meridium

Meridium Enterprise APM Modules and Features

4.2.0.7.0

Meridium Enterprise APM Modules and Features

4.2.0.7.0

About This Document

This file is provided so that you can easily print this section of the Meridium Enterprise APM Help system.

You should, however, use the Help system instead of a printed document. This is because the Help system provides hyperlinks that will assist you in easily locating the related instructions that you need. Such links are not available in a print document format.

The Meridium Enterprise APM Help system can be accessed within Meridium Enterprise APM itself or via the Meridium Enterprise APM Documentation Website (https://www.me-ridium.com/documentation/WebHelp/WebHelpMaster.htm).

> Note: If you do not have access to the Meridium Enterprise APM Documentation Website, contact [Meridium Global Support Services](#).

Table of Contents

Deploy Modules and Features

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

Deploy AMS Analytics

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 AMS Analytics 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 Meridium Enterprise 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.

Step	Task	Notes
1	Assign Security Users to one or more of the AMS Analytics Security Groups.	This step is required.
2	Deploy Reports.	This step is required only if you want to view reports of AMS data.
3	On the Meridium Enterprise APM Server, run the Meridium APM Server and Add-ons installer, selecting the **Meridium Integration Services** check box on the **Select the features you want to install** screen .	This step is required.
4	Create one AMS Asset Data Source record per AMS Analytics data source whose data you want to transfer into Meridium Enterprise APM.	This step is required.
5	Test the connection to each AMS Analytics data source.	This step is required.
6	Link each AMS Asset record to the Equipment or Functional record that represents the piece of equipment or location for which the AMS Asset record exists.	This step is required. You can link AMS Tag records to Equipment or Functional Location records using one of the following: • Record Manager • System and Tags • Tags Data Loader
7	If you are using Asset Criticality Analysis, define the criticality field in the AMS Asset records for the equipment or location linked to each AMS Asset record.	This step is required.

8	For Oracle users only, configure AMS Analytics to use Oracle-specific queries.	This step is required only if you are using an Oracle Meridium Enterprise APM database. If you are using a SQL Server database, the baseline queries will work without any manual configuration.
9	For Oracle users only, in Meridium Enterprise APM, modify the AMS Analytics Overview page.	This step is required only if you are using an Oracle Meridium Enterprise APM database. If you are using a SQL Server database, the overview page will work without any manual configuration.

Upgrade or Update AMS Analytics to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0
This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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	Modify the application-wide Asset Hierarchy configuration to include the Asset Folder and AMS Asset families.	This step is required only if you are not using Equipment and Functional Location records and want to view AMS Asset Folders and AMS Assets in a hierarchy.
2	Configure the message queue section in the **Web Service Details** section of the **AMS Data Source Configuration UI** page.	This step is required only if you are using message queues to receive data from an AMS server.
3	Run the following update query: UPDATE [MI_APTAG] SET [MI_APTAG].[MI_TAG_SYSTEM_ID_C] = [MI_APTAG].[MI_TAG_PATH_C].	This step is required only if you want to use the AMS Asset Tag Data Loader to create relationships between tags and assets.

Step	Task	Notes
4	After you upgrade your database, use the **State Management** option in the Revert to Baseline feature to apply the new baseline State Configuration for the AMS Recommendation family.	This step is required only if you were using State Configuration for the AMS Recommendation family in a version prior to V4.2.0.0. As of V4.2.0.0, the State Configuration for the AMS Asset Recommendation family is enabled and configured to use the parent's (Performance Recommendation family's) State Configuration settings. The baseline state configuration must be applied in order for various queries and lists in Meridium Enterprise APM to function as expected.

Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	Modify the application-wide Asset Hierarchy configuration to include the Asset Folder and AMS Asset families.	This step is required only if you are not using Equipment and Functional Location records and want to view AMS Asset Folders and AMS Assets in a hierarchy.
2	Configure the message queue section in the **Web Service Details** section of the **AMS Data Source Configuration UI** page.	This step is required only if you are using message queues to receive data from an AMS server.
3	Run the following update query: UPDATE [MI_APTAG] SET [MI_APTAG].[MI_TAG_SYSTEM_ID_C] = [MI_APTAG].[MI_TAG_PATH_C].	This step is required only if you want to use the AMS Asset Tag Data Loader to create relationships between tags and assets.

Step	Task	Notes
4	After you upgrade your database, use the **State Management** option in the Revert to Baseline feature to apply the new baseline State Configuration for the AMS Recommendation family.	This step is required only if you were using State Configuration for the AMS Recommendation family in a version prior to V4.2.0.0. As of V4.2.0.0, the State Configuration for the AMS Asset Recommendation family is enabled and configured to use the parent's (Performance Recommendation family's) State Configuration settings. The baseline state configuration must be applied in order for various queries and lists in Meridium Enterprise APM to function as expected.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

Step	Task	Notes
1	Modify the application-wide Asset Hierarchy configuration to include the Asset Folder and AMS Asset families.	This step is required only if you are not using Equipment and Functional Location records and want to view AMS Asset Folders and AMS Assets in a hierarchy.
2	Configure the message queue section in the **Web Service Details** section of the **AMS Data Source Configuration UI** page.	This step is required only if you are using message queues to receive data from an AMS server.
3	Run the following update query: UPDATE [MI_APTAG] SET [MI_APTAG].[MI_TAG_SYSTEM_ID_C] = [MI_APTAG].[MI_TAG_PATH_C].	This step is required only if you want to use the AMS Asset Tag Data Loader to create relationships between tags and assets.

Step	Task	Notes
4	After you upgrade your database, use the **State Management** option in the Revert to Baseline feature to apply the new baseline State Configuration for the AMS Recommendation family.	This step is required only if you were using State Configuration for the AMS Recommendation family in a version prior to V4.2.0.0. As of V4.2.0.0, the State Configuration for the AMS Asset Recommendation family is enabled and configured to use the parent's (Performance Recommendation family's) State Configuration settings. The baseline state configuration must be applied in order for various queries and lists in Meridium Enterprise APM to function as expected.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

Step	Task	Notes
1	Modify the application-wide Asset Hierarchy configuration to include the Asset Folder and AMS Asset families.	This step is required only if you are not using Equipment and Functional Location records and want to view AMS Asset Folders and AMS Assets in a hierarchy.
2	Configure the message queue section in the **Web Service Details** section of the **AMS Data Source Configuration UI** page.	This step is required only if you are using message queues to receive data from an AMS server.
3	Run the following update query: UPDATE [MI_APTAG] SET [MI_APTAG].[MI_TAG_SYSTEM_ID_C] = [MI_APTAG].[MI_TAG_PATH_C].	This step is required only if you want to use the AMS Asset Tag Data Loader to create relationships between tags and assets.

Step	Task	Notes
4	After you upgrade your database, use the **State Management** option in the Revert to Baseline feature to apply the new baseline State Configuration for the AMS Recommendation family.	This step is required only if you were using State Configuration for the AMS Recommendation family in a version prior to V4.2.0.0. As of V4.2.0.0, the State Configuration for the AMS Asset Recommendation family is enabled and configured to use the parent's (Performance Recommendation family's) State Configuration settings. The baseline state configuration must be applied in order for various queries and lists in Meridium Enterprise APM to function as expected.

Upgrade from any version V3.5.1 through V3.5.1.12.0

Step	Task	Notes
1	Modify the application-wide Asset Hierarchy configuration to include the Asset Folder and AMS Asset families.	This step is required only if you are not using Equipment and Functional Location records and want to view AMS Asset Folders and AMS Assets in a hierarchy.
2	Configure the message queue section in the **Web Service Details** section of the **AMS Data Source Configuration UI** page.	This step is required only if you are using message queues to receive data from an AMS server.
3	Run the following update query: UPDATE [MI_APTAG] SET [MI_APTAG].[MI_TAG_SYSTEM_ID_C] = [MI_APTAG].[MI_TAG_PATH_C].	This step is required only if you want to use the AMS Asset Tag Data Loader to create relationships between tags and assets.

Step	Task	Notes
4	After you upgrade your database, use the **State Management** option in the Revert to Baseline feature to apply the new baseline State Configuration for the AMS Recommendation family.	This step is required only if you were using State Configuration for the AMS Recommendation family in a version prior to V4.2.0.0. As of V4.2.0.0, the State Configuration for the AMS Asset Recommendation family is enabled and configured to use the parent's (Performance Recommendation family's) State Configuration settings. The baseline state configuration must be applied in order for various queries and lists in Meridium Enterprise APM to function as expected.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

Step	Task	Notes
1	Modify the application-wide Asset Hierarchy configuration to include the Asset Folder and AMS Asset families.	This step is required only if you are not using Equipment and Functional Location records and want to view AMS Asset Folders and AMS Assets in a hierarchy.
2	Configure the message queue section in the **Web Service Details** section of the **AMS Data Source Configuration UI** page.	This step is required only if you are using message queues to receive data from an AMS server.
3	Run the following update query: UPDATE [MI_APTAG] SET [MI_APTAG].[MI_TAG_SYSTEM_ID_C] = [MI_APTAG].[MI_TAG_PATH_C].	This step is required only if you want to use the AMS Asset Tag Data Loader to create relationships between tags and assets.

Step	Task	Notes
4	After you upgrade your database, use the **State Management** option in the Revert to Baseline feature to apply the new baseline State Configuration for the AMS Recommendation family.	This step is required only if you were using State Configuration for the AMS Recommendation family in a version prior to V4.2.0.0. As of V4.2.0.0, the State Configuration for the AMS Asset Recommendation family is enabled and configured to use the parent's (Performance Recommendation family's) State Configuration settings. The baseline state configuration must be applied in order for various queries and lists in Meridium Enterprise APM to function as expected.

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Modify the application-wide Asset Hierarchy configuration to include the Asset Folder and AMS Asset families.	This step is required only if you are not using Equipment and Functional Location records and want to view AMS Asset Folders and AMS Assets in a hierarchy.
2	Configure the message queue section in the **Web Service Details** section of the **AMS Data Source Configuration UI** page.	This step is required only if you are using message queues to receive data from an AMS server.
3	Run the following update query: UPDATE [MI_APTAG] SET [MI_APTAG].[MI_TAG_SYSTEM_ID_C] = [MI_APTAG].[MI_TAG_PATH_C].	This step is required only if you want to use the AMS Asset Tag Data Loader to create relationships between tags and assets.

Step	Task	Notes
4	After you upgrade your database, use the **State Management** option in the Revert to Baseline feature to apply the new baseline State Configuration for the AMS Recommendation family.	This step is required only if you were using State Configuration for the AMS Recommendation family in a version prior to V4.2.0.0. As of V4.2.0.0, the State Configuration for the AMS Asset Recommendation family is enabled and configured to use the parent's (Performance Recommendation family's) State Configuration settings. The baseline state configuration must be applied in order for various queries and lists in Meridium Enterprise APM to function as expected.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Modify the application-wide Asset Hierarchy configuration to include the Asset Folder and AMS Asset families.	This step is required only if you are not using Equipment and Functional Location records and want to view AMS Asset Folders and AMS Assets in a hierarchy.
2	Configure the message queue section in the **Web Service Details** section of the **AMS Data Source Configuration UI** page.	This step is required only if you are using message queues to receive data from an AMS server.
3	Run the following update query: UPDATE [MI_APTAG] SET [MI_APTAG].[MI_TAG_SYSTEM_ID_C] = [MI_APTAG].[MI_TAG_PATH_C].	This step is required only if you want to use the AMS Asset Tag Data Loader to create relationships between tags and assets.

Step	Task	Notes
4	After you upgrade your database, use the **State Management** option in the Revert to Baseline feature to apply the new baseline State Configuration for the AMS Recommendation family.	This step is required only if you were using State Configuration for the AMS Recommendation family in a version prior to V4.2.0.0. As of V4.2.0.0, the State Configuration for the AMS Asset Recommendation family is enabled and configured to use the parent's (Performance Recommendation family's) State Configuration settings. The baseline state configuration must be applied in order for various queries and lists in Meridium Enterprise APM to function as expected.

Configure Oracle Specific Queries

If you are using a SQL Server database, the product is configured by default to use the SQL Server versions of these queries, so no manual steps are required.

The Event Trend Daily and Event Trend Monthly summary reports are built using multiple queries, where some of those queries contain syntax that is database-specific and can be interpreted only on Oracle or SQL Server databases. If, however, you are using an Oracle database, you will need to configure the product manually to use the Oracle versions of these queries.

Specifically, the following queries are delivered with a SQL Server and Oracle version, where the Oracle version contains the text _Oracle in the name.

SQL Server Version	Oracle Version
Event Trend Daily	Event Trend Daily_Oracle
Event Trend Monthly	Event Trend Monthly_Oracle
Past 10 Days List	Past 10 Days List_Oracle
Past 12 Months List	Past 12 Months List_Oracle

Steps

1. Rename the SQL Server versions of the queries. For example, you might want to rename the Event Trend Daily query Event Trend Daily_SQL.

2. In the Oracle versions of the queries, remove the text _Oracle from the name.

   Queries are configured for Oracle users.

Modify the AMS Analytics Overview Page for Oracle

Steps

1. In Meridium Enterprise APM, access the **Dashboard** page.

2. Open the AMS Analytics Overview Widget Dashboard stored in the Catalog folder **\\Public\Meridium\Modules\AMS Asset Portal\Dashboard**.

   > ⓘ **Note**: By default, this dashboard contains a widget configured for SQL databases. Therefore, an error message may appear when you open the dashboard.

3. Using the options to hide and display widgets:

   a. Hide the **AMS Active Alerts by Duration** widget.

   b. Display the **AMS Active Alerts by Duration (Oracle)** widget.

4. Arrange the widgets at each screen size as necessary.

About Defining the Criticality Value in AMS Asset Records

The value in the Criticality field in AMS Asset records indicates the importance of the health of the piece of equipment or location that is associated with the AMS Asset record. This field is unique to Meridium Enterprise APM. A corresponding field does not exist in any AMS Analytics data source. Therefore, when data is transferred from an AMS Analytics data source to Meridium Enterprise APM and AMS Asset records are created, this field will be empty.

The Criticality field in AMS Asset records is disabled and populated automatically based upon the risk assessment for the Equipment or Functional Location to which the AMS Asset records are linked. Because Asset Criticality Analysis (ACA) is the only feature that allows you to define a risk assessment for an Equipment or Functional Location record, the AMS Analytics implementation assumes that you are also using ACA and that this field is populated automatically.

In addition, the values in the Criticality field of AMS Asset records will be used in combination with values in the Health Index field to calculate the composite health index value for AMS Asset Folder records. After a value exists in the Criticality field of AMS Asset records, when data is collected from an AMS Analytics data source, the Health Index field in AMS Asset Folder records will be populated with a value.

About Creating AMS Asset Data Source Records

AMS Asset Data Source records store connection information that the Meridium Enterprise APM system uses to import data from the following locations:

- AMS Analytics data sources

When you create an AMS Asset Data Source record for an AMS Analytics data source, you will establish a connection between the Meridium Enterprise APM Web Service and the Web Service for the specified data source. In this way, the Meridium Enterprise APM system can import data from the data source into the Meridium Enterprise APM database. Once the data is imported into Meridium Enterprise APM, it can be displayed by adding the AMS Asset Folders and AMS Assets to the asset hierarchy, or linking AMS Assets to Equipment and Locations.

AMS Analytics 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 AMS Suite APM Administrator	MI Health Admin
MI AMS Suite APM Power User	MI Health Power
MI AMS Suite APM User	MI Health User
MI AMS Asset Portal Viewer	None

> 🛈 **Note**: The Security Groups listed in the table above account only for family permissions. Users must also be added to the MI Configuration Role Security Group in order to access the Systems and Tags page, which is required to modify families used by this module.

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

Family	MI AMS Suite APM Administrator	MI AMS Suite APM Power User	MI AMS Suite APM User	MI AMS Asset Portal Viewer
Entity Families				
AMS Asset Recommendation	View, Update, Insert, Delete	View, Update, Insert	View, Update, Insert	View
Equipment	View, Update, Insert, Delete	View, Update, Insert	View	View
Functional Location	View, Update, Insert, Delete	View, Update, Insert	View	View

Tag	View, Update, Insert, Delete	View, Update	View	View
Tag Alert	View, Update, Insert, Delete	View, Update	View	View
Tag Data Source	View, Update, Insert, Delete	View	View	View
Tag Event	View, Update, Insert, Delete	View, Update	View	View
Tag Folder	View, Update, Insert, Delete	View, Update, Insert	View	View
Relationship Families				
Equipment Has Equipment	View, Update, Insert, Delete	View, Update, Insert	View	View
Functional Location Has Equipment	View, Update, Insert, Delete	View, Update, Insert	View	View
Functional Location Has Functional Location	View, Update, Insert, Delete	View, Update, Insert	View	View
Has Consolidated Events	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Recommendations	View, Update, Insert, Delete	View, Update, Insert	View, Update, Insert	View
Has Tag	View, Update, Insert, Delete	View, Update, Insert	View	View
Has Tag Alert	View, Update, Insert, Delete	View, Update, Insert	View	View
Has Tag Data Source	View, Update, Insert, Delete	View, Update, Insert	View	View
Has Tag Event	View, Update, Insert, Delete	View, Update, Insert	View	View
Tag Folder Has Tag Folder	View, Update, Insert, Delete	View, Update, Insert	View	View

APM Connect

Meridium APM Connect is an integration framework designed to connect valuable data that exists in data stores, systems, and applications throughout the enterprise.

Access the full APM Connect Installation and Upgrade Help and associated links from the APM Connect help system.

Deploy APM System Monitoring

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 APM System Monitoring 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 Meridium Enterprise 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.

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 *each* Meridium Enterprise APM Server, modify the web.config file to point to the location of the APM System Monitoring controller.	This step is required.
6	In Meridium Enterprise APM, enable APM System Monitoring.	This step is required.

Upgrade or Update APM System Monitoring to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

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.

