Bad Actors query for the **PLA Overview** page.	This step is optional. The Top 10 Bad Actors query is used by APM to populate the **Top 10 Bad Actors** graph in the **PLA Overview** page. In some databases, when accessing this graph, you may receive an error that prevents the graph from populating correctly. If this error occurs, replace the Top 10 Bad Actors query.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

Step	Task	Notes
1	Confirm the deployment of the Production Data cube and Equipment Costs Data cube in the SQL Server Analysis Server.	This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube in the SQL Server Analysis Server in V3.6.0.0.0.
2	Set the time zones for the Production Units.	This step is required. If the time zones for the Production Units are set, all the Production Plan records, Plan Data records, and Production Target records will be updated based on the time zone for the respective Production Unit. **Note:** Since the date and time in PLA is now stored in UTC format, you must set the time zone for each Production Unit before upgrade. ◦ If you do not set the time zones for the Production Units and if the Production Plan records exist in the database, the Production Plan records, Plan Data records, and Production Target records will be updated based on the time zone of the user who last modified the Production Plan record. ◦ If you do not set the time zones for the Production Units and if the Production Plan records do not exist in the database, the time zone for the Production Unit will be updated based on the time zone of the user who last modified the Production Unit record.

- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

Step	Task	Notes
1	Confirm the deployment of the Production Data cube and Equipment Costs Data cube in the SQL Server Analysis Server.	This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube in the SQL Server Analysis Server in V3.6.0.0.0.
2	Set the time zones for the Production Units.	This step is required. If the time zones for the Production Units are set, all the Production Plan records, Plan Data records, and Production Target records will be updated based on the time zone for the respective Production Unit. **Note:** Since the date and time in PLA is now stored in UTC format, you must set the time zone for each Production Unit before upgrade. ◦ If you do not set the time zones for the Production Units and if the Production Plan records exist in the database, the Production Plan records, Plan Data records, and Production Target records will be updated based on the time zone of the user who last modified the Production Plan record. ◦ If you do not set the time zones for the Production Units and if the Production Plan records do not exist in the database, the time zone for the Production Unit will be updated based on the time zone of the user who last modified the Production Unit record.

- Upgrade from any version V3.5.1 through V3.5.1.12.3

Step	Task	Notes
1	Import the required baseline rules in the APM Server.	**Important:** This step is required and must be completed before upgrading the APM Server and Add Ons software on APM. After completing this step, you should return to the upgrade APM workflow. Then, after completing the remainder of the upgrade APM workflow, when you are ready to upgrade PLA, proceed to Step 2 in this workflow.
2	Confirm the deployment of the Production Data cube and Equipment Costs Data cube in the SQL Server Analysis Server.	This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube in the SQL Server Analysis Server in V3.5.1.

- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

Step	Task	Notes
1	Import the required baseline rules in the APM Server.	**Important:** This step is required and must be completed before upgrading the APM Server and Add Ons software on APM. After completing this step, you should return to the upgrade APM workflow. Then, after completing the remainder of the upgrade APM workflow, when you are ready to upgrade PLA, proceed to Step 2 in this workflow.
2	Confirm the deployment of the Production Data cube and Equipment Costs Data cube in the SQL Server Analysis Server.	This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube in the SQL Server Analysis Server in V3.5.0. SP1 LP.

- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Import the required baseline rules in the APM Server.	**Important:** This step is required and must be completed before upgrading the APM Server and Add Ons software on theAPM. After completing this step, you should return to the upgrade APM workflow. Then, after completing the remainder of the upgrade APM workflow, when you are ready to upgrade PLA, proceed to Step 2 in this workflow.
2	Confirm the deployment of the Production Data cube and Equipment Costs Data cube in the SQL Server Analysis Server.	This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube in the SQL Server Analysis Server in V3.5.0.

- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Import the required baseline rules in the APM Server.	**Important:** This step is required and must be completed before upgrading the APM Server and Add Ons software on APM. After completing this step, you should return to the upgrade APM workflow. Then, after completing the remainder of the upgrade APM workflow, when you are ready to upgrade PLA, proceed to Step 2 in this workflow.
2	Define OEE codes.	This step is required only if you want to use custom OEE Codes instead of or in addition to the baseline OEE Codes that are provided in the APM database. If you do, you will need to create custom OEE codes to identify the types of losses you can incur. Each OEE Code will be stored in an OEE Code record.
3	Define values that will be mapped to a Production Analysis.	By default, certain PLA values are mapped to the production data in a Production Analysis. This step is required only if you want to map different or additional PLA values. If you do, you will need to modify the All Production Data query.
4	Confirm the deployment of the Production Data cube and Equipment Costs Data cube in the SQL Server Analysis Server.	This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube in the SQL Server Analysis Server in V3.4.5.

Import Baseline Rules

Before You Begin

Note: If you are upgrading Production Loss Analysis from a starting version that is earlier than V3.6.0.0.0, this procedure must be completed before upgrading the Meridium Enterprise APM Server and Add Ons software on the Meridium Enterprise APM Server(s). This procedure is part of the upgrade APM and upgrade Production Loss Analysis workflows.

- Acquire a copy of the baseline APM database whose version number matches the version number of your current, pre-upgraded database. If you do not have access to the appropriate baseline database, consult a member of the APM Professional Services department.

Procedure

1. On the APM Server, via the Windows start button, access Configuration Manager.

   The **Meridium APM Login** window appears.

2. Enter your User ID and Password into the appropriate boxes, and then, in the **Data Source** box, select the baseline APM database whose version number matches the version number of your current, pre-upgraded database.
3. Select **Login**.

   Configuration Manager opens.
4. On the top navigation bar, select **Tools**, and then select **Import/Export Meridium Metadata**.

   The **Import/Export Metadata** window appears.
5. Select the **Export** check box, and then select **Select File**.

   The **Save As** window appears.
6. Navigate to the location where you want to save the exported metadata, then enter a name in the **File name:** box, and then select **Save**.

   The **Save As** window closes, and the selected filepath is displayed in the **Select File** box on the **Import/Export Metadata** window.
7. Select the **Selection** check box.
8. In the drop-down list box to the right of the **Family Rule Projects** check box, select **Some**.

   The **Select Rule Projects to Export** window appears.
9. In the **Available Items** section, select the item whose Family Caption is Production Event, and then select .

   The selected item appears in the **Selected Items** section.
10. In the **Available Items** section, select the item whose Family Caption is Production Profile, and then select .

    The selected item appears in the **Selected Items** section.
11. Select **OK**.

    The **Select Rule Projects to Export** window closes, and, on the **Import/Export Metadata** window, the **Family Rule Projects** check box is selected automatically.
12. Select **Export**.

    The **Metadata Import/Export Status** dialog box appears, displaying a progress bar. When the export is complete, a message appears, asking if you want to save the log.
13. Select **Save Log**.

    The **Save As** window appears.
14. Navigate to the location where you want to save the export log, then enter a name in the **File name:** box, and then select **Save**.

    The **Save As** window closes.
15. On the **Metadata Import/Export Status** dialog box, select **Close**.

    The **Metadata Import/Export Status** dialog box closes.
16. On the **Import/Export Metadata** window, select **Close**.

    The **Import/Export Metadata** window closes.
17. In Configuration Manager, on the top navigation bar, select **File**, and then select **LogOff**.

    A dialog box appears, asking if you are sure that you want to log off.
18. Select **OK**.

Configuration Manager closes.

19. On the Meridium Server machine, via the Windows start button, access Configuration Manager.

    The **Meridium APM Login** window appears.

20. Enter your User ID and Password into the appropriate boxes, and then, in the **Data Source** box, select your current, pre-upgraded database.
21. Select **Login**.

    Configuration Manager opens.

22. On the top navigation bar, select **Tools**, and then select **Import/Export Meridium Metadata**.

    The **Import/Export Metadata** window appears.

23. Select **Select File**.

    The **Open** window appears.

24. Navigate to and select the file that you saved in step 6, and then select **Open**.

    The **Open** window closes, and the selected filepath is displayed in the **Select File** box on the **Import/Export Metadata** window.

25. Select the **Selection** check box.
26. In the drop-down list box to the right of the **Family Rule Projects** check box, select **Some**.

    The **Select Rule Projects to Import** window appears.

27. In the **Available Items** section, select the item whose Family Caption is Production Event, and then select .

    The selected item appears in the **Selected Items** section.

28. In the **Available Items** section, select the item whose Family Caption is Production Profile, and then select .

    The selected item appears in the **Selected Items** section.

29. Select **OK**.

    The **Select Rule Projects to Import** window closes, and, on the **Import/Export Metadata** window, the **Family Rule Projects** check box is selected automatically.

30. Select **Import**.

    The **Metadata Import/Export Status** dialog box appears, displaying a progress bar. When the import is complete, a message appears, asking if you want to save the log.

31. Select **Save Log**.

    The **Save As** window appears.

32. Navigate to the location where you want to save the import log, then enter a name in the **File name:** box, and then select **Save**.

    The **Save As** window closes.

33. On the **Metadata Import/Export Status** dialog box, select **Close**.

    The **Metadata Import/Export Status** dialog box closes.

34. On the **Import/Export Metadata** window, select **Close**.

    The **Import/Export Metadata** window closes.

35. In Configuration Manager, in the left pane, select the **Production Event** folder.

36. In the **Tasks** section of the workspace, select **Compile Family**.

    The **Family Compile** window appears.

37. In the **Family Compile** window, select **Compile**.

    In the **Family Compile** window, a progress bar appears, and successfully compiled families appear in a list as the operation progresses.

38. When the progress bar reaches the end, select **Close**.

    The **Family Compile** window closes.

39. In Configuration Manager, in the left pane, select the **Production Profile** folder, and then repeat steps 36 through 38.

    The necessary baseline rules have been imported into your current, pre-upgraded database.

Replace the Top 10 Bad Actors Query

About This Task

Note: The steps in this section are required only if you are upgrading from a version of Meridium Enterprise APM between V4.0.0.0 and V4.1.7.4.0.

The **Top 10 Bad Actors** query is used by APM to populate the **Top 10 Bad Actors** graph on the **Production Loss Analysis Overview** page. In some databases, when viewing this graph, you may receive the following error:

To implement the corrected query and to correct this error, complete the following steps.

Procedure

1. Access the **Query** page
2. In the heading of the **Query** page, select **Browse**.

   The **Select a query from the catalog** window appears.
3. In the left pane, navigate the **Catalog** to: `Meridium/Public/Modules/PLA/Queries`, select the **Top10BadActors** query and then select **Open.**

   The **Enter Parameter Values** window appears.
4. Select **OK**.

   Note: For the purposes of these instructions, you do not need to complete any fields in the **Enter Parameter Values** window.

   The **Top 10 Actors** query page appears, displaying the **Results** tab.
5. Select the **SQL** tab.

   The SQL query text appears in the workspace, displaying the current query.
6. In the SQL workspace, select and delete the current query text.
7. In the blank SQL workspace, copy and paste the following query text:

```
                    SELECT TOP 10 SUM(LossAmount) "Loss Amount" ,
AssetID "Asset ID" FROM
                    (
                    SELECT  DISTINCT [MI_PRDNLOSS].ENTY_KEY
```

```
"ENTY_KEY", [MI_PRDNLOSS].[MI_PRDNLOSS_LOSS_AMOUNT_N] "LossAmount",
[MI_EQUIP000].[MI_EQUIP000_EQUIP_TECH_NBR_C] "AssetID" FROM
[MI_EQUIP000], [MI_PRDNLOSS] JOIN_SUCC [MI_PRDNEVNT] ON
{MIR_CBPRDEVN} WHERE ([MI_PRDNEVNT].[MI_PRDNEVNT_START_DATE_D] >=
MI_DateAdd('dd', ((? :s :id=numofdays) * -1), Now()) AND
[MI_PRDNEVNT].[MI_PRDNEVNT_END_DATE_D] <= MI_DateAdd('dd', 1, Now())
AND [MI_PRDNEVNT].[MI_PRDNEVNT_CAUSE_EQP_KEY_N] IN
((? :ah :id=enty_key :child :all :current))  AND
[MI_EQUIP000].ENTY_KEY = [MI_PRDNEVNT].
[MI_PRDNEVNT_CAUSE_EQP_KEY_N]) and [MI_EQUIP000].
[MI_EQUIP000_EQUIP_TECH_NBR_C] is not null
                    UNION
                    SELECT DISTINCT  [MI_PRDNLOSS].ENTY_KEY
"ENTY_KEY", [MI_PRDNLOSS].[MI_PRDNLOSS_LOSS_AMOUNT_N] "LossAmount",
[MI_FNCLOC00].[MI_FNCLOC00_FNC_LOC_C] "AssetID" FROM [MI_FNCLOC00],
[MI_PRDNLOSS] JOIN_SUCC [MI_PRDNEVNT] ON {MIR_CBPRDEVN} WHERE
([MI_PRDNEVNT].[MI_PRDNEVNT_START_DATE_D] >= MI_DateAdd('dd',
((? :s :id=numofdays) * -1), Now()) AND [MI_PRDNEVNT].
[MI_PRDNEVNT_END_DATE_D] <= MI_DateAdd('dd', 1, Now()) AND
[MI_PRDNEVNT].[MI_PRDNEVNT_CAUSE_EQP_KEY_N] IN
((? :ah :id=enty_key :child :all :current))  AND
[MI_FNCLOC00].ENTY_KEY = [MI_PRDNEVNT].
[MI_PRDNEVNT_CAUSE_EQP_KEY_N]) and [MI_FNCLOC00].
[MI_FNCLOC00_FNC_LOC_C] is not null
                    ) Table1 GROUP BY AssetID  ORDER BY
Sum(LossAmount) Desc
```

8. On the right side of the page heading, select  .

   The new query text is saved.

Results

The corrected query will populate the **Top 10 Bad Actors** graph on the **Production Loss Analysis Overview** page.

R Scripts

R Scripts System Requirements

License Requirements

This feature is available with the core APM application; no specific license is required.

Additional Components Required

In addition to the basic APM system architecture, your system must also contain the following additional components:

- R Server: A machine on which the R Server software is installed. The software requirements of this server are determined by the third-party distributor of the software.

The APM testing environment uses the following:

- DeployR Open 8.0.0 with Microsoft DeployR Enterprise 8.0.0 or Microsoft Machine Learning Server 9.2.1 running on Windows servers
- Rserve 1.8-8 with R V4.1.3 running in Docker containers on Linux servers

Install R Server or Machine Learning Server

You can find more information about Microsoft R Server and Machine Learning Server, including required software dependencies and installation instructions, on https://msdn.microsoft.com/en-us/microsoft-r/rserver-install-windows.

Note: The World Wide Web Publishing service must be enabled on the R Server or Machine Learning Server in order to use R scripts in APM. If this setting is disabled during the installation of R Server, you must enable it.

Note: Microsoft DeployR 8.0.0 and Microsoft Machine Learning Server are out of support from Microsoft. You may continue to use these R servers with APM V4.6.0.0.0 however, we recommend migrating to open source Rserve and R. R Scripts will no longer support DeployR 8.0.0 or Machine Learning Server in APM future releases from V5.1.0.0.0 onwards.

Important: To ensure that the date and time values are handled as expected, the time zone of the Windows server where R Server or Machine Learning Server is installed must be set to UTC.

Install Rserve and R

About Rserve

Rserve is an open-source package that enables TCP/IP connections to R. Details about the Rserve package can be found at http://rforge.net/Rserve/.

Note: APM supports only two forms of Rserve authentication (refer to https://github.com/s-u/Rserve/wiki/Security):

- No authentication

- Plaintext password authentication

Install Rserve and R

Rserve and R can be installed on either Windows or Linux platforms; however, Linux is recommended.

Important: To ensure that the date and time values are handled as expected, the time zone of the Docker container running Rserve must be set to UTC.

GE Vernova has tested Rserve with R V4.1.3 running in a Docker container, using the images provided by the Rocker project (https://www.rocker-project.org/) as base images. The following sample Docker files can be used to build suitable containers:

SAMPLE MINIMAL DOCKERFILE:

```
FROM rocker/r-ver:4.1.3
# install Rserve
RUN install2.r --error \
    -r https://cran.rstudio.com \
    Rserve && \
    rm -rf /tmp/downloaded_packages/ /tmp/*.rds

ENTRYPOINT R -e "Rserve::run.Rserve()"
```

SAMPLE DOCKERFILE WITH SOME PACKAGES PRE-INSTALLED:

```
FROM rocker/r-ver:4.1.3
# install tidyverse
RUN /rocker_scripts/install_tidyverse.sh

# install tidymodels
RUN install2.r --error --skipinstalled tidymodels && \
    rm -rf /tmp/downloaded_packages

# install RcppArmadillo
RUN install2.r --error \
    -r https://cran.rstudio.com \
    RcppArmadillo && \
    rm -rf /tmp/downloaded_packages/ /tmp/*.rds

# install WeibullR
RUN install2.r --error \
    -r http://R-Forge.R-project.org \
    WeibullR && \
    rm -rf /tmp/downloaded_packages/ /tmp/*.rds

# install survival
RUN install2.r --error \
    -r https://cran.rstudio.com \
    survival && \
    rm -rf /tmp/downloaded_packages/ /tmp/*.rds

# install Rserve
RUN install2.r --error \
    -r https://cran.rstudio.com \
    Rserve && \
    rm -rf /tmp/downloaded_packages/ /tmp/*.rds

ENTRYPOINT R -e "Rserve::run.Rserve()"
```

Deploy R Scripts for the First Time

Before You Begin

After you have installed and configured the basic APM system architecture, including the R server of your choice, you will need to perform some configuration steps specifically for R Scripts.

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Ensure that your R Server is configured according to the R Scripts system requirements. For more information, refer to the APM System Requirements documentation.	This step is required.
2	In APM, specify the R Server credentials.	This step is required.

Upgrade or Update R Scripts to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

Step	Task	Notes
1.	Ensure that your R Server is configured according to the R Scripts system requirements. For more information, refer to the APM System Requirements documentation.	This step is required.
2.	In APM, specify the R Server credentials.	This step is required.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1.	Ensure that your R Server is configured according to the R scripts system requirements.	This step is required.
2.	In APM, specify the R Server credentials.	This step is required.

- Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1.	Ensure that your R Server is configured according to the R scripts system requirements.	This step is required.
2.	In APM, specify the R Server credentials.	This step is required.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

Step	Task	Notes
1.	Ensure that your R Server is configured according to the R scripts system requirements.	This step is required.
2.	In APM, specify the R Server credentials.	This step is required.

- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

Step	Task	Notes
1.	If you are upgrading directly from V3.6.0.8.0, run a script in order to upgrade R script metadata.	This step is required only if you are upgrading from V3.6.0.8.0. This step is not required if you are upgrading from any V3.x version that is covered by this section.
2.	Ensure that your R Server is configured according to the R scripts system requirements.	This step is required.
3.	In APM, specify the R Server credentials.	This step is required.

Upgrade R Script Metadata

About This Task

If you are upgrading directly from V3.6.0.8.0, after upgrading your database to V4.6.11.0.0, you must run a script in order to upgrade existing R script metadata. This step is not required if you are upgrading from any V3.x version other than V3.6.0.8.0.

Note: If you are unsure whether you need to complete this step, or if you would like assistance, please contact APM Support Teamhttps://digitalsupport.ge.com/.

Procedure

1. Copy the script corresponding to your type of database.

Oracle

```
                    -- select * from dbo.[MI_CTIT_RSCRIPTS]
                    UPDATE MI_CTIT_RSCRIPTS
                    SET CTIT_RSCR_DEFN_MEM =
REPLACE(CTIT_RSCR_DEFN_MEM, '"DataType":"n"', '"DataType":"N"');
                    UPDATE MI_CTIT_RSCRIPTS
                    SET CTIT_RSCR_DEFN_MEM =
REPLACE(CTIT_RSCR_DEFN_MEM, '"DataType":"c"', '"DataType":"C"');
                    UPDATE MI_CTIT_RSCRIPTS
                    SET CTIT_RSCR_DEFN_MEM =
REPLACE(CTIT_RSCR_DEFN_MEM, '"DataType":"d"', '"DataType":"D"');
                    UPDATE MI_CTIT_RSCRIPTS
                    SET CTIT_RSCR_DEFN_MEM =
REPLACE(CTIT_RSCR_DEFN_MEM, '"DataType":"l"', '"DataType":"L"');
```

SQL

```
                    -- select * from dbo.[MI_CTIT_RSCRIPTS]
                    UPDATE dbo.[MI_CTIT_RSCRIPTS]
                    SET CTIT_RSCR_DEFN_MEM =
CAST(REPLACE(CAST(CTIT_RSCR_DEFN_MEM as
NVarchar(MAX)),'"DataType":"n"', '"DataType":"N"') AS NText)
                    UPDATE dbo.[MI_CTIT_RSCRIPTS]
                    SET CTIT_RSCR_DEFN_MEM =
CAST(REPLACE(CAST(CTIT_RSCR_DEFN_MEM as
```

```
NVarchar(MAX)),'"DataType":"c"', '"DataType":"C"') AS NText)
                    UPDATE dbo.[MI_CTIT_RSCRIPTS]
                    SET CTIT_RSCR_DEFN_MEM =
CAST(REPLACE(CAST(CTIT_RSCR_DEFN_MEM as
NVarchar(MAX)),'"DataType":"d"', '"DataType":"D"') AS NText)
                    UPDATE dbo.[MI_CTIT_RSCRIPTS]
                    SET CTIT_RSCR_DEFN_MEM =
CAST(REPLACE(CAST(CTIT_RSCR_DEFN_MEM as
NVarchar(MAX)),'"DataType":"l"', '"DataType":"L"') AS NText)
```

2. Using SQL Server Management Studio (for SQL) or SQL Developer (for Oracle), run the script.

   The R script metadata is upgraded.

Specify R Server Credentials

Before You Begin

You must be a Super User or member of the MI Configuration Role security group to modify the R Server credentials.

Procedure

1. In the module navigation menu, select **Admin** > **Operations Manager** > **Connections**.
   The **Connections** page appears.
2. Select **R Server**.
   The **R Server** workspace appears.
3. In the **R Server Version** box, specify the version of R Server.
4. In the **Server Address** box, enter the URL of the R Server (for example, `http://MyRServer:7400/deployr`).
5. In the **User Name** and **Password** boxes, enter the user name and password that you want to use for the connection.
6. Select **Save**.
   The R Server credentials are saved.
7. Select **Perform Connection Test** to confirm that the connection is valid.

Reliability Analytics

Deploy Reliability Analytics for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Review the following data models to determine which relationship definitions you will need to modify to include your custom equipment and location families: • Probability Distribution Analysis Data Model • Production Analysis Data Model • Reliability Automation Rule Data Model • Reliability Distribution Analysis Data Model • Reliability Growth Analysis Data Model • Spares Analysis Data Model • System Reliability Analysis Data Model Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to one or more Reliability Analytics Security Groups and Roles.	This step is required.
3	Ensure that the Meridium Simulation Service is installed and running.	If the basic APM system architecture is already installed, the Meridium Simulation Service is automatically installed and run.

Upgrade or Update Reliability Analytics to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

Step	Task	Notes
1	Ensure that the Meridium Simulation Service is installed and running.	If the basic APM system architecture is already installed, the Meridium Simulation Service is automatically installed and run.
2	In the file `C:\ProgramData\Meridium\MeridiumAppSettings.xml`, within the `<appSettings>` element, add the following text: `<add key="simulationServiceUrl" value="net.tcp://{0}/Meridium/Reliability/SimulationService" />`	This step is required.

- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

Step	Task	Notes
1	Ensure that the Meridium Simulation Service is installed and running.	If the basic APM system architecture is already installed, the Meridium Simulation Service is automatically installed and run.
2	In the file `C:\ProgramData\Meridium\MeridiumAppSettings.xml`, within the `<appSettings>` element, add the following text: `<add key="simulationServiceUrl" value="net.tcp://{0}/Meridium/Reliability/SimulationService" />`	This step is required.

- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

Step	Task	Notes
1	Ensure that the Meridium Simulation Service is installed and running.	If the basic APM system architecture is already installed, the Meridium Simulation Service is automatically installed and run.
2	In the file `C:\ProgramData\Meridium\MeridiumAppSettings.xml`, within the `<appSettings>` element, add the following text: `<add key="simulationServiceUrl" value="net.tcp://{0}/Meridium/Reliability/SimulationService" />`	This step is required.

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

Step	Task	Notes
1	Ensure that the Meridium Simulation Service is installed and running.	If the basic APM system architecture is already installed, the Meridium Simulation Service is automatically installed and run.
2	In the file `C:\ProgramData\Meridium\MeridiumAppSettings.xml`, within the `<appSettings>` element, add the following text: `<add key="simulationServiceUrl" value="net.tcp://{0}/Meridium/Reliability/SimulationService" />`	This step is required.

- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

Step	Task	Notes
1	Ensure that the Meridium Simulation Service is installed and running.	If the basic APM system architecture is already installed, the Meridium Simulation Service is automatically installed and run.
2	In the file `C:\ProgramData\Meridium\MeridiumAppSettings.xml`, within the `<appSettings>` element, add the following text: `<add key="simulationServiceUrl" value="net.tcp://{0}/Meridium/Reliability/SimulationService" />`	This step is required.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	Ensure that the Meridium Simulation Service is installed and running.	If the basic APM system architecture is already installed, the Meridium Simulation Service is automatically installed and run.
2	In the file `C:\ProgramData\Meridium\MeridiumAppSettings.xml`, within the `<appSettings>` element, add the following text: `<add key="simulationServiceUrl" value="net.tcp://{0}/Meridium/Reliability/SimulationService" />`	This step is required.

- Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	Ensure that the Meridium Simulation Service is installed and running.	If the basic APM system architecture is already installed, the Meridium Simulation Service is automatically installed and run.
2	In the file `C:\ProgramData\Meridium\MeridiumAppSettings.xml`, within the `<appSettings>` element, add the following text: `<add key="simulationServiceUrl" value="net.tcp://{0}/Meridium/Reliability/SimulationService" />`	This step is required.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

Step	Task	Notes
1	Ensure that the Meridium Simulation Service is installed and running.	If the basic APM system architecture is already installed, the Meridium Simulation Service is automatically installed and run.
2	In the file `C:\ProgramData\Meridium\MeridiumAppSettings.xml`, within the `<appSettings>` element, add the following text: `<add key="simulationServiceUrl" value="net.tcp://{0}/Meridium/Reliability/SimulationService" />`	This step is required.

- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

Step	Task	Notes
1	Ensure that the Meridium Simulation Service is installed and running.	If the basic APM system architecture is already installed, the Meridium Simulation Service is automatically installed and run.
2	In the file `C:\ProgramData\Meridium\MeridiumAppSettings.xml`, within the `<appSettings>` element, add the following text: `<add key="simulationServiceUrl" value="net.tcp://{0}/Meridium/Reliability/SimulationService" />`	This step is required.

- Upgrade from any version V3.5.1 through V3.5.1.12.3

Step	Task	Notes
1	Ensure that the Meridium Simulation Service is installed and running.	If the basic APM system architecture is already installed, the Meridium Simulation Service is automatically installed and run.
2	In the file `C:\ProgramData\Meridium\MeridiumAppSettings.xml`, within the `<appSettings>` element, add the following text: `<add key="simulationServiceUrl" value="net.tcp://{0}/Meridium/Reliability/SimulationService" />`	This step is required.

- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

Step	Task	Notes
1	Ensure that the Meridium Simulation Service is installed and running.	If the basic APM system architecture is already installed, the Meridium Simulation Service is automatically installed and run.
2	In the file `C:\ProgramData\Meridium\MeridiumAppSettings.xml`, within the `<appSettings>` element, add the following text: `<add key="simulationServiceUrl" value="net.tcp://{0}/Meridium/Reliability/SimulationService" />`	This step is required.

- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Ensure that the Meridium Simulation Service is installed and running.	If the basic APM system architecture is already installed, the Meridium Simulation Service is automatically installed and run.
2	In the file `C:\ProgramData\Meridium\MeridiumAppSettings.xml`, within the `<appSettings>` element, add the following text: `<add key="simulationServiceUrl" value="net.tcp://{0}/Meridium/Reliability/SimulationService" />`	This step is required.

- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Configure the ability for users to create Reliability Distribution and Reliability Growth Analyses from Associated Pages.	This step is optional. This feature is new in V3.5.0, so even if you have deployed Reliability Analytics in V3.4.5, you will not have completed this step. You need to complete this step, however, only if you want to implement this functionality.
2	Ensure that the Meridium Simulation Service is installed and running.	If the basic APM system architecture is already installed, the Meridium Simulation Service is automatically installed and run.
3	In the file `C:\ProgramData\Meridium\MeridiumAppSettings.xml`, within the `<appSettings>` element, add the following text: `<add key="simulationServiceUrl" value="net.tcp://{0}/Meridium/Reliability/SimulationService" />`	This step is required.

Reliability Centered Maintenance

Deploy RCM for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Assign Security Users to one or more of the RCM Security Groups and Roles.	This step is required.
2	Review the RCM data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.

Upgrade or Update RCM to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

Step	Task	Notes
1	Prior to upgrading your database, review any RCM Analysis records that are linked to virtual assets. If you want any of those analyses to remain an analysis, link the associated virtual assets to the Asset Hierarchy prior to upgrading. In addition, for any analyses that are linked to both real and virtual assets, link all the virtual assets in the analysis to the Asset Hierarchy prior to upgrading.	This step is required only if your database has virtual assets linked to an RCM analysis, and you do not want the analysis to be converted to an analysis template on upgrading.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.0.0.0 through V4.0.1.0

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.1 through V3.5.1.12.3

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Assign Security Users to the MI RCM Viewer Security Group.	This step is required.
2	Add values to the Recommended Resource System Code Table.	This step is required. This System Code Table is used to populate the Recommended Resource field in RCM FMEA Recommendation records.

Reports

Deploy Reports for the First Time

Results

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Step	Task	Notes
1	Install the Reports Designer.	This step is required.
2	Set up the Reports Designer.	This step is required.

Upgrade or Update Reports to V4.6.11.0.0

About This Task

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.

- Upgrade from any version V4.0.0.0 through V4.0.1.0

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.1 through V3.5.1.12.3

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.

Install the APM Reports Designer

Before You Begin

- Install one of the following versions of Microsoft Visual Studio and the corresponding version of Microsoft SQL Server Data Tools (SSDT):

Visual Studio Version	SSDT Version
Microsoft Visual Studio 2017	Microsoft SQL Server Data Tools (SSDT) - Business Intelligence for Microsoft Visual Studio 2017 (15.8.0)
Microsoft Visual Studio 2019	Microsoft SQL Server Data Tools (SSDT) - Business Intelligence for Microsoft Visual Studio 2019

  - If you install SSDT for Microsoft Visual Studio 2019, install Microsoft Reporting Service Projects (VSIX 2.6.2). For more information on how to install Microsoft Reporting Services Projects (VSIX 2.6.2), refer to the Microsoft SSDT documentation.

  Note: The following versions of SSDT are supported with Microsoft SQL Server 2016:

  - 2017 (15.8.0)
  - 2019

Procedure

1. On the machine that will serve as the APM Reports Designer, access the APM Distribution package, and then navigate to the `Admin` folder.
2. Run `Setup.exe`.
   The **Meridium Admin - InstallShield Wizard** window appears.
3. Select **Next**.
   The **License Agreement** window appears.
4. Read the License Agreement and, if you agree, select the **I accept the terms of the license agreement** check box, and then select **Next**.
   The **Select Installation Location** window appears.
5. Select **Next** to accept the default location.
   The **Select the features you want to install** window appears.
6. Select **SSRS Data Processing extension for Visual Studio**, and then select **Next**.
   The **Complete the Installation** window appears.
7. Select **Install**.
   The **Setup Status** window appears, displaying a progress bar that shows the progress of the installation process.

   When the SSRS Data Processing extension for Visual Studio is installed, a message appears, indicating that the installation is complete.
8. Select **Finish**.
   The **Meridium Admin - InstallShield Wizard** window is closed.
9. As described in the following table, navigate to the paths corresponding to the Microsoft Visual Studio version installed in your system.

Visual Studio Version	Path
Microsoft Visual Studio 2017	`C:\Program Files (x86)\Microsoft Visual Studio\2017\Professional\Common7\IDE\CommonExtensions\Microsoft\SSRS`
Microsoft Visual Studio 2019	`C:\Program Files (x86)\Microsoft Visual Studio\2019\Professional\Common7\IDE\CommonExtensions\Microsoft\SSRS`

10. Open the `RSReportDesigner.config` file using a text editor (for example, Notepad).
11. Locate the following code in the configuration file, and then replace *{meridiumserver}* with the name of the APM server: `<ServerUrl>http://{meridiumserver}/meridium/api/</ServerUrl>`
12. Save the configuration file.

Results

The APM Report Designer is installed.

Set Up the APM Report Designer

After installing the APM Report Designer plugin, you must set up APM Report Designer to interact with APM Server.