Steps

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
   ```

4. On the command prompt window, enter the following:

   > 📄 **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.

   ```
   "C:\Program Files\MongoDB\Server\3.2\bin\mongod.exe" --config "C:\data\-
   mongod.cfg" --install
   ```

   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.

What's Next?

- 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](#).

Steps

1. On the machine on which you want to install APM System Monitoring, access the Meridium APM Enterprise APM distribution package, and then navigate to the folder **Setup\Admin**.

2. Open the file **Setup.exe**.

   The Meridium Admin installer appears.
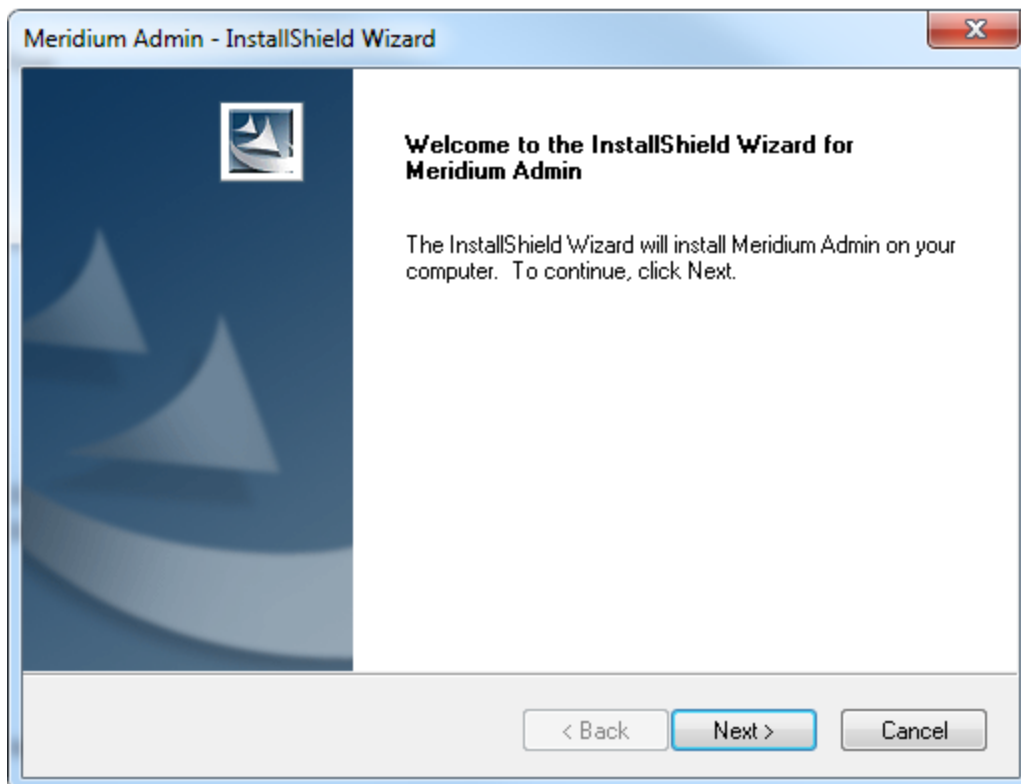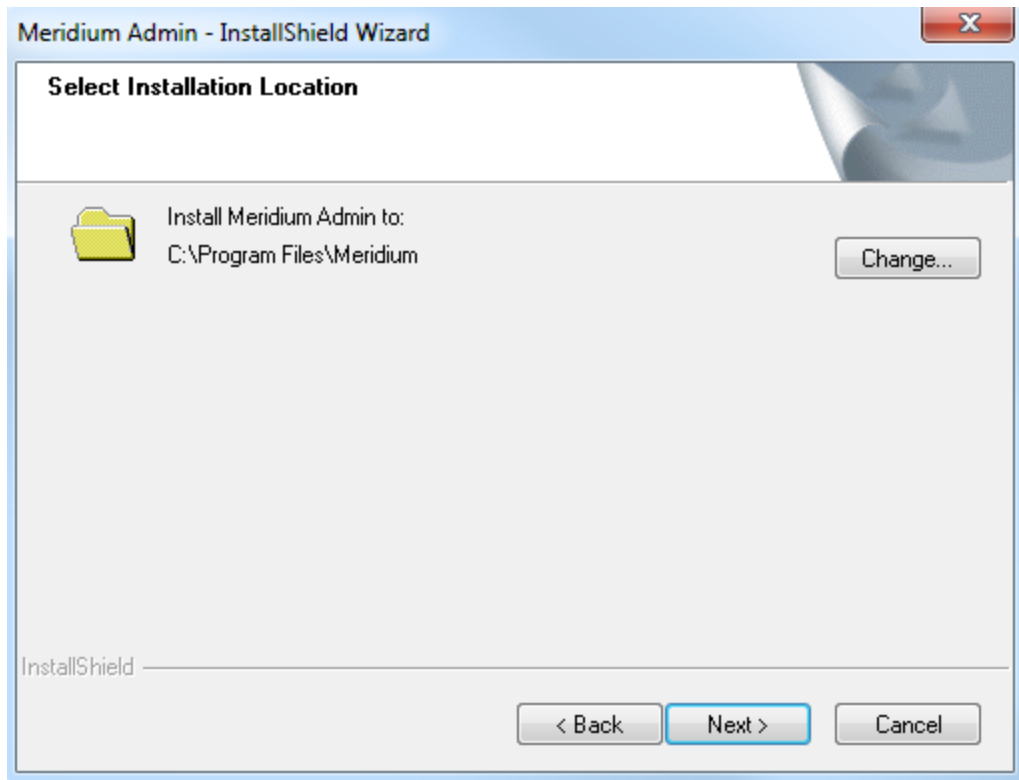
3. Select **Next**.
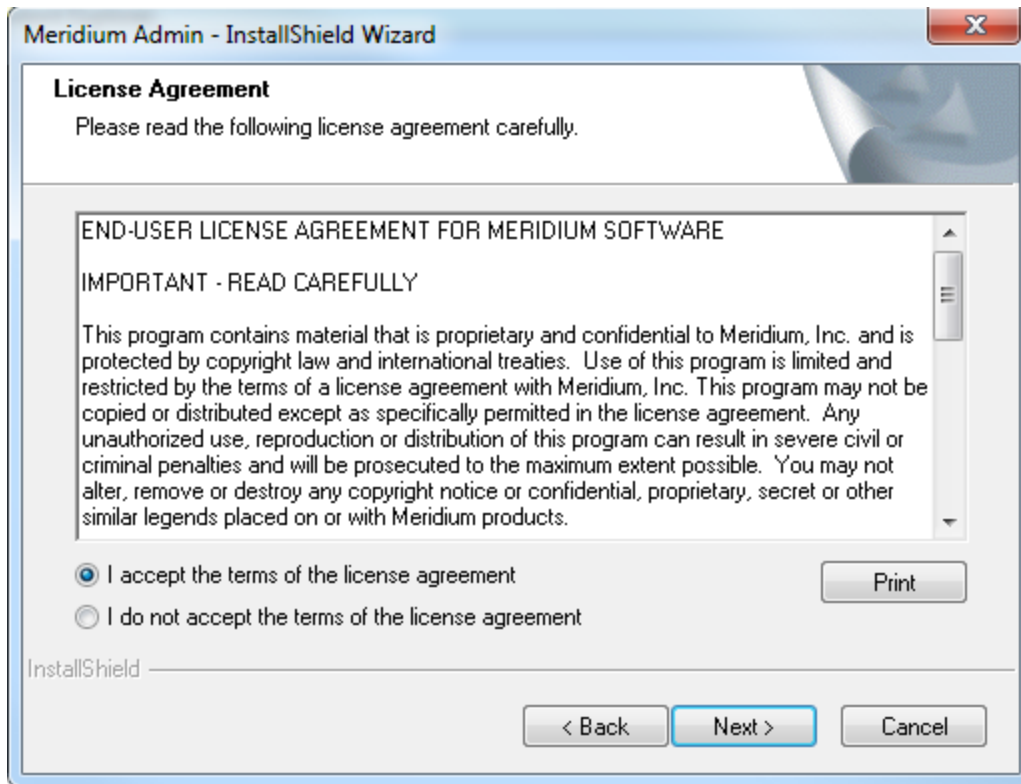
   The **License Agreement** screen appears.

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.
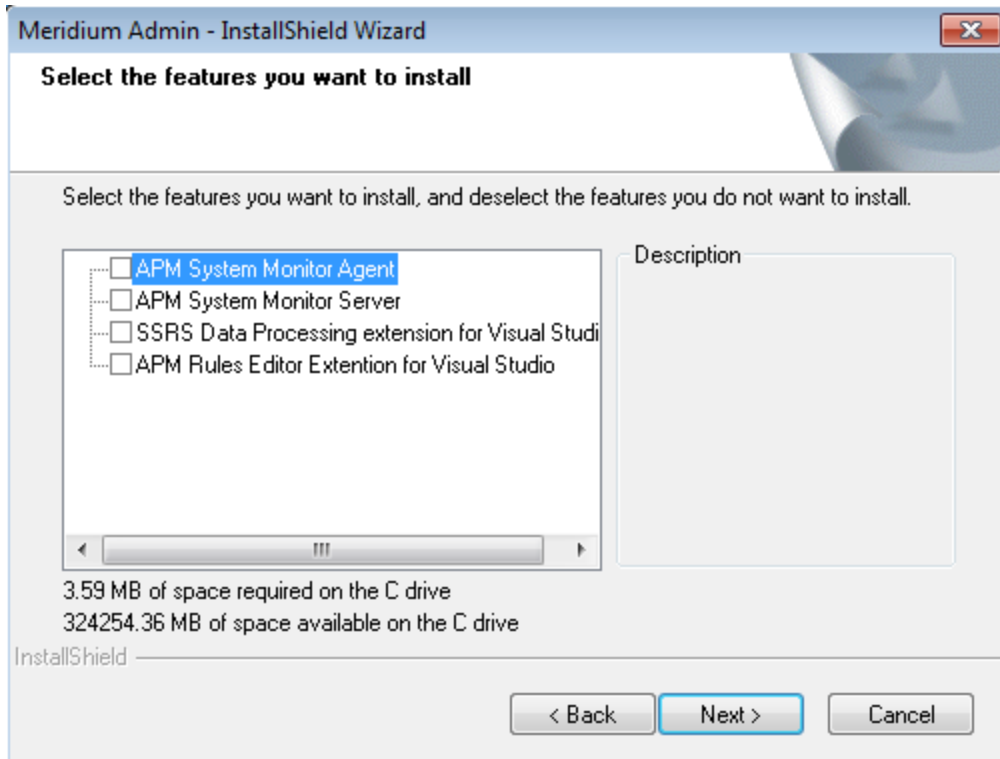
6. If this is the machine that will serve as the APM System Monitoring controller, then select the **APM System Monitor Server** check box.

> ⓘ **Note:** Only one machine will serve as the APM System Monitoring controller.

7. 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 both the APM System Monitoring controller and an APM System Monitoring agent. If you are deploying APM System Monitoring in this way, then select both the **APM System Monitor Server** check box and the **APM System Monitor Agent** check box.

8. Select **Next**.

The **Complete the Installation** screen appears.
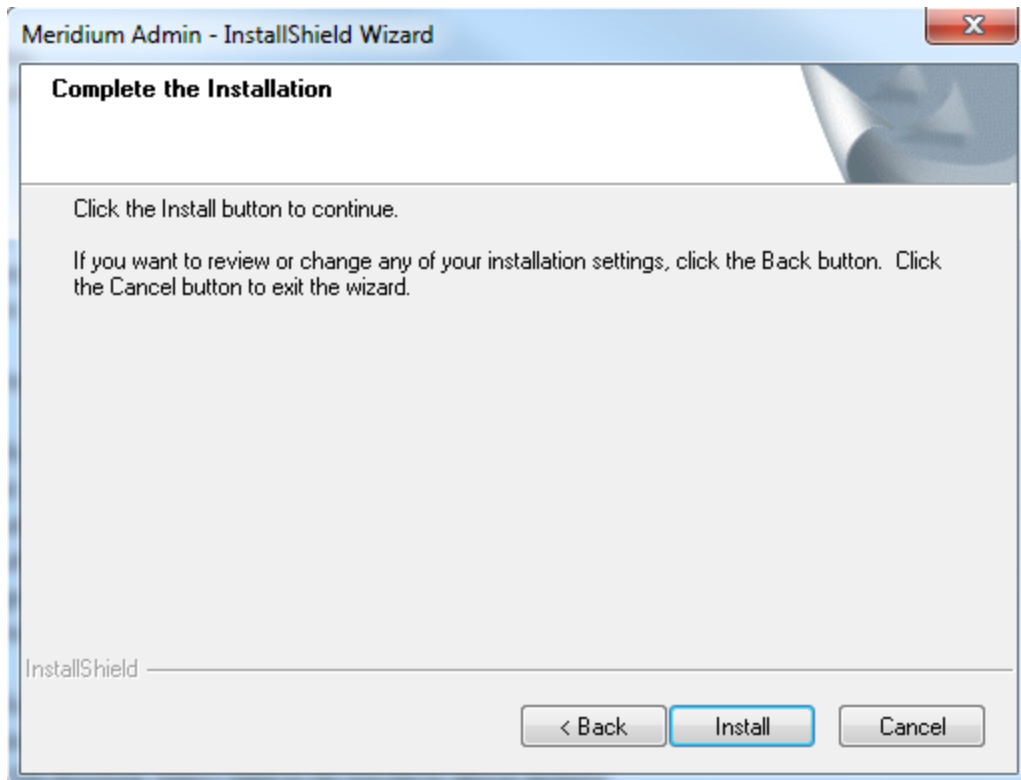
9. Select **Install**.

   The **Setup Status** screen appears, displaying a progress bar. When the installation is complete, the **Installation is Complete** screen appears.
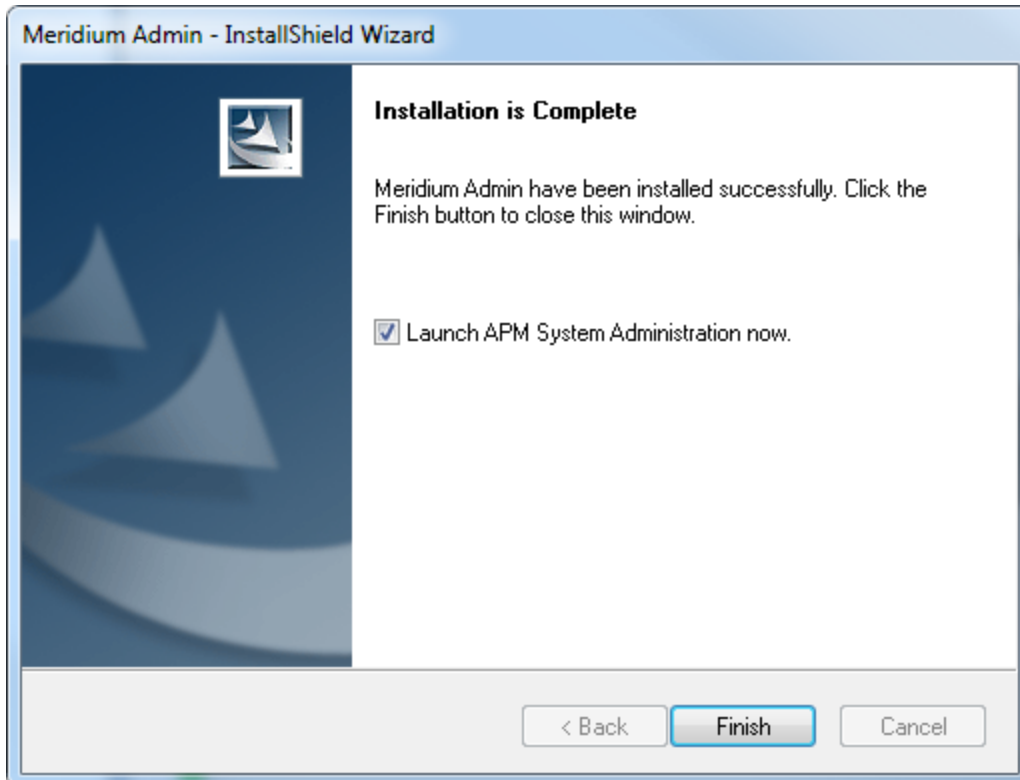
10. Clear the **Launch APM System Administration now** check box, and then select **Finish**.

   The Meridium Admin installer closes.

11. On the same machine, navigate to **C:\Program Files\Meridium\APMSystemMonitor**, and then open the file **Meridium.System.Monitor.ServiceManager.exe**.
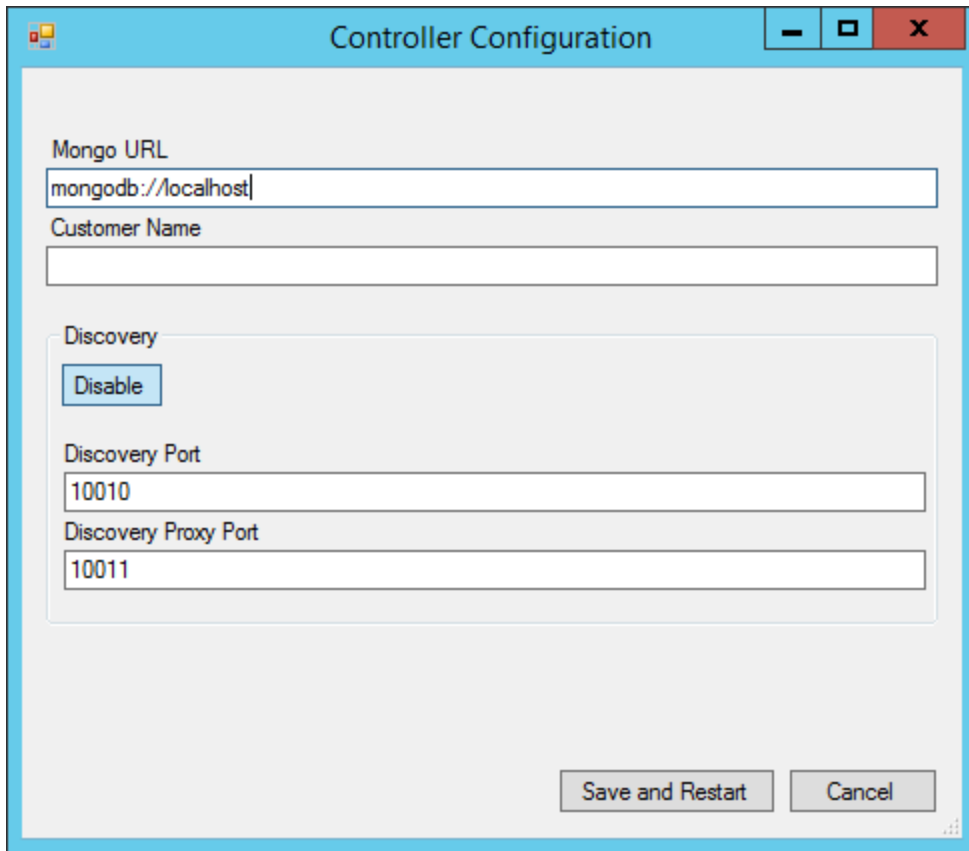
   The **Meridium System Monitor Service Manager** window appears.
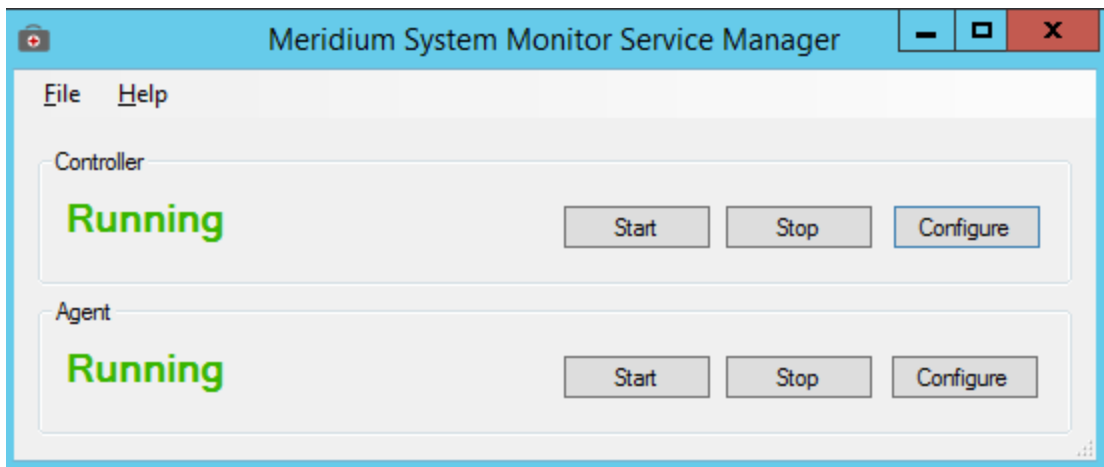
12. If this is the machine that will serve as the APM System Monitoring controller, then, in the

Controller section, select **Configure**. If this *is not* the machine that will serve as the APM System Monitoring controller, then proceed to step 13.

The **Controller Configuration** window appears.

a. In the **Customer Name** box, enter the unique key provided by Meridium, Inc, and then select **Save and Restart**.

> ⚠ **IMPORTANT:** If you do not have this unique key, then please contact the Meridium, Inc. Professional Services department.

The machine is configured as the APM System Monitoring controller.

13. If this is a machine that will serve as an APM System Monitoring agent, then, in the **Agent** section, select **Configure**. If this *is not* a machine that will serve as an APM System Monitoring agent, then proceed to step 14.

The **Agent Configuration** window appears.
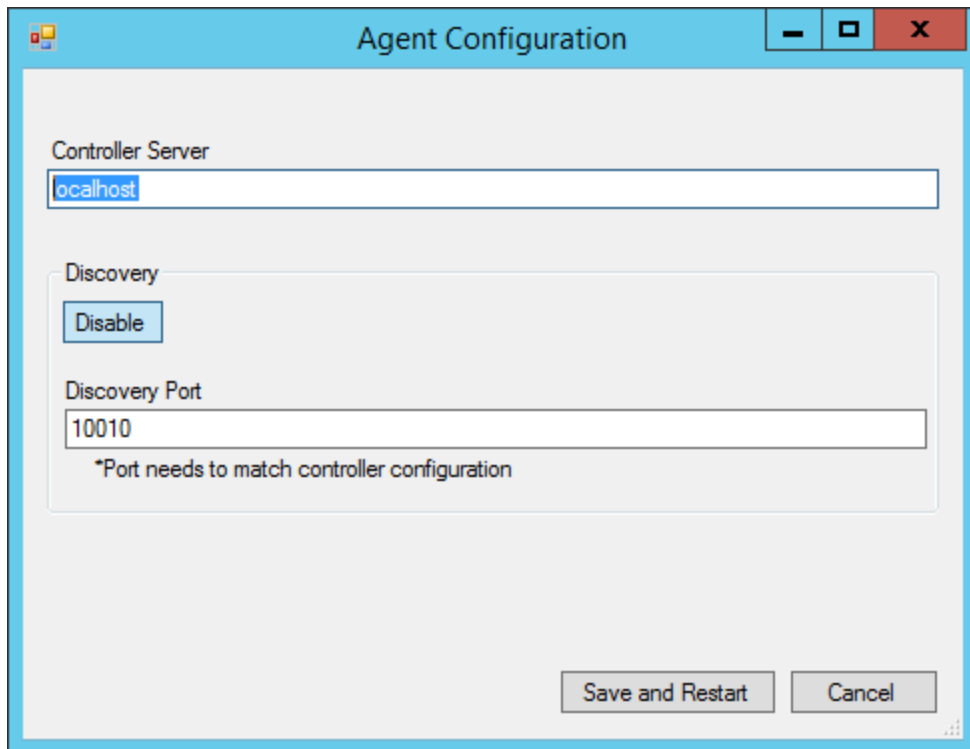
a. Ensure that the values in the **Controller Server** and **Discovery Port** boxes match the values specified for the APM System Monitoring controller, and then select **Save and Restart**.

The machine is configured as an APM System Monitoring agent.

14. Close the **Meridium System Monitor Service Manager** window.

APM System Monitoring is installed on the machine.

What's Next?

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

Modify the Web.config File for APM System Monitoring

Before You Begin

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

Steps

1. On the Meridium Enterprise APM Server, navigate to **C:\Program Files\Meridium\ApplicationServer\api**, and then open the file **web.config**.

   The **web.config** file opens in a text editor.

```
</connectionStrings>
<queueConfiguration>
  <queueSettings>
    <add key="XiDataChangeFilter" type="XI" filter="Meridium.Policies.Triggering.XiSubscriptionF
    <add key="AHMXIDataChangeFilter" type="XI" filter="Meridium.AHI.XiSubscriptionFilter, Meridi
    <add key="PolicyDataChangeFilter" type="ENTITY" filter="Meridium.Policies.Triggering.EntityS
    <add key="AHMDataChangeFilter" type="ENTITY" filter="Meridium.AHI.EntitySubscriptionFilter,
  </queueSettings>
</queueConfiguration>
<appSettings>
  <add key="webpages:Version" value="3.0.0.0" />
  <add key="webpages:Enabled" value="false" />
  <add key="vs:EnableBrowserLink" value="false" />
  <add key="ClientValidationEnabled" value="true" />
  <add key="UnobtrusiveJavaScriptEnabled" value="true" />
  <add key="SessionCookie" value="Meridium-Session-ID" />
  <add key="MIQueueName" value=".\Private$\MechanicalIntegrity_Request" />
  <add key="ApmMonitoringConfigServiceUrl" value="net.tcp://localhost/ETConfig" />
</appSettings>
<system.web>
  <customErrors mode="Off" />
  <compilation debug="true" targetFramework="4.5" />
  <httpRuntime targetFramework="4.5" maxRequestLength="102400" />
```

2. Change the ApmMonitoringConfigServiceUrl to point to the location of the machine that is serving as the APM System Monitoring controller, and then save the file.

   The modification is saved.

   > ⚠ **IMPORTANT:** This procedure must be completed for each Meridium Enterprise APM Server in your system.

What's Next?

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

Enable APM System Monitoring
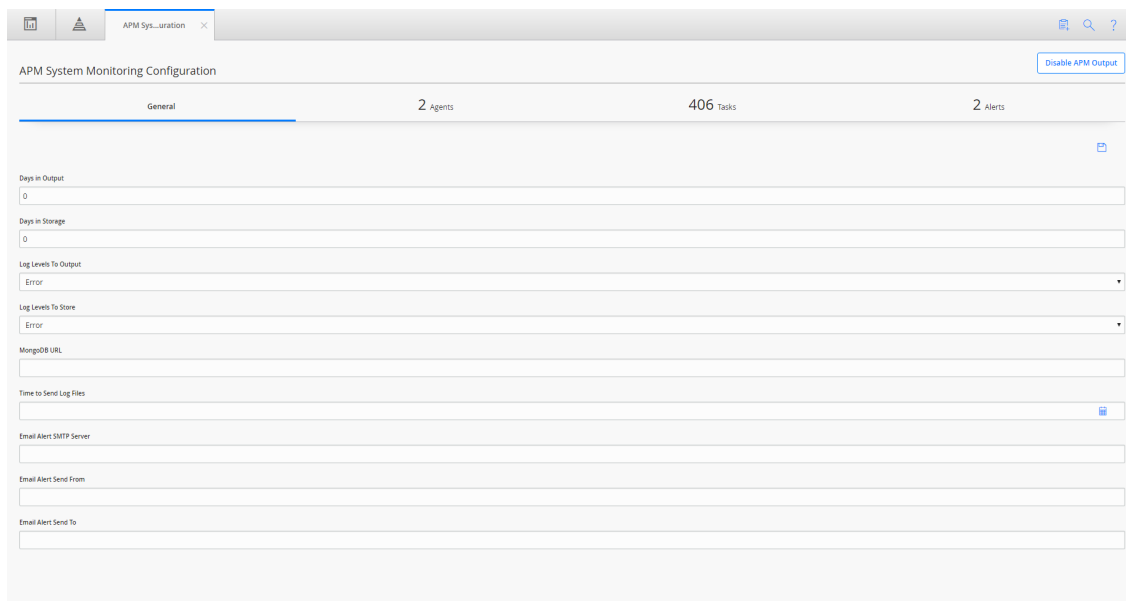
Before You Begin

- Complete all previous steps in the [APM System Monitoring first-time deployment workflow](#).

Steps

1. Access the **APM System Monitoring** page .

2. On the upper-right corner of the page, select ⋮ , and then select **Configure**.

   The **APM System Monitoring Configuration** page appears, displaying the **General** section.

3. On the upper-right corner of the page, select **Disable APM Output**.

   The button label changes to *Enable APM Output*.

4. On the upper-right corner of the page, select **Enable APM Output**.

   The button label changes to *Disable APM Output*. APM System Monitoring is now enabled.

Deploy Asset Health Manager (AHM)

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 Asset Health Manager (AHM) 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 Meridium Enterprise 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.

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	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for AHM.	This step is required.
3	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	This step is required. You may review the log files for this service at **C:\ProgramData\Meridium**.
4	On the Meridium Enterprise APM Server, start the Meridium AHI Service (Asset Health Indicator Service).	This step is required. When you start the service, Health Indicator records are created or updated automatically based on health indicator and reading source records. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
5	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.
6	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.

Step	Task	Notes
7	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 • OPC Tag • Health Indicator
8	Link each asset record to the record(s) that you want to use as a health indicator source records.	This step is required.
9	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.
10	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 .

Upgrade or Update Asset Health Manager (AHM) to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

Step	Task	Notes
1	On the Meridium Enterprise APM Server, con-figure the Meridium Notification Service for AHM.	This step is required.
2	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	This step is required.
3	Start or restart the Meridium AHI Service (Asset Health Indicator Service).	This step is required.
4	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required only if you are using OPC Tag records as health indicators sources.

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	On the Meridium Enterprise APM Server, con-figure the Meridium Notification Service for AHM.	This step is required.
2	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	This step is required.
3	Start or restart the Meridium AHI Service (Asset Health Indicator Service).	This step is required.
4	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required only if you are using OPC Tag records as health indicators sources.

Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for AHM.	This step is required.
2	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	This step is required. You may review the log files for this service at **C:\ProgramData\Meridium**.
3	Start or restart the Meridium AHI Service (Asset Health Indicator Service).	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
4	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required only if you are using OPC Tag records as health indicators sources.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

Step	Task	Notes
1	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for AHM.	This step is required.
2	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	This step is required. You may review the log files for this service at **C:\ProgramData\Meridium**.
3	Start or restart the Meridium AHI Service (Asset Health Indicator Service).	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.

Step	Task	Notes
4	Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each.	This step is required. 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 4.2.0.7.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records.
5	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 Asset Hierarchy configuration.	This step is required.
6	If you are using custom Health Indicator Mapping records, specify values in the Type Field and Type Value fields to ensure that the mappings are used for the appropriate reading type.	This step is required.
7	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required only if you are using OPC Tag records as health indicators sources.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

Step	Task	Notes
1	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for AHM.	This step is required.

Step	Task	Notes
2	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	This step is required. You may review the log files for this service at **C:\ProgramData\Meridium**.
3	Start or restart the Meridium AHI Service (Asset Health Indicator Service).	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
4	Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each.	This step is required. 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 4.2.0.7.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records.
5	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 Asset Hierarchy configuration.	This step is required.
6	If you are using custom Health Indicator Mapping records, specify values in the Type Field and Type Value fields to ensure that the mappings are used for the appropriate reading type.	This step is required.
7	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required only if you are using OPC Tag records as health indicators sources.

Upgrade from any version V3.5.1 through V3.5.1.12.0

Step	Task	Notes
1	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for AHM.	This step is required.
2	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	This step is required. You may review the log files for this service at **C:\ProgramData\Meridium**.
3	Start or restart the Meridium AHI Service (Asset Health Indicator Service).	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
4	Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each.	This step is required. 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 4.2.0.7.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records.
5	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 Asset Hierarchy configuration.	This step is required.

Step	Task	Notes
6	If you are using custom Health Indicator Mapping records, specify values in the Type Field and Type Value fields to ensure that the mappings are used for the appropriate reading type.	This step is required.
7	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required only if you are using OPC Tag records as health indicators sources.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

Step	Task	Notes
1	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for AHM.	This step is required.
2	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	This step is required. You may review the log files for this service at **C:\ProgramData\Meridium**.
3	Start or restart the Meridium AHI Service (Asset Health Indicator Service).	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.

Step	Task	Notes
4	Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each.	This step is required. 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 4.2.0.7.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records.
5	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 Asset Hierarchy configuration.	This step is required.
6	If you are using custom Health Indicator Mapping records, specify values in the Type Field and Type Value fields to ensure that the mappings are used for the appropriate reading type.	This step is required.
7	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required only if you are using OPC Tag records as health indicators sources.

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for AHM.	This step is required.
2	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	This step is required. You may review the log files for this service at **C:\ProgramData\Meridium**.
3	Start or restart the Meridium AHI Service (Asset Health Indicator Service).	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
4	Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each.	This step is required. 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 4.2.0.7.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records.
5	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 Asset Hierarchy configuration.	This step is required.
6	If you are using custom Health Indicator Mapping records, specify values in the Type Field and Type Value fields to ensure that the mappings are used for the appropriate reading type.	This step is required.

Step	Task	Notes
7	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required only if you are using OPC Tag records as health indicators sources.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for AHM.	This step is required.
2	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	This step is required. You may review the log files for this service at **C:\ProgramData\Meridium**.
3	Start or restart the Meridium AHI Service (Asset Health Indicator Service).	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
4	Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each.	This step is required. 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 4.2.0.7.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records.

Step	Task	Notes
5	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 Asset Hierarchy configuration.	This step is required.
6	If you are using custom Health Indicator Mapping records, specify values in the Type Field and Type Value fields to ensure that the mappings are used for the appropriate reading type.	This step is required.
7	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required only if you are using OPC Tag records as health indicators sources.

About the Asset Health Services

When you deploy the Asset Health Manager, Process Data Integration, 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 following topics:

- Deploying Asset Health Manager (AHM) for the First Time
- Deploying Policy Designer for the First Time
- Deploying Process Data Integration (PDI) for the First Time

Services Summary

The following services are used by the Asset Health Manager, Process Data Integration, 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 (e.g., an OPC 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 (i.e., an associated record in the Meridium Enterprise 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. The Policy Trigger Service monitors this queue and sends these messages to an appropriate policy execution queue.

- **Policy Execution Service:** The Meridium Enterprise APM Policy Execution Service handles the execution of policies. Specifically, the Policy Execution Service monitors a corresponding policy execution queue and executes the policies that are added to it.

- **Process Data Integration (PDI) Service:** Monitors the subscribed tags (i.e., tags that are used in policies and health indicators or tags for which readings are being stored in the Meridium 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.

Example: Standard System Architecture Configuration

The following diagram illustrates the machines in the Meridium Enterprise APM system architecture when the Policy Designer, Process Data Integration (PDI), and Asset Health Manager

(AHM) modules are used together. This image depicts the standard configuration, where the OPC Server software and the Process Data Integration 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 Meridium Enterprise APM Servers, multiple OPC Servers, or multiple Meridium Enterprise 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, Policy Designer, and Process Data Integration.

Machine	Software Installed	Asset Health Service Installed Automatically with Service Software
Meridium Enterprise APM Server	Meridium Enterprise APM Server software	Asset Health Indicator Service
		Policy Trigger Service
		Policy Execution Service
Process Data Integration Server, which also acts as the OPC Server	Process Data Integration Service software	Process Data Integration Service
	OPC Server software	NA
Process Historian	Process historian software	NA

Configure the Meridium Notification Service for AHM

In order for the Asset Health Indicator service to work correctly, you must configure the Meridium Notification Service by modifying the file *Meridium.Service.Notification.exe.config* on all Meridium Enterprise APM Servers.

Steps

1. On the Meridium Enterprise APM Server, navigate to the folder where the Meridium Notification Service files are installed. If you installed the software in the default location, you can locate these files in the folder **C:\Program Files\Meridium\Services**.

2. Open the file **Meridium.Service.Notification.exe.config** in an application that you can use to modify XML script (e.g., Notepad).

3. If you have not done so already, complete any necessary basic configuration for the Meridium Notification Service.

4. Within the **<notification>** tags, within the **<notificationSettings>** tags, uncomment the following text string (i.e., delete the **<!--** and **-->**):

   ```
   <!-- <add key="server4" serverType="external" endPointName-
   e="ahmService"/> -->
   ```

5. Within the **<system.serviceModel>** tags, within the **<client>** tags, uncomment the following text string (i.e., delete the **<!--** and **-->**):

   ```
   <!-- <endpoint name="ahmService" address-
   s="net.tcp://localhost/Meridium/AHM/NotifyHandler" bind-
   ing="netTcpBinding"
   contract="Meridium.Core.Common.Contracts.INotificationService"
   /> -->
   ```

6. Save and close the file.

7. Start or restart the Meridium Notification Service.

Asset Health Manager 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 AHI Administrator	MI Health Admin
MI AHI User	MI Health User MI Health Power
MI AHI Viewer	None

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

Family	MI AHI Administrator	MI AHI User	MI AHI Viewer
Entity Families			
Checkpoint Task	View, Update, Insert	View, Update, Insert	View
Event Mapping	View, Update, Insert, Delete	View	View
Health Indicator	View, Update, Insert, Delete	View, Update	View
Health Indicator Mapping	View, Update, Insert, Delete	View	View
Health Indicator Value	View, Update, Insert, Delete	View	View
KPI	View	View	View
KPI Measurement	View	View	View
Measurement Location	View	View	View

Family	MI AHI Administrator	MI AHI User	MI AHI Viewer
Measurement Location Template	View	View	View
OPC Reading	View	View	View
OPC System	View	View	View
OPC Tag	View	View	View
Operator Rounds Allowable Values (Deprecated)	View	View	View
Policy	View	View	View
Policy Instance	View	View	View
Reading	View	View	View
Recommendation	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Timestamped Value	View, Update, Insert, Delete	View	View
Relationship Families			
Has Checkpoint	View	View	View
Has Child Hierarchy Item (Deprecated)	View, Update, Insert, Delete	View	View
Has Consolidated Events	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Health Indicators	View, Update, Insert, Delete	View	View
Has OPC Reading	View	View	View
Has OPC Tag	View	View	View
Has Readings	View	View	View
Has Recommendations	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Timestamped Value	View, Update, Insert, Delete	View	View

Family	MI AHI Administrator	MI AHI User	MI AHI Viewer
Health Indicator Has Mapping	View, Update, Insert, Delete	View	View
Health Indicator Has Source	View, Update, Insert, Delete	View	View

Deploy Asset Criticality Analysis (ACA)

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 Asset Criticality Analysis (ACA) 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 Meridium Enterprise 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.

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	Define sites to associate with ACA Analyses.	This step is required.
4	Specify the alternate label that you want to use for the **Unmitigated Risk** column in the grid on the **Asset Criticality Analysis Systems** page.	This step is required only if you do not want to use the default label, *Unmitigated Risk*.
5	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.

Upgrade or Update Asset Criticality Analysis (ACA) to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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	Specify the alternate label that you want to use for the **Unmitigated Risk** column in the grid on the **Asset Criticality Analysis Systems** page.	This step is required only if you do not want to use the default label, *Unmitigated Risk*.
2	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.
3	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	Specify the alternate label that you want to use for the **Unmitigated Risk** column in the grid on the **Asset Criticality Analysis Systems** page.	This step is required only if you do not want to use the default label, *Unmitigated Risk*.
2	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.

Step	Task	Notes
3	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 V3.6.1.2.0

Step	Task	Notes
1	Specify the alternate label that you want to use for the Unmitigated Risk column in the grid on the Asset Criticality Analysis Systems page.	This step is required only if you do not want to use the default label, *Unmitigated Risk*.
2	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.
3	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 V3.6.0.12.4

Step	Task	Notes
1	Specify the alternate label that you want to use for the Unmitigated Risk column in the grid on the Asset Criticality Analysis Systems page.	This step is required only if you do not want to use the default label, *Unmitigated Risk*.
2	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.
3	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 V3.5.1.12.0

Step	Task	Notes
1	Specify the alternate label that you want to use for the **Unmitigated Risk** column in the grid on the **Asset Criticality Analysis Systems** page.	This step is required only if you do not want to use the default label, *Unmitigated Risk*.
2	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.
3	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 V3.5.0.1.9.0

Step	Task	Notes
1	Specify the alternate label that you want to use for the **Unmitigated Risk** column in the grid on the **Asset Criticality Analysis Systems** page.	This step is required only if you do not want to use the default label, *Unmitigated Risk*.

Step	Task	Notes
2	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.
3	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	Specify the alternate label that you want to use for the **Unmitigated Risk** column in the grid on the **Asset Criticality Analysis Systems** page.	This step is required only if you do not want to use the default label, *Unmitigated Risk*.
2	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.
3	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	Specify the alternate label that you want to use for the **Unmitigated Risk** column in the grid on the **Asset Criticality Analysis Systems** page.	This step is required only if you do not want to use the default label, *Unmitigated Risk*.
2	Lock the Risk Matrix.	This step is required only if you do not want risk values to be specified manually via the Risk Matrix.

Step	Task	Notes
3	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.

Specify an Alternate Unmitigated Risk Label

In ACA, the **Unmitigated Risk** section displays the unmitigated risk for each Asset Criticality Analysis System, Equipment, and Functional Location record. If your company prefers a label other than *Unmitigated Risk*, you can use the following instructions to specify an alternate label.

Note that an alternate label is specified using the Risk Matrix record. This means that after you specify an alternate label in a Risk Matrix record, it will be used by all ACA Analyses that use that Risk Matrix.

Steps

1. On the Meridium navigation menu, on the left toolbar, select **Admin**, and then select **Operations Manager**.

   The **Operations Manager** page appears.

2. Select **Risk Matrix**.

   The **Risk Matrix Admin** page appears.

3. In the **Name** column, select the risk matrix record that you want to access.

   The datasheet for the selected risk matrix appears.

4. To enable editing, on the upper-right corner of the datasheet, select the Edit button (pencil icon).

5. In the **Appearance** section, in the Unmitigated Risk Label field, modify the field value as needed.

6. On the upper-right corner of the datasheet, select the Save button (disk icon).

   The Unmitigated Risk Label for that risk matrix is changed.

ACA 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 ACA Administrator	MI Foundation Admin
MI ACA Member	MI Foundation Admin MI Foundation Power MI Foundation User
MI ACA Owner	MI Foundation Admin MI Foundation Power

The baseline privileges for these Security Groups are summarized in the following table.

Family Entity	MI ACA Administrator	MI ACA Member	MI ACA Owner
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

Family	MI ACA Administrator	MI ACA Member	MI ACA Owner
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
Meridium 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
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

Family	MI ACA Admin-istrator	MI ACA Member	MI ACA Owner
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

Deploy Asset Strategy Implementation (ASI)

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 Asset Strategy Implementation (ASI) 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 Meridium Enterprise 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.

Step	Task	Notes
1	Install the ASI for SAP ABAP add-on on your SAP System.	This step is required.
2	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.
3	Assign Security Users to one or more of the ASI Security Groups and Roles.	This step is required.
4	Configure SAP permissions.	This step is required.
5	Configure secured Maintenance Plants in your SAP System.	This step is optional.
6	Configure Work Management Item Definition records 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.
7	Define Implementation Roles via the ASI Application Settings.	This step is optional.
8	Define the SAP connection that will be used when SAP items are created from records that represent work items. You can do so via the ASI Application Settings.	This step is required.

Upgrade or Update Asset Strategy Implementation (ASI) to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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	Upgrade the ASI for SAP ABAP add-on in your SAP System.	This step is required.

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.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

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

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

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

Upgrade from any version V3.5.1 through V3.5.1.12.0

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

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

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

Upgrade from any version 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.

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.

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 User MI ASI Viewer	MI Strategy User
MI ASI User MI ASI Viewer	MI Strategy Power
MI ASI User MI ASI Administrator MI ASI Viewer	MI Strategy Admin

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

Family Entity Families	MI ASI Administrator	MI ASI User	MI ASI Viewer
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
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
Implementation Role	View, Update, Insert, Delete	View	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 (Deprecated)	None	View	View
Probability	None	View	View
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
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
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
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

Deploy Asset Strategy Management (ASM)

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 Asset Strategy Management (ASM) 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 Meridium Enterprise 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.

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 Asset Strategy Management (ASM) to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.0

ASM will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

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.

Asset Strategy Management (ASM) 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 ASM Analyst MI ASM Viewer	MI Strategy User
MI ASM Analyst MI ASM Reviewer MI ASM Viewer	MI Strategy Power
MI ASM Management Administrator MI ASM Analyst MI ASM Reviewer MI ASM Viewer	MI Strategy Admin

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	Insert, View, Update, Delete	View	Insert, View, Update, Delete	View
Action Mapping	View	None	None	None

Active Strategy	Insert, View, Update, Delete	View	Insert, View, Update, Delete	View
Analysis Link	View	View	View	View
Asset Criticality Analysis	View	View	View	View
Asset Criticality Analysis System	View	View	View	View
Asset Strategy	Insert, View, Update, Delete	View	View, Update	View
Calibration Task	View	None	View	None
Checkpoint Task	Insert, View, Update	Insert, View, Update	Insert, View, Update	Insert, View, Update
Consequence	View	Insert, View, Update, Delete	View	View
Distribution	Insert, View, Update, Delete	View	View	View
Execution Mapping	View	None	None	None
Growth Model	View	View	View	View
Health Indicator	Insert, View, Update, Delete	None	View, Update	View, Update
Health Indicator Mapping	View	Insert, View, Update, Delete	View	View
Hierarchy Item Child Definition	View	Insert, View, Update, Delete	View	View
Hierarchy Item Definition	View	Insert, View, Update, Delete	View	View
Implementation Package	View, Insert	None	None	None
Implementation Role	View	View	View	View
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	Insert, View, Update	None	None	None
Measurement Location Template	View	View	View	View
Operator Rounds Allowable Values	View	View	View	View
Probability	View	Insert, View, Update, Delete	View	View
Proposed Strategy	Insert, View, Update, 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	Insert, View, Update, Delete	View	View	View
Reading	View	View	View	View
Reliability Distribution	View	View	View	View
Reliability Growth	View	View	View	View
Risk Assessment	Insert, View, Update, Delete	View	Insert, View, Update, Delete	View
Risk Category	View	Insert, View, Update, Delete	View	View
Risk Matrix	View	Insert, View, Update, Delete	View	View
Risk Rank	Insert, View, Update, Delete	View	Insert, View, Update, Delete	View

Risk Threshold	View	Insert, View, Update, Delete	View	View
Site Reference	View	View	View	View
System Action	Insert, View, Update, Delete	View	View	View
System Action Mapping	View	Insert, View, Update, Delete	View	View
System Action Optimization	Insert, View, Update, Delete	View	View	View
System Action Result	Insert, View, Update, Delete	View	View	View
System Analysis	Insert, View, Update, Delete	View	View	View
System Element	Insert, View, Update, Delete	View	View	View
System Element Result	Insert, View, Update, Delete	View	View	View
System Global Event	Insert, View, Update, Delete	View	View	View
System Resource	Insert, View, Update, Delete	View	View	View
System Resource Result	Insert, View, Update, Delete	View	View	View
System Resource Usage	Insert, View, Update, Delete	View	View	View

System Risk Assessment	Insert, View, Update, Delete	View	View	View
System Scenario	Insert, View, Update, Delete	View	View	View
System Sensor	Insert, View, Update, Delete	View	View	View
System Strategy	Insert, View, Update, Delete	View	View, Update	View
Unit Strategy	Insert, View, Update, 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	Insert, View, Update, Delete	None	None	None
Has Action Mapping	View	None	None	None
Has Action Revisions	Insert, View, Update, Delete	View	Insert, View, Update, Delete	View
Has Actions	Insert, View, Update, Delete	View	Insert, View, Update, Delete	View

Has Active Strategy	Insert, View, Update, Delete	View	Insert, View, Update, Delete	View
Has Asset Strategy	Insert, View, Update, Delete	View	View	View
Has Associated Recommendation	Insert, View, Update, Delete	View	View	View
Has Associated Strategy	Insert, View, Update, Delete	View	View	View
Has Checkpoint	View	None	None	None
Has Child Hierarchy Item	View	Insert, View, Update, Delete	View	View
Has Child Work Management Item	View	None	None	None
Has Driving Recommendation	Insert, View, Update, Delete	View	View, Delete	View
Has Execution Mapping	View	None	None	None
Has Functional Location	View	n/a	View	n/a
Has Global Events	Insert, View, Update, Delete	View	View	View
Has Health Indicators	Insert, View, Update, Delete	View	View	View
Has Measurement Location Group	Insert, View, Update, Delete	None	None	None
Has Mitigated TTF Distribution	Insert, View, Update, Delete	View	View	View

Has Mitigation Revisions	Insert, View, Update, Delete	View	Insert, View, Update, Delete	View
Has Planned Resource Usages	Insert, View, Update, Delete	View	View	View
Has Proposed Strategy	Insert, View, Update, Delete	View	Insert, View, Update, Delete	View
Has Readings	View	View	View	View
Has Recommendations	Insert, View, Update, Delete	None	None	n/a
Has Reference Values	View	Insert, View, Update, Delete	View	View
Has Resource Usages	Insert, View, Update, Delete	View	View	View
Has Risk	Insert, View, Update, Delete	View	Insert, View, Update, Delete	View