Before You Begin

- Install the APM Report Designer.

Procedure

1. On the APM Server, open Microsoft Visual Studio.
2. On the **Tools** menu, select **Options**.
   The **Options** window appears.
3. On the **Options** window, in the left section, select **APM Report Designer**, and then select **General**.
   The **MeridiumServerURL** box appears in the right section.
4. In the **MeridiumServerURL** box, enter the Meridium Web Services URL in the following format:
   `http://<server_name>//meridium/api/`

   The APM Report Designer setup is complete.

Risk Based Inspection 580

Deploy RBI for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Review the RBI data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Modify any relationship definitions as needed via Configuration Manager.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to one or more of the Security Roles used in RBI.	This step is required.
3	On the APM Server, using Configuration Manager, import the following files • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml These files are located in the following folder: `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks`. You must extract the `4030000` archive from the `MI_DB_MASTER_4300000` archive.	This step is required only if you are deploying Risk Based Inspection on an existing APM database. These data mapping records are used in RBI 581 and Risk Based Inspection. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 000050619.

Step	Task	Notes
4	Assign the following types of RBI users to at least one TM Security Group: • Users who are responsible for completing the steps necessary to use TM Analysis values to calculate RBI 580 corrosion rates. • Users who should be able to navigate to TM via RBI 580.	This step is required only if you are using the integration between the RBI and Thickness Monitoring modules.
5	Modify the MI_DEGRADATION_MECHANISM_TYPES System Code Table.	This step is required only if you want to create your own Potential Degradation Mechanisms records.
6	Select the **Recommendation Creation Enabled** check box in the **Global Preferences** workspace.	This step is required only if you do not want to create Recommendations in RBI, but want to use the Asset Strategy Management (ASM) module to recommend actions and manage mitigated risk. This check box is selected by default.
7	Select the **Enable Recommendations to be Generated at Created State** check box in the **Global Preferences** workspace.	This step is required only if you want to create RBI Recommendation records while RBI Analysis records are in the Created state. This check box is cleared by default.
8	Select the **Allow Override of Calculated Unmitigated Risk Values** check box in the **Global Preferences** workspace.	This step is required only if you want to override the calculated values of unmitigated risk because you use a custom calculator. This check box is cleared by default.
9	Select the **Consider Half-Life when Determining Inspection Task Interval** check box in the **Global Preferences** workspace.	This step is required only if you want additional values such as half-life to determine the inspection task interval. This check box is cleared by default.
10	Select the **Is a Unit?** check box in Functional Location records that represent units in your facility.	This step is required to mark Functional Location records as Process Units.
11	Using the Belongs to a Unit relationship, link Equipment records to Functional Location records representing units to which that equipment belongs (i.e., the **Is a Unit?** check box is selected).	This step is optional.

Step	Task	Notes
12	Configure the APM system to generate RBI Recommendation records automatically.	This step is optional.
13	Create Potential Degradation Mechanisms records.	This step is required only if you want to use additional Potential Degradation Mechanisms records that are not provided in the baseline APM database.
14	Assign a ranking to all Qualitative Potential Degradation Mechanisms records.	This step is required only if you want the Probability Category field in certain Criticality Degradation Mech Evaluation records to be populated automatically based on this ranking.
15	Add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you want to use additional RBI Component type records that are not provided in the baseline APM database.

Upgrade or Update RBI to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

After you upgrade from a version prior to 4.3.1.0:

- All RBI Assets with Active Analyses will have a related Inspection Plan record created.
- All RBI recommendations for an RBI Asset will be related to Inspection Plan record of the RBI Asset.
- The state caption for RBI Recommendation family with State ID MI_ACCEPTED will be updated to “Approved”.
- The Recommendation Methodology field on RBI Recommendation will be updated to RBI 580 where previously the field had the value of "Criticality Calculator”.
- All security users who belong to the 'MI RBI Analyst' security group will belong to the MI Inspection Plan Approver security role.
- The MI Inspection Plan Approver security role will have the MI ASM Analyst security group assigned.
- Piping Stress updated
  - In some of the Piping Stress records for B31.3, WPB was misspelled as WFB. These records are now updated based on ASME standards.
  - In some of the Piping Stress records for B31.3 and B31.1 for the year 2014, where the Material Specification field contained the value B366 and B622, the Material Grade had the value NS instead of N/A. These records are now updated based on ASME standards.

- RBI 580 Representative Fluid contents have been updated for the following fluids to match the API 581, 3rd Edition, Addendum 1 specification:
  - C13-16 (Diesel)
  - C17-25 (Gas Oil)
  - C25+ (Resid)
  - C5
  - Chlorine
  - CO
  - EO
  - H2
  - H2O (Water)
  - H2S
  - HCl
  - HF
  - MEOH (Methanol)
  - NH3
  - Phosgene
  - Steam

  For information on the updated RBI 580 Representative Fluid Contents, refer to the topic.
- The Data Mapping Group record that satisfies the following conditions, along with its child records, will be reverted to baseline:
  - The value in the Source Family field is Criticality RBI Component - Exchanger Bundle.
  - The value in the Target Family field is RBI Criticality Analysis.
- In some of the PV Stress records that contain the value SA/AS 1548, SB-187, SB-308, or SB-211 in the Material Specification field, values in the Minimum Yield Strength field are updated based on ASME 2010 standards.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

Step	Task	Notes
1	Add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you have additional RBI Component type records that are not provided in the baseline APM database.
2	Revert the following Risk Based Inspection queries to baseline ◦ `Public\Meridium\Modules\Mechanical Integrity \Queries\Dashboard Queries` folder. ◦ Equipment Outside Risk Policy ◦ PendingRecommendations ◦ RBI Risk Matrix Query ◦ RiskMatrix ◦ `Public\Meridium\Modules\Mechanical Integrity \Report Queries` folder. ◦ MI RBI Analysis Summary Query ◦ MI Inspection Management Summary Query ◦ MI Thickness Monitoring Summary Query ◦ `Public\Meridium\Modules\Risk Based Inspection \Queries` folder. ◦ Active Analyses for Evergreening – 580 ◦ Analyses Created For Evergreening – 580 ◦ Analyses Ready For Evergreening – 580 ◦ Asset Corrosion Analysis More Current Than All Analyses ◦ Asset Corrosion Analysis More Current Than Analyses ◦ Asset Counts for Units ◦ Assets with No Recommendations ◦ Assets with No Recommendations (580 Only) ◦ Current Risk ◦ Current Risk Overview ◦ Inspections More Current Than All Analysis ◦ Inspections More Current Than Analysis ◦ Past Risk ◦ Past Risk Overview ◦ RBI Asset Risk Query ◦ RBI Assets for a Functional Location ◦ RBI Components for Unit ◦ Select Protected Assets ◦ Select RBI Components ◦ View Protected RBI Components ◦ Review Analyses by Asset ◦ Review Analyses by Asset 580 ◦ Review Analyses by Corrosion Loop ◦ Review Analyses by Corrosion Loop 580 ◦ Process Unit Query ◦ Analyses Ready For Evergreening for Unit - 580	This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
3	Revert the following Risk Based Inspection queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection \Queries` folder. ◦ Inspections More Current Than All Analysis ◦ Inspections More Current Than Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.
4	Update PV Stress content and stress lookup fields for RBI Criticality Analyses in created state.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000051571.

- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

Step	Task	Notes
1	Add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you have additional RBI Component type records that are not provided in the baseline APM database.
2	Revert the following Risk Based Inspection queries to baseline ◦ `Public\Meridium\Modules\Mechanical Integrity \Queries\Dashboard Queries` folder. ◦ Equipment Outside Risk Policy ◦ PendingRecommendations ◦ RBI Risk Matrix Query ◦ RiskMatrix ◦ `Public\Meridium\Modules\Mechanical Integrity \Report Queries` folder. ◦ MI RBI Analysis Summary Query ◦ MI Inspection Management Summary Query ◦ MI Thickness Monitoring Summary Query ◦ `Public\Meridium\Modules\Risk Based Inspection \Queries` folder. ◦ Active Analyses for Evergreening – 580 ◦ Analyses Created For Evergreening – 580 ◦ Analyses Ready For Evergreening – 580 ◦ Asset Corrosion Analysis More Current Than All Analyses ◦ Asset Corrosion Analysis More Current Than Analyses ◦ Asset Counts for Units ◦ Assets with No Recommendations ◦ Assets with No Recommendations (580 Only) ◦ Current Risk ◦ Current Risk Overview ◦ Inspections More Current Than All Analysis ◦ Inspections More Current Than Analysis ◦ Past Risk ◦ Past Risk Overview ◦ RBI Asset Risk Query ◦ RBI Assets for a Functional Location ◦ RBI Components for Unit ◦ Select Protected Assets ◦ Select RBI Components ◦ View Protected RBI Components ◦ Review Analyses by Asset ◦ Review Analyses by Asset 580 ◦ Review Analyses by Corrosion Loop ◦ Review Analyses by Corrosion Loop 580 ◦ Process Unit Query ◦ Analyses Ready For Evergreening for Unit - 580	This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
3	Revert the following Risk Based Inspection queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection \Queries` folder. ◦ Inspections More Current Than All Analysis ◦ Inspections More Current Than Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.
4	Update PV Stress content and stress lookup fields for RBI Criticality Analyses in created state.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000051571.

- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

Step	Task	Notes
1	Revert the following Risk Based Inspection queries to baseline: ◦ `Public/Meridium/Modules/RBI/Queries/Active Analyses for Evergreening - 580` ◦ `Public/Meridium/Modules/RBI/Queries/Analyses Created for Evergreening - 580` ◦ `Public/Meridium/Modules/RBI/Queries/Select RBI Components`	This step is required if you have modified any of the following queries: ◦ Active Analyses for Evergreening – 580 ◦ Analyses Created for Evergreening - 580 **Note:** If you have not modified any of the above mentioned queries, you do not have to complete this step for the specified query.
2	Revert the following Compliance Management query to baseline: `Public/Meridium/Modules/Inspection/Compliance/Queries/Recommended Actions by Selected Plans`	This step is required if you want to use the RBI Inspection Grouping functionality.
3	Update the Column Field Pair mapping for Representative Fluid on Exchange Bundles by following the steps mentioned in KBA 000050154.	This step is required.

<table>
<tr><th>Step</th><th>Task</th><th>Notes</th></tr>
<tr><td>4</td><td>Execute the Revert to Baseline utility to update the following Datasheets:

<table><tr><th>Family</th><th>Datasheet</th></tr><tr><td>RBI PRD Criticality Analysis</td><td>PRD Analysis</td></tr><tr><td>Criticality Over Pressure Deg. Mech. Eval.</td><td>Over Pressure Deg. Mech. Eval.</td></tr><tr><td>Criticality Leak Deg. Mech. Eval.</td><td>Leak Deg. Mech. Eval.</td></tr></table>
or
Using configuration manager you can import the datasheet files provided in KBA 000059942.</td><td>This step is required only if you have modified the following datasheets:
PRD Analysis
Over Pressure Deg. Mech. Eval.
Leak Deg. Mech. Eval.</td></tr>
<tr><td>5</td><td>Add the Susceptible To CUI field to the following datasheets:

<table><tr><th>Datasheet Name</th><th>Family Caption</th></tr><tr><td>RBI Analysis</td><td>RBI Criticality Analysis</td></tr><tr><td>RBI Comp - Cylindrical Shell</td><td>Criticality RBI Component - Cylindrical Shell</td></tr><tr><td>RBI Comp - Exchanger Header</td><td>Criticality RBI Component - Exchanger Header</td></tr><tr><td>RBI Comp - Piping</td><td>Criticality RBI Component - Piping</td></tr><tr><td>RBI Comp - Tank Bottom</td><td>Criticality RBI Component - Tank Bottom</td></tr></table>
Alternatively, you can revert the datasheets to baseline.</td><td>This step is required if you want to use the RBI Inspection Grouping functionality and do not find the Susceptible To CUI field in the datasheets.</td></tr>
</table>

Step	Task	Notes

6	Revert the following Risk Based Inspection queries to baseline
	◦ `Public\Meridium\Modules\Mechanical Integrity \Queries\Dashboard Queries` folder.
	  ◦ Equipment Outside Risk Policy
	  ◦ PendingRecommendations
	  ◦ RBI Risk Matrix Query
	  ◦ RiskMatrix
	◦ `Public\Meridium\Modules\Mechanical Integrity\Report Queries` folder.
	  ◦ MI RBI Analysis Summary Query
	  ◦ MI Inspection Management Summary Query
	  ◦ MI Thickness Monitoring Summary Query
	◦ `Public\Meridium\Modules\Risk Based Inspection \Queries` folder.
	  ◦ Active Analyses for Evergreening – 580
	  ◦ Analyses Created For Evergreening – 580
	  ◦ Analyses Ready For Evergreening – 580
	  ◦ Asset Corrosion Analysis More Current Than All Analyses
	  ◦ Asset Corrosion Analysis More Current Than Analyses
	  ◦ Asset Counts for Units
	  ◦ Assets with No Recommendations
	  ◦ Assets with No Recommendations (580 Only)
	  ◦ Current Risk
	  ◦ Current Risk Overview
	  ◦ Inspections More Current Than All Analysis
	  ◦ Inspections More Current Than Analysis
	  ◦ Past Risk
	  ◦ Past Risk Overview
	  ◦ RBI Asset Risk Query
	  ◦ RBI Assets for a Functional Location
	  ◦ RBI Components for Unit
	  ◦ Select Protected Assets
	  ◦ Select RBI Components
	  ◦ View Protected RBI Components
	  ◦ Review Analyses by Asset
	  ◦ Review Analyses by Asset 580
	  ◦ Review Analyses by Corrosion Loop
	  ◦ Review Analyses by Corrosion Loop 580
	  ◦ Process Unit Query
	  ◦ Analyses Ready For Evergreening for Unit - 580
		This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

7	Add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you have additional RBI Component type records that are not provided in the baseline APM database.

Step	Task	Notes
8	Revert the following Risk Based Inspection queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection \Queries` folder. ◦ Inspections More Current Than All Analysis ◦ Inspections More Current Than Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/ TM Updates** tab, in the **Risk Based Inspection Overview** page.
9	Update PV Stress content and stress lookup fields for RBI Criticality Analyses in created state.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000051571.

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11.

<table>
<tr><th>Step</th><th>Task</th><th>Notes</th></tr>
<tr><td>1</td><td>Add the Completion Comments field to the RBI Recommendation datasheet.</td><td>This step is required only if you have customized the RBI Recommendation datasheet.</td></tr>
<tr><td>2</td><td>Add the following state and operations to RBI Recommendation State Management:

Table 2: State
<table><tr><th>State ID</th><th>State Caption</th></tr><tr><td>MI_NOTREQUIRED</td><td>Not Required</td></tr></table>
Table 3: Operations
<table><tr><th>Operation ID</th><th>Operation Caption</th><th>Predecessor State</th><th>Successor State</th></tr><tr><td>MI_NRQARCHIVED</td><td>Archive</td><td>Not Required</td><td>Archived</td></tr><tr><td>MI_MARKNOTREQUIRED</td><td>Mark Not Required</td><td>Proposed</td><td>Not Required</td></tr></table>
For information on adding State and Operation to a family, refer to the Family Management documentation.</td><td>This step is required because the State Machine for RBI Recommendation is not updated automatically if the RBI Recommendation family has records.</td></tr>
<tr><td>3</td><td>A new Data Mapping Column-Field Pair record has been created to map the Specified Tmin field value from an RBI Component to the associated RBI Criticality Analysis and RBI Pipeline Analysis. The new record may not be available in the current version because of content protection. Verify if the mapping is available. If the mapping is not available, add the mapping manually.</td><td>This step is required only for RBI Criticality Analysis and RBI Pipeline Analysis.</td></tr>
<tr><td>4</td><td>Revert the following Process Units overview queries to baseline:
<code>Public/Meridium/Modules/Risk Based Inspection/Queries/Asset Counts for Units</code>
<code>Public/Meridium/Modules/Risk Based Inspection/Queries/Process Unit Query</code></td><td>This step is required only if you have modified the following queries that are used for the Process Units tab in the Risk Based Inspection Overview page:
Asset Counts for Units
Process Unit Query</td></tr>
</table>

Step	Task	Notes
5	Revert the following Finalize Risk queries to baseline: ◦ `Public/Meridium/Modules/Risk Based Inspection/Queries/Review Analyses by Asset 580` ◦ `Public/Meridium/Modules/Risk Based Inspection/Queries/Review Analyses by Corrosion Loop 580`	This step is required only if you use PRD RBI 580 Analysis and would like to use the Bulk State transition to include this analysis.
6	On the APM Server, using Configuration Manager, import the following files: ◦ `101_MI_STMPCNFG.xml` ◦ `102_MI_STRMAPP.xml` These files are located in the following folder: `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks`. You must extract the `4030000` archive from the `MI_DB_MASTER_4030000` archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, follow the instructions in KBA 000050619.

Step	Task	Notes

7	Revert the following Risk Based Inspection queries to baseline
	◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder.
	  ◦ Equipment Outside Risk Policy
	  ◦ PendingRecommendations
	  ◦ RBI Risk Matrix Query
	  ◦ RiskMatrix
	◦ `Public\Meridium\Modules\Mechanical Integrity\Report Queries` folder.
	  ◦ MI RBI Analysis Summary Query
	  ◦ MI Inspection Management Summary Query
	  ◦ MI Thickness Monitoring Summary Query
	◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder.
	  ◦ Active Analyses for Evergreening – 580
	  ◦ Analyses Created For Evergreening – 580
	  ◦ Analyses Ready For Evergreening – 580
	  ◦ Asset Corrosion Analysis More Current Than All Analyses
	  ◦ Asset Corrosion Analysis More Current Than Analyses
	  ◦ Asset Counts for Units
	  ◦ Assets with No Recommendations
	  ◦ Assets with No Recommendations (580 Only)
	  ◦ Current Risk
	  ◦ Current Risk Overview
	  ◦ Inspections More Current Than All Analysis
	  ◦ Inspections More Current Than Analysis
	  ◦ Past Risk
	  ◦ Past Risk Overview
	  ◦ RBI Asset Risk Query
	  ◦ RBI Assets for a Functional Location
	  ◦ RBI Components for Unit
	  ◦ Select Protected Assets
	  ◦ Select RBI Components
	  ◦ View Protected RBI Components
	  ◦ Review Analyses by Asset
	  ◦ Review Analyses by Asset 580
	  ◦ Review Analyses by
		This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
8	Add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you have additional RBI Component type records that are not provided in the baseline APM database.
9	Revert the following Risk Based Inspection queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder. ◦ Inspections More Current Than All Analysis ◦ Inspections More Current Than Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.
10	Update PV Stress content and stress lookup fields for RBI Criticality Analyses in created state.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000051571.

- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

Step	Task	Notes
1	Modify the Data Mapping Query record RBI-CNAFC MI_CCRBICTB-MI_CRCOEVAL by Component as follows: ◦ In the related Data Mapping Column-Field Pair record where the Source Query Field is set to Toxic Mixture, ensure the Target Field(s) field is also set to Toxic Mixture. ◦ In the related Data Mapping Column-Field Pair record where the Source Query Field is set to Toxic Model, ensure the Target Field(s) field is set to Toxic Fluid.	This step is required only if you have not completed it while upgrading RBI 581.
2	On the APM Server, using Configuration Manager, import the following files: ◦ `09_MI_RRSKMAP.xml` ◦ `10_MI_RRSKMDT.xml` These files are located in the following folder: `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks`. You must extract the `4030000` archive from the `MI_DB_MASTER_4030000` archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.
3	On the APM Server, using Configuration Manager, import the following files ◦ `101_MI_STMPCNFG.xml` ◦ `102_MI_STRMAPP.xml` These files are located in the following folder: `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks`. You must extract the `4030000` archive from the `MI_DB_MASTER_4030000` archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 000050619.

Step	Task	Notes
4	A new Data Mapping Column-Field Pair record has been created to map the Specified Tmin field value from an RBI Component to the associated RBI Criticality Analysis and RBI Pipeline Analysis. The new record may not be available in the current version because of content protection. Verify if the mapping is available. If the mapping is not available, add the mapping manually.	This step is required only for RBI Criticality Analysis and RBI Pipeline Analysis.

Step	Task	Notes

5	Revert the following Risk Based Inspection queries to baseline
	◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder.
	  ◦ Equipment Outside Risk Policy
	  ◦ PendingRecommendations
	  ◦ RBI Risk Matrix Query
	  ◦ RiskMatrix
	◦ `Public\Meridium\Modules\Mechanical Integrity\Report Queries` folder.
	  ◦ MI RBI Analysis Summary Query
	  ◦ MI Inspection Management Summary Query
	  ◦ MI Thickness Monitoring Summary Query
	◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder.
	  ◦ Active Analyses for Evergreening – 580
	  ◦ Analyses Created For Evergreening – 580
	  ◦ Analyses Ready For Evergreening – 580
	  ◦ Asset Corrosion Analysis More Current Than All Analyses
	  ◦ Asset Corrosion Analysis More Current Than Analyses
	  ◦ Asset Counts for Units
	  ◦ Assets with No Recommendations
	  ◦ Assets with No Recommendations (580 Only)
	  ◦ Current Risk
	  ◦ Current Risk Overview
	  ◦ Inspections More Current Than All Analysis
	  ◦ Inspections More Current Than Analysis
	  ◦ Past Risk
	  ◦ Past Risk Overview
	  ◦ RBI Asset Risk Query
	  ◦ RBI Assets for a Functional Location
	  ◦ RBI Components for Unit
	  ◦ Select Protected Assets
	  ◦ Select RBI Components
	  ◦ View Protected RBI Components
	  ◦ Review Analyses by Asset
	  ◦ Review Analyses by Asset 580
	  ◦ Review Analyses by
		This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
6	Add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you have additional RBI Component type records that are not provided in the baseline APM database.
7	Revert the following Risk Based Inspection queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder. ◦ Inspections More Current Than All Analysis ◦ Inspections More Current Than Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.
8	Update PV Stress content and stress lookup fields for RBI Criticality Analyses in created state.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000051571.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	Modify the Data Mapping Query record RBI-CNAFC MI_CCRBICTB-MI_CRCOEVAL by Component as follows: ◦ In the related Data Mapping Column-Field Pair record where the Source Query Field is set to Toxic Mixture, ensure the Target Field(s) field is also set to Toxic Mixture. ◦ In the related Data Mapping Column-Field Pair record where the Source Query Field is set to Toxic Model, ensure the Target Field(s) field is set to Toxic Fluid.	This step is required only if you have not completed it while upgrading RBI 581.
2	On the APM Server, using Configuration Manager, import the following files: ◦ `09_MI_RRSKMAP.xml` ◦ `10_MI_RRSKMDT.xml` These files are located in the following folder: `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks`. You must extract the `4030000` archive from the `MI_DB_MASTER_4030000` archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.
3	On the APM Server, using Configuration Manager, import the following files ◦ `101_MI_STMPCNFG.xml` ◦ `102_MI_STRMAPP.xml` These files are located in the following folder: `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks`. You must extract the `4030000` archive from the `MI_DB_MASTER_4030000` archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 000050619.

Step	Task	Notes
4	A new Data Mapping Column-Field Pair record has been created to map the Specified Tmin field value from an RBI Component to the associated RBI Criticality Analysis and RBI Pipeline Analysis. The new record may not be available in the current version because of content protection. Verify if the mapping is available. If the mapping is not available, add the mapping manually.	This step is required only for RBI Criticality Analysis and RBI Pipeline Analysis.

Step	Task	Notes

5	Revert the following Risk Based Inspection queries to baseline
	◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder.
	  ◦ Equipment Outside Risk Policy
	  ◦ PendingRecommendations
	  ◦ RBI Risk Matrix Query
	  ◦ RiskMatrix
	◦ `Public\Meridium\Modules\Mechanical Integrity\Report Queries` folder.
	  ◦ MI RBI Analysis Summary Query
	  ◦ MI Inspection Management Summary Query
	  ◦ MI Thickness Monitoring Summary Query
	◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder.
	  ◦ Active Analyses for Evergreening – 580
	  ◦ Analyses Created For Evergreening – 580
	  ◦ Analyses Ready For Evergreening – 580
	  ◦ Asset Corrosion Analysis More Current Than All Analyses
	  ◦ Asset Corrosion Analysis More Current Than Analyses
	  ◦ Asset Counts for Units
	  ◦ Assets with No Recommendations
	  ◦ Assets with No Recommendations (580 Only)
	  ◦ Current Risk
	  ◦ Current Risk Overview
	  ◦ Inspections More Current Than All Analysis
	  ◦ Inspections More Current Than Analysis
	  ◦ Past Risk
	  ◦ Past Risk Overview
	  ◦ RBI Asset Risk Query
	  ◦ RBI Assets for a Functional Location
	  ◦ RBI Components for Unit
	  ◦ Select Protected Assets
	  ◦ Select RBI Components
	  ◦ View Protected RBI Components
	  ◦ Review Analyses by Asset
	  ◦ Review Analyses by Asset 580
	  ◦ Review Analyses by
		This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
6	Add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you have additional RBI Component type records that are not provided in the baseline APM database.
7	Revert the following Risk Based Inspection queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder. ◦◦ Inspections More Current Than All Analysis ◦◦ Inspections More Current Than Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.
8	Update PV Stress content and stress lookup fields for RBI Criticality Analyses in created state.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000051571.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

Step	Task	Notes
1	Using Configuration Manager, import the following policies: ◦ Appendix G ◦ Appendix H ◦ Appendix I	This step is required only if you use Policy records to generate RBI Recommendations. This will fix the issues specified in KBA 000042593.
2	Modify the Data Mapping Query record RBI-CNAFC MI_CCRBICTB-MI_CRCOEVAL by Component as follows: ◦ In the related Data Mapping Column-Field Pair record where the Source Query Field is set to Toxic Mixture, ensure the Target Field(s) field is also set to Toxic Mixture. ◦ In the related Data Mapping Column-Field Pair record where the Source Query Field is set to Toxic Model, ensure the Target Field(s) field is set to Toxic Fluid.	This step is required only if you have not completed it while upgrading RBI 581.

Step	Task	Notes
3	On the APM Server, using Configuration Manager, import the following files ◦ 09_MI_RRSKMAP.xml ◦ 10_MI_RRSKMDT.xml These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.
4	On the APM Server, using Configuration Manager, import the following files ◦ 101_MI_STMPCNFG.xml ◦ 102_MI_STRMAPP.xml These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 000050619.
5	A new Data Mapping Column-Field Pair record has been created to map the Specified Tmin field value from an RBI Component to the associated RBI Criticality Analysis and RBI Pipeline Analysis. The new record may not be available in the current version because of content protection. Verify if the mapping is available. If the mapping is not available, add the mapping manually.	This step is required only for RBI Criticality Analysis and RBI Pipeline Analysis.
6	On the APM Server, using Meridium Rules Editor, modify the MI_Has_Recommendations.vb file to remove any RBI rules to manage the RBI Recommendation state process.	Follow the instructions in KBA 000053979 to remove any customization. This step is required only if you have customized the rules to manage the RBI Recommendation state process.

Step	Task	Notes

7	Revert the following Risk Based Inspection queries to baseline
	◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder.
	  ◦ Equipment Outside Risk Policy
	  ◦ PendingRecommendations
	  ◦ RBI Risk Matrix Query
	  ◦ RiskMatrix
	◦ `Public\Meridium\Modules\Mechanical Integrity\Report Queries` folder.
	  ◦ MI RBI Analysis Summary Query
	  ◦ MI Inspection Management Summary Query
	  ◦ MI Thickness Monitoring Summary Query
	◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder.
	  ◦ Active Analyses for Evergreening – 580
	  ◦ Analyses Created For Evergreening – 580
	  ◦ Analyses Ready For Evergreening – 580
	  ◦ Asset Corrosion Analysis More Current Than All Analyses
	  ◦ Asset Corrosion Analysis More Current Than Analyses
	  ◦ Asset Counts for Units
	  ◦ Assets with No Recommendations
	  ◦ Assets with No Recommendations (580 Only)
	  ◦ Current Risk
	  ◦ Current Risk Overview
	  ◦ Inspections More Current Than All Analysis
	  ◦ Inspections More Current Than Analysis
	  ◦ Past Risk
	  ◦ Past Risk Overview
	  ◦ RBI Asset Risk Query
	  ◦ RBI Assets for a Functional Location
	  ◦ RBI Components for Unit
	  ◦ Select Protected Assets
	  ◦ Select RBI Components
	  ◦ View Protected RBI Components
	  ◦ Review Analyses by Asset 580
	  ◦ Review Analyses by Asset
	  ◦ Review Analyses by
		This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes

8	Revert the following Risk Based Inspection queries to baseline
	◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder.
	  ◦ Inspections More Current Than All Analysis
	  ◦ Inspections More Current Than Analysis
		This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.

- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

Step	Task	Notes
1	Using Configuration Manager, import the following policies : ◦ Appendix G ◦ Appendix H ◦ Appendix I	This step is required only if you use Policy records to generate RBI Recommendations. This will fix the issues specified in KBA 000042593.
2	Modify the Data Mapping Query record RBI-CNAFC MI_CCRBICTB-MI_CRCOEVAL by Component as follows: ◦ In the related Data Mapping Column-Field Pair record where the Source Query Field is set to Toxic Mixture, ensure the Target Field(s) field is also set to Toxic Mixture. ◦ In the related Data Mapping Column-Field Pair record where the Source Query Field is set to Toxic Model, ensure the Target Field(s) field is set to Toxic Fluid.	This step is required only if you have not completed it while upgrading RBI 581.
3	On the APM Server, using Configuration Manager, import the following files ◦ `09_MI_RRSKMAP.xml` ◦ `10_MI_RRSKMDT.xml` These files are located in the following folder: `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks`. You must extract the `4030000` archive from the `MI_DB_MASTER_4030000` archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.

Step	Task	Notes
4	On the APM Server, using Configuration Manager, import the following files ◦ `101_MI_STMPCNFG.xml` ◦ `102_MI_STRMAPP.xml` These files are located in the following folder: `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks`. You must extract the `4030000` archive from the `MI_DB_MASTER_4030000` archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 000050619.
5	A new Data Mapping Column-Field Pair record has been created to map the Specified Tmin field value from an RBI Component to the associated RBI Criticality Analysis and RBI Pipeline Analysis. The new record may not be available in the current version because of content protection. Verify if the mapping is available. If the mapping is not available, add the mapping manually.	This step is required only for RBI Criticality Analysis and RBI Pipeline Analysis.
6	On the APM Server, using Meridium Rules Editor, modify the `MI_Has_Recommendations.vb` file to remove any RBI rules to manage the RBI Recommendation state process.	Follow the instructions in KBA 000053979 to remove any customization. This step is required only if you have customized the rules to manage the RBI Recommendation state process.

Step	Task	Notes

7	Revert the following Risk Based Inspection queries to baseline
	◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder.
	  ◦ Equipment Outside Risk Policy
	  ◦ PendingRecommendations
	  ◦ RBI Risk Matrix Query
	  ◦ RiskMatrix
	◦ `Public\Meridium\Modules\Mechanical Integrity\Report Queries` folder.
	  ◦ MI RBI Analysis Summary Query
	  ◦ MI Inspection Management Summary Query
	  ◦ MI Thickness Monitoring Summary Query
	◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder.
	  ◦ Active Analyses for Evergreening – 580
	  ◦ Analyses Created For Evergreening – 580
	  ◦ Analyses Ready For Evergreening – 580
	  ◦ Asset Corrosion Analysis More Current Than All Analyses
	  ◦ Asset Corrosion Analysis More Current Than Analyses
	  ◦ Asset Counts for Units
	  ◦ Assets with No Recommendations
	  ◦ Assets with No Recommendations (580 Only)
	  ◦ Current Risk
	  ◦ Current Risk Overview
	  ◦ Inspections More Current Than All Analysis
	  ◦ Inspections More Current Than Analysis
	  ◦ Past Risk
	  ◦ Past Risk Overview
	  ◦ RBI Asset Risk Query
	  ◦ RBI Assets for a Functional Location
	  ◦ RBI Components for Unit
	  ◦ Select Protected Assets
	  ◦ Select RBI Components
	  ◦ View Protected RBI Components
	  ◦ Review Analyses by Asset
	  ◦ Review Analyses by Asset 580
	  ◦ Review Analyses by
		This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes

8	Revert the following Risk Based Inspection queries to baseline
	◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder.
	  ◦ Inspections More Current Than All Analysis
	  ◦ Inspections More Current Than Analysis
		This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.

- Upgrade from any version V3.5.1 through V3.5.1.12.3

Step	Task	Notes
1	Using Configuration Manager, import the following policies: ◦ Appendix G ◦ Appendix H ◦ Appendix I	This step is required only if you use Policy records to generate RBI Recommendations. This will fix the issues specified in KBA 000042593.
2	Import the Inspection Strategy records that APM modified in order to fix issues in existing Inspection Strategy records. To do so: 1. Using the **Import/Export Metadata** window, navigate to the following location on the APM Server machine: `C:\Meridium\DbUpg\MI_DB_Master_4030000\4030000\20_IEU\50_Other\2_RecordsLinks` 2. Import the file `MI_INSP_STRAT.xml` from the aforementioned location.	This step is required. This will replace the Inspection Strategy records with new ones.
3	On the APM Server, using Configuration Manager, import the following files ◦ `09_MI_RRSKMAP.xml` ◦ `10_MI_RRSKMDT.xml` These files are located in the following folder: `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks`. You must extract the `4030000` archive from the `MI_DB_MASTER_4030000` archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.

Step	Task	Notes
4	On the APM Server, using Configuration Manager, import the following files ◦ `101_MI_STMPCNFG.xml` ◦ `102_MI_STRMAPP.xml` These files are located in the following folder: `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks`. You must extract the `4030000` archive from the `MI_DB_MASTER_4030000` archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 000050619.
5	A new Data Mapping Column-Field Pair record has been created to map the Specified Tmin field value from an RBI Component to the associated RBI Criticality Analysis and RBI Pipeline Analysis. The new record may not be available in the current version because of content protection. Verify if the mapping is available. If the mapping is not available, add the mapping manually.	This step is required only for RBI Criticality Analysis and RBI Pipeline Analysis.
6	On the APM Server, using Meridium Rules Editor, modify the `MI_Has_Recommendations.vb` file to remove any RBI rules to manage the RBI Recommendation state process.	Follow the instructions in KBA 000053979 to remove any customization. This step is required only if you have customized the rules to manage the RBI Recommendation state process.

Step	Task	Notes

7	Revert the following Risk Based Inspection queries to baseline
	◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder.
	  ◦ Equipment Outside Risk Policy
	  ◦ PendingRecommendations
	  ◦ RBI Risk Matrix Query
	  ◦ RiskMatrix
	◦ `Public\Meridium\Modules\Mechanical Integrity\Report Queries` folder.
	  ◦ MI RBI Analysis Summary Query
	  ◦ MI Inspection Management Summary Query
	  ◦ MI Thickness Monitoring Summary Query
	◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder.
	  ◦ Active Analyses for Evergreening – 580
	  ◦ Analyses Created For Evergreening – 580
	  ◦ Analyses Ready For Evergreening – 580
	  ◦ Asset Corrosion Analysis More Current Than All Analyses
	  ◦ Asset Corrosion Analysis More Current Than Analyses
	  ◦ Asset Counts for Units
	  ◦ Assets with No Recommendations
	  ◦ Assets with No Recommendations (580 Only)
	  ◦ Current Risk
	  ◦ Current Risk Overview
	  ◦ Inspections More Current Than All Analysis
	  ◦ Inspections More Current Than Analysis
	  ◦ Past Risk
	  ◦ Past Risk Overview
	  ◦ RBI Asset Risk Query
	  ◦ RBI Assets for a Functional Location
	  ◦ RBI Components for Unit
	  ◦ Select Protected Assets
	  ◦ Select RBI Components
	  ◦ View Protected RBI Components
	  ◦ Review Analyses by Asset
	  ◦ Review Analyses by Asset 580
	  ◦ Review Analyses by
		This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
8	Revert the following Risk Based Inspection queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder. ◦ Inspections More Current Than All Analysis ◦ Inspections More Current Than Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.

- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

Step	Task	Notes
1	Using Configuration Manager, import the following policies: ◦ Appendix G ◦ Appendix H ◦ Appendix I	This step is required only if you use Policy records to generate RBI Recommendations. This will fix the issues specified in KBA 000042593.
2	Import the Inspection Strategy records that APM modified in order to fix issues in existing Inspection Strategy records. To do so: 1. Using the **Import/Export Metadata** window, navigate to the following location on the APM Server machine: `C:\Meridium\DbUpg\MI_DB_Master_4030000\4030000\20_IEU\50_Other\2_RecordsLinks` 2. Import the file `MI_INSP_STRAT.xml` from the aforementioned location.	This step is required. This will replace the Inspection Strategy records with new ones.
3	In Functional Location records that represent units in your facility, select the **Is a Unit?** check box.	This step is required.
4	Using the Belongs to a Unit relationship, link Equipment records to Functional Location records representing units to which that equipment belongs (i.e., the field Is a Unit? contains the value True).	This step is optional.
5	Select the **Enable Recommendations to be Generated at Created State** check box in the RBI **Global Preferences** workspace.	This step is required only if you want to create RBI Recommendation records while RBI Analysis records are in the Created state. This check box is cleared by default.

Step	Task	Notes
6	On the APM Server, using Configuration Manager, import the following files ◦ 09_MI_RRSKMAP.xml ◦ 10_MI_RRSKMDT.xml These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.
7	On the APM Server, using Configuration Manager, import the following files ◦ 101_MI_STMPCNFG.xml ◦ 102_MI_STRMAPP.xml These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 000050619.
8	A new Data Mapping Column-Field Pair record has been created to map the Specified Tmin field value from an RBI Component to the associated RBI Criticality Analysis and RBI Pipeline Analysis. The new record may not be available in the current version because of content protection. Verify if the mapping is available. If the mapping is not available, add the mapping manually.	This step is required only for RBI Criticality Analysis and RBI Pipeline Analysis.
9	On the APM Server, using Meridium Rules Editor, modify the MI_Has_Recommendations.vb file to remove any RBI rules to manage the RBI Recommendation state process.	Follow the instructions in KBA 000053979 to remove any customization. This step is required only if you have customized the rules to manage the RBI Recommendation state process.

Step	Task	Notes

10	Revert the following Risk Based Inspection queries to baseline
	◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder.
	  ◦ Equipment Outside Risk Policy
	  ◦ PendingRecommendations
	  ◦ RBI Risk Matrix Query
	  ◦ RiskMatrix
	◦ `Public\Meridium\Modules\Mechanical Integrity\Report Queries` folder.
	  ◦ MI RBI Analysis Summary Query
	  ◦ MI Inspection Management Summary Query
	  ◦ MI Thickness Monitoring Summary Query
	◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder.
	  ◦ Active Analyses for Evergreening – 580
	  ◦ Analyses Created For Evergreening – 580
	  ◦ Analyses Ready For Evergreening – 580
	  ◦ Asset Corrosion Analysis More Current Than All Analyses
	  ◦ Asset Corrosion Analysis More Current Than Analyses
	  ◦ Asset Counts for Units
	  ◦ Assets with No Recommendations
	  ◦ Assets with No Recommendations (580 Only)
	  ◦ Current Risk
	  ◦ Current Risk Overview
	  ◦ Inspections More Current Than All Analysis
	  ◦ Inspections More Current Than Analysis
	  ◦ Past Risk
	  ◦ Past Risk Overview
	  ◦ RBI Asset Risk Query
	  ◦ RBI Assets for a Functional Location
	  ◦ RBI Components for Unit
	  ◦ Select Protected Assets
	  ◦ Select RBI Components
	  ◦ View Protected RBI Components
	  ◦ Review Analyses by Asset
	  ◦ Review Analyses by Asset 580
	  ◦ Review Analyses by
		This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
11	Revert the following Risk Based Inspection queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder. ◦ Inspections More Current Than All Analysis ◦ Inspections More Current Than Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.

- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Using Configuration Manager, import the following policies: ◦ Appendix G ◦ Appendix H ◦ Appendix I	This step is required only if you use Policy records to generate RBI Recommendations. This will fix the issues specified in KBA 000042593.
2	Import the Inspection Strategy records that APM modified in order to fix issues in existing Inspection Strategy records. To do so: 1. Using the **Import/Export Metadata** window, navigate to the following location on the APM Server machine: `C:\Meridium\DbUpg\MI_DB_Master_4030000\4030000\20_IEU\50_Other\2_RecordsLinks` 2. Import the file `MI_INSP_STRAT.xml` from the aforementioned location.	This step is required. This will replace the Inspection Strategy records with new ones.
3	In Functional Location records that represent units in your facility, select the **Is a Unit?** check box.	This step is required.
4	Using the Belongs to a Unit relationship, link Equipment records to Functional Location records representing units to which that equipment belongs (i.e., the field Is a Unit? contains the value True).	This step is optional.
5	Select the **Enable Recommendations to be Generated at Created State** check box in the RBI **Global Preferences** workspace.	This check box is cleared by default. This step is required only if you want to create RBI Recommendation records while RBI Analysis records are in the Created state.

Step	Task	Notes
6	On the APM Server, using Configuration Manager, import the following files ◦ 09_MI_RRSKMAP.xml ◦ 10_MI_RRSKMDT.xml These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.
7	On the APM Server, using Configuration Manager, import the following files ◦ 101_MI_STMPCNFG.xml ◦ 102_MI_STRMAPP.xml These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 000050619.
8	A new Data Mapping Column-Field Pair record has been created to map the Specified Tmin field value from an RBI Component to the associated RBI Criticality Analysis and RBI Pipeline Analysis. The new record may not be available in the current version because of content protection. Verify if the mapping is available. If the mapping is not available, add the mapping manually.	This step is required only for RBI Criticality Analysis and RBI Pipeline Analysis.
9	On the APM Server, using Meridium Rules Editor, modify the MI_Has_Recommendations.vb file to remove any RBI rules to manage the RBI Recommendation state process.	Follow the instructions in KBA 000053979 to remove any customization. This step is required only if you have customized the rules to manage the RBI Recommendation state process.

Step	Task	Notes

10	Revert the following Risk Based Inspection queries to baseline
	◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder.
	  ◦ Equipment Outside Risk Policy
	  ◦ PendingRecommendations
	  ◦ RBI Risk Matrix Query
	  ◦ RiskMatrix
	◦ `Public\Meridium\Modules\Mechanical Integrity\Report Queries` folder.
	  ◦ MI RBI Analysis Summary Query
	  ◦ MI Inspection Management Summary Query
	  ◦ MI Thickness Monitoring Summary Query
	◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder.
	  ◦ Active Analyses for Evergreening – 580
	  ◦ Analyses Created For Evergreening – 580
	  ◦ Analyses Ready For Evergreening – 580
	  ◦ Asset Corrosion Analysis More Current Than All Analyses
	  ◦ Asset Corrosion Analysis More Current Than Analyses
	  ◦ Asset Counts for Units
	  ◦ Assets with No Recommendations
	  ◦ Assets with No Recommendations (580 Only)
	  ◦ Current Risk
	  ◦ Current Risk Overview
	  ◦ Inspections More Current Than All Analysis
	  ◦ Inspections More Current Than Analysis
	  ◦ Past Risk
	  ◦ Past Risk Overview
	  ◦ RBI Asset Risk Query
	  ◦ RBI Assets for a Functional Location
	  ◦ RBI Components for Unit
	  ◦ Select Protected Assets
	  ◦ Select RBI Components
	  ◦ View Protected RBI Components
	  ◦ Review Analyses by Asset
	  ◦ Review Analyses by Asset 580
	  ◦ Review Analyses by
		This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
11	Revert the following Risk Based Inspection queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder. ◦ Inspections More Current Than All Analysis ◦ Inspections More Current Than Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.

- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Using Configuration Manager, import the following policies: ◦ Appendix G ◦ Appendix H ◦ Appendix I	This step is required only if you use Policy records to generate RBI Recommendations. This will fix the issues specified in KBA 000042593.
2	Import the Inspection Strategy records that APM modified in order to fix issues in existing Inspection Strategy records. To do so: 1. Using the **Import/Export Metadata** window, navigate to the following location on the APM Server machine: `C:\Meridium\DbUpg\MI_DB_Master_4030000\4030000\20_IEU\50_Other\2_RecordsLinks` 2. Import the file `MI_INSP_STRAT.xml` from the aforementioned location.	This step is required. This will replace the Inspection Strategy records with new ones.
3	In Functional Location records that represent units in your facility, select the **Is a Unit?** check box.	This step is required.
4	Using the Belongs to a Unit relationship, link Equipment records to Functional Location records representing units to which that equipment belongs (i.e., the field Is a Unit? contains the value True).	This step is optional.
5	Select the **Enable Recommendations to be Generated at Created State** check box in the RBI **Global Preferences** workspace.	This step is required only if you want to create RBI Recommendation records while RBI Analysis records are in the Created state. This check box is cleared by default.

Step	Task	Notes
6	On the APM Server, using Configuration Manager, import the following files ◦ 09_MI_RRSKMAP.xml ◦ 10_MI_RRSKMDT.xml These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.
7	On the APM Server, using Configuration Manager, import the following files ◦ 101_MI_STMPCNFG.xml ◦ 102_MI_STRMAPP.xml These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 000050619.
8	A new Data Mapping Column-Field Pair record has been created to map the Specified Tmin field value from an RBI Component to the associated RBI Criticality Analysis and RBI Pipeline Analysis. The new record may not be available in the current version because of content protection. Verify if the mapping is available. If the mapping is not available, add the mapping manually.	This step is required only for RBI Criticality Analysis and RBI Pipeline Analysis.
9	On the APM Server, using Meridium Rules Editor, modify the MI_Has_Recommendations.vb file to remove any RBI rules to manage the RBI Recommendation state process.	Follow the instructions in KBA 000053979 to remove any customization. This step is required only if you have customized the rules to manage the RBI Recommendation state process.

Step	Task	Notes

10	Revert the following Risk Based Inspection queries to baseline
	◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder.
	  ◦ Equipment Outside Risk Policy
	  ◦ PendingRecommendations
	  ◦ RBI Risk Matrix Query
	  ◦ RiskMatrix
	◦ `Public\Meridium\Modules\Mechanical Integrity\Report Queries` folder.
	  ◦ MI RBI Analysis Summary Query
	  ◦ MI Inspection Management Summary Query
	  ◦ MI Thickness Monitoring Summary Query
	◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder.
	  ◦ Active Analyses for Evergreening – 580
	  ◦ Analyses Created For Evergreening – 580
	  ◦ Analyses Ready For Evergreening – 580
	  ◦ Asset Corrosion Analysis More Current Than All Analyses
	  ◦ Asset Corrosion Analysis More Current Than Analyses
	  ◦ Asset Counts for Units
	  ◦ Assets with No Recommendations
	  ◦ Assets with No Recommendations (580 Only)
	  ◦ Current Risk
	  ◦ Current Risk Overview
	  ◦ Inspections More Current Than All Analysis
	  ◦ Inspections More Current Than Analysis
	  ◦ Past Risk
	  ◦ Past Risk Overview
	  ◦ RBI Asset Risk Query
	  ◦ RBI Assets for a Functional Location
	  ◦ RBI Components for Unit
	  ◦ Select Protected Assets
	  ◦ Select RBI Components
	  ◦ View Protected RBI Components
	  ◦ Review Analyses by Asset
	  ◦ Review Analyses by Asset 580
	  ◦ Review Analyses by
		This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
11	Revert the following Risk Based Inspection queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder. ◦ Inspections More Current Than All Analysis ◦ Inspections More Current Than Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.

Revert the Process Units Overview Queries to Baseline

This action is required only if you have modified the Process Units Overview queries.

About This Task

Due to changes in the Asset Hierarchy filter, the existing Process Unit query and the Asset Counts for Units sub-query requires updates. If you have modified these queries, perform the following steps to revert the queries to baseline.

Procedure

1. Access the **Query** page.
2. Select **Browse**.

   The **Select a query from the catalog** window appears.
3. Navigate to the `Baseline/Meridium/Modules/Risk Based Inspection/Queries/` folder.
4. Select the link for the Asset Counts for Units baseline query.
   The **Results** workspace appears.
5. Select the **SQL** tab.
6. Copy the code from the **SQL** workspace.
7. From the Catalog, navigate to the `Public/Meridium/Modules/Risk Based Inspection/Queries/` folder.
8. Select the link for the Asset Counts for Units query.
   The **Results** workspace appears.
9. Select the **SQL** tab.
10. Replace the code in the **SQL** workspace with the code that you have copied.
11. Repeat Steps 3-10 for the Process Unit Query.

Revert the Finalize Risk Queries to Baseline

This step is required only if you have modified the queries that are used for the **Finalize Risk** button in the **Assets** section of the **Risk Based Inspection Overview** page and the **Unit Summary** page.

About This Task

To include PRD analyses when performing a bulk Finalize Risk operation, the Finalize Risk queries require updates. If you have modified these queries, perform the following steps to revert the queries to baseline.

Procedure

1. Access the **Query** page.
2. Select **Browse**.

   The **Select a query from the catalog** window appears.
3. Navigate to the `Baseline/Meridium/Modules/Risk Based Inspection/Queries/` folder.
4. Select the link for the Review Analyses by Asset 580 baseline query.
   The **Results** workspace appears.
5. Select the **SQL** tab.
6. Copy the code from the **SQL** workspace.
7. From the Catalog, navigate to the `Public/Meridium/Modules/Risk Based Inspection/Queries/` folder.
8. Select the link for the Review Analyses by Asset 580 query.
   The **Results** workspace appears.
9. Select the **SQL** tab.
10. Replace the code in the **SQL** workspace with the code that you have copied.
11. Repeat Steps 3-10 for the Review Analyses by Corrosion Loop 580 query.

Revert the Risk Based Inspection Queries to Baseline

This action is required only if you have modified the Risk Based Inspection queries.

About This Task

If you have modified the following Risk Based Inspection queries, perform the following steps to revert the queries to baseline:

- Active Analyses for Evergreening - 580
- Analyses Created for Evergreening - 580
- Select RBI Components

Procedure

1. Access the Catalog page.
2. Navigate to the Public folder for the query that you want to revert.

   For Risk Based Inspection 580, the public queries are stored in the following folder:
   `Public/Meridium/Modules/Risk Based Inspection/Queries`

3. Select the check box next to the query that you want to revert, and then select  .
   The **Confirm Delete** window appears, asking you to confirm if you want to delete the selected query.
4. Select **OK**.
   The selected query is deleted.
5. Navigate to the Baseline folder for queries.
   For Risk Based Inspection 580, the baseline queries are stored in the following folder:
   `Baseline/Meridium/Modules/Risk Based Inspection/Queries`
6. Select the check box next to the query that you want to revert, and then select  .
   The **Catalog Folder Browser** window appears.
7. Navigate to the folder containing the public query that you deleted in step 3.
8. Select **OK**.
   A success message appears indicating that the selected item has been copied successfully.
9. Repeat Steps 2-8 for each query that you want to revert to baseline.

Revert the Compliance Management Query to Baseline

This action is required only if you want to use the RBI Inspection Grouping functionality.

About This Task

If you have modified the Recommended Actions by Selected Plans query, perform the following steps to revert the query to baseline:

Procedure

1. Access the Catalog page.
2. Navigate to the following Public folder:
   `Public/Meridium/Modules/Inspection/Compliance/Queries/`
3. Select the check box next to the Recommended Actions by Selected Plans query, and then select  .
   The **Confirm Delete** window appears, asking you to confirm if you want to delete the selected query.
4. Select **OK**.
   The selected query is deleted.
5. Navigate to the following Baseline folder.
   `Baseline/Meridium/Modules/Inspection/Compliance/Queries/`
6. Select the check box next to the Recommended Actions by Selected Plans query, and then select  .
   The **Catalog Folder Browser** window appears.
7. Navigate to the Public folder containing the query that you deleted in step 3.
8. Select **OK**.
   A success message appears indicating that the selected item has been copied successfully.

Add Completion Comments Field to RBI Recommendation Datasheet

Procedure

1. In the module navigation menu, select **Admin** > **Configuration Manager** > **Family Management**.
   The **Family Management** page appears, displaying the list of already existing families.
2. In the left pane, in the **Entity** section, select the RBI Recommendation entity.
   The workspace for the RBI Recommendation entity appears.
3. In the workspace, select the **Datasheets** tabs.
4. Select **Manage Datasheets**.
   The **Datasheet Builder** page appears.
5. On the **Datasheet Caption** drop-down menu, select the RBI Recommendation datasheet.
   The datasheet appears in the **Datasheet Builder** workspace.

   Note: If you have a custom datasheet, select the custom datasheet.
6. In the **Available Items** pane, select the Completion Comments field and drag it into the **Datasheet Builder** workspace.
   The field is added to that datasheet.
7. Select **Save**.
   The datasheet is saved.

Verify Specified Tmin Mapping Availability

Before You Begin

Before you add the Specified Tmin mapping to APM, you must verify if the mapping is already added.

Procedure

1. Using the global search, search for RBI-CNAFC SHARED-MI_MRBIANAL, and then select the data mapping query.
2. In the **Record Explorer**, select **All Possible Families**.
3. Select **Data Mapping Column-Field Pair**.
4. In the **Source Query** box, verify the value. It must be `Public\Meridium\Modules\Risk Based Inspection\Queries\Mapping Queries\RBI-CNAFC Query MI_CCRBICOM`.
5. In the **Datasheet ID** box, select **Mapping Query Details**.
6. Select the **Detail** tab.
7. Verify if the Specified Tmin mapping is available in the list.
8. If the Specified Tmin mapping query is not available, Add Specified Tmin Mapping on page 303 manually.

Add Specified Tmin Mapping

Before You Begin

- Verify if Specified Tmin mapping is already available.

Procedure

1. In the module navigation menu, select **Tools**, and then select **Catalog**.
2. Navigate to Public\Meridium\Modules\Risk Based Inspection\Queries\Mapping Queries.
3. Select the **RBI-CNAFC Query MI_CCRBICOM** data mapping query.

   The **Enter Parameter Values** dialog box appears.
4. Select **Cancel**.
5. Select **Design** tab.
6. In the **Field** row of the table, verify if Specified Tmin is available.
7. If Specified Tmin is available in the table, proceed to step 10.
8. If Specified Tmin is not available, select Specified Tmin from the **Fields** pane.

   Specified Tmin is added to the table.
9. Select  .
10. Using the global search, search for RBI-CNAFC SHARED-MI_MRBIANAL, and then select the data mapping query.
11. In the Record Explorer, select **Data Mapping Column-Field Pair**.
12. In the **Source Query** box, verify the value. It must be Public\Meridium\Modules\Risk Based Inspection\Queries\Mapping Queries\RBI-CNAFC Query MI_CCRBICOM.
13. In the workspace, select  , and then select **Add New Record**.
14. Select **Specified Tmin** in both **Source** and **Target** fields.
15. Select **Save**.

    The Specified Tmin mapping is added.
16. Repeat steps 10 through 15 for the following data mapping queries:
    - RBI-CNAFC MI_CCRBICEB-MI_MRBIANAL by Component
    - RBI-CNAFC MI_CCRBICTB-MI_MRBIANAL by Component
    - RBI-CNAFC SHARED-MI_RBIPIPEANLY

Revert Datasheets to Baseline

About This Task

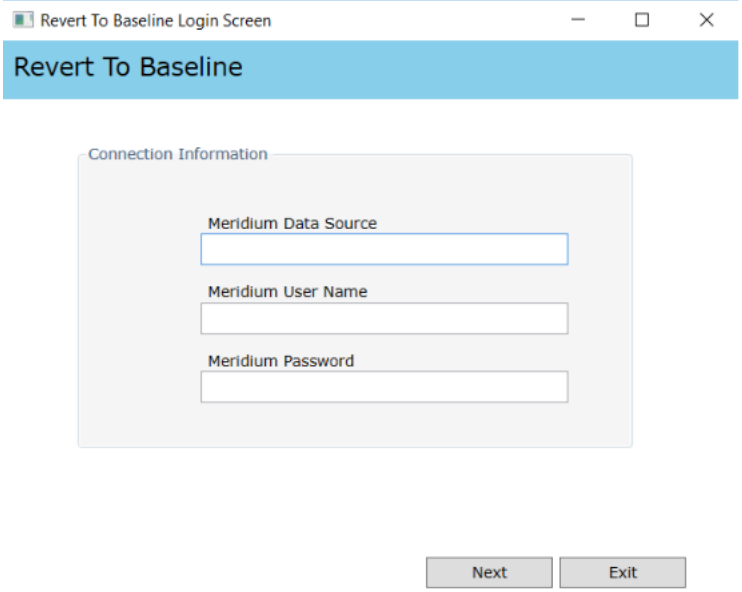
If you have customized the default datasheet, then you must perform the following steps.

Note: Running this utility overwrites your current datasheet and replaces it with the baseline version. You must be a super user in APM to run the Revert to Baseline utility.

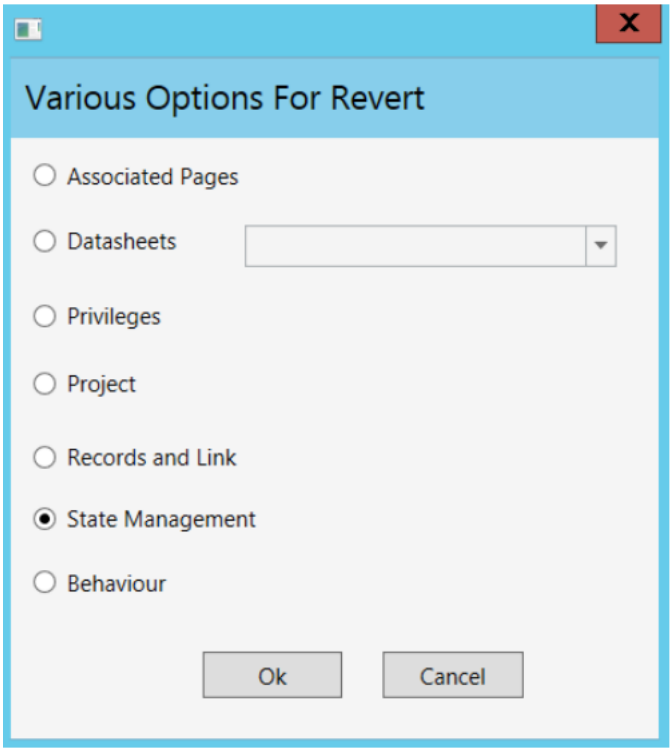
Procedure

1. Log in to the APM Server.

2. Navigate to the `\Meridium\Upgrade\DBUpgrade` folder.
3. Run the `RevertToBaselineApp.exe` file as an administrator.
   The **Revert To Baseline Login Screen** window appears.



4. In the **Meridium Data Source** box, enter the data source name that you want to access.
5. Enter your login credentials, and then select **Next**.
   The available families that can be reverted to baseline appear.
6. Select **Design** tab.
   The available families that can be reverted to baseline appear.
7. Select the family and then select **Revert to Baseline**.
   The **Various Options For Revert** window appears.



8. Select **Datasheets**.
9. Select the default datasheet from the drop-down list box, and then select **Ok**.

Add RBI Component Types

Before You Begin

About This Task

Procedure

1. Log in to APM as an administrator.
2. Go to **Admin > Configuration Manager > System Codes and Tables**.
3. Search for MI RBI COMPONENT TYPES.
4. In the System Code section, select .
   The **Create System Code** window appears.
5. Add the RBI Component Types to the system code table.
6. Select **Save**.
7. Log out of APM and log in.
8. To add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table, perform the following steps:
   a) Select , and enter EquipmentTypes.
      A blank EquipmentTypes datasheet appears.
   b) In the **CriticalityItemType** box, select the existing RBI Component Type that you have added.
   c) Enter values in the required boxes, and then select to save the record.

Risk Based Inspection 581

Deploy RBI 581 for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Review the RBI data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to one or more of the Security Roles used in RBI.	This step is required.
3	Add the following types of RBI 581 users to at least one >TM Security Group: • Users who are responsible for completing the steps necessary to use TM Analysis values to calculate RBI 581 corrosion rates. • Users who should be able to navigate to TM via RBI 581.	This step is required only if you are using the integration between the RBI 581 and Thickness Monitoring modules
4	Select the **Is a Unit?** check box in Functional Location records that represent units in your facility.	This step is required, and marks Functional Location records as Process Units.
5	Using the Belongs to a Unit relationship, link Equipment records to Functional Location records representing units to which that equipment belongs (the **Is a Unit?** check box is selected).	This step is optional.

Step	Task	Notes
6	Add the **RBI-581** tab to the datasheet of the following families: • Criticality RBI Component - Cylindrical Shell • Criticality RBI Component - Exchanger Bundle • Criticality RBI Component - Exchanger Header • Criticality RBI Component - Exchanger Tube • Criticality RBI Component - Piping • Criticality RBI Component - Tank Bottom	This step is required only for families for which you have customized the datasheet.
7	Using Configuration Management, import the following files located in the `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks` folder: • `06_MI_DATA_GRP.xml` • `07_MI_MPPG_QRY.xml` • `08_MI_CLMND_PR.xml`	This step is required only if you are deploying RBI 581 on an existing database. This will create data mappings between families in RBI 581. **Important:** These data mapping records are used in RBI 581 and Risk Based Inspection. After you complete this step, all existing changes to data mapping in the RBI 581 and Risk Based Inspection will be reverted to baseline. All customization for data mappings will be lost. Do not perform this step unless your organization will be satisfied with the baseline data mappings, or you are prepared to customize the records again following the execution of the script.
8	Using Configuration Manager, import the following files located in the `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks` folder: • `101_MI_STMPCNFG.xml` • `102_MI_STRMAPP.xml`	This step is required. This will update the RBI Strategy Mapping Composite entities, overwriting the existing ones.

Step	Task	Notes
9	Update Risk Matrix Mappings and Policies to account for overridden financial consequence for RBI 581 Risk Analyses.	The Operations Category on the Risk Matrix does not account for overridden financial consequence for RBI 581 Risk Analyses. If you are using this feature, you are required to update your Risk Matrix Mappings and Policies by following KBA 000041235.
10	Add RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you want to use additional RBI Component type records that are not provided in the baseline APM database.
11	On the APM Server, restart Redis.	This step is required, and has to be performed after you complete all the previous steps.
12	On the APM Server, reset IIS.	This step is required, and has to be performed after you complete all the previous steps.

Upgrade or Update RBI 581 to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

After you upgrade from a version prior to 4.3.1:

- All RBI Assets with Active Analyses will have a related Inspection Plan record created.
- All RBI recommendations which are not in the Archived state for an RBI Asset with Active Analyses will be related to Inspection Plan record of the RBI Asset.
- The state caption for RBI Recommendation family with State ID MI_ACCEPTED will be updated to Approved.
- The Recommendation Methodology field on RBI Recommendation will be updated to RBI 581 where previously the field had the value RBI 581 Recommendation.
- All security users who belong to the MI RBI Analyst security group will belong to the MI Inspection Plan Approver security role.
- The MI Inspection Plan Approver security role will have the MI ASM Analyst security group assigned.
- Piping Stress updated
  - In some of the Piping Stress records for B31.3, WPB was misspelled as WFB. These records are now updated based on ASME standards.
  - In some of the Piping Stress records for B31.3 and B31.1 for the year 2014, where the Material Specification field contained the value B366 and B622, the Material Grade had

the value NS instead of N/A. These records are now updated based on ASME standards.

- The following new RBI 581 Representative Fluids will be added to match the API 581, 3rd Edition, Addendum 1 specification:
  - Acid-LP
  - Acid-MP
  - Acid-HP
  - C1-C2
  - C3-C4
  - C6-C8
  - C9-C12

  For information on the new RBI 581 Representative Fluid Contents, refer to the topic.
- RBI 581 Representative Fluid contents will be updated for the following fluids to match the API 581, 3rd Edition, Addendum 1 specification:
  - C13-16 (Diesel)
  - C17-25 (Gas Oil)
  - C25+ (Resid)
  - C5
  - Chlorine
  - CO
  - EO
  - H2
  - H2O (Water)
  - H2S
  - HCl
  - HF
  - MEOH (Methanol)
  - NH3
  - Phosgene
  - Steam

  For information on the updated RBI 580 Representative Fluid Contents, refer to the topic.
- RBI 581 Representative Fluid content will be updated for the following families to match the API 581, 3rd Edition, Addendum 1 specification:
  - Component Damage Flammable
  - Toxic Release Constants HFH2S
  - Toxic Cons Eq Constant
  - Toxic Cons Eq Misc Chem

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

Step	Task	Notes
1	Add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you have additional RBI Component type records that are not provided in the baseline APM database.
2	Recalculate the RBI 581 Risk Analyses to get the correct Calculated T-min field value where the Geometry Type field is set to Spherical Head or Hemispherical Head.	This step is required if you have RBI 581 Risk Analyses where Geometry Type field is set to Spherical Head or Hemispherical Head. For more information, refer to KBA 000041564.