Has Risk Assessments	Insert, View, Update, Delete	View	View	View
Has Risk Category	Insert, View, Update, Delete	Insert, View, Update, Delete	Insert, View, Update, Delete	View
Has Risk Matrix	View	None	None	None
Has Risk Revisions	Insert, View, Update, Delete	View	Insert, View, Update, Delete	View
Has Root System	Insert, View, Update, Delete	View	View	View
Has Scenarios	Insert, View, Update, Delete	View	View	View

Has Strategy	Insert, View, Update, Delete	View	View	View
Has Strategy Revision	Insert, View, Update, Delete	View	Insert, View, Update, Delete	View
Has System Actions	Insert, View, Update, Delete	View	View	View
Has System Elements	Insert, View, Update, Delete	View	View	View
Has System Optimization	Insert, View, Update, Delete	View	View	View
Has System Resources	Insert, View, Update, Delete	View	View	View
Has System Results	Insert, View, Update, Delete	View	View	View
Has System Risks	Insert, View, Update, Delete	View	View	View
Has System Strategy	Insert, View, Update, Delete	View	View	View
Has TTF Distribution	Insert, View, Update, Delete	View	View	View
Has TTR Distribution	Insert, View, Update, Delete	View	View	View
Has Unplanned Resource Usages	Insert, View, Update, Delete	View	View	View
Has Work Management Item	Insert, View, Update	None	None	None

Has Work Management Item Definition Configuration	View	None	None	None
Health Indicator Has Mapping	Insert, View, Update, Delete	View	View	View
Health Indicator Has Source	Insert, View, Update, Delete	View	View	View
Implements Action	Insert, View, Update	None	None	None
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	Insert, View, Update, Delete	None	None	None
Is Basis for Asset Strategy Template	Insert, View, Update, Delete	View	View, Update	View
Is Mitigated	Insert, View, Update, Delete	View	Insert, View, Update, Delete	View
Master Template Has Asset Strategy	Insert, View, Update, Delete	View	View, Update	View
Mitigates Risk	Insert, View, Update, Delete	View	Insert, View, Update, Delete	View
Safety Analysis Has Equipment	View	n/a	View	n/a
Was Applied to Asset Strategy	Insert, View, Update, Delete	View	View, Update	View
Was Promoted to ASM Element	View	None	View	View

Deploy Asset Strategy Optimization (ASO)

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 Asset Strategy Optimization (ASO) 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 Meridium Enterprise 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.

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 Asset Strategy Optimization (ASO) to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

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.

Asset Strategy Optimization (ASO) Security Groups and Roles

The Meridium Asset Strategy Optimization module leverages the baseline Meridium [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

Deploy Calibration 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 module.

Deploy Calibration Management 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 Meridium Enterprise 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.

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.	This step is required only if you will store equipment or location data in families other than the baseline Equipment and Functional Location families.
2	Assign the desired Security Users to the Calibration Management Security Groups.	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.
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 Configuration Manager.	This step is required.

Upgrade or Update Calibration Management to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

Calibration Management will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the

basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Install the Meridium Device Service

> ⚠ **IMPORTANT:** You must repeat this procedure on every machine to which you will connect a calibrator.

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

Steps

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

    > 📄 **Note:** A calibrator does not need to be connected.

2. In the upper-right corner of the page, select **Settings**.

    The **Settings** window appears.

    Settings

    Calibrator Device Settings

    Select Device

    | Select Device ∨ |

    | COM Port | | Baud Rate |
    | COM 1 ∨ | | 9600 ∨ |

    ☐ Test Connection

    Device Service Settings

    Service Port

    | 2014 |

    Cancel   Done

3. Select the **Test Connection** check box, and then, in the lower-right corner of the window, select **Done**.

    A message appears, specifying that the Meridium Device Service is not installed.

    Settings

    The Meridium Device Service could not be reached. Please verify that it is installed and running. If the service is not installed please click the download link below to download the installer.

    Download

    Once the installer has completed and the service is running, click the Continue button and retry the operation.

    Continue

    Close

4. Select **Download**.

    The MeridiumDevices.exe file is downloaded.

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

    The Meridium Device Service is installed.

Calibration 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 Calibration Administrator	MI Safety Admin
MI Calibration User	MI Safety Admin MI Safety Power MI Safety User

> 📄 **Note:** Any Security User who is a member of the MI Calibration Administrator Security Group should also be added to MI Devices Administrators Security Group. Members of the MI Calibration User Security Group should also be added to MI Devices Power Users Security Group. This will allow Calibration users to perform automated calibration.

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

Family	MI Calibration Administrator	MI Calibration User
Entity Families		
Alert	View, Update, Insert, Delete	View, Update, Insert, Delete
Calibration (Event)	View, Update, Insert, Delete	View, Update, Insert, Delete
Calibration Recommendation	View, Update, Insert, Delete	View, Update, Insert
Calibration Result	View, Update, Insert, Delete	View, Update, Insert, Delete

Family	MI Calibration Administrator	MI Calibration User
Calibration Setup Defaults	View, Update, Insert, Delete	View
Calibration Task	View, Update, Insert, Delete	View, Update, Insert, Delete
Calibration Template	View, Update, Insert, Delete	View
Calibration Template Defaults	View, Update, Insert, Delete	View
Calibration Template Detail	View, Update, Insert, Delete	View
Calibration Template Detail, Analyzer	View, Update, Insert, Delete	View
Equipment	View	View
Functional Location	View	View
Reference Document	View, Update, Insert, Delete	View
SAP System	View	None
Task	View, Update, Insert, Delete	None
Task Types	View, Update, Insert, Delete	View
Test Equipment	View, Update, Insert, Delete	View, Update, Insert, Delete
Test Equipment History	View, Update, Insert, Delete	View, Update, Insert, Delete
Work History	View	View
Work History Detail	View	View
Relationship Families		
Equipment Has Equipment	View	View
Functional Location Has Equipment	View	View

Family	MI Calibration Administrator	MI Calibration User
Functional Location Has Functional Location(s)	View	View
Has Associated Recommendation	View, Update, Insert, Delete	View
Has Calibration	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Calibration Results	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Consolidated Recommendations	View, Update, Insert, Delete	View
Has Driving Recommendations	View, Update, Insert, Delete	View
Has Event Detail	View	View
Has Recommendations	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Reference Documents	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Standard Gas	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Standard Gas Details	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Superseded Recommendations	View, Update, Insert, Delete	View
Has Task Revision	View, Update, Insert, Delete	None
Has Tasks	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Templates	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Template Detail	View, Update, Insert, Delete	View

Family	MI Calibration Administrator	MI Calibration User
Has Test Equipment	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Work History	View	View
Test Equipment Has Equipment	View, Update, Insert, Delete	View, Update, Insert, Delete
Test Equipment Has History	View, Update, Insert, Delete	View, Update, Insert, Delete

Deploy Cognitive Analytics

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 Cognitive Analytics 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 Meridium Enterprise 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.

Step	Task	Notes
1	Review the Cognitive Analytics data model to determine which relationship definitions you will need to modify to include your custom equipment and location families or to store your classified data in custom families. Via Configuration Manager, modify any 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 if you store classified data in families other than the baseline Classified Equipment Standard and Classified Work History Standard families.
2	Assign Security Users to one or more of the Cognitive Analytics Security Groups or Roles.	This step is required.

Upgrade or Update Cognitive Analytics to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Cognitive Analytics 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 Cognitive User	MI Analytics Power
MI Cognitive Administrator	MI Analytics Administrator

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

Family	MI Cognitive User	MI Cognitive Administrator
Entity Families		
Classified Equipment Standard	View, Update, Insert, Delete	View, Update, Insert, Delete
Classified Work History Standard	View, Update, Insert, Delete	View, Update, Insert, Delete
Classifier Standard List	View	View, Update, Insert, Delete
Cognition	View, Update, Insert, Delete	View, Update, Insert, Delete
Spark Application Log	View, Update, Insert	View, Update, Insert, Delete
Spark Job Configuration	View, Update, Insert	View, Update, Insert, Delete
Spark Job Log	View, Update, Insert	View, Update, Insert, Delete
Relationship Families		
Has Classified Data	View, Update, Insert, Delete	View, Update, Insert, Delete

Deploy Failure Modes and Effects Analysis (FMEA)

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 Failure Modes and Effects Analysis (FMEA) 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 Meridium Enterprise 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.

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

Upgrade or Update Failure Modes and Effects Analysis (FMEA) to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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.

Failure Modes and Effects Analysis (FMEA) 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 RCM User MI RCM Viewer	MI Strategy User
MI RCM User MI RCM Viewer	MI Strategy Power
MI RCM User MI RCM Viewer MI ASI Administrator	MI Strategy Admin

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

Family Caption	MI RCM User	MI RCM Viewer
Entity families		
Action	View	View
Asset Criticality Analysis System	View	None
Consequence Definition	View	View
Decision Tree Consequence	View	View
Decision Tree Response	View	View
Decision Tree Structure	View	View

Human Resource	View, Update, Insert, Delete	View
Mitigates Risk	View, Update, Insert, Delete	View
Probability Definition	View	View
Protection Level	View	View
RCM FMEA Analysis	View, Update, Insert, Delete	View
RCM FMEA Asset	View, Update, Insert, Delete	View
RCM Function	View, Update, Insert, Delete	View
RCM Functional Failure	View, Update, Insert, Delete	View
RCM FMEA Failure Mode	View, Update, Insert, Delete	View
RCM FMEA Failure Effect	View, Update, Insert, Delete	View
RCM FMEA Recommendation	View, Update, Insert, Delete	View
RCM FMEA Template	View, Update, Insert, Delete	View
RCM FMEA Task	View, Update, Insert, Delete	View
Reference Documents	View, Update, Insert, Delete	View
Risk Assessment	View, Update, Insert, Delete	View
Risk Category	View	View
Risk Matrix	View	View
Risk Rank	View, Update, Insert, Delete	View
Risk Threshold	View	View

Site Reference	View	View
Task History ⬛ **Note:** The Task History relationship family is inactive in the baseline Meridium Enterprise APM database.	View, Update, Insert, Delete	View
Relationship Families		
Has Associated Recommendation	View	View
Has Consolidated Recommendations	View	View
Has Driving Recommendation	View	View
Has RCM FMEA Team Member	View, Update, Insert, Delete	View
Has RCM FMEA Analysis	View, Insert, Delete	None
Has RCM FMEA Asset	View, Update, Insert, Delete	View
Has RCM Function	View, Update, Insert, Delete	View
Has RCM Functional Failure	View, Update, Insert, Delete	View
Has RCM FMEA Failure Mode	View, Update, Insert, Delete	View
Has RCM FMEA Failure Effect	View, Update, Insert, Delete	View
Has RCM FMEA Recommendation	View, Update, Insert, Delete	View
Has Reference Values	View	View
Has Recommendations	View, Update, Insert, Delete	View
Has Reference Documents	View, Update, Insert, Delete	View
Has Risk	View	None
Has Risk Category	View, Update, Insert, Delete	View

Has Site Reference	View	View
Has Superseded Recommendations	View	View
Has Task History 📄 Note: The Has Task History relationship family is inactive in the baseline Meridium Enterprise APM database.	View, Update, Insert, Delete	View
Has Tasks	View, Update, Insert, Delete	View
Has Templates	View, Update, Insert, Delete	View
Is Based on RCM FMEA Failure Effect	View	View
Is RCM FMEA Asset	View, Update, Insert, Delete	View

With these privileges, any user who is a member of the MI RCM User Security Group will have access to ALL records involved in FMEA Analyses. In addition to these baseline privileges, which you can grant by assigning users to the MI RCM User Security Group, you will need to grant FMEA users permission to the Equipment or Functional Location family if it is related to the RCM FMEA Asset family through the Is RCM FMEA Asset relationship.

📄 Note: You may also want to grant some users permission to modify the items in the following Catalog folders: \\Public\Meridium\Modules\RCM.

- The current page on your desktop (create shortcut), in an email message, or on a Home Page.
- Help: Displays the context-sensitive Help topic for the FMEA Team Members page for FMEA Templates.

Deploy GE Analytics

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 GE Analytics 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 Meridium Enterprise 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.

Step	Task	Notes
1	Assign Security Users to one or more of the GE Analytics Security Groups and Roles.	This step is required.
2	Modify the file Meridium.AMQP.Service.exe.config to configure the RabbitMQ connection.	This step is required.
3	Restart the Meridium AMQP Service.	This step is required.
4	Install Meridium APM GE System 1 Integration Service.	This step is required.
5	Create and configure the GE Connection record to connect to the GE Message Broker Server.	This step is required. You can test connection using the link on the Associated Pages menu for the GE Connection record.
6	Modify the file Meridium.GE.Service.exe.config to configure the GE Service.	This step is required.
7	Configure the GE Service to restart automatically.	This step is required.
8	Start the GE Service.	This step is required. Once the GE Service is started, the GE Enterprise hierarchy will import automatically into the Meridium Enterprise APM database.
9	Configure GE Enterprise and Filter records.	This step is required. These records are created automatically by the GE Service.
10	Stop and then start the GE Service.	This step is required.
11	Link tags to assets (i.e., equipment and functional locations).	This step is required. You must repeat this step for any GE Tags records that are imported from your GE system. New tags are imported automatically.

12	Import the GE Analytics policies.	This step is required only if you want to use GE policies.

Upgrade or Update GE Analytics to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

Step	Task	Notes
1	Ensure that your version of GE System 1 Fleet is supported by the GE Analytics module.	This step is required.
2	Modify the file Meridium.GE.Service.exe.config.	This step is required.
3.	On the GE Fleet Message Server, restart the Meridium.GE.Service.	This step is required.
4.	Modify the file Meridium.AMQP.Service.exe.config.	This step is required.
5.	On the Meridium Application Server, restart the Meridium.AMQP.Service.	This step is required.

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

The GE Analytics module was introduced in Meridium Enterprise APM V4.2.0.0. To utilize GE Analytics in 4.2.0.7.0, follow the GE Analytics First-Time Deployment Workflow.

Upgrade from any version V4.0.0.0 through V4.0.1.0

The GE Analytics module was introduced in Meridium Enterprise APM V4.2.0.0. To utilize GE Analytics in 4.2.0.7.0, follow the GE Analytics First-Time Deployment Workflow.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

Step	Task	Notes
1	Ensure that your version of GE System 1 Fleet is supported by the GE Analytics module.	This step is required.

Step	Task	Notes
2	Modify the file Meridi- um.GE.Service.exe.config.	This step is required.
3	Modify the file Meridi- um.AMQP.Service.exe.config.	This step is required.
4	Run the following update query: UPDATE [MI_GETAG] SET [MI_GETAG].[MI_TAG_ SYSTEM_ID_C] = [MI_GEENT].[MI_ GEENT_ID_C].	This step is required only if you want to use the Asset and Tag Data Loader to create relationships between GE tags and assets.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

Step	Task	Notes
1	Ensure that your version of GE System 1 Fleet is supported by the GE Analytics mod- ule.	This step is required.
2	Modify the file Meridi- um.GE.Service.exe.config.	This step is required.
3	Modify the file Meridi- um.AMQP.Service.exe.config.	This step is required.
4	Run the following update query: UPDATE [MI_GETAG] SET [MI_GETAG].[MI_TAG_ SYSTEM_ID_C] = [MI_GEENT].[MI_ GEENT_ID_C].	This step is required only if you want to use the Asset and Tag Data Loader to create relationships between GE tags and assets.

Upgrade from any version V3.5.1 through V3.5.1.12.0

GE System 1 Integration was introduced in Meridium APM V3.6.0.6.0. To utilize GE Analytics in 4.2.0.7.0, follow the GE Analytics First-Time Deployment Workflow.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

GE System 1 Integration was introduced in Meridium APM V3.6.0.6.0. To utilize GE Analytics in 4.2.0.7.0, follow the GE Analytics First-Time Deployment Workflow.

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

GE System 1 Integration was introduced in Meridium APM V3.6.0.6.0. To utilize GE Analytics in 4.2.0.7.0, follow the GE Analytics First-Time Deployment Workflow.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

GE System 1 Integration was introduced in Meridium APM V3.6.0.6.0. To utilize GE Analytics in 4.2.0.7.0, follow the GE Analytics First-Time Deployment Workflow.

Modify the File Meridium.AMQP.service.exe.config

Steps

1. On your Meridium Enterprise APM Server, navigate to the folder where the **Meridium.AMQP.service.exe.config** is installed. If you installed the software in the default location, you can locate this file in the following location:C:\Program Files\Meridium\Services.

2. Open the file **Meridium.AMQP.service.exe.config** in an application that you can use to modify XML script (e.g., Notepad).

3. Within the <apmMqConnections> tags, uncomment the example connection tag by deleting <!--EXAMPLE: and the corresponding --> from the beginning and end of the string.

4. Within the <apmMqConnections> tags, configure the attributes, by replacing the values within the quotation marks with the values detailed in the following chart.

> 📄 **Note**: The client and heartbeat attributes should not be edited.

Attribute	Replace text...	... with the following values:	Notes
server key	KEY	A unique connection key.	None
dataSource	DATA_SOURCE	Your Meridium Enterprise APM data source.	The data source value is case sensitive and should be typed exactly as it is defined for the Meridium Enterprise APM Server in the Data Sources section of Operations Manager.
host	ENTER_BROKER_HOSTNAME	The hostname of the GE Fleet Message Broker.	None
port	5672	The appropriate port for your configuration. • The default SSL port is 5671. • The default HTTP port is 5672, and is the port preconfigured in the config file.	None

user	ENTER_MQ_ USER_NAME	The user name for the Rab- bitMQ Message Broker.	This field is not required if using SSL to connect to the mes- sage broker.
password	ENTER_MQ_ PASSWORD	The password for the Rab- bitMQ Message Broker.	This field is not required if using SSL to connect to the mes- sage broker. ⓘ **Note:** Do not delete the **!** in front of the password. This symbol is not part of the password itself. Instead, this symbol will cause the pass- word to be encrypted automatically when the service is restar- ted.

5. If you are using SSL configuration, configure the attributes, by replacing the values within the quotation marks with the values detailed in the following chart.

Attribute	Replace text...	... with the following val- ues:	Notes
sslEnabled	FALSE	TRUE	None
sslServerName	SSL_ SERVER_ NAME	The Common Name (CN) where the SSL certificate stored.	Typically, this is the host name of the server to which this client will connect.

sslCertPassPhrase	SSL_CERT_ PASSWORD	SSL certificate password.	ⓘ **Note:** Do not delete the **!** in front of the password. This symbol is not part of the password itself. Instead, this symbol will cause the password to be encrypted automatically when the service is restarted.
sslCertPath	PATH_TO_ CERT	File path to the directory where the SSL certificate is stored.	The SSL certificate is not supplied by Meridium, Inc. It should be obtained from a third-party certificate authority.
tlsVersions	1.2	The desired encryption algorithm. • The default value is 1.2. • Alternatively, to support multiple algorithms, you can enter multiple values, and then separate the values with a semicolon.	Only tls1.1 and tls1.2 versions are supported.

6. Save and close the file.

Results

Your settings will be applied when you start or restart the Meridium AMQP Service.

What's Next?

Return to the Deploy GE Analytics for the First Time

Install the Meridium APM GE System 1 Integration Service

Steps

1. On GE Fleet Message Server, access the Meridium Enterprise APM distribution package, and then navigate to the folder **\\Setup\Meridium Enterprise APM Server and Add-ons**.

2. Double-click the file **Setup.exe**.

   The **Welcome** screen 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. Select the **Meridium APM GE System 1 Integration Service** option.

   > ⓘ **Note**: While additional options are available for selection, these options are not meant to be installed on the GE Integration Service server. These instructions assume that you want to install only the Meridium Process GE Integration Service software. When this software is installed, the Meridium Enterprise APM System Administration Tool will also be installed automatically.
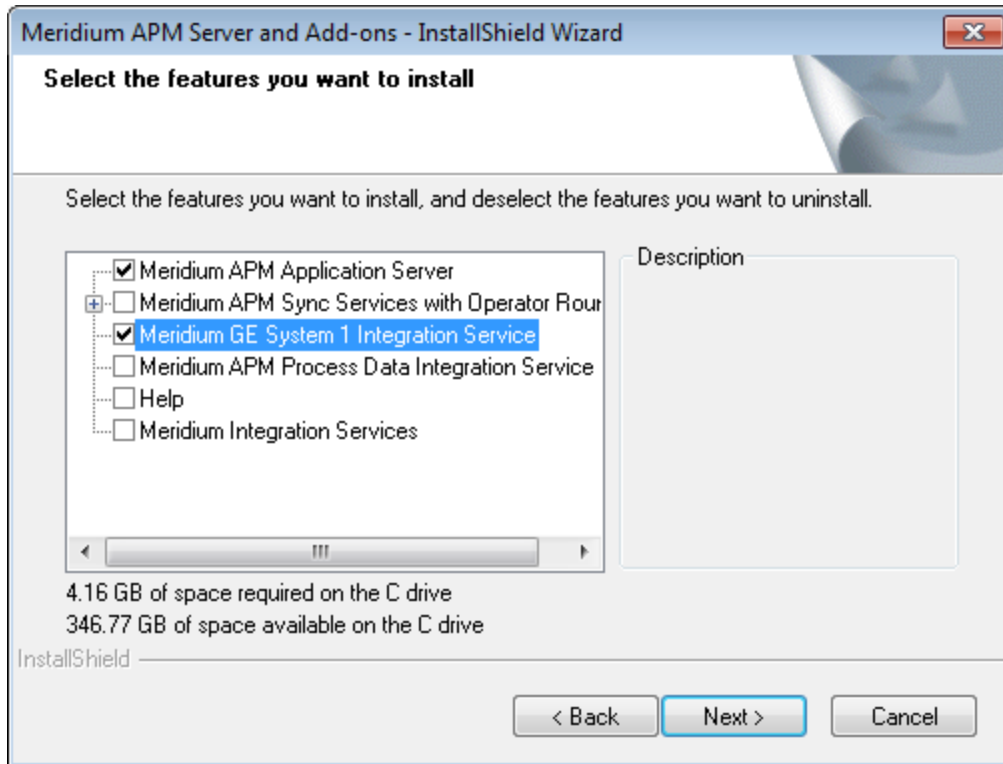
7. Select **Next**.

   The **Complete the Installation** screen appears.

8. Select **Install**.

   The **Installation is Complete** screen appears.

9. Select **Finish**.

   The Meridium APM GE System 1 Integration Service is installed.

What's Next?

Modify the File Meridium.GE.Service.exe.config.

Modify the File Meridium.GE.Service.exe.config

Steps

1. On the machine on which you are configuring the Meridium GE Service, navigate to the folder where the Meridium GE Service is installed. If you installed the software in the default location, you can locate this file in the following location: <root:>\Program Files\Meridium\Services.

2. Open the file **Meridium.GE.Service.exe.config** in an application that you can use to modify XML script (e.g., Notepad).

3. In the file, within the <configuration> tags, locate the following text:

    <apmMqConnections>

4. Within the <apmMqConnections> tags, uncomment the example connection tag by deleting <!--EXAMPLE: and the corresponding --> from the beginning and end of the string.

5. Within the <apmMqConnections> tags, configure the attributes, by replacing the values within the quotation marks with the values detailed in the following chart.

> 📄 **Note**: The client and heartbeat attributes should not be edited.

Attribute	Replace text...	... with the following values:	Notes
server key	KEY	A unique connection key.	None
dataSource	DATA_ SOURCE	Your Meridium Enterprise APM data source.	The data source value is case sensitive and should be typed exactly as it is defined for the Meridium Enterprise APM Server in the Data Sources section of Operations Manager.
host	ENTER_ BROKER_ HOSTNAME	The hostname of the GE Fleet Message Broker.	None

port	5672	The appropriate port for your configuration. • The default SSL port is 5671. • The default HTTP port is 5672, and is the port preconfigured in the config file.	None
user	ENTER_MQ_ USER_NAME	The user name for the Rab-bitMQ Message Broker.	This field is not required if using SSL to connect to the mes-sage broker.
password	ENTER_MQ_ PASSWORD	The password for the Rab-bitMQ Message Broker.	This field is not required if using SSL to connect to the mes-sage broker. ⚠ **Note:** Do not delete the **!** in front of the password. This symbol is not part of the password itself. Instead, this symbol will cause the pass-word to be encrypted automatically when the service is restar-ted.

6. If you are using SSL configuration, configure the attributes, by replacing the values within the quotation marks with the values detailed in the following chart.

Attribute	Replace text...	... with the following val-ues:	Notes
sslEnabled	FALSE	TRUE	None
sslServerName	SSL_ SERVER_ NAME	The Common Name (CN) where the SSL certificate stored.	Typically, this is the host name of the server to which this client will connect.

sslCertPassPhrase	SSL_CERT_PASSWORD	SSL certificate password.	Note: Do not delete the ! in front of the password. This symbol is not part of the password itself. Instead, this symbol will cause the password to be encrypted automatically when the service is restarted.
sslCertPath	PATH_TO_CERT	File path to the directory where the SSL certificate is stored.	The SSL certificate is not supplied by Meridium, Inc. It should be obtained from a third-party certificate authority.
tlsVersions	1.2	The desired encryption algorithm. • The default value is 1.2. • Alternatively, to support multiple algorithms, you can enter multiple values, and then separate the values with a semicolon.	Only tls1.1 and tls1.2 versions are supported.

7. Within the <meridiumconnections> tags, uncomment the example connection tag by deleting <!--EXAMPLE: and the corresponding --> from the beginning and end of the string.

8. Within the <meridiumconnections> tags, configure the attributes by replacing the values within the quotation marks with the values detailed in the following chart.

Attribute	Replace text...	... with the following values:	Notes

connection name	NAME	A name to identify the connection to the database.	This value is used only by the configuration file.
applicationServer	ENTER_ APP_ SERVER	The name of the Meridium Enterprise APM server.	None
datasource	DATA_ SOURCE	The name of the Meridium Enterprise APM data source to which you want to connect.	The data source value is case sensitive and should be typed exactly as it is defined for the Meridium Enterprise APM Server in the Data Sources section of Operations Manager.
userId	ENTER_ USER	The User ID of the Security User whose credentials should be used to log in to the specified Meridium Enterprise APM database.	None
password	ENTER_ PASS	The password for the specified user.	ⓘ **Note:**Do not delete the **!** in front of the password. This symbol is not part of the password itself. Instead, this symbol will cause the password to be encrypted automatically when the service is restarted.

9. Save and close the file.

Results

Your settings will be applied when you start or restart the Meridium GE Service.

What's Next?

[Modify the File Meridium.AMQP.service.exe.config](#).

Import the GE Policies

The following instructions explain how to import Policy records that can be used in GE Analytics. These instructions assume that you have already installed the Meridium Enterprise APM Server software.

Steps

1. Using the Import and Export tool , import the following XML files, one at a time:

    - **GE Event Response.xml**
    - **PLA_Policy.xml**

    These files are located in following location on the Meridium Enterprise APM Server machine: C:\Meridium\DbUpg\MI_DB_Master_<Data-baseVersion>.ZIP\<DatabaseVersion>_IEU_ManualImports\Policy Records, where <DatabaseVersion> is the database version that is currently installed.

    The following policies are now available in Meridium Enterprise APM.

    - GE Event Response Automation Policy
    - GE Production Event Policy - Equip or FLOC Cause
    - GE Production Event Policy - Equip Cause Only

GE Analytics 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 GE Administrator	MI Health Admin
MI GE User	MI Health User MI Health Power
MI GE Viewer	None

> 🛈 **Note**: The Security Groups listed in the table above account only for family permissions. Users must also be added to the MI Configuration Role Security Group in order to access the Systems and Tags page, which is required to modify families used by this module.

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

Family	MI GE Administrator	MI GE User	MI GE Viewer
Entity Families			
GE Connection	View, Update, Insert, Delete	View	View
GE Enterprise	View, Update, Insert, Delete	View	View
GE Filter	View, Update, Insert, Delete	View	View
GE Tag	View, Update, Insert, Delete	View	View
GE Tag Event	View, Update, Insert, Delete	View	View

Relationship Families			
Has Consolidated Events	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has GE Enterprise	View, Update, Insert, Delete	View	View
Has GE Filter	View, Update, Insert, Delete	View	View
Has Tag	View, Update, Insert, Delete	View	View
Has Tag Event	View, Update, Insert, Delete	View	View

Deploy Generation Availability Analysis (GAA)

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 Generation Availability Analysis (GAA) 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 Meridium Enterprise 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.

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	Define Functional Location.	This step is required only if the functional location is not already available. If not already available, you *must* define functional location before adding a GAA Company, GAA Plant, or GAA Unit.
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.

Step	Task	Notes
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.
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 Generation Availability Analysis (GAA) to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Generation Availability Analysis (GAA) 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 GAA Viewer	MI GAA Administrator MI GAA Analyst MI GAA Operator MI GAA Supervisor
MI GAA Administrator	MI GAA Administrator
MI GAA Analyst	MI GAA Analyst MI GAA Operator MI GAA Supervisor

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

Family	MI GAA Viewer	MI GAA Administrator	MI GAA Analyst
Entity Families			