Step	Task	Notes
3	Revert the following Risk Based Inspection 581 queries to baseline ◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder. ◦ Equipment Outside Risk Policy ◦ PendingRecommendations ◦ RBI 581 Assets Mitigation Overview Query ◦ RBI 581 Assets Not Mitigated Query ◦ RBI 581 With Plan Analyses Report ◦ RBI 581 Without Plan Analyses Report ◦ RBI Risk Matrix Query ◦ RiskMatrix ◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Queries` folder. ◦ Active Analyses for Evergreening – 581 ◦ Analyses Created For Evergreening – 581 ◦ Analyses Ready For Evergreening – 581 ◦ Asset Corrosion Analysis More Current Than RBI 581 Analyses ◦ Assets with No Recommendations (581 Only) ◦ Inspections More Current Than RBI 581 Analysis ◦ RBI Components for Inventory Group ◦ Analyses Ready For Evergreening for Unit - 581 ◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Report Queries` folder. ◦ RBI 581 Asset Risk-Components ◦ RBI 581 Asset Risk-Corrosion Analysis ◦ RBI 581 Asset Risk-Degradation Mechanisms ◦ RBI 581 Asset Risk-Equipment Data ◦ RBI 581 Asset Risk-Inspection History ◦ RBI 581 Asset Risk-RBIRecommendations ◦ RBI 581 Asset Risk-RefDocuments ◦ RBI 581 Asset Risk-RiskTargetsResults ◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder. ◦ Asset Corrosion Analysis More Current Than All Analyses ◦ Asset Counts for Units ◦ Assets with No Recommendations ◦ Current Risk ◦ Current Risk Overview ◦ Inspections More Current Than All Analysis ◦ Past Risk ◦ Past Risk Overview ◦ RBI Asset Risk Query ◦ RBI Assets for a Functional Location ◦ RBI Components for Unit ◦ Select Protected Assets ◦ Select RBI Components ◦ View Protected RBI Components ◦ Review Analyses by Asset ◦ Review Analyses by Asset 581 ◦ Review Analyses by Corrosion Loop ◦ Review Analyses by Corrosion Loop 581 ◦ Process Unit Query	This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
4	Update Dynamic Viscosity for H2O (Water) record in RepresentativeFluids.	This step is required only if you have previously modified H2O (Water) record in RepresentativeFluids family. For more information, refer to KBA 000057776.
5	Revert the following Risk Based Inspection 581 queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder. ◦ Inspections More Current Than All Analysis ◦ `Public\Meridium\Modules\Risk Based Inspection -581\Queries` folder. ◦ Inspections More Current Than RBI 581 Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.
6	Update PV Stress content and stress lookup fields for RBI 581 Risk Analyses in created state.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000051571.
7	Update PV Stress content and calculate Flow Stress for RBI 581 Risk Analyses in created state with Design Code ASME VIII DIV 1 and Code Year 1998.	This step is required only if you want to use the Pressure Vessel stress content with updated Minimum Tensile Strength and Minimum Yield Strength for Design Code ASME VIII DIV 1 and Code Year 1998, to calculate the Flow Stress. For more information, refer to KBA 000059269.

- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

Step	Task	Notes
1	Add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you have additional RBI Component type records that are not provided in the baseline APM database.
2	Recalculate the RBI 581 Risk Analyses to get the correct Calculated T-min field value where the Geometry Type field is set to Spherical Head or Hemispherical Head.	This step is required if you have RBI 581 Risk Analyses where Geometry Type field is set to Spherical Head or Hemispherical Head. For more information, refer to KBA 000041564.

Step	Task	Notes
3	Revert the following Risk Based Inspection 581 queries to baseline ◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder. ◦ Equipment Outside Risk Policy ◦ PendingRecommendations ◦ RBI 581 Assets Mitigation Overview Query ◦ RBI 581 Assets Not Mitigated Query ◦ RBI 581 With Plan Analyses Report ◦ RBI 581 Without Plan Analyses Report ◦ RBI Risk Matrix Query ◦ RiskMatrix ◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Queries` folder. ◦ Active Analyses for Evergreening – 581 ◦ Analyses Created For Evergreening – 581 ◦ Analyses Ready For Evergreening – 581 ◦ Asset Corrosion Analysis More Current Than RBI 581 Analyses ◦ Assets with No Recommendations (581 Only) ◦ Inspections More Current Than RBI 581 Analysis ◦ RBI Components for Inventory Group ◦ Analyses Ready For Evergreening for Unit - 581 ◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Report Queries` folder. ◦ RBI 581 Asset Risk-Components ◦ RBI 581 Asset Risk-Corrosion Analysis ◦ RBI 581 Asset Risk-Degradation Mechanisms ◦ RBI 581 Asset Risk-Equipment Data ◦ RBI 581 Asset Risk-Inspection History ◦ RBI 581 Asset Risk-RBIRecommendations ◦ RBI 581 Asset Risk-RefDocuments ◦ RBI 581 Asset Risk-RiskTargetsResults ◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder. ◦ Asset Corrosion Analysis More Current Than All Analyses ◦ Asset Counts for Units ◦ Assets with No Recommendations ◦ Current Risk ◦ Current Risk Overview ◦ Inspections More Current Than All Analysis ◦ Past Risk ◦ Past Risk Overview ◦ RBI Asset Risk Query ◦ RBI Assets for a Functional Location ◦ RBI Components for Unit ◦ Select Protected Assets ◦ Select RBI Components ◦ View Protected RBI Components ◦ Review Analyses by Asset ◦ Review Analyses by Asset 581 ◦ Review Analyses by Corrosion Loop ◦ Review Analyses by Corrosion Loop 581 ◦ Process Unit Query	This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
4	Update Dynamic Viscosity for H2O (Water) record in RepresentativeFluids.	This step is required only if you have previously modified H2O (Water) record in RepresentativeFluids family. For more information, refer to KBA 000057776.
5	Revert the following Risk Based Inspection 581 queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder. ◦ Inspections More Current Than All Analysis ◦ `Public\Meridium\Modules\Risk Based Inspection -581\Queries` folder. ◦ Inspections More Current Than RBI 581 Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.
6	Update PV Stress content and stress lookup fields for RBI 581 Risk Analyses in created state.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000051571.
7	Update PV Stress content and calculate Flow Stress for RBI 581 Risk Analyses in created state with Design Code ASME VIII DIV 1 and Code Year 1998.	This step is required only if you want to use the Pressure Vessel stress content with updated Minimum Tensile Strength and Minimum Yield Strength for Design Code ASME VIII DIV 1 and Code Year 1998, to calculate the Flow Stress. For more information, refer to KBA 000059269.

- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16.

Step	Task	Notes
1	Revert the following Risk Based Inspection 581 queries to baseline: ◦ `Public/Meridium/Modules/RBI 581/Queries/Active Analyses for Evergreening - 581` ◦ `Public/Meridium/Modules/RBI 581/Queries/Analyses Created for Evergreening - 581`	This step is required if you have modified any of the following queries: ◦ Active Analyses for Evergreening – 581 ◦ Analyses Created for Evergreening - 581 **Note:** If you have not modified any of the above-mentioned queries, you do not have to complete this step for the specified query.
2	Update RBI 581 Risk Analyses or RBI Components that have a Storage Tank Bottom as the Component Type and a related RBI Component family other than **Criticality RBI Component – Tank Bottom**.	This step is required if you have RBI 581 Risk Analyses with the Component Type field set to Storage Tank Bottom and the related RBI Component family is not Criticality RBI Component - Tank Bottom. **Note:** RBI 581 Analyses now performs AST Shell calculations for a Component Type defined as Storage Tank regardless of the related RBI Component family. Also, an RBI 581 Risk Analyses calculation will display a validation error message if the Component Type field value on the RBI Analysis is set to Storage Tank Bottom and the related Component Family is not Criticality RBI Component -Tank Bottom. You can verify the existence of these analyses by running the following query: `SELECT DISTINCT [MI_581RANAL].[MI_AN_ANALY_ID_CHR] "Analysis ID", [MI_CCRBICOM].[MI_RBICOMPO_COMPO_C] "Component" FROM [MI_CCRBICTB], [MI_581RANAL] JOIN {MIR_RBICRAN} ON [MI_581RANAL].ENTY_KEY = {MIR_RBICRAN}.SUCC_ENTY_KEY JOIN [MI_CCRBICOM] ON {MIR_RBICRAN}.PRED_ENTY_KEY = [MI_CCRBICOM].ENTY_KEY WHERE ([MI_CCRBICOM].FMLY_KEY <> [MI_CCRBICTB].FMLY_KEY AND [MI_581RANAL].[MI_CRITANAL_COMP_TP_C] = 'Storage Tank Bottom')` For more information, access the KBA 000059408.
3	Recalculate the RBI 581 Risk Analyses where the values for Initial Fluid Phase and Release Fluid Phase fields differ.	This step is required if you have RBI 581 Risk Analyses having different values for Initial Fluid Phase and Release Fluid Phase fields. For more information, access KBA 000060392.
4	Recalculate the RBI 581 Risk Analyses to get the correct Calculated T-min field value where the Geometry Type field is set to Piping.	This step is required if you have RBI 581 Risk Analyses where Geometry Type field is set to Piping. For more information, access KBA 000060763.

Step	Task	Notes
5	Update records for ALCL3 in Toxic Consequence Equation Miscellaneous Chemicals table.This step is required if you have RBI 581 Risk Analyses on AST	This step is required if you have RBI 581 Risk Analyses on AST Shell component having ALCL3 as toxic fluid. For more information, access the KBA 000059939.

Step	Task	Notes
6	Revert the following Risk Based Inspection 581 queries to baseline ◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder. ◦ Equipment Outside Risk Policy ◦ PendingRecommendations ◦ RBI 581 Assets Mitigation Overview Query ◦ RBI 581 Assets Not Mitigated Query ◦ RBI 581 With Plan Analyses Report ◦ RBI 581 Without Plan Analyses Report ◦ RBI Risk Matrix Query ◦ RiskMatrix ◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Queries` folder. ◦ Active Analyses for Evergreening – 581 ◦ Analyses Created For Evergreening – 581 ◦ Analyses Ready For Evergreening – 581 ◦ Asset Corrosion Analysis More Current Than RBI 581 Analyses ◦ Assets with No Recommendations (581 Only) ◦ Inspections More Current Than RBI 581 Analysis ◦ RBI Components for Inventory Group ◦ Analyses Ready For Evergreening for Unit - 581 ◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Report Queries` folder. ◦ RBI 581 Asset Risk-Components ◦ RBI 581 Asset Risk-Corrosion Analysis ◦ RBI 581 Asset Risk-Degradation Mechanisms ◦ RBI 581 Asset Risk-Equipment Data ◦ RBI 581 Asset Risk-Inspection History ◦ RBI 581 Asset Risk-RBIRecommendations ◦ RBI 581 Asset Risk-RefDocuments ◦ RBI 581 Asset Risk-	This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
7	Update Dynamic Viscosity for H2O (Water) record in RepresentativeFluids.	This step is required only if you have previously modified H2O (Water) record in RepresentativeFluids family. For more information, refer to KBA 000057776.
8	Add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you have additional RBI Component type records that are not provided in the baseline APM database.
9	Recalculate the RBI 581 Risk Analyses to get the correct Calculated T-min field value where the Geometry Type field is set to Spherical Head or Hemispherical Head.	This step is required if you have RBI 581 Risk Analyses where Geometry Type field is set to Spherical Head or Hemispherical Head. For more information, refer to KBA 000041564.
10	Revert the following Risk Based Inspection 581 queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder. ◦ Inspections More Current Than All Analysis ◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Queries` folder. ◦ Inspections More Current Than RBI 581 Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.
11	Update PV Stress content and stress lookup fields for RBI 581 Risk Analyses in created state.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000051571.
12	Update PV Stress content and calculate Flow Stress for RBI 581 Risk Analyses in created state with Design Code ASME VIII DIV 1 and Code Year 1998.	This step is required only if you want to use the Pressure Vessel stress content with updated Minimum Tensile Strength and Minimum Yield Strength for Design Code ASME VIII DIV 1 and Code Year 1998, to calculate the Flow Stress. For more information, refer to KBA 000059269

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11.

<table>
<tr><th>Step</th><th>Task</th><th>Notes</th></tr>
<tr><td>1</td><td>Add the Completion Comments field to the RBI Recommendation datasheet.</td><td>This step is required only if you have customized the RBI Recommendation datasheet.</td></tr>
<tr><td>2</td><td>Add the following state and operations to RBI Recommendation State Management:

Table 4: State
<table><tr><th>State ID</th><th>State Caption</th></tr><tr><td>MI_NOTREQUIRED</td><td>Not Required</td></tr></table>
Table 5: Operations
<table><tr><th>Operation ID</th><th>Operation Caption</th><th>Predecessor State</th><th>Successor State</th></tr><tr><td>MI_NRQARCHIVED</td><td>Archive</td><td>Not Required</td><td>Archived</td></tr><tr><td>MI_MARKNOTREQUIRED</td><td>Mark Not Required</td><td>Proposed</td><td>Not Required</td></tr></table>
For information on adding State and Operation to a family, refer to the Family Management documentation.</td><td>This step is required because the State Machine for RBI Recommendation is not updated automatically if the RBI Recommendation family has records.</td></tr>
<tr><td>3</td><td>Using the Query tool, run the following query:
<pre>UPDATE [MI_RMMPG]
SET [MI_RMMPG].
[MI_RMMPG_SOURCE_FLD_
C] =
'MI_RBDEMECH_TOTAL_PF
_RBI_DTE_N'
WHERE [MI_RMMPG].
[MI_RMMPG_SOURCE_FLD_
C] =
'MI_RBDEMECH_POF_N'</pre></td><td>This step is required. This will update the RBI Risk Matrix Mapping records such that the Total POF - RBI Date value is used to plot probability of failure (POF) on the risk matrix, instead of the Total POF With Plan value.
Important:
This step is only applicable to version 4.3.0.0.0 or if you have modified the RBI Risk Matrix Mapping family.
After you complete this step, any customization done on the POF data mapping will be lost. Do not perform this step unless your organization will be satisfied with the baseline data mappings, or you are prepared to customize the records again following the execution of the query.</td></tr>
<tr><td>4</td><td>Revert the following Process Units overview queries to baseline:
Public/Meridium/Modules/Risk Based Inspection/Queries/Asset Counts for Units
Public/Meridium/Modules/Risk Based Inspection/Queries/Process Unit Query</td><td>This step is required only if you have modified the following queries that are used for the Process Units tab in the Risk Based Inspection Overview page:
Asset Counts for Units
Process Unit Query</td></tr>
</table>

Step	Task	Notes
5	Update Risk Matrix Mappings and Policies to account for overridden financial consequence for RBI 581 Risk Analyses.	The Operations Category on the Risk Matrix does not account for overridden financial consequence for RBI 581 Risk Analyses. If you are using this feature, you are required to update your Risk Matrix Mappings and Policies by following KBA 000041235.

Step	Task	Notes

6	Revert the following Risk Based Inspection 581 queries to baseline
	◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder.
	  ◦ Equipment Outside Risk Policy
	  ◦ PendingRecommendations
	  ◦ RBI 581 Assets Mitigation Overview Query
	  ◦ RBI 581 Assets Not Mitigated Query
	  ◦ RBI 581 With Plan Analyses Report
	  ◦ RBI 581 Without Plan Analyses Report
	  ◦ RBI Risk Matrix Query
	  ◦ RiskMatrix
	◦ `Public\Meridium\Modules\Risk Based Inspection – 581\Queries` folder.
	  ◦ Active Analyses for Evergreening – 581
	  ◦ Analyses Created For Evergreening – 581
	  ◦ Analyses Ready For Evergreening – 581
	  ◦ Asset Corrosion Analysis More Current Than RBI 581 Analyses
	  ◦ Assets with No Recommendations (581 Only)
	  ◦ Inspections More Current Than RBI 581 Analysis
	  ◦ RBI Components for Inventory Group
	  ◦ Analyses Ready For Evergreening for Unit - 581
	◦ `Public\Meridium\Modules\Risk Based Inspection – 581\Report Queries` folder.
	  ◦ RBI 581 Asset Risk-Components
	  ◦ RBI 581 Asset Risk-Corrosion Analysis
	  ◦ RBI 581 Asset Risk-Degradation Mechanisms
	  ◦ RBI 581 Asset Risk-Equipment Data
	  ◦ RBI 581 Asset Risk-Inspection History
	  ◦ RBI 581 Asset Risk-RBIRecommendations
	  ◦ RBI 581 Asset Risk-RefDocuments
	  ◦ RBI 581 Asset Risk-RiskTargetsResults
	◦ `Public\Meridium`
		This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
7	Update Dynamic Viscosity for H2O (Water) record in RepresentativeFluids.	This step is required only if you have previously modified H2O (Water) record in RepresentativeFluids family. For more information, refer to KBA 000057776.
8	Using Configuration Manager, import the following files located in the ◦ `C:\Meridium\DbUpg\MI_DB_MASTER_4050100\4050100\_IEU_ManualImports` folder. ◦ MI_PRL_CNS0.xml ◦ MI_REPFLUID_581.xml ◦ MI_CMT_FLE0.xml	This step is required only if you have modified the properties of any of the 580 Representative fluids: ◦ Acid ◦ Acid-HP ◦ Acid-LP ◦ Acid-MP ◦ ALCL3 ◦ C13-16 (Diesel) ◦ C17-25 (Gas Oil) ◦ C1-C2 ◦ C25+ (Resid) ◦ C3-C4 ◦ C5 ◦ C6 ◦ C6-C8 ◦ C9-C12 ◦ CO ◦ DEE ◦ EE ◦ EEA ◦ EG ◦ EO ◦ H2 ◦ H2O (Water) ◦ H2S ◦ HCl ◦ HF ◦ MEOH (Methanol) ◦ NH3 ◦ Nitric Acid ◦ NO2 ◦ Phosgene ◦ PO ◦ Pyrophoric ◦ Steam ◦ Styrene (Aromatic) ◦ TD
9	Add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you have additional RBI Component type records that are not provided in the baseline APM database.
10	Recalculate the RBI 581 Risk Analyses to get the correct Calculated T-min field value where the Geometry Type field is set to Spherical Head or Hemispherical Head.	This step is required if you have RBI 581 Risk Analyses where Geometry Type field is set to Spherical Head or Hemispherical Head. For more information, refer to KBA 000041564.

Step	Task	Notes
11	Revert the following Risk Based Inspection 581 queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder. ◦ Inspections More Current Than All Analysis ◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Queries` folder. ◦ Inspections More Current Than RBI 581 Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.
12	Update PV Stress content and stress lookup fields for RBI 581 Risk Analyses in created state.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000051571.
13	Update PV Stress content and calculate Flow Stress for RBI 581 Risk Analyses in created state with Design Code ASME VIII DIV 1 and Code Year 1998.	This step is required only if you want to use the Pressure Vessel stress content with updated Minimum Tensile Strength and Minimum Yield Strength for Design Code ASME VIII DIV 1 and Code Year 1998, to calculate the Flow Stress. For more information, refer to KBA 000059269

- Upgrade from any version V4.2.0.0 through V4.2.0.9.5.

Step	Task	Notes
1	Using Configuration Manager, import the following files located in the `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks` folder: ◦ `06_MI_DATA_GRP.xml` ◦ `07_MI_MPPG_QRY.xml` ◦ `08_MI_CLMND_PR.xml`	This step is required only if you have not performed it during a previous upgrade. This will create data mappings between families in RBI 581. **Important:** After you complete this step, all existing changes to data mapping in the RBI 581and Risk Based Inspection modules will be reverted to baseline. All customization for data mappings will be lost. Do not perform this step unless your organization will be satisfied with the baseline data mappings, or you are prepared to customize the records again following the execution of the script.
2	Using Configuration Manager, import the following files located in the `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks` folder: ◦ `101_MI_STMPCNFG.xml` ◦ `102_MI_STRMAPP.xml`	This step is required. This will update the RBI Strategy Mapping Composite entities, overwriting the existing ones.
3	Add the **RBI-581** tab to the datasheet of the following families: ◦ Criticality RBI Component - Cylindrical Shell ◦ Criticality RBI Component - Exchanger Bundle ◦ Criticality RBI Component - Exchanger Header ◦ Criticality RBI Component - Exchanger Tube ◦ Criticality RBI Component - Piping ◦ Criticality RBI Component - Tank Bottom	This step is required only for families for which you have customized the datasheet and if you have not performed it during a previous upgrade.
4	Using the Query tool, run the following query: `UPDATE [MI_RMMPG] SET [MI_RMMPG].[MI_RMMPG_SOURCE_FLD_C] = 'MI_RBDEMECH_TOTAL_PF_RBI_DTE_N' WHERE [MI_RMMPG].[MI_RMMPG_SOURCE_FLD_C] = 'MI_RBDEMECH_POF_N'`	This step is required. This will update the RBI Risk Matrix Mapping records such that Total POF - RBI Date value is used to plot probability of failure (POF) on the risk matrix, instead of the Total POF With Plan value. **Important:** After you complete this step, any customization done on the POF data mapping will be lost. Do not perform this step unless your organization will be satisfied with the baseline data mappings, or you are prepared to customize the records again following the execution of the query.

Step	Task	Notes
5	On the APM Server, reset IIS.	This step is required, and has to be performed after you complete all the aforementioned steps.

Step	Task	Notes
6	Revert the following Risk Based Inspection 581 queries to baseline ◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder. ◦ Equipment Outside Risk Policy ◦ PendingRecommendations ◦ RBI 581 Assets Mitigation Overview Query ◦ RBI 581 Assets Not Mitigated Query ◦ RBI 581 With Plan Analyses Report ◦ RBI 581 Without Plan Analyses Report ◦ RBI Risk Matrix Query ◦ RiskMatrix ◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Queries` folder. ◦ Active Analyses for Evergreening – 581 ◦ Analyses Created For Evergreening – 581 ◦ Analyses Ready For Evergreening – 581 ◦ Asset Corrosion Analysis More Current Than RBI 581 Analyses ◦ Assets with No Recommendations (581 Only) ◦ Inspections More Current Than RBI 581 Analysis ◦ RBI Components for Inventory Group ◦ Analyses Ready For Evergreening for Unit - 581 ◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Report Queries` folder. ◦ RBI 581 Asset Risk-Components ◦ RBI 581 Asset Risk-Corrosion Analysis ◦ RBI 581 Asset Risk-Degradation Mechanisms ◦ RBI 581 Asset Risk-Equipment Data ◦ RBI 581 Asset Risk-Inspection History ◦ RBI 581 Asset Risk-RBIRecommendations ◦ RBI 581 Asset Risk-RefDocuments ◦ RBI 581 Asset Risk-RiskTargetsResults ◦ `Public\Meridium\Modules\Risk Based`	This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
7	Update Dynamic Viscosity for H2O (Water) record in RepresentativeFluids.	This step is required only if you have previously modified H2O (Water) record in RepresentativeFluids family. For more information, refer to KBA 000057776.
8	Using Configuration Manager, import the following files located in the ◦ `C:\Meridium\DbUpg\MI_DB_MASTER_4050100\4050100\_IEU_ManualImports` folder. ◦ MI_PRL_CNS0.xml ◦ MI_REPFLUID_581.xml ◦ MI_CMT_FLE0.xml	This step is required only if you have modified the properties of any of the 580 Representative fluids: ◦ Acid ◦ Acid-HP ◦ Acid-LP ◦ Acid-MP ◦ ALCL3 ◦ C13-16 (Diesel) ◦ C17-25 (Gas Oil) ◦ C1-C2 ◦ C25+ (Resid) ◦ C3-C4 ◦ C5 ◦ C6 ◦ C6-C8 ◦ C9-C12 ◦ CO ◦ DEE ◦ EE ◦ EEA ◦ EG ◦ EO ◦ H2 ◦ H2O (Water) ◦ H2S ◦ HCl ◦ HF ◦ MEOH (Methanol) ◦ NH3 ◦ Nitric Acid ◦ NO2 ◦ Phosgene ◦ PO ◦ Pyrophoric ◦ Steam ◦ Styrene (Aromatic) ◦ TD
9	Add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you have additional RBI Component type records that are not provided in the baseline APM database.
10	Recalculate the RBI 581 Risk Analyses to get the correct Calculated T-min field value where the Geometry Type field is set to Spherical Head or Hemispherical Head.	This step is required if you have RBI 581 Risk Analyses where Geometry Type field is set to Spherical Head or Hemispherical Head. For more information, refer to KBA 000041564.

Step	Task	Notes

11	Revert the following Risk Based Inspection 581 queries to baseline
	◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder.
	  ◦ Inspections More Current Than All Analysis
	◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Queries` folder.
	  ◦ Inspections More Current Than RBI 581 Analysis
		This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.

12	Update PV Stress content and stress lookup fields for RBI 581 Risk Analyses in created state.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000051571.
13	Update PV Stress content and calculate Flow Stress for RBI 581 Risk Analyses in created state with Design Code ASME VIII DIV 1 and Code Year 1998.	This step is required only if you want to use the Pressure Vessel stress content with updated Minimum Tensile Strength and Minimum Yield Strength for Design Code ASME VIII DIV 1 and Code Year 1998, to calculate the Flow Stress. For more information, refer to KBA 000059269.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	Using Configuration Manager, import the following files located in the `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks` folder: ◦ `06_MI_DATA_GRP.xml` ◦ `07_MI_MPPG_QRY.xml` ◦ `08_MI_CLMND_PR.xml`	This step is required only if you have not performed it during a previous upgrade. This will create data mappings between families in RBI 581. **Important:** After you complete this step, all existing changes to data mapping in the RBI 581and Risk Based Inspection modules will be reverted to baseline. All customization for data mappings will be lost. Do not perform this step unless your organization will be satisfied with the baseline data mappings, or you are prepared to customize the records again following the execution of the script.
2	Using Configuration Manager, import the following files located in the `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks` folder: ◦ `101_MI_STMPCNFG.xml` ◦ `102_MI_STRMAPP.xml`	This step is required. This will update the RBI Strategy Mapping Composite entities, overwriting the existing ones.
3	Add the **RBI-581** tab to the datasheet of the following families: ◦ Criticality RBI Component - Cylindrical Shell ◦ Criticality RBI Component - Exchanger Bundle ◦ Criticality RBI Component - Exchanger Header ◦ Criticality RBI Component - Exchanger Tube ◦ Criticality RBI Component - Piping ◦ Criticality RBI Component - Tank Bottom	This step is required only for families for which you have customized the datasheet and if you have not performed it during a previous upgrade.
4	Using the Query tool, run the following query: `UPDATE [MI_RMMPG] SET [MI_RMMPG].[MI_RMMPG_SOURCE_FLD_C] = 'MI_RBDEMECH_TOTAL_PF_RBI_DTE_N' WHERE [MI_RMMPG].[MI_RMMPG_SOURCE_FLD_C] = 'MI_RBDEMECH_POF_N'`	This step is required. This will update the RBI Risk Matrix Mapping records such that Total POF - RBI Date value is used to plot probability of failure (POF) on the risk matrix, instead of the Total POF With Plan value. **Important:** After you complete this step, any customization done on the POF data mapping will be lost. Do not perform this step unless your organization will be satisfied with the baseline data mappings, or you are prepared to customize the records again following the execution of the query.

Step	Task	Notes
5	On the APM Server, reset IIS.	This step is required, and has to be performed after you complete all the aforementioned steps.

Step	Task	Notes

6	Revert the following Risk Based Inspection 581 queries to baseline
	◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder.
	  ◦ Equipment Outside Risk Policy
	  ◦ PendingRecommendations
	  ◦ RBI 581 Assets Mitigation Overview Query
	  ◦ RBI 581 Assets Not Mitigated Query
	  ◦ RBI 581 With Plan Analyses Report
	  ◦ RBI 581 Without Plan Analyses Report
	  ◦ RBI Risk Matrix Query
	  ◦ RiskMatrix
	◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Queries` folder.
	  ◦ Active Analyses for Evergreening – 581
	  ◦ Analyses Created For Evergreening – 581
	  ◦ Analyses Ready For Evergreening – 581
	  ◦ Asset Corrosion Analysis More Current Than RBI 581 Analyses
	  ◦ Assets with No Recommendations (581 Only)
	  ◦ Inspections More Current Than RBI 581 Analysis
	  ◦ RBI Components for Inventory Group
	  ◦ Analyses Ready For Evergreening for Unit - 581
	◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Report Queries` folder.
	  ◦ RBI 581 Asset Risk-Components
	  ◦ RBI 581 Asset Risk-Corrosion Analysis
	  ◦ RBI 581 Asset Risk-Degradation Mechanisms
	  ◦ RBI 581 Asset Risk-Equipment Data
	  ◦ RBI 581 Asset Risk-Inspection History
	  ◦ RBI 581 Asset Risk-RBIRecommendations
	  ◦ RBI 581 Asset Risk-RefDocuments
	  ◦ RBI 581 Asset Risk-RiskTargetsResults
	◦ `Public\Meridium\Modules\Risk Based`
		This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
7	Update Dynamic Viscosity for H2O (Water) record in RepresentativeFluids.	This step is required only if you have previously modified H2O (Water) record in RepresentativeFluids family. For more information, refer to KBA 000057776.
8	Using Configuration Manager, import the following files located in the ◦ `C:\Meridium\DbUpg\MI_DB_MASTER_4050100\4050100\_IEU_ManualImports` folder. ◦ MI_PRL_CNS0.xml ◦ MI_REPFLUID_581.xml ◦ MI_CMT_FLE0.xml	This step is required only if you have modified the properties of any of the 580 Representative fluids: ◦ Acid ◦ Acid-HP ◦ Acid-LP ◦ Acid-MP ◦ ALCL3 ◦ C13-16 (Diesel) ◦ C17-25 (Gas Oil) ◦ C1-C2 ◦ C25+ (Resid) ◦ C3-C4 ◦ C5 ◦ C6 ◦ C6-C8 ◦ C9-C12 ◦ CO ◦ DEE ◦ EE ◦ EEA ◦ EG ◦ EO ◦ H2 ◦ H2O (Water) ◦ H2S ◦ HCl ◦ HF ◦ MEOH (Methanol) ◦ NH3 ◦ Nitric Acid ◦ NO2 ◦ Phosgene ◦ PO ◦ Pyrophoric ◦ Steam ◦ Styrene (Aromatic) ◦ TD
9	Add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you have additional RBI Component type records that are not provided in the baseline APM database.
10	Recalculate the RBI 581 Risk Analyses to get the correct Calculated T-min field value where the Geometry Type field is set to Spherical Head or Hemispherical Head.	This step is required if you have RBI 581 Risk Analyses where Geometry Type field is set to Spherical Head or Hemispherical Head. For more information, refer to KBA 000041564.

Step	Task	Notes

11	Revert the following Risk Based Inspection 581 queries to baseline
	◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder.
	  ◦ Inspections More Current Than All Analysis
	◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Queries` folder.
	  ◦ Inspections More Current Than RBI 581 Analysis
		This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.

12	Update PV Stress content and stress lookup fields for RBI 581 Risk Analyses in created state.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000051571.
13	Update PV Stress content and calculate Flow Stress for RBI 581 Risk Analyses in created state with Design Code ASME VIII DIV 1 and Code Year 1998.	This step is required only if you want to use the Pressure Vessel stress content with updated Minimum Tensile Strength and Minimum Yield Strength for Design Code ASME VIII DIV 1 and Code Year 1998, to calculate the Flow Stress. For more information, refer to KBA 000059269.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

Step	Task	Notes
1	Copy your customized SQL code from the Review Analyses by Asset query to the Review Analyses by Asset 580 query, and then replace the Review Analyses by Asset query with its baseline version.	This step is required only if you have previously customized the query that is used to populate the list of analyses on the **RBI - Review Analyses** page, and only if you will have the RBI 581 and Risk Based Inspection modules active at the same time.
2	Add the **RBI-581** tab to the datasheet of the following families: ◦ Criticality RBI Component - Cylindrical Shell ◦ Criticality RBI Component - Exchanger Bundle ◦ Criticality RBI Component - Exchanger Header ◦ Criticality RBI Component - Exchanger Tube ◦ Criticality RBI Component - Piping ◦ Criticality RBI Component - Tank Bottom	This step is required only for families for which you have customized the datasheet.

Step	Task	Notes

3	Revert the following Risk Based Inspection 581 queries to baseline
	◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder.
	  ◦ Equipment Outside Risk Policy
	  ◦ PendingRecommendations
	  ◦ RBI 581 Assets Mitigation Overview Query
	  ◦ RBI 581 Assets Not Mitigated Query
	  ◦ RBI 581 With Plan Analyses Report
	  ◦ RBI 581 Without Plan Analyses Report
	  ◦ RBI Risk Matrix Query
	  ◦ RiskMatrix
	◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Queries` folder.
	  ◦ Active Analyses for Evergreening – 581
	  ◦ Analyses Created For Evergreening – 581
	  ◦ Analyses Ready For Evergreening – 581
	  ◦ Asset Corrosion Analysis More Current Than RBI 581 Analyses
	  ◦ Assets with No Recommendations (581 Only)
	  ◦ Inspections More Current Than RBI 581 Analysis
	  ◦ RBI Components for Inventory Group
	  ◦ Analyses Ready For Evergreening for Unit - 581
	◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Report Queries` folder.
	  ◦ RBI 581 Asset Risk-Components
	  ◦ RBI 581 Asset Risk-Corrosion Analysis
	  ◦ RBI 581 Asset Risk-Degradation Mechanisms
	  ◦ RBI 581 Asset Risk-Equipment Data
	  ◦ RBI 581 Asset Risk-Inspection History
	  ◦ RBI 581 Asset Risk-RBIRecommendations
	  ◦ RBI 581 Asset Risk-RefDocuments
	  ◦ RBI 581 Asset Risk-RiskTargetsResults
	◦ `Public\Meridium\Modules\Risk Based`
		This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
4	Update Dynamic Viscosity for H2O (Water) record in RepresentativeFluids.	This step is required only if you have previously modified H2O (Water) record in RepresentativeFluids family. For more information, refer to KBA 000057776.
5	Using Configuration Manager, import the following files located in the ◦ `C:\Meridium\DbUpg\MI_DB_MASTER_4050100\4050100\_IEU_ManualImports` folder. ◦ MI_PRL_CNS0.xml ◦ MI_REPFLUID_581.xml ◦ MI_CMT_FLE0.xml	This step is required only if you have modified the properties of any of the 580 Representative fluids: ◦ Acid ◦ Acid-HP ◦ Acid-LP ◦ Acid-MP ◦ ALCL3 ◦ C13-16 (Diesel) ◦ C17-25 (Gas Oil) ◦ C1-C2 ◦ C25+ (Resid) ◦ C3-C4 ◦ C5 ◦ C6 ◦ C6-C8 ◦ C9-C12 ◦ CO ◦ DEE ◦ EE ◦ EEA ◦ EG ◦ EO ◦ H2 ◦ H2O (Water) ◦ H2S ◦ HCl ◦ HF ◦ MEOH (Methanol) ◦ NH3 ◦ Nitric Acid ◦ NO2 ◦ Phosgene ◦ PO ◦ Pyrophoric ◦ Steam ◦ Styrene (Aromatic) ◦ TD
6	Add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you have additional RBI Component type records that are not provided in the baseline APM database.

Step	Task	Notes
7	Recalculate the RBI 581 Risk Analyses to get the correct Calculated T-min field value where the Geometry Type field is set to Spherical Head or Hemispherical Head.	This step is required if you have RBI 581 Risk Analyses where Geometry Type field is set to Spherical Head or Hemispherical Head. For more information, refer to KBA 000041564.
8	Revert the following Risk Based Inspection 581 queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder. ◦ Inspections More Current Than All Analysis ◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Queries` folder. ◦ Inspections More Current Than RBI 581 Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.

- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

  RBI 581 has been introduced in APM V3.6.0.8.0. Therefore, if you have an earlier version of APM, then you must follow the steps in the first-time deployment of RBI 581. If you have deployed RBI 581 in APM V3.6.0.8.0 or later, you must follow the steps outlined in the following table.

Step	Task	Notes
1	Copy your customized SQL code from the Review Analyses by Asset query to the Review Analyses by Asset 580 query, and then replace the Review Analyses by Asset query with its baseline version.	This step is required only if you have previously customized the query that is used to populate the list of analyses on the **RBI - Review Analyses** page, and only if you will have the RBI 581 and Risk Based Inspection modules active at the same time.
2	Add the **RBI-581** tab to the datasheet of the following families: ◦ Criticality RBI Component - Cylindrical Shell ◦ Criticality RBI Component - Exchanger Bundle ◦ Criticality RBI Component - Exchanger Header ◦ Criticality RBI Component - Exchanger Tube ◦ Criticality RBI Component - Piping ◦ Criticality RBI Component - Tank Bottom	This step is required only for families for which you have customized the datasheet.

Step	Task	Notes

3	Revert the following Risk Based Inspection 581 queries to baseline
	◦ `Public\Meridium\Modules\Mechanical Integrity\Queries\Dashboard Queries` folder.
	  ◦ Equipment Outside Risk Policy
	  ◦ PendingRecommendations
	  ◦ RBI 581 Assets Mitigation Overview Query
	  ◦ RBI 581 Assets Not Mitigated Query
	  ◦ RBI 581 With Plan Analyses Report
	  ◦ RBI 581 Without Plan Analyses Report
	  ◦ RBI Risk Matrix Query
	  ◦ RiskMatrix
	◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Queries` folder.
	  ◦ Active Analyses for Evergreening – 581
	  ◦ Analyses Created For Evergreening – 581
	  ◦ Analyses Ready For Evergreening – 581
	  ◦ Asset Corrosion Analysis More Current Than RBI 581 Analyses
	  ◦ Assets with No Recommendations (581 Only)
	  ◦ Inspections More Current Than RBI 581 Analysis
	  ◦ RBI Components for Inventory Group
	  ◦ Analyses Ready For Evergreening for Unit - 581
	◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Report Queries` folder.
	  ◦ RBI 581 Asset Risk-Components
	  ◦ RBI 581 Asset Risk-Corrosion Analysis
	  ◦ RBI 581 Asset Risk-Degradation Mechanisms
	  ◦ RBI 581 Asset Risk-Equipment Data
	  ◦ RBI 581 Asset Risk-Inspection History
	  ◦ RBI 581 Asset Risk-RBIRecommendations
	  ◦ RBI 581 Asset Risk-RefDocuments
	  ◦ RBI 581 Asset Risk-RiskTargetsResults
	◦ `Public\Meridium\Modules\Risk Based`
		This step is required only if you have previously modified the queries and you want to support Functional Location as an Asset.

Step	Task	Notes
4	Update Dynamic Viscosity for H2O (Water) record in RepresentativeFluids.	This step is required only if you have previously modified H2O (Water) record in RepresentativeFluids family. For more information, refer to KBA 000057776.
5	Using Configuration Manager, import the following files located in the ◦ `C:\Meridium\DbUpg\MI_DB_MASTER_4050100\4050100\_IEU_ManualImports` folder. ◦ MI_PRL_CNS0.xml ◦ MI_REPFLUID_581.xml ◦ MI_CMT_FLE0.xml	This step is required only if you have modified the properties of any of the 580 Representative fluids: ◦ Acid ◦ Acid-HP ◦ Acid-LP ◦ Acid-MP ◦ ALCL3 ◦ C13-16 (Diesel) ◦ C17-25 (Gas Oil) ◦ C1-C2 ◦ C25+ (Resid) ◦ C3-C4 ◦ C5 ◦ C6 ◦ C6-C8 ◦ C9-C12 ◦ CO ◦ DEE ◦ EE ◦ EEA ◦ EG ◦ EO ◦ H2 ◦ H2O (Water) ◦ H2S ◦ HCl ◦ HF ◦ MEOH (Methanol) ◦ NH3 ◦ Nitric Acid ◦ NO2 ◦ Phosgene ◦ PO ◦ Pyrophoric ◦ Steam ◦ Styrene (Aromatic) ◦ TD
6	Add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you have additional RBI Component type records that are not provided in the baseline APM database.

Step	Task	Notes
7	Recalculate the RBI 581 Risk Analyses to get the correct Calculated T-min field value where the Geometry Type field is set to Spherical Head or Hemispherical Head.	This step is required if you have RBI 581 Risk Analyses where Geometry Type field is set to Spherical Head or Hemispherical Head. For more information, refer to KBA 000041564.
8	Revert the following Risk Based Inspection 581 queries to baseline ◦ `Public\Meridium\Modules\Risk Based Inspection\Queries` folder. ◦ Inspections More Current Than All Analysis ◦ `Public\Meridium\Modules\Risk Based Inspection - 581\Queries` folder. ◦ Inspections More Current Than RBI 581 Analysis	This step is required only if you have modified the queries that are used for the **Inspection Updates** section of the **Inspection/TM Updates** tab, in the **Risk Based Inspection Overview** page.

Revert the Process Units Overview Queries to Baseline

This action is required only if you have modified the Process Units Overview queries.

About This Task

Due to changes in the Asset Hierarchy filter, the existing Process Unit query and the Asset Counts for Units sub-query requires updates. If you have modified these queries, perform the following steps to revert the queries to baseline.

Procedure

1. Access the **Query** page.
2. Select **Browse**.

   The **Select a query from the catalog** window appears.
3. Navigate to the `Baseline/Meridium/Modules/Risk Based Inspection/Queries/` folder.
4. Select the link for the Asset Counts for Units baseline query.
   The **Results** workspace appears.
5. Select the **SQL** tab.
6. Copy the code from the **SQL** workspace.
7. From the Catalog, navigate to the `Public/Meridium/Modules/Risk Based Inspection/Queries/` folder.
8. Select the link for the Asset Counts for Units query.
   The **Results** workspace appears.
9. Select the **SQL** tab.
10. Replace the code in the **SQL** workspace with the code that you have copied.
11. Repeat Steps 3-10 for the Process Unit Query.

Revert the Risk Based Inspection 581 Queries to Baseline

This action is required only if you have modified the Risk Based Inspection 581 queries.

About This Task

f you have modified the following Risk Based Inspection 581 queries, perform the following steps to revert the queries to baseline:

- Active Analyses for Evergreening – 581
- Analyses Created for Evergreening – 581

Procedure

1. Access the Catalog page.
2. Navigate to the Public folder for the query that you want to revert.
   For Risk Based Inspection 581, the public queries are stored in the following folder:
   `Public/Meridium/Modules/RBI 581/Queries`
3. Select the check box next to the query that you want to revert, and then select  .
   The **Confirm Delete** window appears, asking you to confirm if you want to delete the selected query.
4. Select **OK**.
   The selected query is deleted.
5. Navigate to the Baseline folder for queries.
   For Risk Based Inspection 581, the baseline queries are stored in the following folder:
   `Baseline/Meridium/Modules/RBI 581/Queries`
6. Select the check box next to the query that you want to revert, and then select  .
   The **Catalog Folder Browser** window appears.
7. Navigate to the folder containing the public query that you deleted in step 3.
8. Select **OK**.
   A success message appears indicating that the selected item has been copied successfully.
9. Repeat Steps 2-8 for each query that you want to revert to baseline.

Add the RBI-581 Tab to Criticality RBI Component Datasheets

Before You Begin

Note: You must repeat this procedure for each Criticality RBI Component datasheet that you have customized.

If you have customized the datasheet for one or more of the Criticality RBI Components, after activating the RBI 581 license, you must perform the following procedure to add the **RBI-581** section to those customized datasheets. The following table indicates the fields that must appear on each datasheet.

Caption	Field ID	Criticality RBI Component - Cylindrical Shell	Criticality RBI Component - Exchanger Bundle	Criticality RBI Component - Exchanger Header	Criticality RBI Component - Exchanger Tube	Criticality RBI Component - Piping	Criticality RBI Component - Tank Bottom
Base Material	Base MaterialMI_CCRBICOM_BASE_MATER_C	✓	✓	✓	✓	✓	✓
Cladding Material	MI_CCRBICOM_CLADDING_MATERIL_C	✓	✓	✓	✓	✓	✓
Cladding Present	MI_CCRBICOM_CLADDING_PRESENT_L	✓	✓	✓	✓	✓	✓
CM Corrosion Rate	MI_CCRBICOM_CM_COR_RT_C	✓	✓	✓	✓	✓	✓
Coefficient Y Material	MI_CCRBICOM_COEFFICNT_Y_MTRL_C	✕	✕	✕	✕	✓	✕
Corrosion Allow	MI_RBICOMPO_CORRO_ALLOW_N	✓	✓	✓	✓	✓	✓
Detection System	MI_CCRBICOM_DETECTION_SYSTEM_C	✓	✓	✓	✓	✓	✓
Fluid Velocity	MI_CCRBICOM_FLUID_VELOCITY_N	✓	✓	✓	✓	✓	✓
Furnished Cladding Thk	MI_CCRBICOM_FRNSHD_CLDDG_THK_N	✓	✓	✓	✓	✓	✓
Geometry Type	MI_CCRBICOM_GEOMETRY_TYPE_C	✓	✓	✓	✓	✓	✓
GFF Component Type	MI_CCRBICOM_GFF_COMPO_TYPE_CHR	✓	✓	✓	✓	✓	✓

Caption	Field ID	Criticality RBI Component - Cylindrical Shell	Criticality RBI Component - Exchanger Bundle	Criticality RBI Component - Exchanger Header	Criticality RBI Component - Exchanger Tube	Criticality RBI Component - Piping	Criticality RBI Component - Tank Bottom
Has Release Prevention Barrier?	MI_CCRBICTB_HAS_RELEA_PREVE_F	✗	✗	✗	✗	✗	✓
Is Intrusive?	MI_RBICOMPO_IS_INTRU_CHR	✓	✓	✓	✓	✓	✓
Isolation System	MI_CCRBICOM_ISOLA_SYSTE_CHR	✓	✓	✓	✓	✓	✓
Liner Present	MI_CCRBICOM_LINER_PRESE_CHR	✓	✓	✓	✓	✓	✓
Liner Type	MI_CCRBICOM_LINER_TP_C	✓	✓	✓	✓	✓	✓
Minimum Structural Thickness	MI_CCRBICOM_MNMM_STRCTRL_THS_N	✓	✓	✓	✓	✓	✓
Mitigation System	MI_CCRBICOM_MITIGATION_SYSTM_C	✓	✓	✓	✓	✓	✓
Percent Liquid Volume	MI_RBICOMPO_PER_LIQ_VOL_N	✓	✓	✓	✓	✓	✓
pH of Water	MI_CCRBICOM_PH_OF_WATER_N	✓	✓	✓	✓	✓	✓
Specified Tmin	MI_CCRBICOM_SPECIFIED_TMIN_N	✓	✓	✓	✓	✓	✓
Total Acid Number	MI_CCRBICOM_TOTAL_ACID_NUMBR_N	✓	✓	✓	✓	✓	✓

Procedure

1. Access the Family Management page.

2. In the left section, select the Criticality RBI Component whose datasheet you want to modify.

   In the workspace, the corresponding Criticality RBI Component family appears, displaying the **Information** section.

3. In the workspace, select the **Datasheets** tab, and then select **Manage Datasheets**.

   The **Datasheet Builder** page appears, displaying the datasheet layout of the selected Criticality RBI Component family.

4. In the upper-right corner of the page, select 

   A **new section** tab appears at the top of the workspace, displaying a blank section.

5. On the new tab, rename new section to RBI-581.
6. In the **RBI-581** section, select  .
7. In the right column, in the top cell, enter Value(s).
8. In the left pane, locate a field that corresponds to the table at the beginning of this topic, and then add that field into the empty cell in the **Value(s)** column using the drag-and-drop method.

   In the cell, an input box that corresponds to the selected field appears.

9. In the left column, enter the caption that corresponds to the field. For example, if you added the Coefficient Y Material field to the **Value(s)** column, then enter Coefficient Y Material in the corresponding cell in the left column.
10. In the upper-right corner of the page, select  .

    In the **RBI-581** section, in the table, a new row appears.

11. Repeat steps 8 to 10 for each of the fields specified in the table at the beginning of this topic.
12. In the upper-right corner of the page, select **Save**.

    The datasheet for the Criticality RBI Component that you selected in step 2 is saved, and the **RBI-581** tab appears on the selected Criticality RBI Component datasheet.

Add Completion Comments Field to RBI Recommendation Datasheet

Procedure

1. In the module navigation menu, select **Admin** > **Configuration Manager** > **Family Management**.
   The **Family Management** page appears, displaying the list of already existing families.
2. In the left pane, in the **Entity** section, select the RBI Recommendation entity.
   The workspace for the RBI Recommendation entity appears.
3. In the workspace, select the **Datasheets** tabs.
4. Select **Manage Datasheets**.
   The **Datasheet Builder** page appears.
5. On the **Datasheet Caption** drop-down menu, select the RBI Recommendation datasheet.
   The datasheet appears in the **Datasheet Builder** workspace.

   Note: If you have a custom datasheet, select the custom datasheet.

6. In the **Available Items** pane, select the Completion Comments field and drag it into the **Datasheet Builder** workspace.
   The field is added to that datasheet.
7. Select **Save**.
   The datasheet is saved.

Add RBI Component Types

Before You Begin

About This Task

Procedure

1. Log in to APM as an administrator.
2. Go to **Admin > Configuration Manager > System Codes and Tables**.
3. Search for MI RBI COMPONENT TYPES.
4. In the System Code section, select .
   The **Create System Code** window appears.
5. Add the RBI Component Types to the system code table.
6. Select **Save**.
7. Log out of APM and log in.
8. To add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table, perform the following steps:

   a) Select , and enter EquipmentTypes.
   A blank EquipmentTypes datasheet appears.
   b) In the **CriticalityItemType** box, select the existing RBI Component Type that you have added.
   c) Enter values in the required boxes, and then select to save the record.

Root Cause Analysis

Deploy RCA for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Review the RCA data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Modify any relationship definitions as required.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to one or more of the RCA Security Groups and Roles.	This step is required. Users will not be able to access Root Cause Analysis unless they belong to an RCA Security Group.
3	Specify the Team Charter after you create a new Root Cause Analysis record.	This step is optional. A default Team Charter exists in the baseline APM database. You can select the default Team Charter or define your own.
4	Specify the Critical Success Factors after you create a new Root Cause Analysis record.	This step is optional. Default Critical Success Factors exist in the baseline APM database. You can select one or more default Critical Success Factors or define your own.

Upgrade or Update RCA to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.0.0.0 through V4.0.1.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.1 through V3.5.1.12.3

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

Rounds Designer

Deploy Rounds for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Module-level Configuration Tasks:

Step	Task	Notes
1	Review the Rounds data model to determine which relationship definitions you will need to modify to include your custom asset families. Modify any relationship definitions as needed. For example, if you have created a new asset family, create a relationship definition as follows: ◦ Relationship family: Has Checkpoint ◦ Predecessor: The asset family ◦ Successor: The Measurement Location family or Lubrication Requirement family ◦ Cardinality: One to Many	This step is required only if you have asset data in families outside of the baseline Equipment and Functional Location families.
2	Assign Security Users to the following Rounds Security Groups and Roles: ◦ MI Operator Rounds Administrator ◦ MI Operator Rounds Mobile User	This step is required. **Note:** The MAPM Security Group that has been provided with APM v3.6 is also available. The user privileges are the same for the MAPM Security User and the MI Operator Rounds Security User. However, we recommend that you use the MI Operator Rounds User Security Group instead of the MAPM Security Group.
3	Manage Measurement Location Template mappings.	This step is required only if you added fields to the Measurement Location Template family via Configuration Manager.
4	Install the APM application on the mobile device that you plan to use for data collection.	This step is required only if you will use a mobile device for data collection.

Step	Task	Notes
5	Set the local time zone on the mobile device that you will use for data collection, typically the user time zone.	This step is required only if you will use a mobile device for data collection.
6	Set up the Scheduled Compliance task.	This step is required. The scheduled compliance task should be configured to start as soon as the Rounds module is deployed and set to run continuously as long as Rounds in use.
7	As needed, modify your server timeout settings.	This step is only required if you want to process large amounts of data in a single transaction (for example, if you collect a large number of readings for a Route or several Routes and then attempt to upload all of those readings simultaneously). If you need to modify server timeout settings, follow the instructions in KBA 000054028.
8	Configure automatic synchronization of Measurement Location and Measurement Location Template Records with Allowable Values.	This step is optional.
9	Grant permissions to the Everyone group to view records that belong to the Site Reference family.	This step is required.

Upgrade or Update Rounds to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

Step	Task	Notes
1	Grant permissions to the Everyone group to view records that belong to the Site Reference family.	This step is required.
2	Ensure all existing checkpoints have descriptions.	This step is required.

Step	Task	Notes
3	Ensure that the Source ML Description field is present on the Offline Forms datasheet for the Operator rounds Recommendation family.	This field is present by default on the datasheet in baseline APM. If you did not modify this Offline Forms datasheet, no change is required. However, if you previously removed the Source ML Description field from the Offline Forms datasheet, you must return the field to the datasheet.
4	As needed, modify your server timeout settings.	This step is only required if you want to process large amounts of data in a single transaction (for example, if you collect a large number of readings for a Route or several Routes and then attempt to upload all of those readings simultaneously). If you need to modify server timeout settings, follow the instructions in KBA 000054028.
5	Delete the Reading Value Character and Reading Value Numeric fields from the ID Template for the Reading family.	This step is optional. In V4.3.0.7.0, to enhance the performance of uploading readings, the Reading Value Character and Reading Value Numeric fields in the ID Template for the Reading family were removed. However, if you previously modified the ID Template fields for this family, your configuration is preserved when you upgrade to V4.3.0.7.0 or later. As a result, if you want to apply the performance increase, you must manually remove these fields. For more details, see KBA 000054893.

- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

Step	Task	Notes
1	Grant permissions to the Everyone group to view records that belong to the Site Reference family.	This step is required.
2	Ensure all existing checkpoints have descriptions.	This step is required.
3	Ensure that the Source ML Description field is present on the Offline Forms datasheet for the Operator rounds Recommendation family.	This field is present by default on the datasheet in baseline APM. If you did not modify this Offline Forms datasheet, no change is required. However, if you previously removed the Source ML Description field from the Offline Forms datasheet, you must return the field to the datasheet.

Step	Task	Notes
4	As needed, modify your server timeout settings.	This step is only required if you want to process large amounts of data in a single transaction (for example, if you collect a large number of readings for a Route or several Routes and then attempt to upload all of those readings simultaneously). If you need to modify server timeout settings, follow the instructions in KBA 000054028.
5	Delete the Reading Value Character and Reading Value Numeric fields from the ID Template for the Reading family.	This step is optional. In V4.3.0.7.0, to enhance the performance of uploading readings, the Reading Value Character and Reading Value Numeric fields in the ID Template for the Reading family were removed. However, if you previously modified the ID Template fields for this family, your configuration is preserved when you upgrade to V4.3.0.7.0 or later. As a result, if you want to apply the performance increase, you must manually remove these fields. For more details, see KBA 000054893.

- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

Step	Task	Notes
1	Grant permissions to the Everyone group to view records that belong to the Site Reference family.	This step is required.
2	Ensure all existing checkpoints have descriptions.	This step is required.
3	Ensure that the Source ML Description field is present on the Offline Forms datasheet for the Operator rounds Recommendation family.	This field is present by default on the datasheet in baseline APM. If you did not modify this Offline Forms datasheet, no change is required. However, if you previously removed the Source ML Description field from the Offline Forms datasheet, you must return the field to the datasheet.

Step	Task	Notes
4	As needed, modify your server timeout settings.	This step is only required if you want to process large amounts of data in a single transaction (for example, if you collect a large number of readings for a Route or several Routes and then attempt to upload all of those readings simultaneously). If you need to modify server timeout settings, follow the instructions in KBA 000054028.
5	Delete the Reading Value Character and Reading Value Numeric fields from the ID Template for the Reading family.	This step is optional. In V4.3.0.7.0, to enhance the performance of uploading readings, the Reading Value Character and Reading Value Numeric fields in the ID Template for the Reading family were removed. However, if you previously modified the ID Template fields for this family, your configuration is preserved when you upgrade to V4.3.0.7.0 or later. As a result, if you want to apply the performance increase, you must manually remove these fields. For more details, see KBA 000054893.

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

Step	Task	Notes
1	Grant permissions to the Everyone group to view records that belong to the Site Reference family.	This step is required.
2	Ensure all existing checkpoints have descriptions.	This step is required.
3	Ensure that the Source ML Description field is present on the Offline Forms datasheet for the Operator rounds Recommendation family.	This field is present by default on the datasheet in baseline APM. If you did not modify this Offline Forms datasheet, no change is required. However, if you previously removed the Source ML Description field from the Offline Forms datasheet, you must return the field to the datasheet.

Step	Task	Notes
4	As needed, modify your server timeout settings.	This step is only required if you want to process large amounts of data in a single transaction (for example, if you collect a large number of readings for a Route or several Routes and then attempt to upload all of those readings simultaneously). If you need to modify server timeout settings, follow the instructions in KBA 000054028.
5	Delete the Reading Value Character and Reading Value Numeric fields from the ID Template for the Reading family.	This step is optional. In V4.3.0.7.0, to enhance the performance of uploading readings, the Reading Value Character and Reading Value Numeric fields in the ID Template for the Reading family were removed. However, if you previously modified the ID Template fields for this family, your configuration is preserved when you upgrade to V4.3.0.7.0 or later. As a result, if you want to apply the performance increase, you must manually remove these fields. For more details, see KBA 000054893.

- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

Step	Task	Notes
1	Prior to upgrading your database, complete the pre-upgrade steps for lubrication.	This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
2	After upgrading your database, complete the post-upgrade steps for lubrication.	This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
3	Install the APM mobile application on mobile devices.	This step is required only if you will use a mobile device for data collection.
4	Set the local time zone on the mobile device that you will use for data collection.	This step is required only if you will use a mobile device for data collection.
5	Create the initial default sequencing schedule by accessing the Rounds Designer administration page.	This step is required.

Step	Task	Notes
6	Grant permissions to the Everyone group to view records that belong to the Site Reference family.	This step is required.
7	Ensure all existing checkpoints have descriptions.	This step is required.
8	Ensure that the Source ML Description field is present on the Offline Forms datasheet for the Operator rounds Recommendation family.	This field is present by default on the datasheet in baseline APM. If you did not modify this Offline Forms datasheet, no change is required. However, if you previously removed the Source ML Description field from the Offline Forms datasheet, you must return the field to the datasheet.
9	As needed, modify your server timeout settings.	This step is only required if you want to process large amounts of data in a single transaction (for example, if you collect a large number of readings for a Route or several Routes and then attempt to upload all of those readings simultaneously). If you need to modify server timeout settings, follow the instructions in KBA 000054028.
10	Delete the Reading Value Character and Reading Value Numeric fields from the ID Template for the Reading family.	This step is optional. In V4.3.0.7.0, to enhance the performance of uploading readings, the Reading Value Character and Reading Value Numeric fields in the ID Template for the Reading family were removed. However, if you previously modified the ID Template fields for this family, your configuration is preserved when you upgrade to V4.3.0.7.0 or later. As a result, if you want to apply the performance increase, you must manually remove these fields. For more details, see KBA 000054893.

1

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	Prior to upgrading your database, complete the pre-upgrade steps for lubrication.	This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
2	After upgrading your database, complete the post-upgrade steps for lubrication.	This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
3	Install the APM mobile application on mobile devices.	This step is required only if you will use a mobile device for data collection.
4	Set the local time zone on the mobile device that you will use for data collection.	This step is required only if you will use a mobile device for data collection.
5	Grant permissions to the Everyone group to view records that belong to the Site Reference family.	This step is required.
6	Ensure all existing checkpoints have descriptions.	This step is required.
7	Ensure that the Source ML Description field is present on the Offline Forms datasheet for the Operator rounds Recommendation family.	This field is present by default on the datasheet in baseline APM. If you did not modify this Offline Forms datasheet, no change is required. However, if you previously removed the Source ML Description field from the Offline Forms datasheet, you must return the field to the datasheet.

Step	Task	Notes
8	As needed, modify your server timeout settings.	This step is only required if you want to process large amounts of data in a single transaction (for example, if you collect a large number of readings for a Route or several Routes and then attempt to upload all of those readings simultaneously). If you need to modify server timeout settings, follow the instructions in KBA 000054028.
9	Delete the Reading Value Character and Reading Value Numeric fields from the ID Template for the Reading family.	This step is optional. In V4.3.0.7.0, to enhance the performance of uploading readings, the Reading Value Character and Reading Value Numeric fields in the ID Template for the Reading family were removed. However, if you previously modified the ID Template fields for this family, your configuration is preserved when you upgrade to V4.3.0.7.0 or later. As a result, if you want to apply the performance increase, you must manually remove these fields. For more details, see KBA 000054893.

- Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	Prior to upgrading your database, complete the pre-upgrade steps for lubrication.	This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
2	After upgrading your database, complete the post-upgrade steps for lubrication.	This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
3	Install the APM mobile application on mobile devices.	This step is required only if you will use a mobile device for data collection.
4	Set the local time zone on the mobile device that you will use for data collection.	This step is required only if you will use a mobile device for data collection.
5	Grant permissions to the Everyone group to view records that belong to the Site Reference family.	This step is required.
6	Ensure all existing checkpoints have descriptions.	This step is required.

Step	Task	Notes
7	Ensure that the Source ML Description field is present on the Offline Forms datasheet for the Operator rounds Recommendation family.	This field is present by default on the datasheet in baseline APM. If you did not modify this Offline Forms datasheet, no change is required. However, if you previously removed the Source ML Description field from the Offline Forms datasheet, you must return the field to the datasheet.
8	As needed, modify your server timeout settings.	This step is only required if you want to process large amounts of data in a single transaction (for example, if you collect a large number of readings for a Route or several Routes and then attempt to upload all of those readings simultaneously). If you need to modify server timeout settings, follow the instructions in KBA 000054028.
9	Delete the Reading Value Character and Reading Value Numeric fields from the ID Template for the Reading family.	This step is optional. In V4.3.0.7.0, to enhance the performance of uploading readings, the Reading Value Character and Reading Value Numeric fields in the ID Template for the Reading family were removed. However, if you previously modified the ID Template fields for this family, your configuration is preserved when you upgrade to V4.3.0.7.0 or later. As a result, if you want to apply the performance increase, you must manually remove these fields. For more details, see KBA 000054893.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

Step	Task	Notes
1	Prior to upgrading your database, complete the pre-upgrade steps for lubrication.	This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
2	Prior to upgrading your database, modify Checkpoints linked to multiple assets so that they are only linked to one asset.	This step is necessary because a Checkpoint can now be linked to only one asset.
3	Prior to upgrading your database, complete specific steps to upgrade records with schedules containing end dates.	This step is required only if you have any records with schedules containing end dates.

Step	Task	Notes
4	After upgrading your database, complete the post-upgrade steps for lubrication.	This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
5	Install the APM mobile application on mobile devices.	This step is required only if you will use a mobile device for data collection.
6	Set the local time zone on the mobile device that you will use for data collection.	This step is required only if you will use a mobile device for data collection.
7	Confirm the assignment of Security Users for the existing route subscriptions and make additional assignments if needed.	This step is required. Routes that a user was subscribed to via the Meridium V3.6 mobileAPM application will be assigned to that user automatically through the database upgrade process.
8	Grant permissions to the Everyone group to view records that belong to the Site Reference family.	This step is required.
9	Ensure all existing checkpoints have descriptions.	This step is required.
10	Ensure that the Source ML Description field is present on the Offline Forms datasheet for the Operator rounds Recommendation family.	This field is present by default on the datasheet in baseline APM. If you did not modify this Offline Forms datasheet, no change is required. However, if you previously removed the Source ML Description field from the Offline Forms datasheet, you must return the field to the datasheet.

Step	Task	Notes
11	As needed, modify your server timeout settings.	This step is only required if you want to process large amounts of data in a single transaction (for example, if you collect a large number of readings for a Route or several Routes and then attempt to upload all of those readings simultaneously). If you need to modify server timeout settings, follow the instructions in KBA 000054028.
12	Delete the Reading Value Character and Reading Value Numeric fields from the ID Template for the Reading family.	This step is optional. In V4.3.0.7.0, to enhance the performance of uploading readings, the Reading Value Character and Reading Value Numeric fields in the ID Template for the Reading family were removed. However, if you previously modified the ID Template fields for this family, your configuration is preserved when you upgrade to V4.3.0.7.0 or later. As a result, if you want to apply the performance increase, you must manually remove these fields. For more details, see KBA 000054893.

- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

Step	Task	Notes
1	Prior to upgrading your database, complete the pre-upgrade steps for lubrication.	This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
2	Prior to upgrading your database, modify Checkpoints linked to multiple assets so that they are only linked to one asset.	This step is necessary because a Checkpoint can now be linked to only one asset.
3	Prior to upgrading your database, complete specific steps to upgrade records with schedules containing end dates.	This step is required only if you have any records with schedules containing end dates.
4	After upgrading your database, complete the post-upgrade steps for lubrication.	This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
5	Install the APM mobile application on mobile devices.	This step is required only if you will use a mobile device for data collection.

Step	Task	Notes
6	Set the local time zone on the mobile device that you will use for data collection.	This step is required only if you will use a mobile device for data collection.
7	Confirm the assignment of Security Users for the existing route subscriptions and make additional assignments if needed.	This step is required. Routes that a user was subscribed to via the Meridium V3.6 mobileAPM application will be assigned to that user automatically through the database upgrade process.
8	Grant permissions to the Everyone group to view records that belong to the Site Reference family.	This step is required.
9	Ensure all existing checkpoints have descriptions.	This step is required.
10	Ensure that the Source ML Description field is present on the Offline Forms datasheet for the Operator rounds Recommendation family.	This field is present by default on the datasheet in baseline APM. If you did not modify this Offline Forms datasheet, no change is required. However, if you previously removed the Source ML Description field from the Offline Forms datasheet, you must return the field to the datasheet.
11	As needed, modify your server timeout settings.	This step is only required if you want to process large amounts of data in a single transaction (for example, if you collect a large number of readings for a Route or several Routes and then attempt to upload all of those readings simultaneously). If you need to modify server timeout settings, follow the instructions in KBA 000054028.
12	Delete the Reading Value Character and Reading Value Numeric fields from the ID Template for the Reading family.	This step is optional. In V4.3.0.7.0, to enhance the performance of uploading readings, the Reading Value Character and Reading Value Numeric fields in the ID Template for the Reading family were removed. However, if you previously modified the ID Template fields for this family, your configuration is preserved when you upgrade to V4.3.0.7.0 or later. As a result, if you want to apply the performance increase, you must manually remove these fields. For more details, see KBA 000054893.