APM Event	View	View, Update, Insert, Delete	View, Update, Insert
Associated with APM Event	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Capacity Incident	View	View, Update, Insert, Delete	View, Update, Insert

Family	MI GAA Viewer	MI GAA Administrator	MI GAA Analyst
Contributing Event	View	View, Update, Insert, Delete	View, Update, Insert
GAA Company	View	View, Update, Insert, Delete	View
GAA Performance	View	View, Update, Insert, Delete	View, Update, Insert
GAA Plant	View	View, Update, Insert, Delete	View
GAA Unit	View	View, Update, Insert, Delete	View
GAA Report	View	View, Update, Insert, Delete	View
GAA Report Details	View	View, Update, Insert, Delete	View, Update, Insert
GAA Unit Capacity	View	View, Update, Insert, Delete	View
GADS Amplification Codes	View	View, Update, Insert, Delete	View, Update, Insert
GADS Cause Codes	View	View, Update, Insert, Delete	View
Heating Value Ranges	View	View, Update, Insert, Delete	View, Update, Insert
Primary Event	View	View, Update, Insert, Delete	View, Update, Insert
Primary Event Details	View	View, Update, Insert, Delete	View, Update, Insert, Delete
RCA Analysis	View	View	View
Reference Document	View	View, Update, Insert, Delete	View, Update, Insert
Relationship Families			
Accumulates Capacity Incident	View	View, Update, Insert, Delete	Update, Insert, Delete

Family	MI GAA Viewer	MI GAA Administrator	MI GAA Analyst
Functional Location Has Generation Company	View	View, Update, Insert, Delete	View
Functional Location Has Generation Plant	View	View, Update, Insert, Delete	View
Functional Location Has Generation Unit	View	View, Update, Insert, Delete	View
Has Capacity History	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Incident	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Plant	View	View, Update, Insert, Delete	View
Has Reference Documents	View	View, Update, Insert, Delete	View, Update, Insert
Has Unit	View	View, Update, Insert, Delete	View
Primary Incident Has RCA	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Unit Has Record	View	View, Update, Insert, Delete	View

Deploy Hazards Analysis

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 Hazards Analysis 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 Meridium Enterprise 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.

Step	Task	Notes
1	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.
2	Assign the desired Security Users to one or more Hazards Analysis Security Groups in Configuration Manager.	This step is required. Users will not be able to access Hazards Analysis unless they have permissions to the Hazards Analysis families.
3	Define alternate search queries.	This step is required only if you do not want to use the baseline search queries.
4	Manage the types of Deviations in a HAZOP Analysis. To do so, add a code to the MI_HAZOP_ DEVIATIONS system code table.	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.
5	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.
6	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

Upgrade or Update Hazards Analysis to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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	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.	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.	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 V3.6.1.2.0

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.	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 V3.6.0.12.4

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.	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 V3.5.1.12.0

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.	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 V3.5.0.1.9.0

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.	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.	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.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

Hazards Analysis 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 HA Administrator	MI Safety Admin
MI HA Owner	MI Safety Admin
	MI Safety Power
MI HA Facilitator	MI Safety Admin
	MI Safety Power
	MI Safety User
MI HA Member	MI Safety Admin
	MI Safety Power
	MI Safety User

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

Family	MI HA Administrator	MI HA Owner	MI HA Facilitator	MI HA Member
Entity Families				
Alert	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	None
Consequence	View, Update, Insert, Delete	View	View	View
Equipment	View	View	View	View

Family	MI HA Admin-istrator	MI HA Owner	MI HA Facilitator	MI HA Member
Functional Loca-tion	View	View	View	View
Hazards Analysis	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Hazards Analysis Cause	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Hazards Analysis Consequence	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Hazards Analysis Safeguard	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Hazards Analysis System/Node	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
HAZOP Deviation	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Human Resource	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Independent Pro-tection Layer	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Instrumented Func-tion	View	View	View	View

Family	MI HA Admin-istrator	MI HA Owner	MI HA Facilitator	MI HA Member
Probability	View, Update, Insert, Delete	View	View	View
Protection Level	View, Update, Insert, Delete	View, Insert	View, Insert	View, Insert
Reference Document	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Risk Assessment	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Risk Assessment Recommendation	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Risk Category	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Risk Matrix	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Risk Rank	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Risk Threshold	View, Update, Insert, Delete	View	View	View
Site Reference	View	View	View	View
What If	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Relationship Families				

Family	MI HA Admin-istrator	MI HA Owner	MI HA Facilitator	MI HA Member
Analysis Has Human Resource	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Cause Has Con-sequence	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Cause Revision Has Consequence Revision	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Consequence Has Safeguard	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Consequence Revision Has Safe-guard Revision	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Deviation\What If Has Cause	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Deviation\What If Revision Has Cause Revision	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Equipment Has Equipment	View	View	View	View
Functional Loca-tion Has Equip-ment	View	View	View	View
Functional Loca-tion Has Func-tional Location	View	View	View	View

Family	MI HA Admin- istrator	MI HA Owner	MI HA Facilitator	MI HA Member
Has Hazards Ana- lysis Revision	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has HAZOP Refer- ence	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has IF	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Functional Location	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Recom- mendations	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Reference Documents	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Reference Val- ues	View, Update, Insert, Delete	View	View	View
Has Risk	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Risk Category	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Risk Matrix	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI HA Admin-istrator	MI HA Owner	MI HA Facilitator	MI HA Member
Has Site Refer-ence	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Hazards Analysis Has Assets	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Hazards Analysis Revision Has Sys-tems/Nodes Revi-sion	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Is Independent Pro-tection Layer	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Mitigates Risk	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Safety Analysis Has Equipment	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Safeguard Revi-sion Has IPL Revi-sion	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System/Node Has Deviations/What Ifs	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System/Node Has Deviations/What Ifs Revision	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View

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 module.

Deploy Inspection Management 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 Meridium Enterprise 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.

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	Assign Security Users to one or more of the Inspection Management Security Groups and Roles.	This step is required. Security Users will need permissions to the Inspection Management families before they can use the Inspection Management features.
3	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.
4	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* sub-families.

5	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.
6	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.
7	Assign certifications to users.	This step is optional.
8	Group inspection work into Work Packs.	This step is optional.
9	Define Time-Based Inspection settings.	This step is optional.

Upgrade or Update Inspection Management to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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	Revert the My Open Inspections Query to baseline.	This step is required only if you have previously 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. ⓘ **Tip**: 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.

Upgrade from any version V4.0.0.0 through V4.0.1.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the

basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

Step	Task	Notes
1	Define Time-Based Inspection settings.	This step is optional.

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.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	If you have added System Codes to the MI_INSPECTION_TYPE System Code Table, 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.

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

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

Family	MI Inspection
Entity Families	
Alert	View, Insert, Update, Delete
Certification	View, Insert, Update, Delete
Checklist Finding	View, Insert, Update, Delete
Conditional Alerts	View, Insert, Update, Delete
Corrosion	View, Insert, Update, Delete
Equipment	View, Insert, Update, Delete
Event	View, Insert, Update, Delete
Finding	View, Insert, Update, Delete
Human Resource	View
Inspection Method	View, Insert, Update, Delete
Inspection Profile	View, Insert, Update, Delete
Inspection Team Member	View, Insert, Update, Delete

Family	MI Inspection
Potential Degradation Mechanisms	View
RBI Degradation Mechanisms	View
Recommendation	View, Insert, Update, Delete
Reference Document	View, Insert, Update, Delete
Resource Role	View, Insert, Update, Delete
SAP System	View
Security User	View
Strategy	View, Update
Task	View, Insert, Update, Delete
Taxonomy References	View
Time Based Inspection Interval	View, Insert, Update, Delete
Time Based Inspection Setting	View, Insert, Update, Delete
Work Pack	View, Insert, Update, Delete
Relationship Families	
Belongs to a Unit	View, Update, Insert, Delete
Checklist Has Finding	View, Insert, Update, Delete
Has Certifications	View, Insert, Update, Delete
Has Degradation Mechanisms	View
Has Findings	View, Insert, Update, Delete
Has Inspection Method	View, Insert, Update, Delete
Has Inspection Profile	View, Insert, Update, Delete
Has Inspection Scope	View, Insert, Update, Delete
Has Inspections	View, Insert, Update, Delete
Has Potential Degradation Mechanisms	View
Has Recommendations	View, Insert, Update, Delete
Has Reference Documents	View, Insert, Update, Delete
Has Roles	View, Insert, Update, Delete

Family	MI Inspection
Has Sub-Inspections	View, Insert, Update, Delete
Has Tasks	View, Insert, Update, Delete
Has Task History	View, Insert
Has Task Revision	View, Insert
Has Team Member	View, Insert, Update, Delete
Has Taxonomy Hierarchy Element	View
Has Taxonomy Mapping	View
Has Time Based Inspection Interval	View, Insert, Update, Delete
Has Work Pack	View, Update, Insert, Delete
Is a User	View
Is Planned By	View, Insert, Update, Delete
Is Executed By	View, Insert, Update, Delete

> **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 Meridium Enterprise 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.

Deploy Life Cycle Cost Analysis (LCC)

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 Life Cycle Cost Analysis (LCC) 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 Meridium Enterprise 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.

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 Life Cycle Cost Analysis (LCC) to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Life Cycle Cost Analysis Security Groups and Roles

> 🗋 **Note**: To import a Production Event from Production Loss Analysis, you must be a member of the MI Production Loss Accounting User Security Group. To import a Strategy Action, you must be a member of the MI ASM Viewer Security Group.

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 User MI LCC Viewer	MI Strategy User
MI LCC User	MI Strategy Power

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

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

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

Deploy Metrics and Scorecards

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 Metrics and Scorecards 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 Meridium Enterprise 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.

Step	Task	Notes
1	Deploy SQL Server Analysis Services 2012 or Microsoft SQL Server Analysis Services 2014. 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: a. Install SQL Server Analysis Services. b. Deploy the Work History Analysis Services database. This Work History cube is a replacement for *Meridium_Event_Analysis* database, and *Equipment and Functional Location Work History* cubes delivered as packaged solution. c. 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 Meridium Enterprise 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) d. Add the user created in Step c to a role on all SQL Analysis Services databases you want to access in Meridium Enterprise 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 doc-	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
	umentation regarding Roles and Permissions for Analysis Services. e. 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 documentation regarding configuring the HTTP access to Analysis Services on Internet Information Service (IIS).	
2	Verify that your event and asset criticality data meet the standard classification requirements, and modify the views 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 Meridium Enterprise 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 optional.
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 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Metrics and Scorecards will be upgraded to V4.2.0.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. However, to upgrade Metric Views, ensure that the user running the upgrade utility has read permissions on the cubes associated with Metric Views and that the cubes are active. Additionally, you need to perform the following steps.

Step	Task	Notes
1	Deploy the new Work History cube.	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 Work History cube, with minor modifications to SQL views used by the cube, the cube can still 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.

Step	Task	Notes
3	Verify that your event and asset criticality data meet the standard classification requirements, and modify the views for the Work History cube as needed.	This step is required.
4	Localize the event and equipment values in the Meridium Enterprise 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

Metrics and Scorecards will be upgraded to V4.2.0.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. However, to upgrade Metric Views, ensure that the user running the upgrade utility has read permissions on the cubes associated with Metric Views and that the cubes are active. Additionally, you need to perform the following steps.

Step	Task	Notes
1	Deploy the new Work History cube.	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 Work History cube, with minor modifications to SQL views used by the cube, the cube can still work with the non-standard event and equipment data.

Step	Task	Notes
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 views for the Work History cube as needed.	This step is required.
4	Localize the event and equipment values in the Meridium Enterprise 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 V3.6.1.2.0

Metrics and Scorecards will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. However, to upgrade Metric Views, ensure that the user running the upgrade utility has read permissions on the cubes associated with Metric Views and that the cubes are active. Additionally, you need to perform the following steps.

Step	Task	Notes
1	Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: • 2012 • 2014	This step is required only if you were previously using SQL Server Analysis Services 2008 R2.

Step	Task	Notes
2	Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication.	This step is required.
3	a. Deploy Work History Analysis Services database. This Work History cube is a replacement of *Meridium_Event_Analysis* database, and *Equipment and Functional Location Work History* cubes delivered as packaged solution. b. 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 Meridium Enterprise 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. Ex: meridium_ssas_user. c. Add the user created in step b to a role on all SQL Analysis Services databases that you want to access in Meridium Enterprise 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.
4	Verify that your event and asset criticality data meet the standard classification requirements, and modify the views for the Work History cube as needed.	This step is required.

Step	Task	Notes
6	[Localize the event and equipment values in Meridium Enterprise APM](#).	Required only if you want to localize the event and equipment values in the Work History cube.
7	[Schedule cubes for processing](#) on the SQL Server Analysis Server.	This step is required.
8	Update the existing Analysis Services Cube records so that Meridium Enterprise APM connects to the cube using the HTTP/ HTTPS access.	This step is required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

Metrics and Scorecards will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. However, to upgrade Metric Views, ensure that the user running the upgrade utility has read permissions on the cubes associated with Metric Views and that the cubes are active. Additionally, you need to perform the following steps.

Step	Task	Notes
1	Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: • 2012 • 2014	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	a. Deploy Work History Analysis Services database. This Work History cube is a replacement of *Meridium_Event_Analysis* database, and *Equipment and Functional Location Work History* cubes delivered as packaged solution. b. 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 Meridium Enterprise 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. Ex: meridium_ssas_user. c. Add the user created in step b to a role on all SQL Analysis Services databases that you want to access in Meridium Enterprise 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.
4	Verify that your event and asset criticality data meet the standard classification requirements, and modify the views for the Work History cube as needed.	This step is required.
6	Localize the event and equipment values in Meridium Enterprise APM.	Required only if you want to localize the event and equipment values in the Work History cube.

Step	Task	Notes
7	[Schedule cubes for processing](#) on the SQL Server Analysis Server.	This step is required.
8	Update the existing Analysis Services Cube records so that Meridium Enterprise APM connects to the cube using the HTTP/ HTTPS access.	This step is required.

Upgrade from any version V3.5.1 through V3.5.1.12.0

Metrics and Scorecards will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. However, to upgrade Metric Views, ensure that the user running the upgrade utility has read permissions on the cubes associated with Metric Views and that the cubes are active. Additionally, you need to perform the following steps.

Step	Task	Notes
1	Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: • 2012 • 2014	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	a. Deploy Work History Analysis Services database. This Work History cube is a replacement of *Meridium_Event_Analysis* database, and *Equipment and Functional Location Work History* cubes delivered as packaged solution. b. 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 Meridium Enterprise 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. Ex: meridium_ssas_user. c. Add the user created in step b to a role on all SQL Analysis Services databases that you want to access in Meridium Enterprise 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.
4	Verify that your event and asset criticality data meet the standard classification requirements, and modify the views for the Work History cube as needed.	This step is required.
6	Localize the event and equipment values in Meridium Enterprise APM.	Required only if you want to localize the event and equipment values in the Work History cube.

Step	Task	Notes
7	[Schedule cubes for processing](#) on the SQL Server Analysis Server.	This step is required.
8	Update the existing Analysis Services Cube records so that Meridium Enterprise APM connects to the cube using the HTTP/ HTTPS access.	This step is required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

Metrics and Scorecards will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. However, to upgrade Metric Views, ensure that the user running the upgrade utility has read permissions on the cubes associated with Metric Views and that the cubes are active. Additionally, you need to perform the following steps.

Step	Task	Notes
1	Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: • 2012 • 2014	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	a. Deploy Work History Analysis Services database. This Work History cube is a replacement of *Meridium_Event_Analysis* database, and *Equipment and Functional Location Work History* cubes delivered as packaged solution. b. 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 Meridium Enterprise 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. Ex: meridium_ssas_user. c. Add the user created in step b to a role on all SQL Analysis Services databases that you want to access in Meridium Enterprise 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.
4	Verify that your event and asset criticality data meet the standard classification requirements, and modify the views for the Work History cube as needed.	This step is required.
5	Localize the event and equipment values in Meridium Enterprise APM.	Required only if you want to localize the event and equipment values in the Work History cube.

Step	Task	Notes
6	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.
7	Update the existing Analysis Services Cube records so that Meridium Enterprise 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

Metrics and Scorecards will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. However, to upgrade Metric Views, ensure that the user running the upgrade utility has read permissions on the cubes associated with Metric Views and that the cubes are active. Additionally, you need to perform the following steps.

Step	Task	Notes
1	Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: • 2012 • 2014	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	a. Deploy Work History Analysis Services database.
	
	This Work History cube is a replacement of *Meridium_Event_Analysis* database, and *Equipment and Functional Location Work History* cubes delivered as packaged solution.
	
	b. 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 Meridium Enterprise 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. Ex: meridium_ssas_user.
	
	c. Add the user created in step b to a role on all SQL Analysis Services databases that you want to access in Meridium Enterprise 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.

4	Verify that your event and asset criticality data meet the standard classification requirements, and modify the views for the Work History cube as needed.	This step is required.
5	Localize the event and equipment values in Meridium Enterprise APM.	Required only if you want to localize the event and equipment values in the Work History cube.

Step	Task	Notes
6	[Schedule cubes for processing](#) on the SQL Server Analysis Server.	This step is required.
7	Update the existing Analysis Services Cube records so that Meridium Enterprise 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

Metrics and Scorecards will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. However, to upgrade Metric Views, ensure that the user running the upgrade utility has read permissions on the cubes associated with Metric Views and that the cubes are active. Additionally, you need to perform the following steps.

Step	Task	Notes
1	Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: • 2012 • 2014	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	a. Deploy Work History Analysis Services database. This Work History cube is a replacement of *Meridium_Event_Analysis* database, and *Equipment and Functional Location Work History* cubes delivered as packaged solution. b. 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 Meridium Enterprise 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. Ex: meridium_ssas_user. c. Add the user created in step b to a role on all SQL Analysis Services databases that you want to access in Meridium Enterprise 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.
4	Verify that your event and asset criticality data meet the standard classification requirements, and modify the views for the Work History cube as needed.	This step is required.
5	Localize the event and equipment values in Meridium Enterprise APM.	Required only if you want to localize the event and equipment values in the Work History cube.

Step	Task	Notes
6	[Schedule cubes for processing](#) on the SQL Server Analysis Server.	This step is required.
7	Update the existing Analysis Services Cube records so that Meridium Enterprise 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 usage of users in your system. Usage metrics are stored in the MI_USAGE_ METRICS system table. When a user logs in to Meridium Enterprise APM, actions for which usage metrics tracking has been enabled will be stored for that session and saved in batch to the MI_USAGE_METRICS table when the user logs out of Meridium Enterprise APM.

The following actions can be recorded in the MI_USAGE_METRICS table:

- Login.
- Logout.
- Session time.
- URL visit.

The following columns of data are stored in the MI_USAGE_METRICS table:

- **USME_KEY**: The key value assigned to the action to identify it in the usage metrics table.
- **USME_EVENT_TYPE_DVD**: The type of event (login, logout, session time, or URL visit).
- **SEUS_KEY**: The key value associated with the Security User who performed the action.
- **USME_EVENT_DT**: The date and time the action was performed.
- **USME_EVENT_DESC_TX**: A description of the action. For URL visits, this column stores the URL.
- **USME_MEASR_NBR**: For session time entries, a numeric value that represents the session time.

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

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

Note: Before you can 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 Meridium Enterprise APM Metrics and Scorecards module because it serves as a storage and management mechanism for cubes, which can then be accessed and viewed via the Meridium Enterprise 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 Meridium Enterprise 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 Meridium, Inc. or from a third-party vendor, depending upon the licensing options you selected when you purchased the Meridium Enterprise 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 Meridium Enterprise APM system. For details on completing these tasks, consult your SQL Server documentation.

Migrate SQL Server Cubes

If you are upgrading from a previous version of Meridium Enterprise 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 Meridium Enterprise APM objects.

- If you have SQL Server Server 2008 cubes, you must migrate them to SQL Server 2012.

- If you have SQL Server 2012 cubes, you can migrate them to SQL Server 2014.

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.

Steps

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 text 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 cell, 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 cell, 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 Meridium Enterprise 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 Scorecard 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

Steps

1. Create a copy of the **Cubes** folder from the Release CD to a folder in SQL Server Analysis Services Server.

2. In the copied **Cubes** folder, select the **Work History** folder.

   The folder contains following files:

   - Work History.asdatabase
   - Work History.configsettings
   - Work History.deploymentoptions
   - Work History.deploymenttargets

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 file **Work History.asdatabase**.

6. Run through all steps of the wizard to deploy the Work History database to SQL Server Analysis Services Server.

   For more information, consult 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 Views for Work History Cube

If the event or asset criticality data in your database does not match the standard IDs used by the Work History cube, then you need to modify the views used for the Work History cube.

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.

Modify the Non Standard Event Type Data

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 Breakdown Data

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 Event Priority Data

1. In the **Views**, select MIV_MI_FAC_WORK_HSTY view, and then run the following queries to check if the Event Breakdown 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

1. In the **Views**, select MIV_MI_FAC_WORK_HSTY view, and then run the following queries to check if the Event Breakdown 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 Equipment Criticality Data

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 event detection method 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 event detection method 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 Equipment Criticality Data

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 event detection method 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
```