- Upgrade from any version V3.5.1 through V3.5.1.12.3

Step	Task	Notes
1	Prior to upgrading your database, complete the pre-upgrade steps for lubrication.	This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
2	Prior to upgrading your database, modify Checkpoints linked to multiple assets so that they are only linked to one asset.	This step is necessary because a Checkpoint can now be linked to only one asset.
3	Prior to upgrading your database, complete specific steps to upgrade records with schedules containing end dates.	This step is required only if you have any records with schedules containing end dates.
4	After upgrading your database, complete the post-upgrade steps for lubrication.	This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
5	Install the APM mobile application on mobile devices.	This step is required only if you will use a mobile device for data collection.
6	Set the local time zone on the mobile device that you will use for data collection.	This step is required only if you will use a mobile device for data collection.
7	Confirm the assignment of Security Users for the existing route subscriptions and make additional assignments if needed.	This step is required. Routes that a user was subscribed to via the Meridium V3.6 mobileAPM application will be assigned to that user automatically through the database upgrade process.
8	Grant permissions to the Everyone group to view records that belong to the Site Reference family.	This step is required.
9	Ensure all existing checkpoints have descriptions.	This step is required.
10	Ensure that the Source ML Description field is present on the Offline Forms datasheet for the Operator rounds Recommendation family.	This field is present by default on the datasheet in baseline APM. If you did not modify this Offline Forms datasheet, no change is required. However, if you previously removed the Source ML Description field from the Offline Forms datasheet, you must return the field to the datasheet.

Step	Task	Notes
11	As needed, modify your server timeout settings.	This step is only required if you want to process large amounts of data in a single transaction (for example, if you collect a large number of readings for a Route or several Routes and then attempt to upload all of those readings simultaneously). If you need to modify server timeout settings, follow the instructions in KBA 000054028.
12	Delete the Reading Value Character and Reading Value Numeric fields from the ID Template for the Reading family.	This step is optional. In V4.3.0.7.0, to enhance the performance of uploading readings, the Reading Value Character and Reading Value Numeric fields in the ID Template for the Reading family were removed. However, if you previously modified the ID Template fields for this family, your configuration is preserved when you upgrade to V4.3.0.7.0 or later. As a result, if you want to apply the performance increase, you must manually remove these fields. For more details, see KBA 000054893.

- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

Step	Task	Notes
1	Prior to upgrading your database, complete the pre-upgrade steps for lubrication.	This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
2	Prior to upgrading your database, modify Checkpoints linked to multiple assets so that they are only linked to one asset.	This step is necessary because a Checkpoint can now be linked to only one asset.
3	Prior to upgrading your database, complete specific steps to upgrade records with schedules containing end dates.	This step is required only if you have any records with schedules containing end dates.
4	After upgrading your database, complete the post-upgrade steps for lubrication.	This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
5	Install the APM mobile application on mobile devices.	This step is required only if you will use a mobile device for data collection.

Step	Task	Notes
6	Set the local time zone on the mobile device that you will use for data collection.	This step is required only if you will use a mobile device for data collection.
7	Confirm the assignment of Security Users for the existing route subscriptions and make additional assignments if needed.	This step is required. Routes that a user was subscribed to via the Meridium V3.6 mobileAPM application will be assigned to that user automatically through the database upgrade process.
8	Grant permissions to the Everyone group to view records that belong to the Site Reference family.	This step is required.
9	Ensure all existing checkpoints have descriptions.	This step is required.
10	Ensure that the Source ML Description field is present on the Offline Forms datasheet for the Operator rounds Recommendation family.	This field is present by default on the datasheet in baseline APM. If you did not modify this Offline Forms datasheet, no change is required. However, if you previously removed the Source ML Description field from the Offline Forms datasheet, you must return the field to the datasheet.
11	As needed, modify your server timeout settings.	This step is only required if you want to process large amounts of data in a single transaction (for example, if you collect a large number of readings for a Route or several Routes and then attempt to upload all of those readings simultaneously). If you need to modify server timeout settings, follow the instructions in KBA 000054028.
12	Delete the Reading Value Character and Reading Value Numeric fields from the ID Template for the Reading family.	This step is optional. In V4.3.0.7.0, to enhance the performance of uploading readings, the Reading Value Character and Reading Value Numeric fields in the ID Template for the Reading family were removed. However, if you previously modified the ID Template fields for this family, your configuration is preserved when you upgrade to V4.3.0.7.0 or later. As a result, if you want to apply the performance increase, you must manually remove these fields. For more details, see KBA 000054893.

- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Prior to upgrading your database, complete the pre-upgrade steps for lubrication.	This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
2	Prior to upgrading your database, modify Checkpoints linked to multiple assets so that they are only linked to one asset.	This step is necessary because a Checkpoint can now be linked to only one asset.
3	Prior to upgrading your database, complete specific steps to upgrade records with schedules containing end dates.	This step is required only if you have any records with schedules containing end dates.
4	After upgrading your database, complete the post-upgrade steps for lubrication.	This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
5	Install the APM mobile application on mobile devices.	This step is required only if you will use a mobile device for data collection.
6	Set the local time zone on the mobile device that you will use for data collection.	This step is required only if you will use a mobile device for data collection.
7	Confirm the assignment of Security Users for the existing route subscriptions and make additional assignments if needed.	This step is required. Routes that a user was subscribed to via the Meridium V3.6 mobileAPM application will be assigned to that user automatically through the database upgrade process.
8	Grant permissions to the Everyone group to view records that belong to the Site Reference family.	This step is required.
9	Ensure all existing checkpoints have descriptions.	This step is required.
10	Ensure that the Source ML Description field is present on the Offline Forms datasheet for the Operator rounds Recommendation family.	This field is present by default on the datasheet in baseline APM. If you did not modify this Offline Forms datasheet, no change is required. However, if you previously removed the Source ML Description field from the Offline Forms datasheet, you must return the field to the datasheet.

Step	Task	Notes
11	As needed, modify your server timeout settings.	This step is only required if you want to process large amounts of data in a single transaction (for example, if you collect a large number of readings for a Route or several Routes and then attempt to upload all of those readings simultaneously). If you need to modify server timeout settings, follow the instructions in KBA 000054028.
12	Delete the Reading Value Character and Reading Value Numeric fields from the ID Template for the Reading family.	This step is optional. In V4.3.0.7.0, to enhance the performance of uploading readings, the Reading Value Character and Reading Value Numeric fields in the ID Template for the Reading family were removed. However, if you previously modified the ID Template fields for this family, your configuration is preserved when you upgrade to V4.3.0.7.0 or later. As a result, if you want to apply the performance increase, you must manually remove these fields. For more details, see KBA 000054893.

- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Prior to upgrading your database, complete the pre-upgrade steps for lubrication.	This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
2	Prior to upgrading your database, modify Checkpoints linked to multiple assets so that they are only linked to one asset.	This step is necessary because a Checkpoint can now be linked to only one asset.
3	Prior to upgrading your database, complete specific steps to upgrade records with schedules containing end dates.	This step is required only if you have any records with schedules containing end dates.
4	After upgrading your database, complete the post-upgrade steps for lubrication.	This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database. This step is necessary due to various changes in the data model for records related to lubrication.
5	Install the APM mobile application on mobile devices.	This step is required only if you will use a mobile device for data collection.

Step	Task	Notes
6	Set the local time zone on the mobile device that you will use for data collection.	This step is required only if you will use a mobile device for data collection.
7	Confirm the assignment of Security Users for the existing route subscriptions and make additional assignments if needed.	This step is required. Routes that a user was subscribed to via the Meridium V3.6 mobileAPM application will be assigned to that user automatically through the database upgrade process.
8	Grant permissions to the Everyone group to view records that belong to the Site Reference family.	This step is required.
9	Ensure all existing checkpoints have descriptions.	This step is required.
10	Ensure that the Source ML Description field is present on the Offline Forms datasheet for the Operator rounds Recommendation family.	This field is present by default on the datasheet in baseline APM. If you did not modify this Offline Forms datasheet, no change is required. However, if you previously removed the Source ML Description field from the Offline Forms datasheet, you must return the field to the datasheet.
11	As needed, modify your server timeout settings.	This step is only required if you want to process large amounts of data in a single transaction (for example, if you collect a large number of readings for a Route or several Routes and then attempt to upload all of those readings simultaneously). If you need to modify server timeout settings, follow the instructions in KBA 000054028.
12	Delete the Reading Value Character and Reading Value Numeric fields from the ID Template for the Reading family.	This step is optional. In V4.3.0.7.0, to enhance the performance of uploading readings, the Reading Value Character and Reading Value Numeric fields in the ID Template for the Reading family were removed. However, if you previously modified the ID Template fields for this family, your configuration is preserved when you upgrade to V4.3.0.7.0 or later. As a result, if you want to apply the performance increase, you must manually remove these fields. For more details, see KBA 000054893.

Manage the Measurement Location Template Mappings

About This Task

The Measurement Location Template family and the Measurement Location family are provided as part of the baseline Rounds data model. If you create a Measurement Location Template in the APM application, you can then create a Measurement Location based on that template. If you do so, all values in Measurement Location Template fields that also exist on the Measurement Location will be mapped automatically to the new Measurement Location.

You might find that the Measurement Location Template and Measurement Location datasheets do not contain all the fields that you need. If so, you can add fields to the Measurement Location Template family so that the values from the new fields will be mapped to Measurement Locations based on that template. To do so, you will need to complete the following steps.

Procedure

1. Create a new Measurement Location Template field.
2. Add the new Measurement Location Template field to the Measurement Location Template datasheet.
3. Create a new Measurement Location field. We recommend that the field caption of this field be the same as the field caption you defined for the Measurement Location Template field. This will ensure that the text in the field IDs that identify the fields are the same. If they are not the same, the values will not be mapped from the Measurement Location Template to the Measurement Location.
4. Add the new Measurement Location field to the Measurement Location datasheet.

   Note: For more information on Measurement Location templates, refer the Family Management documentation.

Upgrade Steps for Lubrication

If you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database, complete these steps.

Procedure

- Complete the following steps prior to upgrading your database:

Table 6: Pre-Upgrade Steps

Step	Task	Notes
1	Review the values in the Manufacturer field in Lubricant records and consolidate any near-matches. For example, if some of your existing records contain the value “ABC Company” and others contain “A B C Company“ to refer to the same manufacturer, you should modify one or the other so that the values match exactly. **Tip:** You can use the following query, which returns a list of manufacturers in alphabetical order, to review the values: `SELECT DISTINCT [MI_LUBRICANT].[MI_LUBRICANT_MFR_C] "Lubricant Manufacturer" FROM [MI_LUBRICANT] ORDER BY [MI_LUBRICANT].[MI_LUBRICANT_MFR_C] Asc`	This step is required only if you have Lubricant records in your database. This step is necessary because a new Lubricant Manufacturer record will be created during the upgrade for each value in the Manufacturer field in Lubricant records prior to upgrading (and the value will be replaced with a reference to the corresponding Lubricant Manufacturer record).
2	Review the values in the Priority field in Lubrication Requirement and Lubrication Requirement Template records and consolidate any near-matches. For example, if some of your existing records contain the value "High" and others contain "Hihg" to refer to the same level of priority, you should modify one or the other so that the values match exactly. **Tip:** You can use the following query, which returns a list of priority values in alphabetical order, to review the values: `SELECT DISTINCT [MI_LUBR_REQ].[MI_LUBR_REQ_PRIOR_C] "Priority" FROM [MI_LUBR_REQ] ORDER BY [MI_LUBR_REQ].[MI_LUBR_REQ_PRIOR_C] ASC`	This step is required only if you have Lubrication Requirement and Lubrication Requirement Template records in your database. This step is necessary because a new entry in the system code table MI_LUBR_PRIORITY will be added during the upgrade for each value in the Priority field in Lubrication Requirement and Lubrication Requirement Template records prior to upgrading.

Step	Task	Notes
3	Review the values in the Component field in Lubrication Requirement and Lubrication Requirement Template records and consolidate any near-matches. For example, if some of your existing records contain the value "Bearing" and others contain "Bearings" to refer to the component, you should modify one or the other so that the values match exactly. **Tip:** You can use the following query, which returns a list of components in alphabetical order, to review the values: `SELECT DISTINCT [MI_LUBR_REQ].[MI_LUBR_REQ_COMP_C] "Component" FROM [MI_LUBR_REQ] ORDER BY [MI_LUBR_REQ].[MI_LUBR_REQ_COMP_C] ASC`	This step is required only if you have Lubrication Requirement and Lubrication Requirement Template records in your database. This step is necessary because a new Lubrication Component record will be created during the upgrade for each value in the Component field in Lubrication Requirement and Lubrication Requirement Template records prior to upgrading (and the Component Type field will be updated with a reference to the corresponding Lubrication Component record).

Step	Task	Notes
4	Review the values in the Method field in Lubricant records and consolidate any near-matches. For example, if some of your existing records contain the value "Grease Gun" and others contain "greasegun" to refer to the method, you should modify one or the other so that the values match exactly. **Tip:** You can use the following query, which returns a list of methods in alphabetical order, to review the values: `SELECT DISTINCT [MI_LUBRICANT].[MI_LUBRICANT_METHOD_C] "Method" FROM [MI_LUBRICANT] ORDER BY [MI_LUBRICANT].[MI_LUBRICANT_METHOD_C] Asc`	This step is required only if you have Lubricant records in your database. This step is necessary because a new Lubrication Method record will be created during the upgrade for each unique value in the Method field in Lubricant records prior to upgrading (and the Method field will be deprecated). In addition, the new Method Type field in Lubrication Requirement and Lubrication Requirement Template records will be populated with the Entity Key of the corresponding Lubrication Method record.

Step	Task	Notes

5	Review the values in the Capacity Unit of Measure field in Lubrication Requirement and Lubrication Requirement Template records and consolidate any near-matches. Then, ensure that each value matches exactly the system code Description value for an entry in the MI_LM_REFERENCES System Code Table. If a corresponding entry does not exist, and you want to use the value in your upgraded database, add an entry.
	
	Important: You can add an entry directly to the MI_LM_REFERENCES System Code Table or you can add a reference to an entry in the global UOME System Code Table. However, do not add a given value to the MI_LM_REFERENCES System Code Table using both methods.
	
	Tip: You can use the following queries, which return a list of Capacity Unit of Measure values in alphabetical order, to review the values:
	◦ Lubrication Requirement records:
	`SELECT DISTINCT [MI_LUBR_REQ].[MI_LUBR_REQ_CAPTY_UOM_C] "Capacity Unit of Measure" FROM [MI_LUBR_REQ] WHERE [MI_LUBR_REQ].[MI_LUBR_REQ_CAPTY_UOM_C] IS NOT NULL ORDER BY [MI_LUBR_REQ].[MI_LUBR_REQ_CAPTY_UOM_C] Asc`
	◦ Lubrication Requirement Template records:
	`SELECT DISTINCT [MI_LR_TMPLT].[MI_LR_TMPLT_CAPTY_UOM_C] "Capacity Unit of Measure" FROM [MI_LR_TMPLT] WHERE [MI_LR_TMPLT].[MI_LR_TMPLT_CAPTY_UOM_C] IS NOT NULL ORDER BY [MI_LR_TMPLT].`
		This step is required only if you have Lubrication Requirement and Lubrication Requirement Template records in your database.
		
		This step is necessary because the new Capacity Unit of Measure field in Lubrication Requirement and Lubrication Requirement Template records will be populated automatically with a reference to the unit of measure that corresponds to the value in the deprecated Capacity Unit of Measure field.
		
		If the deprecated Capacity Unit of Measure field contains a value that does not correspond to an entry in the MI_LM_REFERENCES System Code Table, no value will be added to the new field.

- Complete the following steps after upgrading your database:

Table 7: Post-Upgrade Steps

Step	Task	Notes

1	Confirm that appropriate the Lubricant Manufacturer records were created. Add or remove records as necessary.
	Tip: You can use the following query, which returns a list of the Lubricant Manufacturer records in your upgraded database, to review the values:
	`SELECT DISTINCT [MI_LUBR_MANU].[MI_LUBR_MANU_MANU_ID_C]`
	`"Manufacturer ID" FROM [MI_LUBR_MANU] ORDER BY [MI_LUBR_MANU].[MI_LUBR_MANU_MANU_ID_C] Asc`
		See notes for Step 1 in the pre-upgrade steps.

2	Confirm that appropriate entries were created in the system code table MI_LUBR_PRIORITY. **Tip:** ◦ Access the System Codes and Tables page to confirm the entries. ◦ For more information, refer the System Codes and Tables documentation.	See notes for Step 2 in the pre-upgrade steps.
3	Confirm that appropriate entries were created in the system code table MI_LUBR_PRIORITY. **Tip:** You can use the following query, which returns a list of the Lubrication Component records in your upgraded database, to review the values: `SELECT DISTINCT [MI_LUBR_COMP].[MI_LUBR_COMP_ID_C] "ID" FROM [MI_LUBR_COMP] ORDER BY [MI_LUBR_COMP].[MI_LUBR_COMP_ID_C] Asc`	See notes for Step 3 in the pre-upgrade steps.

Step	Task	Notes
4	Confirm that appropriate Lubrication Method records were created. Add or remove records as necessary. **Tip:** You can use the following query, which returns a list of the Lubrication Method records in your upgraded database, to review the values: `SELECT DISTINCT [MI_LUBR_METH]. [MI_LUBR_METH_ID_C] "Method ID" FROM [MI_LUBR_METH] ORDER BY [MI_LUBR_METH]. [MI_LUBR_METH_ID_C] Asc`	See notes for Step 4 in the pre-upgrade steps.

Step	Task	Notes
5	For all Lubrication Requirement and Lubrication Requirement Template records that contained a value in the deprecated Capacity Unit of Measure field, confirm that the new Capacity Unit of Measure field contains a reference to the corresponding unit of measure. **Tip:** You can use the following queries to locate records where the deprecated field contains a value, but the new field does not. ◦ Lubrication Requirement records: `SELECT [MI_LUBR_REQ].[MI_LUBR_REQ_CAPTY_UOM_C] "Capacity Unit of Measure(Depr", [MI_LUBR_REQ].[MI_LUBR_REQ_CAPACITY_UOM_C] "Capacity Unit of Measure", [MI_LUBR_REQ].ENTY_KEY "ENTY_KEY", [MI_LUBR_REQ].[MI_LUBR_REQ_COMP_TYPE_N] "Component Type", [MI_LUBR_REQ].[MI_MEAS_LOC_DESC_C] "Description" FROM [MI_LUBR_REQ] WHERE ([MI_LUBR_REQ].[MI_LUBR_REQ_CAPTY_UOM_C] IS NOT NULL AND [MI_LUBR_REQ].[MI_LUBR_REQ_CAPACITY_UOM_C] IS NULL) ORDER BY [MI_LUBR_REQ].[MI_LUBR_REQ_CAPTY_UOM_C] Asc` ◦ Lubrication Requirement Template records: `SELECT DISTINCT [MI_LR_TMPLT].[MI_LR_TMPLT_CAPTY_UOM_C] "Capacity Unit of Measure(Depr", [MI_LR_TMPLT].[MI_LR_TMPLT_CAPACITY_UOM_C] "Capacity Unit of Measure_", [MI_LR_TMPLT].ENTY_KEY "ENTY_KEY", [MI_LR_TMPLT].`	See notes for Step 5 in the pre-upgrade steps.

Modify Checkpoints Linked to Multiple Assets

About This Task

Note: The steps in this section are required only if you are upgrading from a version of Meridium Enterprise APM prior to V4.0.0.0.

In APM, a Checkpoint can be linked to one asset. During upgrade from versions V3.x to APM, the related asset entity key is added to a field on the Checkpoint family. Therefore, if you have Checkpoints that are linked to more than one asset, then you must remove the links to the additional assets prior to upgrading.

Procedure

1. Using an appropriate database management tool, prior to upgrading your database to APM, run a query to locate Checkpoints that are linked to multiple assets.

   For example, for each of the following Checkpoint types in the database, run the following query:

Checkpoint Type	Query Example
Measurement Location	SELECT MI_MEAS_LOC.ENTY_KEY as "ML_KEY", MI_ENTITIES.ENTY_ID as "ML ID", MIV_MIR_HS_MEASLOC.PRED_ENTY_KEY as "Asset Key" FROM MI_MEAS_LOC JOIN MIV_MIR_HS_MEASLOC ON MI_MEAS_LOC.ENTY_KEY = MIV_MIR_HS_MEASLOC.SUCC_ENTY_KEY JOIN MI_ENTITIES on MIV_MIR_HS_MEASLOC.SUCC_ENTY_KEY = MI_ENTITIES.ENTY_KEY AND SUCC_ENTY_KEY IN (SELECT SUCC_ENTY_KEY FROM MIV_MIR_HS_MEASLOC GROUP BY SUCC_ENTY_KEY HAVING COUNT(*) > 1) ORDER BY 1,2; GO

Checkpoint Type	Query Example
Lubrication Requirement	SELECT MI_LUBR_REQ.ENTY_KEY as "LR_KEY", MI_ENTITIES.ENTY_ID as "LR ID", MIV_MIR_HS_MEASLOC.PRED_ENTY_KEY as "Asset Key" FROM MI_LUBR_REQ JOIN MIV_MIR_HS_MEASLOC ON MI_LUBR_REQ.ENTY_KEY = MIV_MIR_HS_MEASLOC.SUCC_ENTY_KEY JOIN MI_ENTITIES on MIV_MIR_HS_MEASLOC.SUCC_ENTY_KEY = MI_ENTITIES.ENTY_KEY AND SUCC_ENTY_KEY IN (SELECT SUCC_ENTY_KEY FROM MIV_MIR_HS_MEASLOC GROUP BY SUCC_ENTY_KEY HAVING COUNT(*) > 1) ORDER BY 1,2; GO

A list of Checkpoints that are linked to multiple assets appears, providing the Checkpoint key, Checkpoint ID, and the Asset Key of the assets linked to the Checkpoint.

2. Access each Checkpoint in Record Manager in the current version of APM.
   The left pane displays the records that are related to the Checkpoint.
3. Unlink the additional assets from the Checkpoint so that it is linked only to one asset (for example, either a Functional Location or an Equipment if you are using the default asset families).

Upgrade Records with Schedules Containing End Dates

About This Task

Note: The steps in this section are required only if you are upgrading from a version of Meridium Enterprise APM prior to V4.0.0.0.

When upgrading from any V3.x version to a V4.x version, follow these steps to ensure that schedules for the following record types are upgraded successfully:

- Checkpoint Task
- Measurement Location
- Lubrication Requirement
- Measurement Location Template
- Lubrication Requirement Template

These steps are required to ensure that any records containing schedules with end dates are upgraded successfully.

Note: If preferred, instead of completing the following steps prior to upgrading, you can instead upgrade your database as normal. When you do so, the log for the Rounds upgrade utility will record entries for schedules that failed to upgrade. You can then use this information to recreate the schedules in V4.2.0.0.

Procedure

1. Review the affected record types to determine whether there are any schedules containing end dates. You can use the following queries to locate these records:

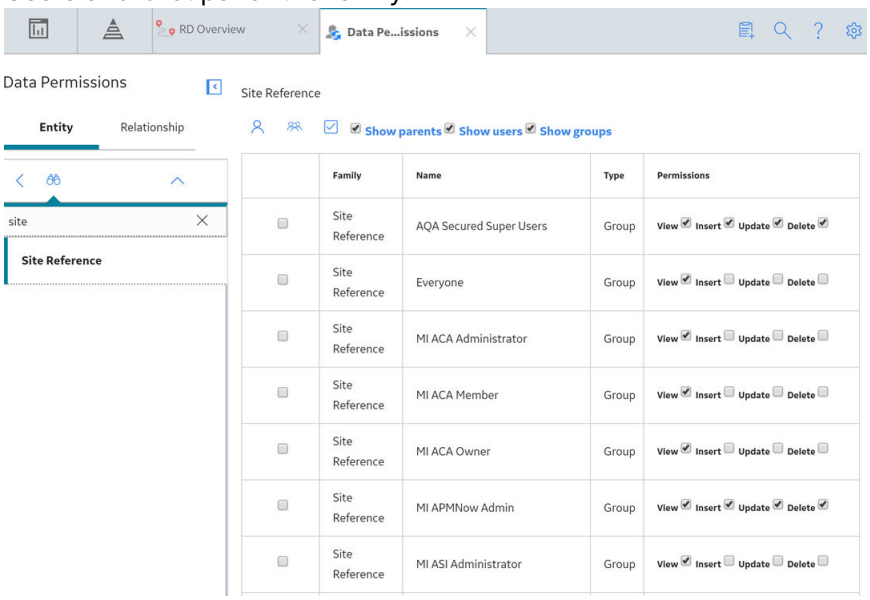
Record Type	Query
Checkpoint Templates (that is, Measurement Template and Lubrication Requirement Template records)	`SELECT ENTY_KEY, ENTY_ID, MI_ML_TMPLT_SCHEDULE_C FROM MIV_MI_CP_TMPLT WHERE MI_ML_TMPLT_SCHEDULE_C LIKE '<?xml %' AND MI_ML_TMPLT_SCHEDULE_C NOT LIKE '%<EndDate xsi:nil="true" /> %'`
Checkpoints (that is, Measurement Location and Lubrication Requirement records)	`SELECT MI_MEAS_LOC_SCHEDULE_C FROM MIV_MI_CHECK_PT WHERE MI_MEAS_LOC_SCHEDULE_C LIKE '<?xml %' AND MI_MEAS_LOC_SCHEDULE_C NOT LIKE '%<EndDate xsi:nil="true" /> %'`
Checkpoint Tasks	`SELECT ENTY_KEY, ENTY_ID, MI_TASK_SCHEDULE_C FROM MIV_MI_CP_TASK0 WHERE MI_TASK_SCHEDULE_C LIKE '<?xml%' AND MI_TASK_SCHEDULE_C NOT LIKE '%<EndDate xsi:nil="true" />%'`

2. For each record with a schedule containing an end date:
   a) Note the record and the end date value.
   b) In the Schedule field, select the **[...]** button to open the **Schedule** window.
   c) In the **Range of recurrence** section, select **No end date**, and then select **OK**.
3. Proceed with the database upgrade as normal.
4. Once the database upgrade is complete, in APM, locate the records you noted in step 2.
5. In each record, update the schedule to set the required end date.

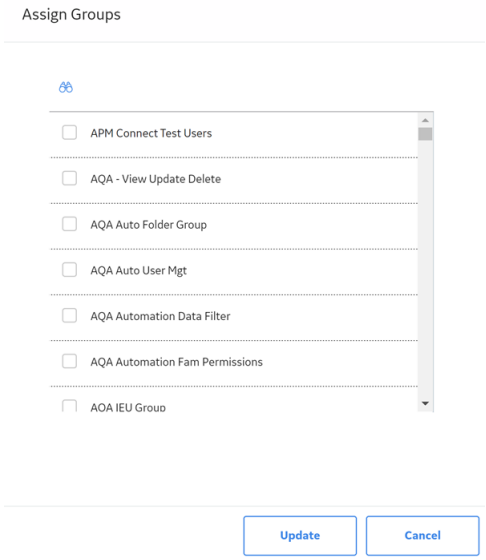
Grant Data Permissions to the Everyone Group

Procedure

1. In the module navigation menu, select **Admin** > **Configuration Manager** > **Data Permissions**.
2. Select the Site Reference family.
   The workspace for the Site Reference family appears, displaying a list of assigned Security Users and Groups for the family.



3. Select  .
   The **Assign Groups** window appears.



4. In the list, select the Everyone group, and then select **Update**.
   The Everyone group is assigned to the family and appears in the workspace.
5. On the row containing the Everyone group, select the **View** check box.

6. Select  .
   The Everyone group is granted permission to view records that belong to the Site Reference family.

Rounds Security Groups

The following table lists the baseline Security Groups available for users within this module, as well as the baseline Roles to which those Security Groups are assigned.

Important: Assigning a Security User to a Role grants that user the privileges associated with all of the Security Groups that are assigned to that Role. To avoid granting a Security User unintended privileges, before assigning a Security User to a Role, be sure to review all of the privileges associated with the Security Groups assigned to that Role. Also, be aware that additional Roles, as well as Security Groups assigned to existing Roles, can be added via Security Manager.

Security Group	Roles
MI Operator Rounds Administrator	MI Health Admin
MI Operator Rounds Mobile User	MI Health Admin MI Health Power MI Health User
MI Lubrication Management Administrator	MI Health Admin
MI Lubrication Management User	MI Health Admin MI Health Power MI Health User
MI Rounds Designer Viewer	MI APM Viewer
MI Rounds Pro Administrator	MI Rounds-Pro Admin
MI Rounds Pro Mobile User	Mi Rounds-Pro User

The following table lists the default privileges that members of each group have to the Rounds entity and relationship families.

Note:

- Users who should be able to run Rounds queries to view the Rounds data after it has been uploaded from a tablet or a mobile device will need a combination of the privileges listed in the following table, depending on the families included in the queries they want to run.
- To create work requests via Operator Rounds Recommendations, users must also have the appropriate privileges to create EAM notifications (e.g., be a member of the MI SAP Interface User Security Group).
- The privileges assigned to the members of the MAPM Security Group, which was provided in the baseline Rounds module in Meridium Enterprise APM V3.6.0, are also assigned to the members of the MI Operator Rounds Mobile User Security Group. We recommend that you use the MI Operator Rounds User Security Group instead of the MAPM Security Group.

Family	MI Operator Rounds Administrator	MI Operator Rounds Mobile User	MAPM Security Group	MI Rounds Designer Viewer	MI Lubrication Management Administrator	MI Lubrication Management User
Entity Families						
Checkpoint Condition	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Checkpoint Task	View, Update, Insert, Delete	View, Update	View, Update	View	View, Update, Insert, Delete	View, Update
Health Indicator	View	View	View	View	View	View
Health Indicator Mapping	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Hierarchy Item Child Definition (Deprecated)	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Hierarchy Item Definition (Deprecated)	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Lubricant	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Lubrication Component	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Lubrication Management Recommendation	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Lubricant Manufacturer	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Lubrication Method	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Lubrication Requirement	View, Update, Insert, Delete	View, Update	View, Update	View	View, Update, Insert, Delete	View
Lubrication Requirement Template	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Measurement Location	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Measurement Location Template	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View

Family	MI Operator Rounds Administrator	MI Operator Rounds Mobile User	MAPM Security Group	MI Rounds Designer Viewer	MI Lubrication Management Administrator	MI Lubrication Management User
Operator Rounds Allowable Values	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Operator Rounds Recommendation	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Reading	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Reference Document	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Route	View, Update, Insert, Delete	View, Update	View, Update	View	View, Update, Insert, Delete	View, Update
Route History	View, Update, Insert, Delete	View, Insert, Update, Delete	View, Insert, Update, Delete	View	View, Update, Insert, Delete	View, Insert, Update, Delete
Rounds Allowable Value	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Rounds Category	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Rounds Sequence Information	View, Update, Insert, Delete	View	View	None	View, Update, Insert, Delete	View
Task	None	View, Update	View, Update	View		View, Update
Template Group	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Relationship Families						
Condition Has ML	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Condition Has LR	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Category Has Allowable Values	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Has Checkpoint	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View

Family	MI Operator Rounds Administrator	MI Operator Rounds Mobile User	MAPM Security Group	MI Rounds Designer Viewer	MI Lubrication Management Administrator	MI Lubrication Management User
Has Checkpoint Template	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Has Health Indicators	View	View	View	View	View	View
Has History	View, Insert, Delete	View, Insert, Delete	View, Insert, Delete	View	View, Update, Insert, Delete	View, Insert, Delete
Has Readings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Recommendations	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Reference Documents	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Route	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Tasks	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Health Indicator Has Mapping	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Lubricant Has Method	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Health Indicator Has Source	View	View	View	View	View	View
ML Has Condition	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
ML Has OPR Recommendation	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Route Has Checkpoint	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Route Has Human Resource	View, Update, Insert, Delete	Insert	Insert	View	View, Update, Insert, Delete	Insert
Template Has Checkpoint	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View

Rounds Pro

Deploy Rounds Pro for the First Time

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Step	Task	Notes
1	Review the data model to determine which relationship definitions you will need to modify to include your custom Equipment and Functional Location families. Modify any relationship definitions as needed via Configuration Manager.	This step is required only if you have asset data in families outside of the baseline Equipment and Functional Location families.
2	Assign Security Users to the following Rounds Pro Security Groups: • MI Rounds-Pro Administrator • MI Rounds-Pro Mobile User	This step is required.
3	Install the Rounds Pro mobile app on the mobile device that you plan to use for data collection.	This step is required only if you will use a mobile device for data collection. For information on installation of Rounds Pro on mobile devices see the following sections: • • •
4	Set the local time zone on the mobile device that you will use for data collection, typically the user time zone.	This step is required only if you will use a mobile device for data collection.