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 Meridium Enterprise APM. The examples in this topic explain how to modify event and asset criticality values, and how you can verify, in Meridium Enterprise 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

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 the Meridium Enterprise 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 appear.

7. In the **Event Type**, select **Event Type-Breakdown**, and then select **Event Type**.

   The caption for the event type values appears in the language to which you have modified.
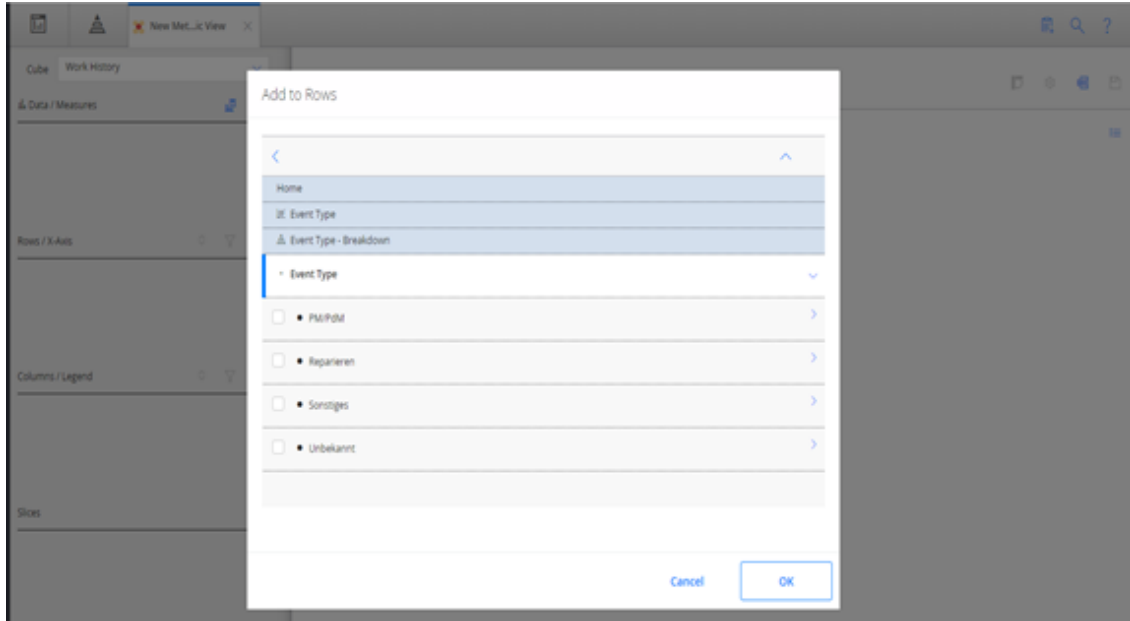
Example: Localize the Event Breakdown Values

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 the Meridium Enterprise 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 View design page, in **Rows/X-Axis** subsection, select +.

   The **Add to Rows** window appear.

7. In the **Event Type**, select **Event Type-Breakdown** and then select **Breakdown**.

   The caption for the event breakdown values appear in the language to which you have modified.
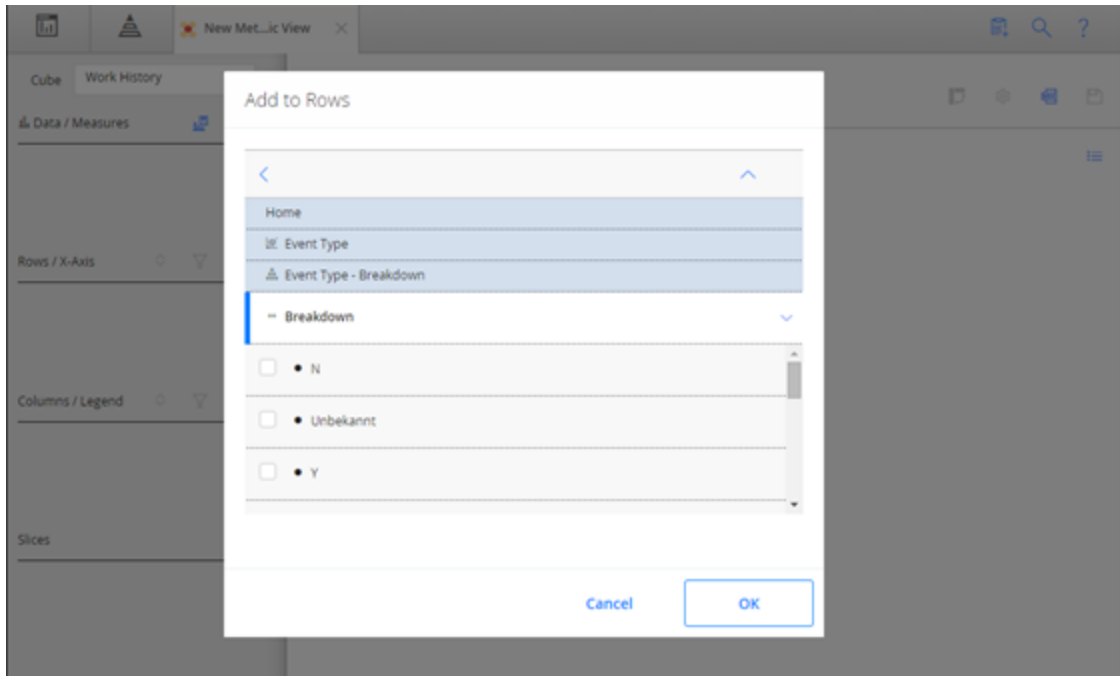
Example: Localize the Event Priority Values
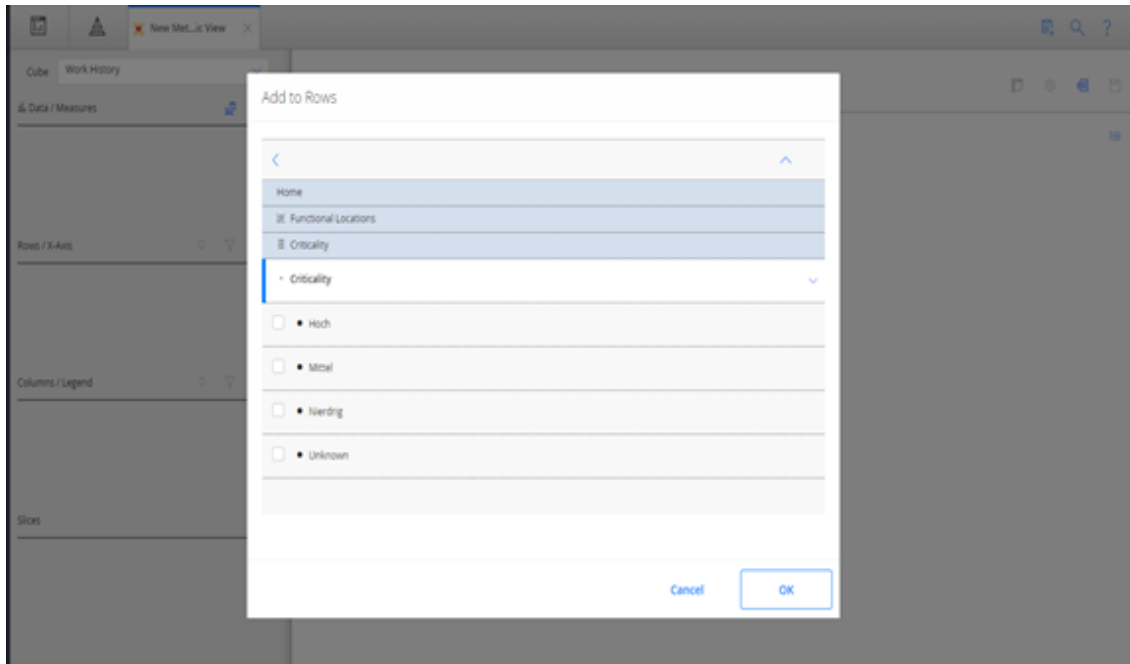
1. In the **Tables**, select the table MI_DIM_EVENT_PRIORITY.

   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 loc-alize, and then manually modify the caption.

3. Save the modification and then process the cube.

4. Log in to the Meridium Enterprise 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 View design page, in **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 event priorities appear in the language to which it was modified.
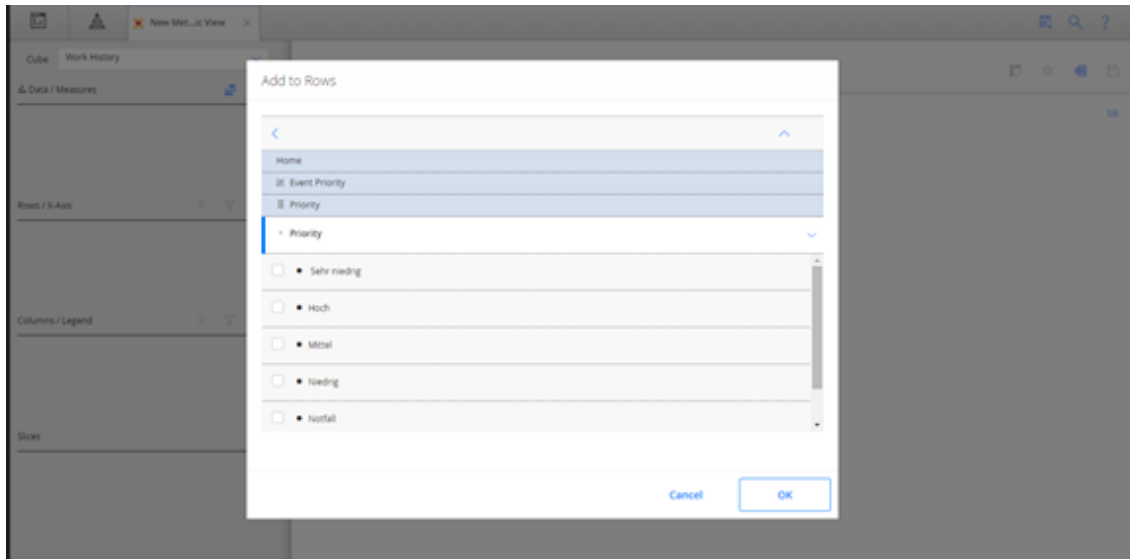
Example: Localize Event Detection Method Values

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 the detection method that you want to localize, and then manually modify the caption.

3. Save the modifications and then process the cube.

4. Log in to the Meridium Enterprise APM application.

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 View design page, in **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.
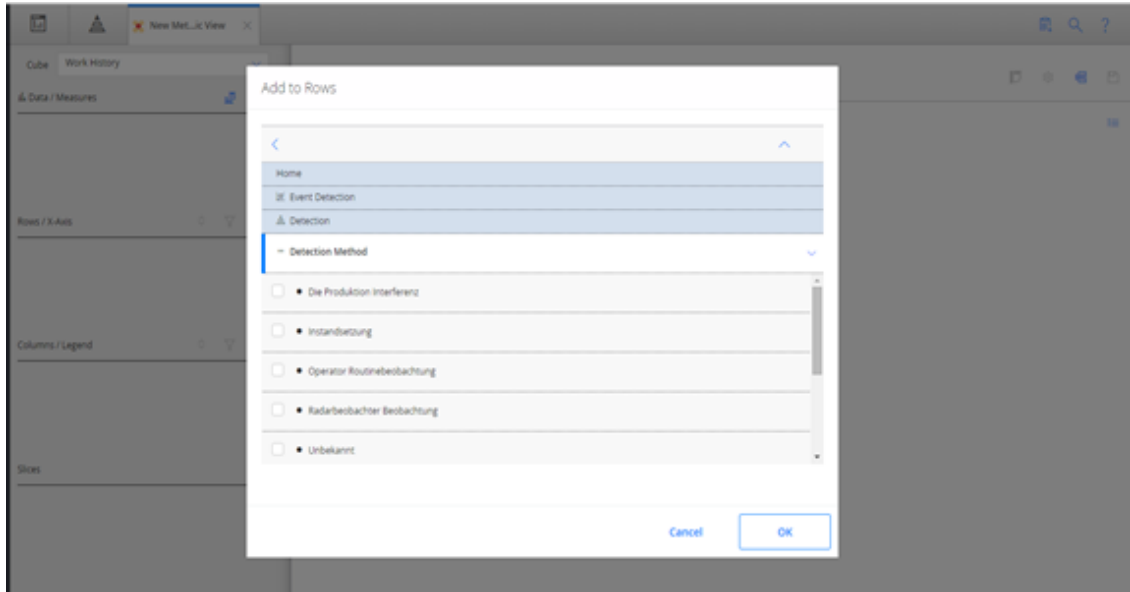
Example: Localize Equipment Criticality Values

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 modifications and then process the cube.

4. Log in to the Meridium Enterprise 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 View design page, in **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.
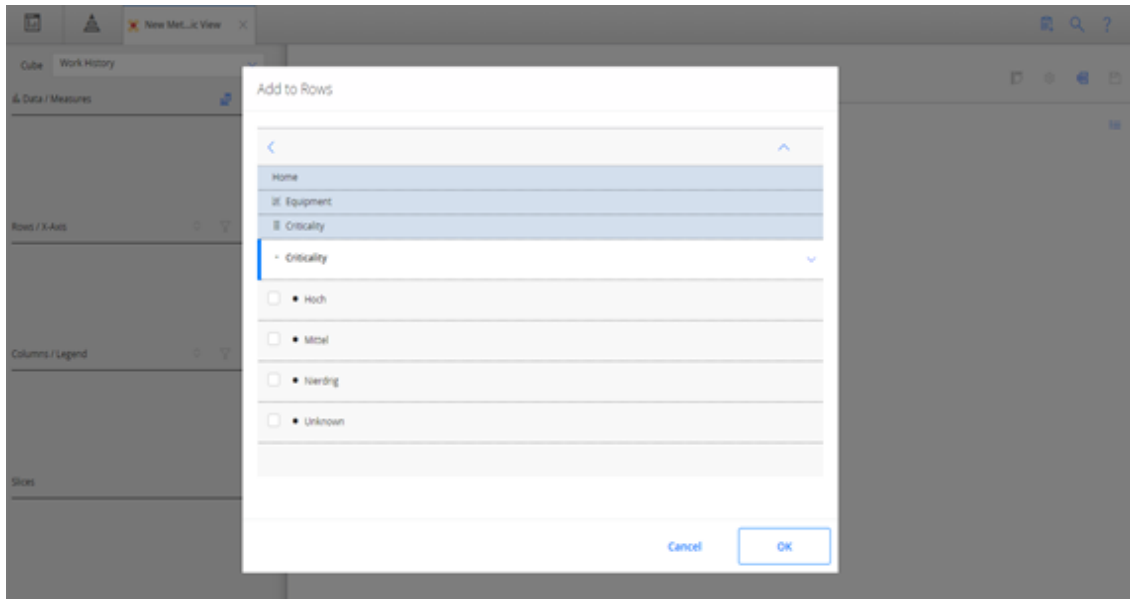
Example: Localize Functional Location Criticality Values

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 modifications and then process the cube.

4. Log in to the Meridium Enterprise 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 View design page, in **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.

Metrics and Scorecards 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 Metrics Administrator	MI Foundation Admin MI APMNow Admin
MI Metrics User	MI Foundation Power MI Foundation User
Everyone	MI Foundation Admin MI Foundation Power MI Foundation User

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

Family	MI Metrics Administrator	MI Metrics User	Everyone
Entity Families			
Analysis Services Cube	View, Update, Insert, Delete	View	View
KPI	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
KPI Measurement	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Scorecard	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Relationship Families			

Family	MI Metrics Administrator	MI Metrics User	Everyone
Has KPI Measurement	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Privileges	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Sub Indicators	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Is Used By Scorecard	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete

In addition to performing functions associated with the family-level privileges described in this table, members of the MI Metrics Administrator Security Group:

- Can manage cube privileges by granting view access to the users.
- Has full access to all KPIs, Scorecards, and Cubes without needing to be granted additional privileges via the Meridium Enterprise APM.

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

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 Meridium Enterprise 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.

Step	Task	Notes
1	Assign Security Users to one or more of the Policy Designer Security Groups and Roles.	This step is required.
2	On the Meridium Enterprise APM Server, start the Policy Execution Service.	This step is required. If your system architecture contains more than one Meridium Enterprise APM Server, you must complete this step for every server in the load-balanced cluster that you want to use for policy execution. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
3	On the Meridium Enterprise APM Server, start the Policy Trigger Service.	This step is required. If your system architecture contains more than one Meridium Enterprise APM Server, you must configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
4	On the Meridium Enterprise APM Server, reset IIS.	This step is required.
5	On the Meridium Process Data Integration Server, start or restart the Process Data Integration Service.	This step is required only if you want to use OPC Tag records in your policies.

Upgrade or Update Policy Designer to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

If your system architecture contains multiple servers to process policy executions, these steps assume that you have configured them according to your company's preference for server load-balancing.

Update from version V4.2.0.0 through V4.2.0.6.0

Step	Task	Notes
1	On the Meridium Enterprise APM Server, start or restart the Policy Execution Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
2	On Meridium Enterprise APM Server, start or restart the Policy Trigger Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
3	On the Meridium Enterprise APM Server, reset IIS.	This step is required.
4	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required *only* if you want to use OPC Tag records in your policies.

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	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: | Custom (incorrect)	Baseline (correct)
---	---
Accepted by ASM	Completed
Closed	Completed
Consolidated	Superseded
Open	Proposed
Pending	Pending Approval
Superseded	Superseded		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 Meridium Enterprise 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
2	On the Meridium Enterprise APM Server, start or restart the Policy Execution Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
3	If your system architecture contains more than one Meridium Enterprise APM Server, you must configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution.	This step is required.

Step	Task	Notes
4	Start or restart the Policy Trigger Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
5	On the Meridium Enterprise APM Server, reset IIS.	This step is required.
6	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required *only* if you want to use OPC Tag records in your policies.

Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	On the Meridium Enterprise APM Server, start or restart the Policy Execution Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
2	If your system architecture contains more than one Meridium Enterprise APM Server, you must configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution.	This step is required.
3	Start or restart the Policy Trigger Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
4	On the Meridium Enterprise APM Server, reset IIS.	This step is required.

Step	Task	Notes
5	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required *only* if you want to use OPC Tag records in your policies.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

Step	Task	Notes
1	On the Meridium Enterprise APM Server, start or restart the Policy Execution Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
2	If your system architecture contains more than one Meridium Enterprise APM Server, you must configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution.	This step is required.
3	Start or restart the Policy Trigger Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
4	On the Meridium Enterprise APM Server, reset IIS.	This step is required.
5	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required *only* if you want to use OPC Tag records in your policies.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

Step	Task	Notes
1	On the Meridium Enterprise APM Server, start or restart the Policy Execution Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
2	If your system architecture contains more than one Meridium Enterprise APM Server, you must configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution.	This step is required.
3	Start or restart the Policy Trigger Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
4	On the Meridium Enterprise APM Server, reset IIS.	This step is required.
5	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required *only* if you want to use OPC Tag records in your policies.

Upgrade from any version V3.5.1 through V3.5.1.12.0

Step	Task	Notes
1	On the Meridium Enterprise APM Server, start or restart the Policy Execution Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.

Step	Task	Notes
2	If your system architecture contains more than one Meridium Enterprise APM Server, you must configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution.	This step is required.
3	Start or restart the Policy Trigger Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
4	On the Meridium Enterprise APM Server, reset IIS.	This step is required.
5	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required *only* if you want to use OPC Tag records in your policies.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

Step	Task	Notes
1	On the Meridium Enterprise APM Server, start or restart the Policy Execution Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
2	If your system architecture contains more than one Meridium Enterprise APM Server, you must configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution.	This step is required.

Step	Task	Notes
3	Start or restart the Policy Trigger Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
4	On the Meridium Enterprise APM Server, reset IIS.	This step is required.
5	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required *only* if you want to use OPC Tag records in your policies.

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	On the Meridium Enterprise APM Server, start or restart the Policy Execution Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
2	If your system architecture contains more than one Meridium Enterprise APM Server, you must configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution.	This step is required.
3	Start or restart the Policy Trigger Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
4	On the Meridium Enterprise APM Server, reset IIS.	This step is required.