Upgrade or Update Rounds Pro to V4.6.11.0.0

About This Task

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be updated to V4.6.11.0.0 automatically when you update the components in the basic APM system architecture. No additional steps are required.

SIS Management

Deploy SIS Management for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Define alternate search queries.	This step is required only if you do not want to use the baseline search queries.
2	Modify threshold values in the SIL Threshold family.	This step is required only if you want to modify the default boundary values specified in the SIL Threshold family. **Tip:** To prevent ambiguity in SIL values for driving risk ranks that fall on the boundary value of two SIL thresholds, avoid specifying contiguous boundary values where the lower boundary value of one threshold is the upper boundary value of the preceding SIL threshold. For example, for the SIL value of 1, if you have specified a SIL threshold of 10 through 100, then, for a SIL value of 2 you can specify the SIL threshold of 100.1 through 1000.
3	Import data from an Exida project file.	This step is required only if you want to create SIL Analyses using an Exida project file.
4	Export data from an Exida project file.	This step is optional.
5	Activate the Hazards Analysis license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

Step	Task	Notes
6	Assign View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges.	This step is required only for Security Groups that will be used in the integration between the SIS Management module and Hazards Analysis.
7	Review the SIS Management data model to determine which relationship definitions you will need to modify to include your custom equipment or location families. Modify any relationship definitions as needed using the Configuration Manager.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
8	Assign Security Users to one or more of the SIS Management Security Groups and Roles.	This step is required.

Upgrade or Update SIS Management to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

  This module will be upgraded to V4.6.11.0.0 automatically when you upgrade the components in the basic APM system architecture. No additional steps are required.
- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

  This module will be upgraded automatically when you upgrade the components in the basic APM system architecture. Additionally, as needed, perform the following steps:

Step	Task	Notes
1	Activate the Hazards Analysis license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

  This module will be upgraded automatically when you upgrade the components in the basic APM system architecture. Additionally, as needed, perform the following steps:

Step	Task	Notes
1	Activate the Hazards Analysis license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
3	Verify the LOPA Assessment records that are linked to Instrumented Functions after upgrade.	This step is optional.

- Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	Activate the Hazards Analysis license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

Step	Task	Notes
1	Activate the Hazards Analysis license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

Step	Task	Notes
1	Activate the Hazards Analysis license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V3.5.1 through V3.5.1.12.3

Step	Task	Notes
1	Activate the Hazards Analysis license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

Step	Task	Notes
1	Activate the Hazards Analysis license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Activate the Hazards Analysis license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Activate the Hazards Analysis license.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.
2	Assign View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

Thickness Monitoring

Deploy TM for the First Time

Before You Begin

The following table outlines the steps that you must complete to deploy and configure this module for the first time. These instructions assume that you have completed the steps for deploying the basic system architecture.

These tasks may be completed by multiple people in your organization. GE Vernova recommends, however, that the tasks be completed in the order in which they are listed.

Results

Step	Task	Notes
1	Review the TM data model to determine which relationship definitions you will need to modify to include your custom equipment families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to one or more of the Security Roles used in TM.	This step is required. User must have permissions to the TM families in order to use the TM functionality.
3	Assign Resource Roles to users by performing the following steps: 1. Access the Human Resource record for each user. 2. In the **Role** box, select **TM Technician**.	This step is required to allow a user (typically, a TM Inspector) to enter details in an Inspection record.

Step	Task	Notes
4	Configure Family Preference Application Settings.	This step is required. You must configure preferences for the families that will be used to store equipment data in Thickness Monitoring. The following relationships must be defined: • For the Equipment family, the Asset to Subcomponent Relationship field must be set to **Has TML Group**, and the Component ID field must be set to **Equipment ID**. The Subcomponent to Asset Relationship field should be left blank. • For the TML Group family, the Subcomponent to Asset Relationship field must be set to **Has TML Group**, and the Component ID field must be set to **TML Group ID**. The Asset to Subcomponent Relationship field should be left blank.
5	Configure Global Preference Application Settings.	This step is required only if you want to use custom reading preferences and Nominal T-Min preferences. Baseline reading preferences and Nominal T-Min preferences will be used if you do not define your own. You can also define additional, optional global preferences that are not defined in the baseline APM database.
6	Configure the system to use custom TML Types.	This step is required only if you want to use custom TML Types. You can define additional TML Types to use in your Corrosion Analyses.
7	Manage Thickness Monitoring Rules Lookup records.	This step is required only if you want to view or modify Thickness Monitoring Rules Lookup records whose values are used to perform certain TM calculations.

Step	Task	Notes
8	Define additional fields that will be displayed in the header section of the TM Measurement Data Entry.	This step is required only if default Thickness Measurement fields are displayed on the headings of these pages in the baseline APM database. You can specify that additional fields be displayed in the header section of these pages.
9	Disable the Auto Manage Tasks setting.	This step is required only if you are planning to use TM tasks.
10	Install the Meridium Device Service on all of the machines that will connect to devices that will be used with Thickness Monitoring.	This step is required only if you will use any device to collect data that you transfer to Thickness Monitoring. If you are using HTTPS to connect to APM, follow the instructions in https://ge-ip.my.salesforce.com/kA20h0000009SCN?srPos=0&srKp=ka2&lang=en_US.
11	Install the drivers and supporting files for any devices on all of the machines that will connect to devices that will be used with Thickness Monitoring.	This step is required only if you will use these devices to collect data that you transfer to Thickness Monitoring.

Upgrade or Update Thickness Monitoring to V4.6.11.0.0

Before You Begin

The following tables outline the steps that you must complete to upgrade this module to V4.6.11.0.0. These instructions assume that you have completed the steps for upgrading the basic APM system architecture.

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Procedure

- Upgrade from any version V4.6.0.0.0 through V4.6.10.0.0.

Step	Task	Notes
1	Revert the following Thickness Monitoring queries to baseline: ◦ `Public\Meridium\Modules\Thickness Monitoring \Queries\Assets Near or Past Retirement` ◦ `Public\Meridium\Modules\Thickness Monitoring \Queries\Assets with TM Tasks` ◦ `Public\Meridium\Modules\Thickness Monitoring \Queries\Corrosion Distribution` ◦ `Public\Meridium\Modules\Thickness Monitoring \Queries\Excessive Corrosion` ◦ `Public\Meridium\Modules\Thickness Monitoring \Queries\Remaining Life Less Than 180 Months` ◦ `Public\Meridium\Modules\Thickness Monitoring \Queries\Thickness Inspections`	This step is required only if you have modified the following queries: ◦ Assets Near or Past Retirement. ◦ Assets with TM Tasks ◦ Corrosion Distribution ◦ Excessive Corrosion. ◦ Remaining Life Less Than 180 Months. ◦ Thickness Inspections.
2	Update PV Stress content and stress lookup fields for Thickness Measurement Locations for Non-Piping Assets.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000038584.
3	Update the datasheet of Thickness Measurement Location family by adding the Minimum Thickness Type Field.	If you have customized the default datasheet of the Thickness Measurement Location family and want to see the Minimum Thickness Type data, you must do the following: ◦ Using the Family Management, edit the default datasheet of MI Thickness Measurement Location family. Remove the existing Minimum Thickness Type (Obsolete) field and add the Minimum Thickness Type field in the Datasheet.

<table>
<tr><th>Step</th><th>Task</th><th>Notes</th></tr>
<tr><td>4</td><td>Update the datasheet of Thickness Monitoring Rules Lookup family by adding the T-Min Formula Policy Field.</td><td>If you have customized the default datasheet of Thickness Monitoring Rules Lookup family and want to see the T-Min Formula Policy data, you must do the following:
Using the Family Management, edit the default datasheet of Thickness Monitoring Rules Lookup family. Add the T-Min Formula Policy field in the Datasheet.</td></tr>
<tr><td>5</td><td>Update the values in the newly added Minimum Thickness Type field from the existing Minimum Thickness Type (Obsolete) field.</td><td>This will be automatically done by a Utility during an upgrade process. User does not need to do anything.

Below is the mapping from the existing data to the new data:

<table><tr><th>Minimum Thickness Type (Obsolete)</th><th>Minimum Thickness Type</th></tr><tr><td>Calculated</td><td>CALCULATED</td></tr><tr><td>Nominal</td><td>NOMINAL</td></tr><tr><td>User Defined</td><td>USER DEFINED</td></tr><tr><td>Default</td><td>DEFAULT</td></tr></table>
Note: Any other values other than NULL will be mapped to USER DEFINED.</td></tr>
</table>

- Upgrade from any version V4.5.0.0.0 through V4.5.0.0.21.

Step	Task	Notes
1	Revert the following Thickness Monitoring queries to baseline: ◦ `Public\Meridium\Modules\Thickness Monitoring \Queries\Assets Near or Past Retirement` ◦ `Public\Meridium\Modules\Thickness Monitoring \Queries\Assets with TM Tasks` ◦ `Public\Meridium\Modules\Thickness Monitoring \Queries\Corrosion Distribution` ◦ `Public\Meridium\Modules\Thickness Monitoring \Queries\Excessive Corrosion` ◦ `Public\Meridium\Modules\Thickness Monitoring \Queries\Remaining Life Less Than 180 Months` ◦ `Public\Meridium\Modules\Thickness Monitoring \Queries\Thickness Inspections`	This step is required only if you have modified the following queries: ◦ Assets Near or Past Retirement. ◦ Assets with TM Tasks ◦ Corrosion Distribution ◦ Excessive Corrosion. ◦ Remaining Life Less Than 180 Months. ◦ Thickness Inspections.
2	Update PV Stress content and stress lookup fields for Thickness Measurement Locations for Non-Piping Assets.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000038584.
3	Update the datasheet of Thickness Measurement Location family by adding the Minimum Thickness Type Field.	If you have customized the default datasheet of the Thickness Measurement Location family and want to see the Minimum Thickness Type data, you must do the following: ◦ Using the Family Management, edit the default datasheet of MI Thickness Measurement Location family. Remove the existing Minimum Thickness Type (Obsolete) field and add the Minimum Thickness Type field in the Datasheet.

<table>
<tr><th>Step</th><th>Task</th><th>Notes</th></tr>
<tr><td>4</td><td>Update the datasheet of Thickness Monitoring Rules Lookup family by adding the T-Min Formula Policy Field.</td><td>If you have customized the default datasheet of Thickness Monitoring Rules Lookup family and want to see the T-Min Formula Policy data, you must do the following:
Using the Family Management, edit the default datasheet of Thickness Monitoring Rules Lookup family. Add the T-Min Formula Policy field in the Datasheet.</td></tr>
<tr><td>5</td><td>Update the values in the newly added Minimum Thickness Type field from the existing Minimum Thickness Type (Obsolete) field.</td><td>This will be automatically done by a Utility during an upgrade process. User does not need to do anything.

Below is the mapping from the existing data to the new data:

<table><tr><th>Minimum Thickness Type (Obsolete)</th><th>Minimum Thickness Type</th></tr><tr><td>Calculated</td><td>CALCULATED</td></tr><tr><td>Nominal</td><td>NOMINAL</td></tr><tr><td>User Defined</td><td>USER DEFINED</td></tr><tr><td>Default</td><td>DEFAULT</td></tr></table>
Note: Any other values other than NULL will be mapped to USER DEFINED.</td></tr>
</table>

- Upgrade from any version V4.4.0.0.0 through V4.4.0.0.16.

Step	Task	Notes
1	Revert the following Thickness Monitoring queries to baseline: ◦ `Public/Meridium/Modules/Thickness Monitoring/Queries/Assets Near or Past Retirement` ◦ `Public/Meridium/Modules/Thickness Monitoring/Queries/Assets with TM Tasks` ◦ `Public/Meridium/Modules/Thickness Monitoring/Queries/Corrosion Distribution` ◦ `Public/Meridium/Modules/Thickness Monitoring/Queries/Excessive Corrosion` ◦ `Public/Meridium/Modules/Thickness Monitoring/Queries/Remaining Life Less Than 180 Months` ◦ `Public/Meridium/Modules/Thickness Monitoring/Queries/Thickness Inspections` ◦ `Public/Meridium/Modules/Thickness Monitoring/Queries/TM Assets` ◦ `Public/Meridium/Modules/Thickness Monitoring/Queries/TM Assets Requiring a Calculation`	This step is required if you have modified any of the following queries: ◦ Assets Near or Past Retirement ◦ Assets with TM Tasks ◦ Corrosion Distribution ◦ Excessive Corrosion ◦ Remaining Life Less Than 180 Months ◦ Thickness Inspections ◦ TM Assets ◦ TM Assets Requiring a Calculation **Note:** If you have not modified any of the above mentioned queries, you do not have to complete this step for the specified query.
2	Uninstall the previous version of the Meridium Device Service on all of the machines that will connect to devices that will be used with Thickness Monitoring.	This step is required only if you will use any device to collect data that you transfer to Thickness Monitoring.
3	Install the Meridium Device Service on all of the machines that will connect to devices that will be used with Thickness Monitoring.	This step is required only if you will use any device to collect data that you transfer to Thickness Monitoring. If you are using HTTPS to connect to APM, follow the instructions in https://ge-ip.my.salesforce.com/kA20h0000009SCN?srPos=0&srKp=ka2&lang=en_US.

<table>
<tr><th>Step</th><th>Task</th><th>Notes</th></tr>
<tr><td>4</td><td>If you have previously modified the following Pipe Properties records, follow the steps mentioned in KBA 000048342 to get the updated values for the records.

<table><tr><th>Schedule</th><th>Nominal Diameter - NPS</th><th>Nominal Diameter - DN</th><th>Outside Diameter</th><th>Nominal Wall Thickness (Old)</th><th>Internal Diameter (Old)</th><th>Nominal Wall Thickness (New)</th><th>Internal Diameter (New)</th></tr><tr><td>30</td><td>2.5</td><td>65</td><td>2.875 (inches)</td><td>0.125 (inches)</td><td>2.625 (inches)</td><td>0.188 (inches)</td><td>2.499 (inches)</td></tr><tr><td>40</td><td>36</td><td>900</td><td>36 (inches)</td><td>0.688 (inches)</td><td>34.624 (inches)</td><td>0.75 (inches)</td><td>34.5 (inches)</td></tr></table></td><td>This step is optional.</td></tr>
<tr><td>5</td><td>If you have modified the datasheets for the following families, the datasheets must be reverted to use the new fields. Alternatively, the following fields can be added to the modified datasheets:

<table><tr><th>Family</th><th>Datasheet</th><th>Field</th></tr><tr><td>TML Group</td><td>TML Group</td><td>TML Group Type</td></tr><tr><td>Thickness Measurement Location</td><td>Thickness Measurement Location</td><td>The following fields are added to the Piping sub-section:
Position
Previous Position
Band
Previous Band</td></tr><tr><td>Thickness Measurements</td><td>Thickness Measurements</td><td>Calculated
Measurement Status Indicator Basis</td></tr></table></td><td>This step is required only if you want to use the Piping Rotation workflow.</td></tr>
<tr><td>6</td><td>Revert the following Thickness Monitoring queries to baseline:
<code>Public\Meridium\Modules\Thickness Monitoring \Queries\Assets Near or Past Retirement</code>
<code>Public\Meridium\Modules\Thickness Monitoring \Queries\Assets with TM Tasks</code>
<code>Public\Meridium\Modules\Thickness Monitoring \Queries\Corrosion Distribution</code>
<code>Public\Meridium\Modules\Thickness Monitoring \Queries\Excessive Corrosion</code>
<code>Public\Meridium\Modules\Thickness Monitoring \Queries\Remaining Life Less Than 180 Months</code>
<code>Public\Meridium\Modules\Thickness Monitoring \Queries\Thickness Inspections</code></td><td>This step is required only if you have modified the following queries:
Assets Near or Past Retirement.
Assets with TM Tasks
Corrosion Distribution
Excessive Corrosion.
Remaining Life Less Than 180 Months.
Thickness Inspections.</td></tr>
</table>

Step	Task	Notes
7	Update PV Stress content and stress lookup fields for Thickness Measurement Locations for Non-Piping Assets.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000038584.
8	Update the datasheet of Thickness Measurement Location family by adding the Minimum Thickness Type Field.	If you have customized the default datasheet of the Thickness Measurement Location family and want to see the Minimum Thickness Type data, you must do the following: ◦ Using the Family Management, edit the default datasheet of MI Thickness Measurement Location family. Remove the existing Minimum Thickness Type (Obsolete) field and add the Minimum Thickness Type field in the Datasheet.

<table>
<tr><th>Step</th><th>Task</th><th>Notes</th></tr>
<tr><td>9</td><td>Update the datasheet of Thickness Monitoring Rules Lookup family by adding the T-Min Formula Policy Field.</td><td>If you have customized the default datasheet of Thickness Monitoring Rules Lookup family and want to see the T-Min Formula Policy data, you must do the following:
Using the Family Management, edit the default datasheet of Thickness Monitoring Rules Lookup family. Add the T-Min Formula Policy field in the Datasheet.</td></tr>
<tr><td>10</td><td>Update the values in the newly added Minimum Thickness Type field from the existing Minimum Thickness Type (Obsolete) field.</td><td>This will be automatically done by a Utility during an upgrade process. User does not need to do anything.

Below is the mapping from the existing data to the new data:

<table><tr><th>Minimum Thickness Type (Obsolete)</th><th>Minimum Thickness Type</th></tr><tr><td>Calculated</td><td>CALCULATED</td></tr><tr><td>Nominal</td><td>NOMINAL</td></tr><tr><td>User Defined</td><td>USER DEFINED</td></tr><tr><td>Default</td><td>DEFAULT</td></tr></table>
Note: Any other values other than NULL will be mapped to USER DEFINED.</td></tr>
</table>

- Upgrade from any version V4.3.0.0.0 through V4.3.1.0.11

<table>
<tr><th>Step</th><th>Task</th><th>Notes</th></tr>
<tr><td>1</td><td>Uninstall the previous version of the Meridium Device Service on all of the machines that will connect to devices that will be used with Thickness Monitoring.</td><td>This step is required only if you will use any device to collect data that you transfer to Thickness Monitoring.</td></tr>
<tr><td>2</td><td>Install the Meridium Device Service on all of the machines that will connect to devices that will be used with Thickness Monitoring.</td><td>This step is required only if you will use any device to collect data that you transfer to Thickness Monitoring. If you are using HTTPS to connect to APM, follow the instructions in https://ge-ip.my.salesforce.com/kA20h0000009SCN?srPos=0&srKp=ka2&lang=en_US.</td></tr>
<tr><td>3</td><td>If you have previously modified the following Pipe Properties records, follow the steps mentioned in KBA 000048342 to get the updated values for the records.
<table>
<tr><th>Schedule</th><th>Nominal Diameter - NPS</th><th>Nominal Diameter - DN</th><th>Outside Diameter</th><th>Nominal Wall Thickness (Old)</th><th>Internal Diameter (Old)</th><th>Nominal Wall Thickness (New)</th><th>Internal Diameter (New)</th></tr>
<tr><td>30</td><td>2.5</td><td>65</td><td>2.875 (Inches)</td><td>0.125 (Inches)</td><td>2.625 (Inches)</td><td>0.188 (Inches)</td><td>2.499 (Inches)</td></tr>
<tr><td>40</td><td>36</td><td>900</td><td>36 (Inches)</td><td>0.688 (Inches)</td><td>34.624 (Inches)</td><td>0.75 (Inches)</td><td>34.5 (Inches)</td></tr>
</table></td><td>This step is optional.</td></tr>
<tr><td>4</td><td>Revert the following Thickness Monitoring queries to baseline:
<code>Public\Meridium\Modules\Thickness Monitoring \Queries\Assets Near or Past Retirement</code>
<code>Public\Meridium\Modules\Thickness Monitoring \Queries\Assets with TM Tasks</code>
<code>Public\Meridium\Modules\Thickness Monitoring \Queries\Corrosion Distribution</code>
<code>Public\Meridium\Modules\Thickness Monitoring \Queries\Excessive Corrosion</code>
<code>Public\Meridium\Modules\Thickness Monitoring \Queries\Remaining Life Less Than 180 Months</code>
<code>Public\Meridium\Modules\Thickness Monitoring \Queries\Thickness Inspections</code></td><td>This step is required only if you have modified the following queries:
Assets Near or Past Retirement.
Assets with TM Tasks
Corrosion Distribution
Excessive Corrosion.
Remaining Life Less Than 180 Months.
Thickness Inspections.</td></tr>
</table>

Step	Task	Notes
5	Update PV Stress content and stress lookup fields for Thickness Measurement Locations for Non-Piping Assets.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000038584.
6	Update the datasheet of Thickness Measurement Location family by adding the Minimum Thickness Type Field.	If you have customized the default datasheet of the Thickness Measurement Location family and want to see the Minimum Thickness Type data, you must do the following: ◦ Using the Family Management, edit the default datasheet of MI Thickness Measurement Location family. Remove the existing Minimum Thickness Type (Obsolete) field and add the Minimum Thickness Type field in the Datasheet.

<table>
<tr><th>Step</th><th>Task</th><th>Notes</th></tr>
<tr><td>7</td><td>Update the datasheet of Thickness Monitoring Rules Lookup family by adding the T-Min Formula Policy Field.</td><td>If you have customized the default datasheet of Thickness Monitoring Rules Lookup family and want to see the T-Min Formula Policy data, you must do the following:
Using the Family Management, edit the default datasheet of Thickness Monitoring Rules Lookup family. Add the T-Min Formula Policy field in the Datasheet.</td></tr>
<tr><td>8</td><td>Update the values in the newly added Minimum Thickness Type field from the existing Minimum Thickness Type (Obsolete) field.</td><td>This will be automatically done by a Utility during an upgrade process. User does not need to do anything.
Below is the mapping from the existing data to the new data:
<table><tr><th>Minimum Thickness Type (Obsolete)</th><th>Minimum Thickness Type</th></tr><tr><td>Calculated</td><td>CALCULATED</td></tr><tr><td>Nominal</td><td>NOMINAL</td></tr><tr><td>User Defined</td><td>USER DEFINED</td></tr><tr><td>Default</td><td>DEFAULT</td></tr></table>Note: Any other values other than NULL will be mapped to USER DEFINED.</td></tr>
</table>

- Upgrade from any version V4.2.0.0 through V4.2.0.9.5

Step	Task	Notes
1	If you are using HTTPS to connect to APM, follow the instructions in https://ge-ip.my.salesforce.com/kA20h0000009SCN?srPos=0&srKp=ka2&lang=en_US.	This step is required.
2	Revert the following Thickness Monitoring queries to baseline: ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets Near or Past Retirement` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets with TM Tasks` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Corrosion Distribution` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Excessive Corrosion` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Remaining Life Less Than 180 Months` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Thickness Inspections`	This step is required only if you have modified the following queries: ◦ Assets Near or Past Retirement. ◦ Assets with TM Tasks ◦ Corrosion Distribution ◦ Excessive Corrosion. ◦ Remaining Life Less Than 180 Months. ◦ Thickness Inspections.
3	Update PV Stress content and stress lookup fields for Thickness Measurement Locations for Non-Piping Assets.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000038584.

Step	Task	Notes
4	Update the datasheet of Thickness Measurement Location family by adding the Minimum Thickness Type Field.	If you have customized the default datasheet of the Thickness Measurement Location family and want to see the Minimum Thickness Type data, you must do the following: ◦ Using the Family Management, edit the default datasheet of MI Thickness Measurement Location family. Remove the existing Minimum Thickness Type (Obsolete) field and add the Minimum Thickness Type field in the Datasheet.
5	Update the datasheet of Thickness Monitoring Rules Lookup family by adding the T-Min Formula Policy Field.	If you have customized the default datasheet of Thickness Monitoring Rules Lookup family and want to see the T-Min Formula Policy data, you must do the following: ◦ Using the Family Management, edit the default datasheet of Thickness Monitoring Rules Lookup family. Add the T-Min Formula Policy field in the Datasheet.
6	Update the values in the newly added Minimum Thickness Type field from the existing Minimum Thickness Type (Obsolete) field.	This will be automatically done by a Utility during an upgrade process. User does not need to do anything. Below is the mapping from the existing data to the new data: **Minimum Thickness Type (Obsolete)** → **Minimum Thickness Type** Calculated → CALCULATED Nominal → NOMINAL User Defined → USER DEFINED Default → DEFAULT **Note:** Any other values other than NULL will be mapped to USER DEFINED.

- Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	If you are using HTTPS to connect to APM, follow the instructions in https://ge-ip.my.salesforce.com/kA20h0000009SCN?srPos=0&srKp=ka2&lang=en_US.	This step is required.
2	Revert the following Thickness Monitoring queries to baseline: ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets Near or Past Retirement` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets with TM Tasks` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Corrosion Distribution` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Excessive Corrosion` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Remaining Life Less Than 180 Months` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Thickness Inspections`	This step is required only if you have modified the following queries: ◦ Assets Near or Past Retirement. ◦ Assets with TM Tasks ◦ Corrosion Distribution ◦ Excessive Corrosion. ◦ Remaining Life Less Than 180 Months. ◦ Thickness Inspections.
3	Update PV Stress content and stress lookup fields for Thickness Measurement Locations for Non-Piping Assets.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000038584.

Step	Task	Notes
4	Update the datasheet of Thickness Measurement Location family by adding the Minimum Thickness Type Field.	If you have customized the default datasheet of the Thickness Measurement Location family and want to see the Minimum Thickness Type data, you must do the following: ◦ Using the Family Management, edit the default datasheet of MI Thickness Measurement Location family. Remove the existing Minimum Thickness Type (Obsolete) field and add the Minimum Thickness Type field in the Datasheet.
5	Update the datasheet of Thickness Monitoring Rules Lookup family by adding the T-Min Formula Policy Field.	If you have customized the default datasheet of Thickness Monitoring Rules Lookup family and want to see the T-Min Formula Policy data, you must do the following: ◦ Using the Family Management, edit the default datasheet of Thickness Monitoring Rules Lookup family. Add the T-Min Formula Policy field in the Datasheet.
6	Update the values in the newly added Minimum Thickness Type field from the existing Minimum Thickness Type (Obsolete) field.	This will be automatically done by a Utility during an upgrade process. User does not need to do anything. Below is the mapping from the existing data to the new data: **Minimum Thickness Type (Obsolete)** / **Minimum Thickness Type** Calculated / CALCULATED Nominal / NOMINAL User Defined / USER DEFINED Default / DEFAULT **Note:** Any other values other than NULL will be mapped to USER DEFINED.

- Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	If you are using HTTPS to connect to APM, follow the instructions in https://ge-ip.my.salesforce.com/kA20h0000009SCN?srPos=0&srKp=ka2&lang=en_US.	This step is required.
2	Revert the following Thickness Monitoring queries to baseline: ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets Near or Past Retirement` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets with TM Tasks` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Corrosion Distribution` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Excessive Corrosion` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Remaining Life Less Than 180 Months` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Thickness Inspections`	This step is required only if you have modified the following queries: ◦ Assets Near or Past Retirement. ◦ Assets with TM Tasks ◦ Corrosion Distribution ◦ Excessive Corrosion. ◦ Remaining Life Less Than 180 Months. ◦ Thickness Inspections.
3	Update PV Stress content and stress lookup fields for Thickness Measurement Locations for Non-Piping Assets.	This step is required only if you want to use the Pressure Vessel stress content with updated Material Grade in accordance with Tables 1A and 1B of ASME Section II, Part D, 2010. For more information, refer to KBA 000038584.

Step	Task	Notes
4	Update the datasheet of Thickness Measurement Location family by adding the Minimum Thickness Type Field.	If you have customized the default datasheet of the Thickness Measurement Location family and want to see the Minimum Thickness Type data, you must do the following: ◦ Using the Family Management, edit the default datasheet of MI Thickness Measurement Location family. Remove the existing Minimum Thickness Type (Obsolete) field and add the Minimum Thickness Type field in the Datasheet.
5	Update the datasheet of Thickness Monitoring Rules Lookup family by adding the T-Min Formula Policy Field.	If you have customized the default datasheet of Thickness Monitoring Rules Lookup family and want to see the T-Min Formula Policy data, you must do the following: ◦ Using the Family Management, edit the default datasheet of Thickness Monitoring Rules Lookup family. Add the T-Min Formula Policy field in the Datasheet.
6	Update the values in the newly added Minimum Thickness Type field from the existing Minimum Thickness Type (Obsolete) field.	This will be automatically done by a Utility during an upgrade process. User does not need to do anything. Below is the mapping from the existing data to the new data: **Minimum Thickness Type (Obsolete)** / **Minimum Thickness Type** Calculated / CALCULATED Nominal / NOMINAL User Defined / USER DEFINED Default / DEFAULT **Note:** Any other values other than NULL will be mapped to USER DEFINED.

- Upgrade from any version V3.6.1.0.0 through V3.6.1.7.5

Step	Task	Notes
1	If you are using HTTPS to connect to APM, follow the instructions in https://ge-ip.my.salesforce.com/kA20h0000009SCN?srPos=0&srKp=ka2&lang=en_US.	This step is required.
2	Revert the following Thickness Monitoring queries to baseline: ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets Near or Past Retirement` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets with TM Tasks` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Corrosion Distribution` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Excessive Corrosion` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Remaining Life Less Than 180 Months` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Thickness Inspections`	This step is required only if you have modified the following queries: ◦ Assets Near or Past Retirement. ◦ Assets with TM Tasks ◦ Corrosion Distribution ◦ Excessive Corrosion. ◦ Remaining Life Less Than 180 Months. ◦ Thickness Inspections.
3	Update the datasheet of Thickness Measurement Location family by adding the Minimum Thickness Type Field.	If you have customized the default datasheet of the Thickness Measurement Location family and want to see the Minimum Thickness Type data, you must do the following: ◦ Using the Family Management, edit the default datasheet of MI Thickness Measurement Location family. Remove the existing Minimum Thickness Type (Obsolete) field and add the Minimum Thickness Type field in the Datasheet.

Step	Task	Notes
4	Update the datasheet of Thickness Monitoring Rules Lookup family by adding the T-Min Formula Policy Field.	If you have customized the default datasheet of Thickness Monitoring Rules Lookup family and want to see the T-Min Formula Policy data, you must do the following: ◦ Using the Family Management, edit the default datasheet of Thickness Monitoring Rules Lookup family. Add the T-Min Formula Policy field in the Datasheet.
5	Update the values in the newly added Minimum Thickness Type field from the existing Minimum Thickness Type (Obsolete) field.	This will be automatically done by a Utility during an upgrade process. User does not need to do anything. Below is the mapping from the existing data to the new data: **Minimum Thickness Type (Obsolete)** / **Minimum Thickness Type** Calculated / CALCULATED Nominal / NOMINAL User Defined / USER DEFINED Default / DEFAULT **Note:** Any other values other than NULL will be mapped to USER DEFINED.

- Upgrade from any version V3.6.0.0.0 through V3.6.0.12.9

Step	Task	Notes
1	If you are using HTTPS to connect to APM, follow the instructions in https://ge-ip.my.salesforce.com/kA20h0000009SCN?srPos=0&srKp=ka2&lang=en_US.	This step is required.
2	Revert the following Thickness Monitoring queries to baseline: ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets Near or Past Retirement` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets with TM Tasks` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Corrosion Distribution` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Excessive Corrosion` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Remaining Life Less Than 180 Months` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Thickness Inspections`	This step is required only if you have modified the following queries: ◦ Assets Near or Past Retirement. ◦ Assets with TM Tasks ◦ Corrosion Distribution ◦ Excessive Corrosion. ◦ Remaining Life Less Than 180 Months. ◦ Thickness Inspections.
3	Update the datasheet of Thickness Measurement Location family by adding the Minimum Thickness Type Field.	If you have customized the default datasheet of the Thickness Measurement Location family and want to see the Minimum Thickness Type data, you must do the following: ◦ Using the Family Management, edit the default datasheet of MI Thickness Measurement Location family. Remove the existing Minimum Thickness Type (Obsolete) field and add the Minimum Thickness Type field in the Datasheet.

Step	Task	Notes
4	Update the datasheet of Thickness Monitoring Rules Lookup family by adding the T-Min Formula Policy Field.	If you have customized the default datasheet of Thickness Monitoring Rules Lookup family and want to see the T-Min Formula Policy data, you must do the following: ◦ Using the Family Management, edit the default datasheet of Thickness Monitoring Rules Lookup family. Add the T-Min Formula Policy field in the Datasheet.
5	Update the values in the newly added Minimum Thickness Type field from the existing Minimum Thickness Type (Obsolete) field.	This will be automatically done by a Utility during an upgrade process. User does not need to do anything. Below is the mapping from the existing data to the new data: **Minimum Thickness Type (Obsolete)** / **Minimum Thickness Type** Calculated / CALCULATED Nominal / NOMINAL User Defined / USER DEFINED Default / DEFAULT **Note:** Any other values other than NULL will be mapped to USER DEFINED.