Step	Task	Notes
5	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required *only* if you want to use OPC Tag records in your policies.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	On the Meridium Enterprise APM Server, start or restart the Policy Execution Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
2	If your system architecture contains more than one Meridium Enterprise APM Server, you must configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution.	This step is required.
3	Start or restart the Policy Trigger Service.	This step is required. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
4	On the Meridium Enterprise APM Server, reset IIS.	This step is required.
5	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	This step is required *only* if you want to use OPC Tag records in your policies.

About the Asset Health Services

When you deploy the Asset Health Manager, Process Data Integration, 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 following topics:

- [Deploying Asset Health Manager (AHM) for the First Time](#)
- [Deploying Policy Designer for the First Time](#)
- [Deploying Process Data Integration (PDI) for the First Time](#)

Services Summary

The following services are used by the Asset Health Manager, Process Data Integration, 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 (e.g., an OPC 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 (i.e., an associated record in the Meridium Enterprise 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. The Policy Trigger Service monitors this queue and sends these messages to an appropriate policy execution queue.
- **Policy Execution Service:** The Meridium Enterprise APM Policy Execution Service handles the execution of policies. Specifically, the Policy Execution Service monitors a corresponding policy execution queue and executes the policies that are added to it.
- **Process Data Integration (PDI) Service:** Monitors the subscribed tags (i.e., tags that are used in policies and health indicators or tags for which readings are being stored in the Meridium 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.

Example: Standard System Architecture Configuration

The following diagram illustrates the machines in the Meridium Enterprise APM system architecture when the Policy Designer, Process Data Integration (PDI), and Asset Health Manager

(AHM) modules are used together. This image depicts the standard configuration, where the OPC Server software and the Process Data Integration 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 Meridium Enterprise APM Servers, multiple OPC Servers, or multiple Meridium Enterprise 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, Policy Designer, and Process Data Integration.

Machine	Software Installed	Asset Health Service Installed Automatically with Service Software
Meridium Enterprise APM Server	Meridium Enterprise APM Server software	Asset Health Indicator Service
		Policy Trigger Service
		Policy Execution Service
Process Data Integration Server, which also acts as the OPC Server	Process Data Integration Service software	Process Data Integration Service
	OPC Server software	NA
Process Historian	Process historian software	NA

About Configuring 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. 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 records or reading values associated with the policy are updated, the Meridium Enterprise APM Server adds messages to the policy trigger queue. The Policy Trigger Service monitors the trigger queue and sends any messages to the appropriate policy execution queue. Finally, the corresponding Policy Execution Service executes the policies associated with the records or reading values that were updated.

Scheduled Execution

When a policy is due, the scheduled job adds a message to the policy trigger queue. The Policy Trigger Service monitors the trigger queue and sends messages to the appropriate policy execution queue. Finally, the corresponding Policy Execution Service executes the policies that are due.

Configure the Policy Trigger Service

Steps

1. On the Meridium Enterprise APM Server, navigate to the folder where the Policy Trigger Service files are installed. If you installed the software in the default location, you can locate this file in the folder **C:\Program Files\Meridium\Services**.

2. Open the file **Meridium.Policies.Service.exe.config** in an application that you can use to modify XML script (e.g., Notepad).

3. Within the **<executionServers>** tags, locate the following text:

```
<add url="http://localhost/Meridium" />
```

4. Within the **add url** attribute:
   - If you have only one Meridium Enterprise APM Server in your system architecture, accept the default value (i.e., *localhost*).

     -or-

   - If you have more than one Meridium Enterprise APM Server in your system architecture, replace **localhost** with the name of the server cluster that you want to use for policy executions.

5. Save and close the file.

   Your settings will be applied when the Policy Trigger Service is started or restarted.

Configure Multiple Meridium Enterprise APM Servers for Policy Execution

Depending on the number of policies that you need to manage in your system, you may have multiple Meridium Enterprise APM Servers to process policy executions. Based on your company's preference for server load balancing, you can configure your Meridium Enterprise APM System Architecture using *global* load balancing or *isolated* load balancing.

Regardless of the approach you use, you must fully configure each Meridium Enterprise APM Server according to the steps for deploying the basic Meridium Enterprise APM system architecture. In addition, each Meridium Enterprise APM Server must be configured to use the same instance of Redis.

Global Load Balancing

In global load balancing, you configure all Meridium Enterprise APM Server(s) to process policy executions in a single load-balanced cluster. In this scenario, an increase in activity from any server can be absorbed across all servers in your system architecture. Because there is only one cluster to manage in this scenario, this is the simpler configuration to set up and manage.

In this scenario, you must:

- Configure the Policy Trigger service on all Meridium Enterprise APM Servers to specify the name of the cluster.
- Start the Policy Execution Service on all Meridium Enterprise APM Servers.
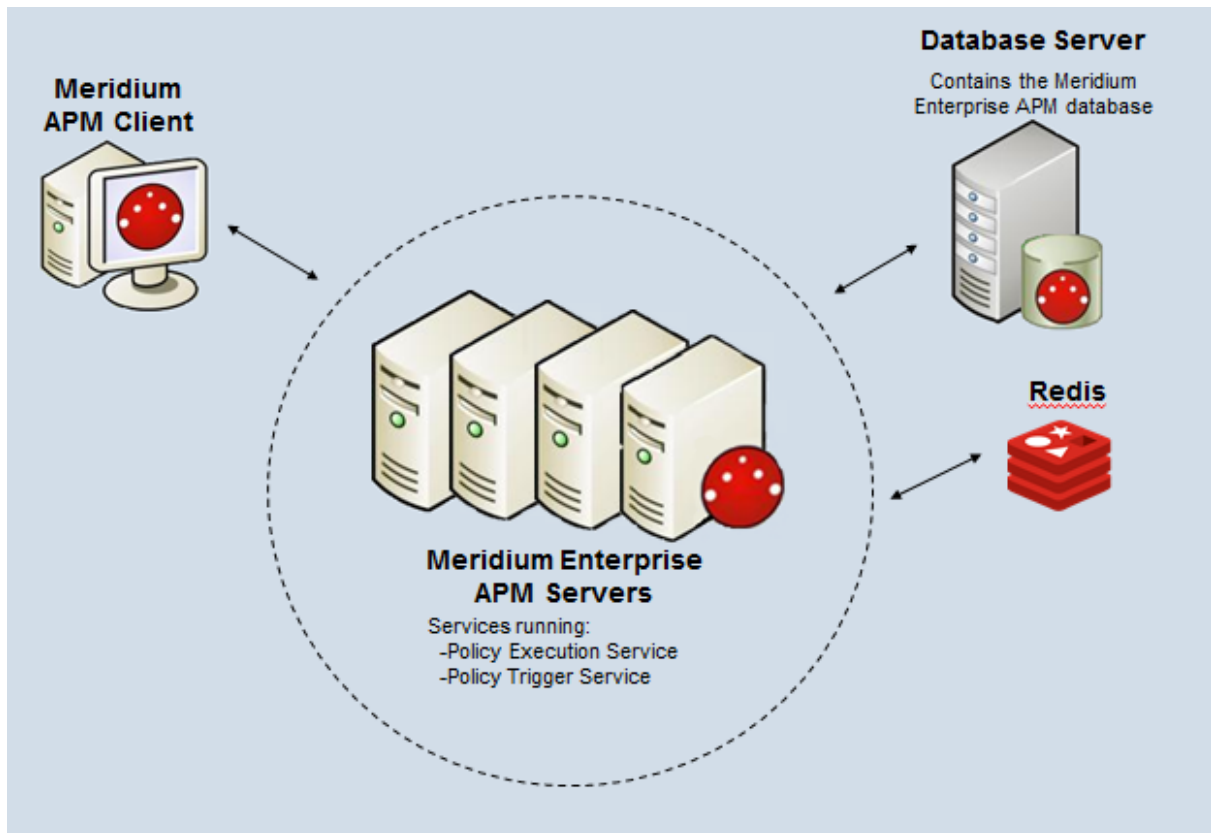
Isolated Load Balancing

In isolated load balancing, you configure designated Meridium Enterprise APM Server(s) to process policy executions in a *separate* load-balanced cluster from other Meridium Enterprise APM Server(s). In this scenario, the policy execution processes are isolated from the Meridium Enterprise APM Server processes, therefore preventing an increase in activity in one cluster from negatively impacting the processes of the other.

In this scenario, you must:

- Configure the Policy Trigger service on all Meridium Enterprise APM Servers to specify the name of the cluster used for policy executions.
- Start the Policy Execution Service on *only* the Meridium Enterprise APM Servers in the cluster designated to process policy executions.

Policy Designer 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 Policy Designer	MI Health Power MI Health Admin
MI Policy User	MI Health User
MI Policy Viewer	None

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

Family	MI Policy Designer	MI Policy User	MI Policy Viewer
Entity Families			
Health Indicator Value	View, Update, Insert, Delete	None	View
Policy	View, Update, Insert, Delete	View	View
Policy Event	View, Update, Insert, Delete	View, Update	View
Policy Instance	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Policy Recommendation	View, Update, Insert, Delete	View, Update	View
Relationship Families			
Has Event	View, Update, Insert, Delete	View, Update	View

Deploy Process Data Integration (PDI)

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 Process Data Integration (PDI) 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 Meridium Enterprise 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:** These steps assume that your system architecture contains only one Process Data Integration Server and one OPC Server. If your system architecture contains more than one Process Data Integration Server and OPC Server, you must install and configure the Process Data Integration Service on *each* Process Data Integration Server machine.

Step	Task	Notes
1	Ensure that your OPC Server and process historian are configured according to the PDI system requirements.	This step is required.
2	Review the server roles that are configured for the Process Data Integration Server in the Meridium Enterprise APM testing environment, and then configure roles on your Process Data Integration Server accordingly.	This step is required.
3	Assign Security Users to one or more of the Process Data Integration Security Groups and Roles.	This step is required.
4	In Meridium Enterprise APM, create an OPC System record to represent the OPC-compliant system from which you want to retrieve data.	This step is required.
5	On the Process Data Integration Server, install the Process Data Integration Service.	This step is required. We recommend that the OPC Server is the same machine as the Process Data Integration server. However, if it is a separate machine, refer to the PDI system requirements for information on additional configuration that is required.

Step	Task	Notes
6	On the Process Data Integration Server, modify the Process Data Integration Service configuration file to specify your OPC Server, the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	This step is required.
7	On the Process Data Integration Server, start the Process Data Integration Service.	This step is required. When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records. You may review the log files for this service at **C:\Program Files\Meridium\Logs**.
8	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for PDI.	This step is required.
9	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	This step is required. You may review the log files for this service at **C:\ProgramData\Meridium**.
10	Review the Process Data Integration data model to determine which relationship definitions you will need to modify to include your custom equipment and location families.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
11	In Meridium Enterprise APM, link OPC Tag records to related asset records.	This step is required.

Upgrade or Update Process Data Integration (PDI) to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

Step	Task	Notes
1	On the Process Data Integration Server, upgrade the Process Data Integration Service.	This step is required.
2	On the Process Data Integration Server, modify the Process Data Integration Service configuration file to specify your OPC Server, the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	This step is required.
3	On the Process Data Integration Server, start or restart the Process Data Integration Service.	This step is required. When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records.
4	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for PDI.	This step is required.
5	On the Meridium Enterprise APM Server, restart the Meridium Notification Service.	This step is required.
6	In Meridium Enterprise APM, link any new OPC Tag records to related asset records.	This step is required.

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	On the Process Data Integration Server, upgrade the Process Data Integration Service.	This step is required.
2	On the Process Data Integration Server, modify the Process Data Integration Service configuration file to specify your OPC Server, the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	This step is required.
3	On the Process Data Integration Server, start or restart the Process Data Integration Service.	This step is required. When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records.
4	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for PDI.	This step is required.
5	On the Meridium Enterprise APM Server, restart the Meridium Notification Service.	This step is required.
6	In Meridium Enterprise APM, link any new OPC Tag records to related asset records.	This step is required.

Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	On the Process Data Integration Server, upgrade the Process Data Integration Service.	This step is required.
2	On the Process Data Integration Server, modify the Process Data Integration Service configuration file to specify your OPC Server, the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	This step is required.

Step	Task	Notes
3	On the Process Data Integration Server, start or restart the Process Data Integration Service.	This step is required. When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records.
4	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for PDI.	This step is required.
5	On the Meridium Enterprise APM Server, restart the Meridium Notification Service.	This step is required.
6	In Meridium Enterprise APM, link any new OPC Tag records to related asset records.	This step is required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

Step	Task	Notes
1	On the Process Data Integration Server, upgrade the Process Data Integration Service.	This step is required.
2	On the Process Data Integration Server, modify the Process Data Integration Service configuration file to specify your OPC Server, the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	This step is required.
3	On the Process Data Integration Server, start or restart the Process Data Integration Service.	This step is required. When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records.
4	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for PDI.	This step is required.
5	On the Meridium Enterprise APM Server, restart the Meridium Notification Service.	This step is required.

Step	Task	Notes
6	In Meridium Enterprise APM, link any new OPC Tag records to related asset records.	This step is required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

Step	Task	Notes
1	On the Process Data Integration Server, upgrade the Process Data Integration Service.	This step is required.
2	On the Process Data Integration Server, modify the Process Data Integration Service configuration file to specify your OPC Server, the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	This step is required.
3	On the Process Data Integration Server, start or restart the Process Data Integration Service.	This step is required. When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records.
4	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for PDI.	This step is required.
5	On the Meridium Enterprise APM Server, restart the Meridium Notification Service.	This step is required.
6	In Meridium Enterprise APM, link any new OPC Tag records to related asset records.	This step is required.

Upgrade from any version V3.5.1 through V3.5.1.12.0

Step	Task	Notes
1	On the Process Data Integration Server, upgrade the Process Data Integration Service.	This step is required.

Step	Task	Notes
2	On the Process Data Integration Server, modify the Process Data Integration Service configuration file to specify your OPC Server, the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	This step is required.
3	On the Process Data Integration Server, start or restart the Process Data Integration Service.	This step is required. When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records.
4	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for PDI.	This step is required.
5	On the Meridium Enterprise APM Server, restart the Meridium Notification Service.	This step is required.
6	In Meridium Enterprise APM, link any new OPC Tag records to related asset records.	This step is required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

Step	Task	Notes
1	On the Process Data Integration Server, upgrade the Process Data Integration Service.	This step is required.
2	On the Process Data Integration Server, modify the Process Data Integration Service configuration file to specify your OPC Server, the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	This step is required.

Step	Task	Notes
3	On the Process Data Integration Server, start or restart the Process Data Integration Service.	This step is required. When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records.
4	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for PDI.	This step is required.
5	On the Meridium Enterprise APM Server, restart the Meridium Notification Service.	This step is required.
6	In Meridium APM, link any new OPC Tag records to related asset records.	This step is required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	On the Process Data Integration Server, upgrade the Process Data Integration Service.	This step is required.
2	On the Process Data Integration Server, modify the Process Data Integration Service configuration file to specify your OPC Server, the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	This step is required.
3	On the Process Data Integration Server, start or restart the Process Data Integration Service.	This step is required. When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records.
4	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for PDI.	This step is required.
5	On the Meridium Enterprise APM Server, restart the Meridium Notification Service.	This step is required.

Step	Task	Notes
6	In Meridium APM, link any new OPC Tag records to related asset records.	This step is required.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	On the Process Data Integration Server, upgrade the Process Data Integration Service.	This step is required.
2	On the Process Data Integration Server, modify the Process Data Integration Service configuration file to specify your OPC Server, the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	This step is required.
3	On the Process Data Integration Server, start or restart the Process Data Integration Service.	This step is required. When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records.
4	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for PDI.	This step is required.
5	On the Meridium Enterprise APM Server, restart the Meridium Notification Service.	This step is required.
6	In Meridium APM, link any new OPC Tag records to related asset records.	This step is required.

Process Data Integration Server Roles

The following server roles are configured on the Process Data Integration Server in the Meridium Enterprise APM test environment.

> ⓘ **Note:** Roles and features can be added via the Add Roles and Features Wizard on a Windows Server machine. To add roles and features, in Server Manager, on the **Manage** menu, select **Add Roles and Features** to open the wizard. Select role-based or feature based installation and then continue through the wizard.

In the **Server Roles** section:

- Application Server

In the **Role Services** section for the **Application Server**:

- .NET Framework 4.5
- TCP Port Sharing
- Windows Process Activation Service Support
    - Message Queuing Activation, and all features
    - Named Pipes Activation, and all features
    - TCP Activation, and all features

About the Asset Health Services

When you deploy the Asset Health Manager, Process Data Integration, 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 following topics:

- Deploying Asset Health Manager (AHM) for the First Time
- Deploying Policy Designer for the First Time
- Deploying Process Data Integration (PDI) for the First Time

Services Summary

The following services are used by the Asset Health Manager, Process Data Integration, 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 (e.g., an OPC 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 (i.e., an associated record in the Meridium Enterprise 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. The Policy Trigger Service monitors this queue and sends these messages to an appropriate policy execution queue.
- **Policy Execution Service:** The Meridium Enterprise APM Policy Execution Service handles the execution of policies. Specifically, the Policy Execution Service monitors a corresponding policy execution queue and executes the policies that are added to it.
- **Process Data Integration (PDI) Service:** Monitors the subscribed tags (i.e., tags that are used in policies and health indicators or tags for which readings are being stored in the Meridium 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.

Example: Standard System Architecture Configuration

The following diagram illustrates the machines in the Meridium Enterprise APM system architecture when the Policy Designer, Process Data Integration (PDI), and Asset Health Manager

(AHM) modules are used together. This image depicts the standard configuration, where the OPC Server software and the Process Data Integration 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 Meridium Enterprise APM Servers, multiple OPC Servers, or multiple Meridium Enterprise 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, Policy Designer, and Process Data Integration.

Machine	Software Installed	Asset Health Service Installed Automatically with Service Software
Meridium Enterprise APM Server	Meridium Enterprise APM Server software	Asset Health Indicator Service
		Policy Trigger Service
		Policy Execution Service
Process Data Integration Server, which also acts as the OPC Server	Process Data Integration Service software	Process Data Integration Service
	OPC Server software	NA
Process Historian	Process historian software	NA

Install the Process Data Integration Service

The following instructions provide details on installing the Process Data Integration Service using the Meridium Enterprise APM Server and Add-ons installer.

Steps

1. On the machine that will serve as the Meridium Process Data Integration Server, access the Meridium Enterprise APM distribution package, and then navigate to the folder **\\Setup\Meridium Enterprise APM Server and Add-ons**.

2. Double-click the file **Setup.exe**.

   The **Welcome** screen 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. Select the **Meridium Process Data Integration Service** option.

   > 🛈 **Note:** While additional options are available for selection, these options are not meant to be installed on the Process Data Integration Server. These instructions assume that you want to install only the Meridium Process Data Integration Service software. When this software is installed, the Meridium Enterprise APM System Administration Tool will also be installed automatically.

7. Select **Next**.

   Meridium Enterprise APM performs a check to make sure that your machine contains the required prerequisites for the features that you want to install.

   - If one or more prerequisites are missing on the machine, a dialog box will appear, explaining which prerequisites are missing. If this occurs, close the installer, install the missing prerequisite, and then run the installer again.

   - If all the prerequisites for the selected components are installed on the machine, or you have selected components that do not require any prerequisites, the **Complete the Installation** screen appears.

8. Select **Install**.

The **Setup Status** screen appears, which displays a progress bar that shows the progress of the installation process. After the progress bar reaches the end, a message appears, indicating that your server is being configured. After your server is configured, the **Installation is Complete** screen appears.

You can also select to optionally launch the APM System Administration tool when the installer window closes.

9. Select **Finish**.

You should now [refer back to the checklist](#).

Upgrade the Process Data Integration Service

The following instructions provide details on upgrading the Process Data Integration Service on the Process Data Integration Server. These instructions assume that you are an Administrator with full access to the Meridium Process Data Integration server machine.

Steps

1. On the machine that will serve as the Meridium Process Data Integration Server, access the Meridium Enterprise APM distribution package, and then navigate to the folder **\\Setup\Meridium Enterprise APM Server and Add-ons**.

2. Select the file **setup.exe**.

   A message appears, asking if you want to allow setup.exe to make changes to your machine.

3. Select **Yes**.

   The **Meridium Enterprise APM Server and Add-ons** installer appears, displaying the **Preparing Setup** screen. The **Preparing Setup** screen contains a progress bar that indicates when the installer is ready to upgrade the components on your machine.
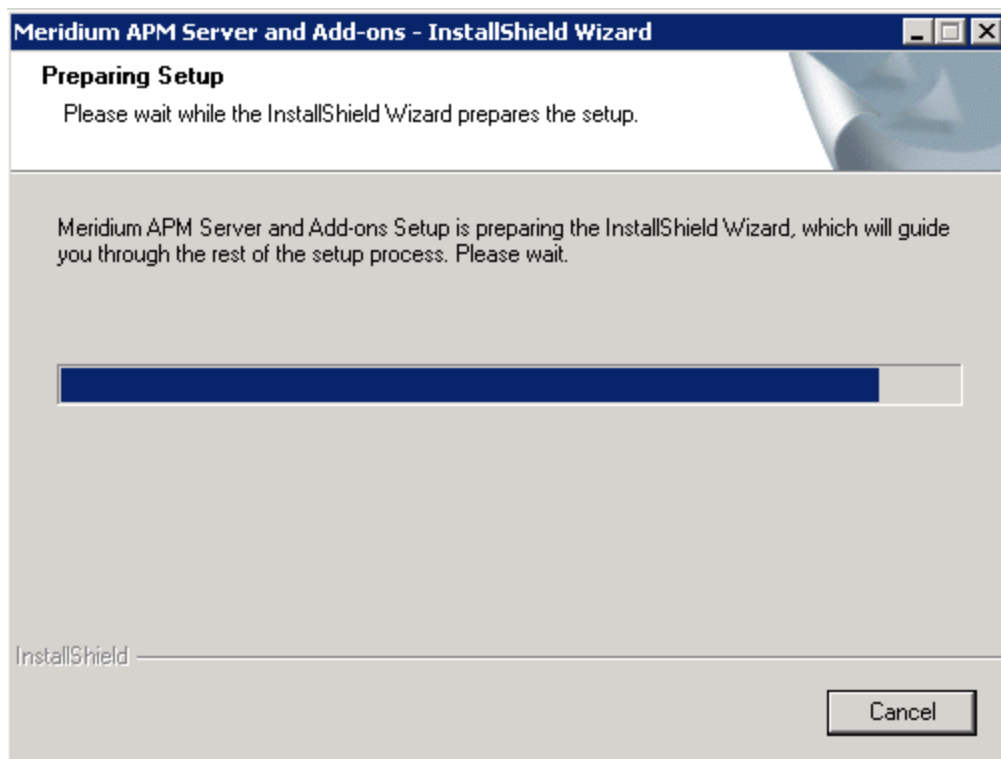
When the progress bar reaches the end, a message appears, asking if you want to upgrade your server.