- Upgrade from any version V3.5.1 through V3.5.1.12.3

Step	Task	Notes
1	If you are using HTTPS to connect to APM, follow the instructions in https://ge-ip.my.salesforce.com/kA20h0000009SCN?srPos=0&srKp=ka2&lang=en_US.	This step is required.
2	Revert the following Thickness Monitoring queries to baseline: ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets Near or Past Retirement` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets with TM Tasks` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Corrosion Distribution` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Excessive Corrosion` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Remaining Life Less Than 180 Months` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Thickness Inspections`	This step is required only if you have modified the following queries: ◦ Assets Near or Past Retirement. ◦ Assets with TM Tasks ◦ Corrosion Distribution ◦ Excessive Corrosion. ◦ Remaining Life Less Than 180 Months. ◦ Thickness Inspections.
3	Update the datasheet of Thickness Measurement Location family by adding the Minimum Thickness Type Field.	If you have customized the default datasheet of the Thickness Measurement Location family and want to see the Minimum Thickness Type data, you must do the following: ◦ Using the Family Management, edit the default datasheet of MI Thickness Measurement Location family. Remove the existing Minimum Thickness Type (Obsolete) field and add the Minimum Thickness Type field in the Datasheet.

Step	Task	Notes
4	Update the datasheet of Thickness Monitoring Rules Lookup family by adding the T-Min Formula Policy Field.	If you have customized the default datasheet of Thickness Monitoring Rules Lookup family and want to see the T-Min Formula Policy data, you must do the following: ◦ Using the Family Management, edit the default datasheet of Thickness Monitoring Rules Lookup family. Add the T-Min Formula Policy field in the Datasheet.
5	Update the values in the newly added Minimum Thickness Type field from the existing Minimum Thickness Type (Obsolete) field.	This will be automatically done by a Utility during an upgrade process. User does not need to do anything. Below is the mapping from the existing data to the new data: **Minimum Thickness Type (Obsolete)** / **Minimum Thickness Type** Calculated / CALCULATED Nominal / NOMINAL User Defined / USER DEFINED Default / DEFAULT **Note:** Any other values other than NULL will be mapped to USER DEFINED.

- Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.1

Step	Task	Notes
1	If you are using HTTPS to connect to APM, follow the instructions in https://ge-ip.my.salesforce.com/kA20h0000009SCN?srPos=0&srKp=ka2&lang=en_US.	This step is required.
2	Revert the following Thickness Monitoring queries to baseline: ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets Near or Past Retirement` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets with TM Tasks` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Corrosion Distribution` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Excessive Corrosion` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Remaining Life Less Than 180 Months` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Thickness Inspections`	This step is required only if you have modified the following queries: ◦ Assets Near or Past Retirement. ◦ Assets with TM Tasks ◦ Corrosion Distribution ◦ Excessive Corrosion. ◦ Remaining Life Less Than 180 Months. ◦ Thickness Inspections.
3	Update the datasheet of Thickness Measurement Location family by adding the Minimum Thickness Type Field.	If you have customized the default datasheet of the Thickness Measurement Location family and want to see the Minimum Thickness Type data, you must do the following: ◦ Using the Family Management, edit the default datasheet of MI Thickness Measurement Location family. Remove the existing Minimum Thickness Type (Obsolete) field and add the Minimum Thickness Type field in the Datasheet.

<table>
<tr><th>Step</th><th>Task</th><th>Notes</th></tr>
<tr><td>4</td><td>Update the datasheet of Thickness Monitoring Rules Lookup family by adding the T-Min Formula Policy Field.</td><td>If you have customized the default datasheet of Thickness Monitoring Rules Lookup family and want to see the T-Min Formula Policy data, you must do the following:
Using the Family Management, edit the default datasheet of Thickness Monitoring Rules Lookup family. Add the T-Min Formula Policy field in the Datasheet.</td></tr>
<tr><td>5</td><td>Update the values in the newly added Minimum Thickness Type field from the existing Minimum Thickness Type (Obsolete) field.</td><td>This will be automatically done by a Utility during an upgrade process. User does not need to do anything.
Below is the mapping from the existing data to the new data:<table><tr><th>Minimum Thickness Type (Obsolete)</th><th>Minimum Thickness Type</th></tr><tr><td>Calculated</td><td>CALCULATED</td></tr><tr><td>Nominal</td><td>NOMINAL</td></tr><tr><td>User Defined</td><td>USER DEFINED</td></tr><tr><td>Default</td><td>DEFAULT</td></tr></table>Note: Any other values other than NULL will be mapped to USER DEFINED.</td></tr>
</table>

- Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Manually update TM Analyses for which you used custom corrosion rates. To do so: 1. Locate the records that you will need to update by running the following query: SELECT [MI_EQUIP000].[MI_EQUIP000_EQUIP_ID_C] "Equipment ID", [MI_TMLGROUP].[MI_TMLGROUP_ID_C] "TML Group ID", [MI Thickness Measurement Location].[MI_DP_ASSET_ID_CHR] "TML Asset ID", [MI Thickness Measurement Location].[MI_DP_ID_CHR] "TML ID", [MI TML Corrosion Analysis].[MI_TML_CA_A_CR_N] "Custom Calculation A Corros", [MI TML Corrosion Analysis].[MI_TML_CA_B_CR_N] "Custom Calculation B Corros" FROM [MI_EQUIP000] JOIN_SUCC [MI_TMLGROUP] JOIN_SUCC [MI Thickness Measurement Location] JOIN_SUCC [MI TML Corrosion Analysis] ON {MI Has Corrosion Analyses} ON {MI Has Datapoints} ON {MIR_HSTMLGP} WHERE ([MI TML Corrosion Analysis].[MI_TML_CA_A_CR_N] > 0 AND [MI TML Corrosion Analysis].[MI_TML_CA_B_CR_N] > 0) 2. Use the Bulk Analyze tool to update TM Analyses associated with the Equipment and TML Group records returned by this query. **Note:** These instructions assume that you are using the baseline Equipment and TML Group families. If you use custom equipment families, you must replace the following values before running the query in order to identify the records requiring update: ◦ MI_EQUIP000 and MI_TMLGROUP with your custom family IDs. ◦ MI_EQUIP000_EQUIP_ID_C and MI_TMLGROUP_ID_C with the field IDs used to identify these custom equipment records. 3. Run the Bulk Analyze tool using your custom records.	This step is required only if, in previous versions of Meridium APM, you used custom corrosion rates in your TM Analyses. If you did so, certain fields in the associated TML Corrosion Analysis records were populated with values using the unit of measure (UOM) inches per day instead of IN/YR (TM) (i.e., inches per year), which is the UOM that is specified in the properties of the fields. To correct this issue in existing records, you must perform this step to manually update TM Analyses. For more information about this issue, see the V3.5.1 Release Notes.

Step	Task	Notes
2	If you are using HTTPS to connect to APM, follow the instructions in https://ge-ip.my.salesforce.com/kA20h0000009SCN?srPos=0&srKp=ka2&lang=en_US.	
3	Revert the following Thickness Monitoring queries to baseline: ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets Near or Past Retirement` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets with TM Tasks` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Corrosion Distribution` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Excessive Corrosion` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Remaining Life Less Than 180 Months` Public\Meridium\Modules\Thickness Monitoring\Queries\Thickness Inspections	This step is required only if you have modified the following queries: ◦ Assets Near or Past Retirement. ◦ Assets with TM Tasks ◦ Corrosion Distribution ◦ Excessive Corrosion. ◦ Remaining Life Less Than 180 Months. ◦ Thickness Inspections.
4	Update the datasheet of Thickness Measurement Location family by adding the Minimum Thickness Type Field.	If you have customized the default datasheet of the Thickness Measurement Location family and want to see the Minimum Thickness Type data, you must do the following: ◦ Using the Family Management, edit the default datasheet of MI Thickness Measurement Location family. Remove the existing Minimum Thickness Type (Obsolete) field and add the Minimum Thickness Type field in the Datasheet.

Step	Task	Notes
5	Update the datasheet of Thickness Monitoring Rules Lookup family by adding the T-Min Formula Policy Field.	If you have customized the default datasheet of Thickness Monitoring Rules Lookup family and want to see the T-Min Formula Policy data, you must do the following: ◦ Using the Family Management, edit the default datasheet of Thickness Monitoring Rules Lookup family. Add the T-Min Formula Policy field in the Datasheet.
6	Update the values in the newly added Minimum Thickness Type field from the existing Minimum Thickness Type (Obsolete) field.	This will be automatically done by a Utility during an upgrade process. User does not need to do anything. Below is the mapping from the existing data to the new data: **Minimum Thickness Type (Obsolete)** / **Minimum Thickness Type** Calculated / CALCULATED Nominal / NOMINAL User Defined / USER DEFINED Default / DEFAULT **Note:** Any other values other than NULL will be mapped to USER DEFINED.

- Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Update certain TM Analyses to correct TML Corrosion Analyses for which you performed measurement variance evaluation prior to APM. To do so: 1. Locate the records that you will need to update by creating a query that returns TML Corrosion Analyses whose: ◦ Short Term Corrosion Rate field contains the value 0 (zero). ◦ Allowable Measurement Variance Applied field is set to True. 2. Use the Bulk Analyze tool to update TM Analyses that are associated with TML Corrosion Analyses returned by the query you created in step 1.	This step is required.

Step	Task	Notes
2	Manually update TM Analyses for which you used custom corrosion rates. To do so: 1. Locate the records that you will need to update by running the following query: SELECT [MI_EQUIP000].[MI_EQUIP000_EQUIP_ID_C] "Equipment ID", [MI_TMLGROUP].[MI_TMLGROUP_ID_C] "TML Group ID", [MI Thickness Measurement Location].[MI_DP_ASSET_ID_CHR] "TML Asset ID", [MI Thickness Measurement Location].[MI_DP_ID_CHR] "TML ID", [MI TML Corrosion Analysis].[MI_TML_CA_A_CR_N] "Custom Calculation A Corros", [MI TML Corrosion Analysis].[MI_TML_CA_B_CR_N] "Custom Calculation B Corros" FROM [MI_EQUIP000] JOIN_SUCC [MI_TMLGROUP] JOIN_SUCC [MI Thickness Measurement Location] JOIN_SUCC [MI TML Corrosion Analysis] ON {MI Has Corrosion Analyses} ON {MI Has Datapoints} ON {MIR_HSTMLGP} WHERE ([MI TML Corrosion Analysis].[MI_TML_CA_A_CR_N] > 0 AND [MI TML Corrosion Analysis].[MI_TML_CA_B_CR_N] > 0) 2. Use the Bulk Analyze tool to update TM Analyses associated with the Equipment and TML Group records returned by this query. **Note:** These instructions assume that you are using the baseline Equipment and TML Group families. If you use custom equipment families, you must replace the following values before running the query in order to identify the records requiring update: ◦ MI_EQUIP000 and MI_TMLGROUP with your custom family IDs. ◦ MI_EQUIP000_EQUIP_ID_C and MI_TMLGROUP_ID_C with the field IDs used to identify these custom equipment records. 3. Run the Bulk Analyze tool using your custom records.	This step is required only if, in previous versions of Meridium APM, you used custom corrosion rates in your TM Analyses. If you did so, certain fields in the associated TML Corrosion Analysis records were populated with values using the unit of measure (UOM) inches per day instead of IN/YR (TM) (i.e., inches per year), which is the UOM that is specified in the properties of the fields. To correct this issue in existing records, you must perform this step to manually update TM Analyses. For more information about this issue, see the V3.5.1 Release Notes.

Step	Task	Notes
3	If you are using HTTPS to connect to APM, follow the instructions in https://ge-ip.my.salesforce.com/kA20h0000009SCN?srPos=0&srKp=ka2&lang=en_US.	
4	Revert the following Thickness Monitoring queries to baseline: ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets Near or Past Retirement` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Assets with TM Tasks` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Corrosion Distribution` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Excessive Corrosion` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Remaining Life Less Than 180 Months` ◦ `Public\Meridium\Modules\Thickness Monitoring\Queries\Thickness Inspections`	This step is required only if you have modified the following queries: ◦ Assets Near or Past Retirement. ◦ Assets with TM Tasks ◦ Corrosion Distribution ◦ Excessive Corrosion. ◦ Remaining Life Less Than 180 Months. ◦ Thickness Inspections.
5	Update the datasheet of Thickness Measurement Location family by adding the Minimum Thickness Type Field.	If you have customized the default datasheet of the Thickness Measurement Location family and want to see the Minimum Thickness Type data, you must do the following: ◦ Using the Family Management, edit the default datasheet of MI Thickness Measurement Location family. Remove the existing Minimum Thickness Type (Obsolete) field and add the Minimum Thickness Type field in the Datasheet.

<table>
<tr><th>Step</th><th>Task</th><th>Notes</th></tr>
<tr><td>6</td><td>Update the datasheet of Thickness Monitoring Rules Lookup family by adding the T-Min Formula Policy Field.</td><td>If you have customized the default datasheet of Thickness Monitoring Rules Lookup family and want to see the T-Min Formula Policy data, you must do the following:
Using the Family Management, edit the default datasheet of Thickness Monitoring Rules Lookup family. Add the T-Min Formula Policy field in the Datasheet.</td></tr>
<tr><td>7</td><td>Update the values in the newly added Minimum Thickness Type field from the existing Minimum Thickness Type (Obsolete) field.</td><td>This will be automatically done by a Utility during an upgrade process. User does not need to do anything.
Below is the mapping from the existing data to the new data:<table><tr><th>Minimum Thickness Type (Obsolete)</th><th>Minimum Thickness Type</th></tr><tr><td>Calculated</td><td>CALCULATED</td></tr><tr><td>Nominal</td><td>NOMINAL</td></tr><tr><td>User Defined</td><td>USER DEFINED</td></tr><tr><td>Default</td><td>DEFAULT</td></tr></table>Note: Any other values other than NULL will be mapped to USER DEFINED.</td></tr>
</table>

Revert the Thickness Monitoring Queries to Baseline

This action is required only if you have modified the Thickness Monitoring queries.

About This Task

If you have modified the following Thickness Monitoring queries, perform the following steps to revert the queries to baseline:

- Assets Near or Past Retirement
- Assets with TM Tasks
- Corrosion Distribution
- Excessive Corrosion
- Remaining Life Less than 180 Months
- Thickness Inspections
- TM Assets
- TM Assets Requiring a Calculation

Procedure

1. Access the Catalog page.
2. Navigate to the Public folder for the query that you want to revert.
   For Thickness Monitoring, the public queries are stored in the following folder:

`Public/Meridium/Modules/Thickness Monitoring/Queries`

3. Select the check box next to the query that you want to revert, and then select  .
   The **Confirm Delete** window appears, asking you to confirm if you want to delete the selected query.
4. Select **OK**.
   The selected query is deleted.
5. Navigate to the Baseline folder for queries.
   For Thickness Monitoring, the baseline queries are stored in the following folder:
   `Baseline/Meridium/Modules/Thickness Monitoring/Queries`
6. Select the check box next to the query that you want to revert, and then select  .
   The **Catalog Folder Browser** window appears.
7. Navigate to the folder containing the public query that you deleted in step 3.
8. Select **OK**.
   A success message appears indicating that the selected item has been copied successfully.
9. Repeat Steps 2-8 for each query that you want to revert to baseline.

Use Custom TML Analysis Types

The baseline APM database includes the Thickness Measurement Location family, which contains the TML Analysis Type field. This field is used to classify TMLs based upon the collection method that will be used for recording Thickness Measurements at that location.

The TML Analysis Type field contains a list of values that is populated with the Corrosion Inspection Type values from all Corrosion Analysis Settings records that are associated with the asset or TML Group to which the Thickness Measurement Location record is linked.

The values that are used to populate the Corrosion Inspection Type field in the Corrosion Analysis Settings family are stored in the System Code Table CITP (Corrosion Inspection Type). In the baseline APM database, this table contains three System Codes: UT, RT, and TML. You can only create Thickness Measurement Location records with a given TML Analysis Type value if an associated Corrosion Analysis Settings record contains the same value in the Corrosion Inspection Type field.

Using the baseline functionality, you can separate Corrosion Analysis calculations into groups based upon TML Analysis Type. If you want to use this functionality, you will want to classify your TMLs as UT (measurements collected using ultrasonic thickness) or RT (measurements collected using radiographic thickness). This separation will be desirable for some implementations. Other implementations will prefer not to separate TMLs according to collection method and instead perform calculations on the entire group of TMLs that exists for an asset. For these implementations, you will want to classify all TMLs using the TML Analysis Type TML.

Depending upon your preferred implementation, you may choose to make one or more of the following changes to the System Code Table CITP (Corrosion Inspection Type):

- Add System Codes if you want to classify TMLs using methods in addition to UT and RT.
- Delete System Codes that you do not want to use.
- Modify the IDs and descriptions of the System Codes so that the classification options are more intuitive to your users.

If you make changes to this System Code Table, keep in mind that the analysis types that are stored in the System Code Table CITP (Corrosion Inspection Type) will be used when you

create Corrosion Analysis Settings records, and therefore, will determine the analysis types for which you can create Thickness Measurement Location records.

Additionally, in Thickness Measurement Location records, the TML Analysis Type field has a baseline Default Value rule that is coded to present UT as the default value when you have defined the UT TML Analysis Type in your Corrosion Analysis (i.e., you have created a Corrosion Analysis Settings record with a Corrosion Inspection Type of UT). You could modify this rule if, for example, you wanted RT to be presented as the default value when you have defined the RT TML Analysis Type in your Corrosion Analysis (i.e., you have created a Corrosion Analysis Settings record with a Corrosion Inspection Type of RT). To do this, you would modify the MI_TML_TYPE_CHR class as follows:

```
            <MetadataField("MI_TML_TYPE_CHR")>  _
            Public Class MI_TML_TYPE_CHR
                Inherits
Baseline.MI_Thickness_Measurement_Location.MI_TML_TYPE_CHR
                Public Sub New(ByVal record As
Meridium.Core.DataManager.DataRecord, ByVal field As
Meridium.Core.DataManager.DataField)
                    MyBase.New(record, field)
                End Sub
                Public Overrides Function GetDefaultInitialValue() As
Object
                    Return CStr("RT")
                End Function
            End Class
```

Note: For more information on customizing baseline rules, refer to the Rules section of the documentation.

Install the Meridium Device Service

About This Task

Important: You must repeat this procedure on every machine to which a datalogger will be connected.

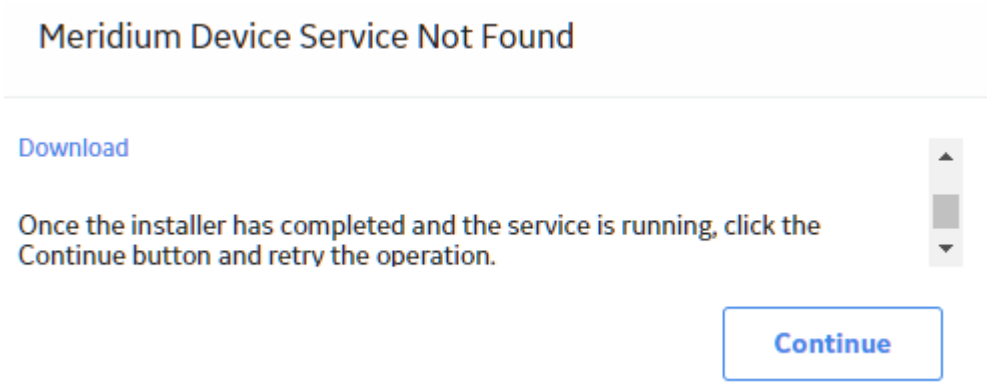
Note: If you are using Predix APM or the URL is secured (https), follow the instructions in KBA 000055071 to install the Meridium Device Service.

Procedure

1. Access the **TM Dataloggers** page.
2. In the **Select TMLs** pane, select the check box next to a TML, and then select **Apply**.
3. Select **Send To Device**.

   Note: A datalogger does not need to be connected.

   The **Meridium Device Service Not Found** window appears.



4. Select the **Download** link.
   MeridiumDevices.exe is downloaded.
5. Run **MeridiumDevices.exe**, and then follow the instructions in the installer.
   The Meridium Device Service is installed.
6. In the **Meridium Device Service Not Found** window, select **Continue**.
   Dataloggers can now be used with Thickness Monitoring.

Configure the Meridium Device Service

Procedure

1. In Windows Explorer, navigate to **C:\Program Files\Meridium\Services**.
2. Using a text editor, open the **Meridium.Service.Devices.exe.config** file.
3. In the text editor, navigate to the **appSettings** section (lines 24 to 28).
   - On line 25, edit the port number used by the service.

     Note: The datalogger settings in Thickness Monitoring must be modified so that the port number matches the one defined in this step.
   - On line 26, edit the timeout value in milliseconds. By default, the value for this setting is 60000, or 1 minute.
   - On line 27, if your organization utilizes a different URL protocol for APM, edit the protocol the service should use. For example, http://* can be changed to https://*.
4. Save the file, and then close the text editor.
5. Restart the Meridium Device Service.

   The Meridium Device Service configuration settings are updated.

Thickness Measurement Location – Update Datasheet

The default datasheet of Thickness Measurement Location family has been updated to include the newly added Minimum Thickness Type field:

Family	Family ID	Datasheet Updated (Default)
Thickness Measurement Location	MI Thickness Measurement Location	Thickness Measurement Location

If you have customized the default datasheet of Thickness Measurement Location family and want to see the Minimum Thickness Type data, you must do the following:

- Using the Family Management, modify the default datasheet of the MI Thickness Measurement Location family. Remove the existing Minimum Thickness Type (Obsolete) field and add the Minimum Thickness Type field in the Datasheet.

Thickness Monitoring Rules Lookup – Update Datasheet

The default datasheet of Thickness Monitoring Rules Lookup family has been updated to include the newly added T-Min Formula Policy field:

Family	Family ID	Datasheet Updated (Default)
Thickness Monitoring Rules Lookup	Thickness Monitoring Rules Lookup	MI_TMIN_CRL

If you have customized the default datasheet of Thickness Monitoring Rules Lookup family and want to see the T-Min Formula Policy data, you must do the following:

- Using Family Management, modify the default datasheet Thickness Monitoring Rules Lookup family. Add the T-Min Formula Policy field in the Datasheet.

TM Functional Security Privileges

APM provides the following baseline Security Groups for use with Thickness Monitoring and provides baseline family-level privileges for these groups:

- MI Thickness Monitoring Administrator
- MI Thickness Monitoring Inspector
- MI Thickness Monitoring User

Access to certain functions in APM is determined by membership in these Security Groups. Note that in addition to the baseline family-level privileges that exist for these Security Groups, users will also need at least View privileges for all customer-defined predecessor or successor families that participate in the Thickness Monitoring relationships. Keep in mind that:

- Users who will need to create new records in TM will need Insert privileges to these families.
- Users who will need to modify records will need Update privileges to these families.
- Any user who should be allowed to delete TM records will need Delete privileges to these families.

The following table summarizes the functional privileges associated with each group.

Function	Can be done by members of the MI Thickness Monitoring Administrator Group?	Can be done by members of the MI Thickness Monitoring Inspector Group?	Can be done by members of the MI Thickness Monitoring User Group?
Configure Global Preferences	Yes	No	No
Configure Family Preferences	Yes	No	No
Use the T-Min Calculator	No	Yes	No

Function	Can be done by members of the MI Thickness Monitoring Administrator Group?	Can be done by members of the MI Thickness Monitoring Inspector Group?	Can be done by members of the MI Thickness Monitoring User Group?
Archive Corrosion Rates	No	Yes	No
Reset the Maximum Historical Corrosion Rate	Yes	No	No
Exclude TMLs	No	Yes	No
Renew TMLs	No	Yes	No
Reset User Preferences	Yes	No	No

APM provides the following baseline Security Groups for use with Thickness Monitoring and provides baseline family-level privileges for these groups:

- MI Thickness Monitoring Administrator
- MI Thickness Monitoring Inspector
- MI Thickness Monitoring User

Access to certain functions in APM is determined by membership in these Security Groups. Note that in addition to the baseline family-level privileges that exist for these Security Groups, users will also need at least View privileges for all customer-defined predecessor or successor families that participate in the Thickness Monitoring relationships. Keep in mind that:

- Users who will need to create new records in TM will need Insert privileges to these families.
- Users who will need to modify records will need Update privileges to these families.
- Any user who should be allowed to delete TM records will need Delete privileges to these families.

The following table summarizes the functional privileges associated with each group.

Function	Can be done by members of the MI Thickness Monitoring Administrator Group?	Can be done by members of the MI Thickness Monitoring Inspector Group?	Can be done by members of the MI Thickness Monitoring User Group?
Configure Global Preferences	Yes	No	No
Configure Family Preferences	Yes	No	No
Use the T-Min Calculator	No	Yes	No
Archive Corrosion Rates	No	Yes	No
Reset the Maximum Historical Corrosion Rate	Yes	No	No
Exclude TMLs	No	Yes	No
Renew TMLs	No	Yes	No
Reset User Preferences	Yes	No	No

TM Security Groups

The following table lists the baseline Security Groups available for users within this module, as well as the baseline Roles to which those Security Groups are assigned.

Important: Assigning a Security User to a Role grants that user the privileges associated with all of the Security Groups that are assigned to that Role. To avoid granting a Security User unintended privileges, before assigning a Security User to a Role, be sure to review all of the privileges associated with the Security Groups assigned to that Role. Also, be aware that additional Roles, as well as Security Groups assigned to existing Roles, can be added via Security Manager.

Security Group	Roles
MI Thickness Monitoring Administrator	MI Mechanical Integrity Administrator
MI Thickness Monitoring Inspector	MI Mechanical Integrity Administrator MI Mechanical Integrity Power MI Mechanical Integrity User
MI Thickness Monitoring User	MI Mechanical Integrity Administrator MI Mechanical Integrity Power MI Mechanical Integrity User
MI Thickness Monitoring Viewer	MI APM Viewer MI Mechanical Integrity Viewer

The baseline family-level privileges that exist for these Security Groups are summarized in the following table.

Family	MI Thickness Monitoring Administrator	MI Thickness Monitoring Inspector	MI Thickness Monitoring User	MI Thickness Monitoring Viewer
Entity Families				
Corrosion	View, Update, Insert	View, Update, Insert	View, Update, Insert	View
Datapoint	View, Update, Insert	View, Update, Insert	View, Update, Insert	View
Datapoint Measurement	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert	View
Equipment	View	View	View	View
Human Resource	View, Update, Insert, Delete	View	View	View
Inspection Task	View	View, Update	View	View
Inventory Group Configuration	View	View	View	View

Family	MI Thickness Monitoring Administrator	MI Thickness Monitoring Inspector	MI Thickness Monitoring User	MI Thickness Monitoring Viewer
Materials of Construction	View	View	View	View
Meridium Reference Tables	View, Update, Insert, Delete	View	View	View
RBI Inspection Auto-Selection Criteria	View	View	View	View
Resource Role	View, Update, Insert, Delete	View	View	View
Security Group	View	View	View	View
Security User	View	View	View	View
Settings	View, Update, Insert	View, Update, Insert	View	View
Task Execution	View, Insert	View, Insert	View	View
Thickness Monitoring Task	View, Update, Insert, Delete	View, Update, Insert	View, Update, Insert	View
TML Group	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View
Relationship Families				
Belongs to a Unit	View, Update, Insert, Delete	View, Update, Insert	View, Update, Insert	View
Equipment Has Equipment	View	View	View	View
Group Assignment	View	View	View	View
Has Archived Corrosion Analyses	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Archived Corrosion Analysis Settings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Archived Subcomponent Analysis Settings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Archived Subcomponent Corrosion Analyses	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Corrosion Analyses	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Corrosion Analysis Settings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI Thickness Monitoring Administrator	MI Thickness Monitoring Inspector	MI Thickness Monitoring User	MI Thickness Monitoring Viewer
Has Datapoints	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Inspections	None	None	None	View
Has Measurements	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Roles	View, Update, Insert, Delete	View	View	View
Has Task Execution	View, Insert	View, Insert	View	View
Has Task Revision	View, Insert	View, Insert	View	View
Has Tasks	View, Insert	View, Insert	View, Insert	View
Has TML Group	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View
Is a User	View	View	View	View
User Assignment	View	View	View	View

The following table lists the baseline Security Groups available for users within this module, as well as the baseline Roles to which those Security Groups are assigned.

Important: Assigning a Security User to a Role grants that user the privileges associated with all of the Security Groups that are assigned to that Role. To avoid granting a Security User unintended privileges, before assigning a Security User to a Role, be sure to review all of the privileges associated with the Security Groups assigned to that Role. Also, be aware that additional Roles, as well as Security Groups assigned to existing Roles, can be added via Security Manager.

Security Group	Roles
MI Thickness Monitoring Administrator	MI Mechanical Integrity Administrator
MI Thickness Monitoring Inspector	MI Mechanical Integrity Administrator MI Mechanical Integrity Power MI Mechanical Integrity User
MI Thickness Monitoring User	MI Mechanical Integrity Administrator MI Mechanical Integrity Power MI Mechanical Integrity User
MI Thickness Monitoring Viewer	MI APM Viewer MI Mechanical Integrity Viewer

The baseline family-level privileges that exist for these Security Groups are summarized in the following table.

Family	MI Thickness Monitoring Administrator	MI Thickness Monitoring Inspector	MI Thickness Monitoring User	MI Thickness Monitoring Viewer
Entity Families				
Corrosion	View, Update, Insert	View, Update, Insert	View, Update, Insert	View
Datapoint	View, Update, Insert	View, Update, Insert	View, Update, Insert	View
Datapoint Measurement	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert	View
Equipment	View	View	View	View
Human Resource	View, Update, Insert, Delete	View	View	View
Inspection Task	View	View, Update	View	View
Inventory Group Configuration	View	View	View	View
Materials of Construction	View	View	View	View
Meridium Reference Tables	View, Update, Insert, Delete	View	View	View
RBI Inspection Auto-Selection Criteria	View	View	View	View
Resource Role	View, Update, Insert, Delete	View	View	View
Security Group	View	View	View	View
Security User	View	View	View	View
Settings	View, Update, Insert	View, Update, Insert	View	View
Task Execution	View, Insert	View, Insert	View	View
Thickness Monitoring Task	View, Update, Insert, Delete	View, Update, Insert	View, Update, Insert	View
TML Group	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View
Relationship Families				
Belongs to a Unit	View, Update, Insert, Delete	View, Update, Insert	View, Update, Insert	View
Equipment Has Equipment	View	View	View	View
Group Assignment	View	View	View	View
Has Archived Corrosion Analyses	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI Thickness Monitoring Administrator	MI Thickness Monitoring Inspector	MI Thickness Monitoring User	MI Thickness Monitoring Viewer
Has Archived Corrosion Analysis Settings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Archived Subcomponent Analysis Settings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Archived Subcomponent Corrosion Analyses	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Corrosion Analyses	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Corrosion Analysis Settings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Datapoints	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Inspections	None	None	None	View
Has Measurements	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Roles	View, Update, Insert, Delete	View	View	View
Has Task Execution	View, Insert	View, Insert	View	View
Has Task Revision	View, Insert	View, Insert	View	View
Has Tasks	View, Insert	View, Insert	View, Insert	View
Has TML Group	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View
Is a User	View	View	View	View
User Assignment	View	View	View	View

Translation

Deploy Translations

You must deploy translations if you want to use non-English translations in APM.

Before You Begin

Deploying translations is part of both the APM first time deployment workflow and the APM upgrade workflow. Ensure that you have completed the preceding steps in the appropriate workflow before attempting to deploy translations.

Procedure

1. If you have not already done so, activate the licenses for the translations you have purchased.
2. On the APM server, run the file `Meridium.Version.EnableTranslations.exe`, which is located on that machine in the folder `C:\Program Files\Meridium\Upgrade \TranslationUnzip`.

   Note: To run this file, open a command prompt window, and then enter and execute the following:

   C:\Program Files\Meridium\Upgrade\TranslationUnzip\ Meridium.Version.EnableTranslations.exe `-l:`*<path to license>* `-p:`*<PIN>* `-e:`*<True or False>*

   ...where *<Path to license>* is a valid path to the license file and *<PIN>* is the pin for the license file. The parameter `-e` is optional. *<True or False>* indicates whether the help files should be extracted. Specify True if you want to extract the help files and False if you do not want to extract the help files. If you do not use this parameter, the help files are not extracted.
3. On the APM server, reset IIS.
4. You can now manage translations.

Next Steps

- Configure one of the virtual machine to execute all the scheduled jobs.