4. Select **Yes**.

    The **Setup Status** screen appears, displaying a progress bar that indicates the status of the upgrade process. After the progress bar reaches the end, the **Maintenance Complete** screen appears.

    You can also select to optionally launch the APM System Administration tool when the installer window closes.

5. Select **Finish**.

    You should now refer back to the upgrade checklist.

Configure the Meridium Notification Service for PDI

In order for the Process Data Integration service to work correctly, you must configure the Meridium Notification Service by modifying the file *Meridium.Service.Notification.exe.config* on the Meridium Enterprise APM Server.

Steps

1. On the Meridium Enterprise APM Server, navigate to the folder where the Meridium Notification Service files are installed. If you installed the software in the default location, you can locate these files in the folder **C:\Program Files\Meridium\Services**.

2. Open the file **Meridium.Service.Notification.exe.config** in an application that you can use to modify XML script (e.g., Notepad).

3. If you have not done so already, complete any necessary basic configuration for the Meridium Notification Service.

4. Within the **<notification>** tags, within the **<notificationSettings>** tags, uncomment the following text string (i.e., delete the **<!--** and **-->**):

    ```
    <!-- <add key="server3" serverType="external" endPointName-
    e="pdiService"/> -->
    ```

5. Within the **<system.serviceModel>** tags, within the **<client>** tags, uncomment the following text string (i.e., delete the **<!--** and **-->**):

    ```
    <!-- <endpoint name="pdiService" address-
    s="net.tcp://PDISERVERNAME/Meridium/PDI/NotifyHandler" bind-
    ing="netTcpBinding"
    contract="Meridium.Core.Common.Contracts.INotificationService"
    /> -->
    ```

6. Within the **address** attribute, replace **PDISERVERNAME** with the name or IP Address of the Process Data Integration Server.

7. If you have only one Process Data Integration Server in your system architecture, save and close the file.

    -or

    If you have multiple Process Data Integration Servers, complete the following steps for each additional server:

    a. Copy the string within the **<notificationSettings>** tags that you uncommented in Step 4.

    b. Directly after the text that you copied (after the />), paste the copied text.

    c. Within the **key** attribute, specify a unique name for the connection.

    d. Within the **endPointName** attribute, specify a unique name for the end point.

e. Copy the string within the **<client>** tags that you uncommented in Step 5.

f. Within the **name** attribute, enter the name for the endpoint that you specified in Step d.

g. Modify the **address** attribute to specify the name or IP Address of the additional Process Data Integration Server.

h. Save and close the file.

8. Start or restart the Meridium Notification Service.

Example

If your system architecture has two Process Data Integration Servers, the strings in the **<notificationSettings>** tags might look like this:

```
<add key="PDIserver1" serverType="external" endPointName-
e="pdiService"/>

<add key="PDIserver2" serverType="external" endPointName-
e="pdiService2"/>
```

...and the corresponding strings in the **<client>** tags might look like this:

```
<endpoint name="pdiService" address-
s="net.tcp://Matrikon/Meridium/PDI/NotifyHandler" bind-
ing="netTcpBinding"
contract="Meridium.Core.Common.Contracts.INotificationService" />

<endpoint name="pdiService2" address-
s="net.tcp://OsiPi/Meridium/PDI/NotifyHandler" bind-
ing="netTcpBinding"
contract="Meridium.Core.Common.Contracts.INotificationService" />
```

Configure the Process Data Integration Service

In order to use Process Data Integration, you must configure the Process Data Integration Service by modifying the file *Meridium.PDI.Service.exe.config* on the Meridium Process Data Integration Server. If you installed the Process Data Integration Service in the default location, you can locate this file in the folder **C:\Program Files\Meridium\Services**.

Some modifications can be made using the APM System Administration tool and other modifications must be made by opening the file in an application that you can use to modify XML script (e.g., Notepad). The following instructions provide details on making all required modifications at one time, using both the APM System Administration tool and a text editor.

> ℹ **Note:** This configuration file defines several endpoints on the Process Data Integration Server with URLs and ports that must be accessible from the Meridium Enterprise APM Server. You should ensure that your firewalls are configured to allow this access.

Steps

1. On the Meridium Process Data Integration Server, access the APM System Administration tool.

2. In the **APM System Administration** window, in the **Configuration** section, click the **PDI Service** link.

   Some contents of the **Meridium.PDI.Service.exe.config** file appear to the right of the **Configuration** section.

3. In the **OPCDA** and **OPCHDA** boxes, enter the values that identify your OPC Server.

   The following table contains the default values that identify the OPC Servers for the process historians that have been tested by Meridium, Inc. We recommend, however, that you contact the third-party distributor of your process historian software to confirm the values that you should use for your system configuration.

Process Historian	OPCDA	OPCHDA
OSIsoft® PI Server	OSI.DA.1	OSI.HDA.1
Matrikon Simulation tool	Matrikon.OPC.Simulation.1	Matrikon.OPC.Simulation.1
IP21	Aspen.Infoplus21_DA.1	N/A
MatrikonOPC HDA Server for IP21*	Matrikon.OPC.IP21.1	Matrikon.OPC.IP21.1
Honeywell Uniformance® Process History Database (PHD)	OPC.PHDServerDA.1	OPC.PHDServerHDA.1

*In the Meridium Enterprise APM testing environment, IP21 and MatrikonOPC for IP21 are installed on separate machines.

4. In the **OPCDAHOST** and **OPCHDAHOST** boxes:

    - If the Process Data Integration Service and OPC software are installed on the *same* machine, leave these text boxes empty.

      -or-

    - If the Process Data Integration Service and OPC software are installed on *different* machines, enter the name or IP address of your OPC Server. Note that we do not recommend this configuration. For additional information, refer to the PDI system requirements.

5. In the **Tag Sync Interval** box, replace the example value with the frequency (in hours) at which you want the tag synchronization to occur.

6. In the **Initial Tag Sync Time** box, replace the example value with the date and time (in UTC) that you want the first scheduled tag synchronization to occur.

> **Note:** This value must be specified using the ISO 8601 standard for UTC date formats (i.e., the letters *T* and *Z* must be included), for example, *2014-01-01T04:00:00Z*.

7. In the **Max Sync Time** box, replace the example value with the maximum length of time (in hours) that you want to allow the tag synchronization to run.

> **Note:** The purpose of this setting is to stop a synchronization that is running significantly longer than expected (e.g., because it encountered an error) so that the synchronization will start over at the next scheduled time. Therefore, the maximum synchronization time that you allow should be longer than the length of time that it takes for tags to synchronize under normal circumstances and should account for known factors that may extend the synchronization time (e.g., network connection speed).

8. At the bottom of the **APM System Administration** window, click the **Save** button.

    Your changes are saved to the file Meridium.PDI.Service.exe.config. You must now open the actual file to complete the service configuration.

9. Click the **Open File** link.

10. Within the **<meridiumConnections>** tags, uncomment the example connection tag by deleting **<!--EXAMPLE:** and the corresponding **-->** from the beginning and end of the string.

11. Within the **<meridiumConnections>** tags, modify the attributes as described in the following table.

Within this attribute...	Make this change	Notes
connection name	Replace **CONNECTION 1** with a name to identify the connection to the database.	This value is used only by the configuration file. If you are configuring connections to multiple data sources, each connection name must be unique.
applicationServer	Replace **APPSERVER_ NAME** with the name or IP Address of the Meridium Enterprise APM Server on which the data source specified in the **datasource** attribute is configured.	None
datasource	Replace **DATASOURCE_ NAME** with the name of the Meridium Enterprise APM database to which you want to connect.	The data source value is case sensitive and should be typed exactly as it is defined for the Meridium Enterprise APM Server in the Data Sources section of Operations Manager.
userId	Replace **SERVICE_ USER_NAME** with the User ID of the Security User whose credentials should be used to log in to the specified Meridium Enterprise APM database.	The user you specify should be a member of the MI Process Data Integration Service Security Group.

Within this attribute...	Make this change	Notes
password	Replace **PaSsWoRd** with the password for the specified user.	Do not delete the **!** in front of the password. This symbol is not part of the password itself. Instead, this symbol will cause the password to be encrypted automatically when the service is restarted. ⚠ **IMPORTANT**: If you need to change the password for the specified user, you should first stop the Process Data Integration service. Then, after changing the user's password, update the password in this configuration file and restart the service. If you change the user's password without restarting the service, the account will become locked.
xiServers	Replace **OPC System1** with the value that exists in the OPC System ID field in an OPC System record in the Meridium Enterprise APM database.	If multiple OPC System records exist to identify multiple OPC Servers, you can specify multiple values and separate them with a semicolon (e.g., "OPC System1;OPC System2").

12. Save and close the file.

    When the Process Data Integration Service is started or restarted, your settings will be applied and the initial tag synchronization will occur.

Configure Multiple Data Sources

For each unique Meridium Enterprise APM Server and data source combination that exists in your architecture, you must specify a separate connection string in the PDI Service configuration file. For example, if your system architecture contains two Meridium Enterprise APM Servers writing to the same database, regardless of whether the same or different data source names are specified on each, you need to configure two connection strings.

Steps

1. Configure the first connection by modifying the attributes within **<meridiumConnections>** tags, as described in the instructions for [configuring the Process Data Integration Service](#).

2. Copy the text within the **<meridiumConnections>** tags (e.g., `<connection name-e="CONNECTION 1" applicationServer="" datasource="DATASOURCE_NAME" userId="SERVICE_USER_NAME" password="!PaSsWoRd" />`)

3. Directly after the text that you copied (after the />), paste the copied text.

4. Modify the attributes as needed.

   > 📄 **Note:** The connection name that you specify in each connection string must be unique.

5. Repeat these steps for each required connection.

Configure Multiple Process Data Integration and OPC Servers

Depending on your specific system architecture, you may have multiple Process Data Integration and OPC Server machines.

The following diagram illustrates multiple OPC Servers in the standard configuration where the OPC Server is the same machine as the Process Data Integration (PDI) Server (i.e., the OPC Server software is installed on the PDI Server).
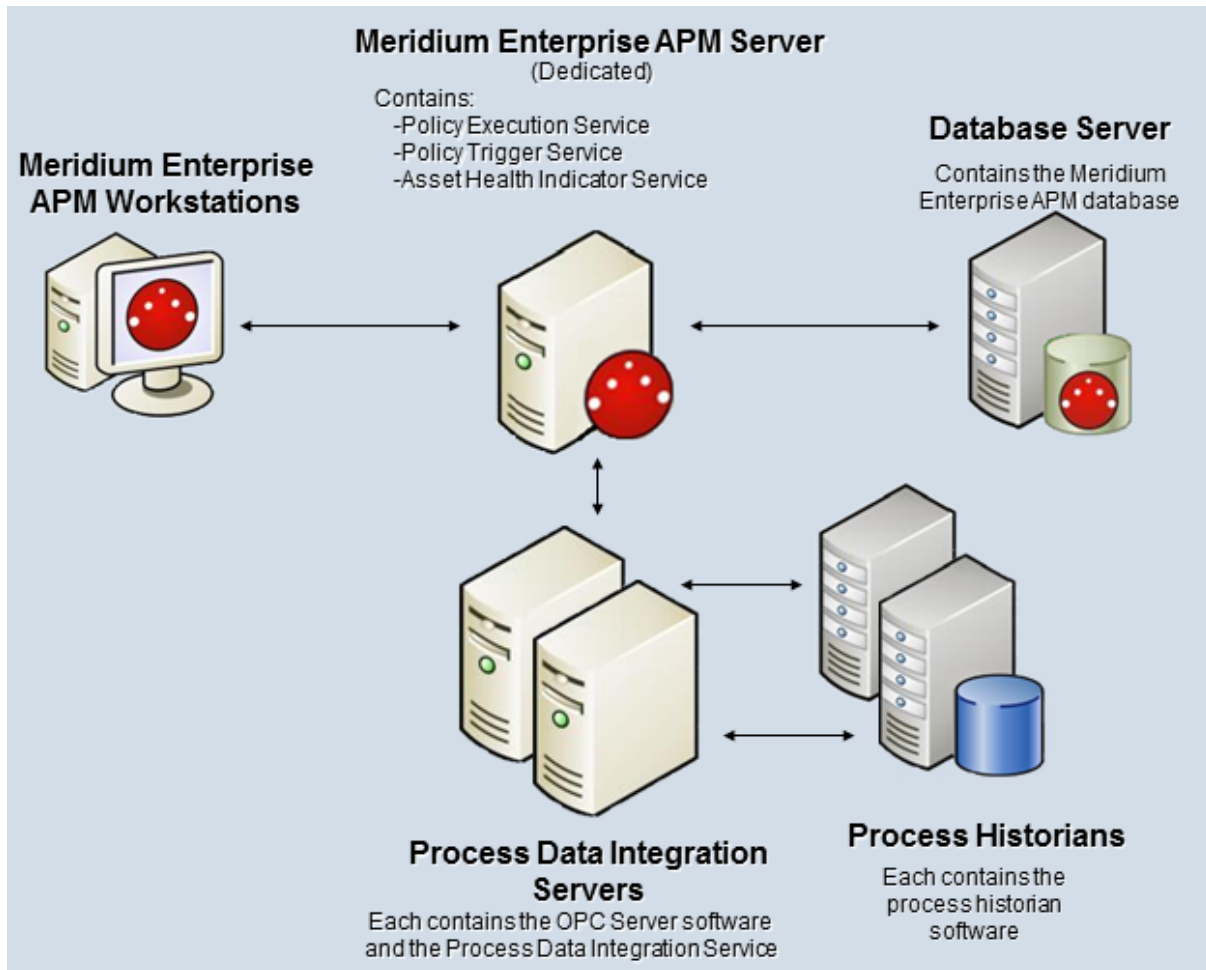
The following diagram illustrates multiple OPC Servers in an alternative configuration where the OPC Servers are separate machines from the PDI Servers.
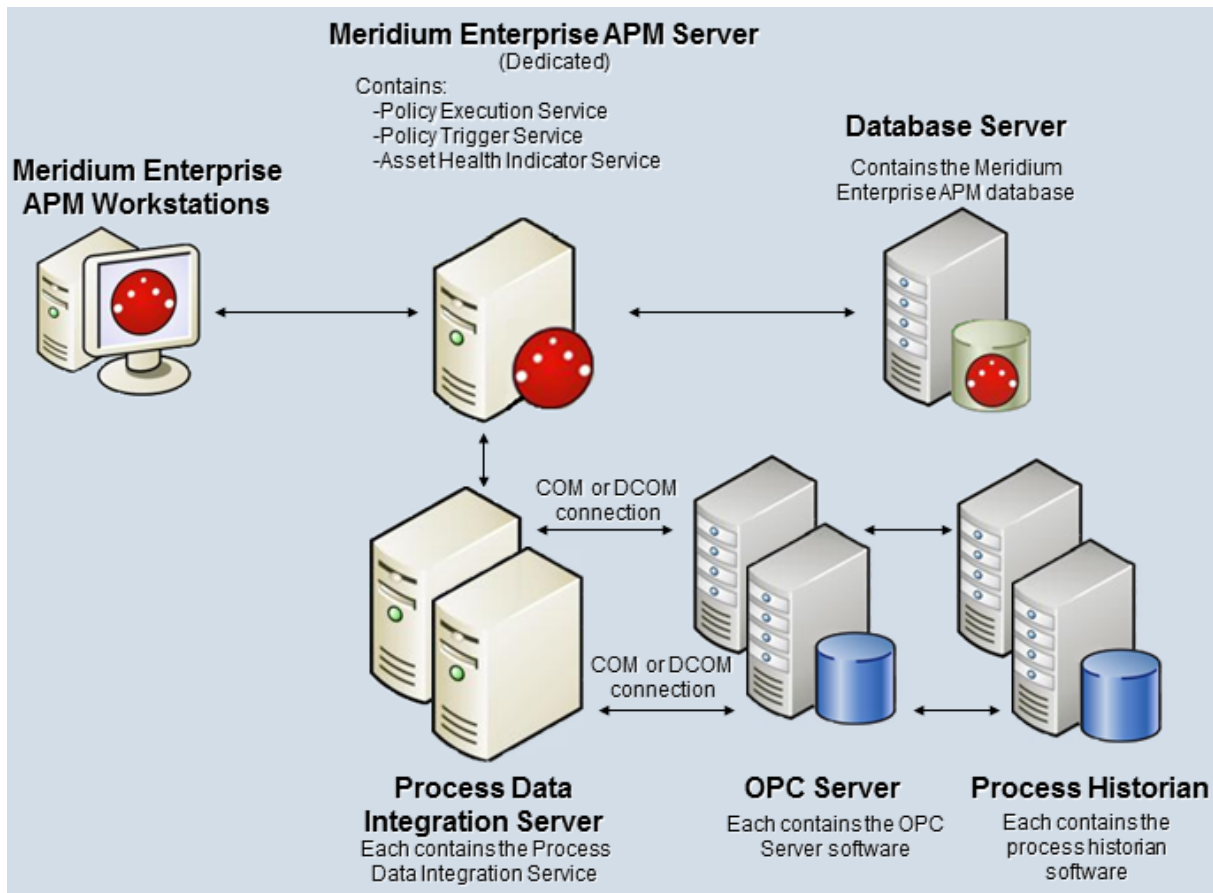
In either of these scenarios, when you complete the first-time deployment steps for PDI, you must install and configure the Process Data Integration Service on *each* Process Data Integration Server machine.

Whether the OPC Servers are the same machine as the Process Data Integration Servers or not, in the Meridium Enterprise APM application, you will create an OPC System record for each OPC Server (e.g., OPCServer1 and OPCServer2). Then, when you configure the Process Data Integration Service, you must specify the appropriate OPC Server record in the **xiServers** attribute within the **meridumConnections** tags. For example, the connection string on each machine might look like this:

- On the first Process Data Integration Server: `<connection name="EXAMPLE_CONNECTION" applicationServer="APPSERVER_NAME" data-source="DATASOURCE_NAME" userId=" SERVICE_USER_NAME" password="!PaSsWoRd" xiServers="OPCSystem1" />`

- On the second Process Data Integration Server: `<connection name="EXAMPLE_CONNECTION" applicationServer="APPSERVER_NAME" data-source="DATASOURCE_NAME" userId="SERVICE_USER_NAME" password="!PaSsWoRd" xiServers="OPCSystem2" />`

Process Data Integration 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 Process Data Integration Administrator	MI Health Admin
MI Process Data Integration Service	None
MI Process Data Integration User	MI Health User MI Health Power

> 📄 **Note**: The Security Groups listed in the table above account only for family permissions. Users must also be added to the MI Configuration Role Security Group in order to access the Systems and Tags page, which is required to modify families used by this module.

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

Family	MI Process Data Integration Administrator	MI Process Data Integration Service	MI Process Data Integration User
Entity Families			
OPC Reading	View, Update, Insert, Delete	View, Update, Insert, Delete	View
OPC System	View, Update, Insert, Delete	View	View
OPC Tag	View, Update, Insert, Delete	View	View
Relationship Families			
Has OPC Reading	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has OPC Tag	View, Update, Insert, Delete	View	View

Deploy Production Loss Analysis (PLA)

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 Production Loss Analysis (PLA) 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 Meridium Enterprise 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.

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 displayed 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 more 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 they produce 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.
7	Define production event codes.	The baseline Meridium Enterprise 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 event type will be stored in a separate *Production Event Code* record.

Step	Task	Notes
8	Define impact codes.	The baseline Meridium Enterprise 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 Meridium Enterprise 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.
10	Define values that will be mapped to a Production Analysis.	This step is optional. By default, certain PLA values are mapped to the production data in a Production Analysis. If you want to map different or additional PLA values, you can do so by modifying the All Production Data query.
11	Configure PLA for PDI Integration: • Link Production Profile records to OPC Tag records.	This step is required if you want to use the integration between PLA and the Process Data Integration feature where Production Event records are created automatically.
12	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 Meridium Enterprise 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 an error that prevents the graph from populating correctly. If this error occurs, replace the Top 10 Bad Actors query.

Upgrade or Update Production Loss Analysis (PLA) to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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 Meridium Enterprise 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 an error that prevents the graph from populating correctly. If this error occurs, then 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 Meridium Enterprise 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 an error that prevents the graph from populating correctly. If this error occurs, then replace the Top 10 Bad Actors query.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

Step	Task	Notes
1	On the Meridium Enterprise APM Server, import the required baseline rules.	⚠ **IMPORTANT:** This step is required and must be completed *before* upgrading the Meridium Enterprise APM Server and Add Ons software on the Meridium Enterprise APM Server(s). After completing this step, you should return to the upgrade Meridium Enterprise APM workflow. Then, after completing the remainder of the upgrade Meridium Enterprise 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 on the SQL Server Analysis Server.	This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server in V3.6.0.0.0.
3	Set the timezones for the Production Units.	This step is required. If the timezones for the Production Units are set, all the Production Plan records, Plan Data records, and Production Target records will be updated based on the timezone for the respective Production Unit. ℹ **Note:** Since the date and time in PLA is now stored in UTC format, you *must* set the timezone for each Production Unit before upgrade. • If you do not set the timezones for the Production Units, and if the Production Plan records exist in the database, then the Production Plan records, Plan Data records, and Production Target records will be updated based on the timezone of the user who last modified the Production Plan record. • If you do not set the timezones for the Production Units, and if the Production Plan records do not exist in the database, then the timezone for the Production Unit will be updated based on the timezone of the user who last modified the Production Unit record.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

Step	Task	Notes
1	On the Meridium Enterprise APM Server, import the required baseline rules.	⚠ **IMPORTANT:** This step is required and must be completed *before* upgrading the Meridium Enterprise APM Server and Add Ons software on the Meridium Enterprise APM Server(s). After completing this step, you should return to the upgrade Meridium Enterprise APM workflow. Then, after completing the remainder of the upgrade Meridium Enterprise 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 on the SQL Server Analysis Server.	This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server in V3.6.0.0.0.
3	Set the timezones for the Production Units.	This step is required. If the timezones for the Production Units are set, all the Production Plan records, Plan Data records, and Production Target records will be updated based on the timezone for the respective Production Unit. ℹ **Note:** Since the date and time in PLA is now stored in UTC format, you *must* set the timezone for each Production Unit before upgrade. • If you do not set the timezones for the Production Units, and if the Production Plan records exist in the database, then the Production Plan records, Plan Data records, and Production Target records will be updated based on the timezone of the user who last modified the Production Plan record. • If you do not set the timezones for the Production Units, and if the Production Plan records do not exist in the database, then the timezone for the Production Unit will be updated based on the timezone of the user who last modified the Production Unit record.

Upgrade from any version V3.5.1 through V3.5.1.12.0

Step	Task	Notes
1	On the Meridium Enterprise APM Server, import the required baseline rules.	⚠ **IMPORTANT:** This step is required and must be completed *before* upgrading the Meridium Enterprise APM Server and Add Ons software on the Meridium Enterprise APM Server(s). After completing this step, you should return to the upgrade Meridium Enterprise APM workflow. Then, after completing the remainder of the upgrade Meridium Enterprise 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 on the SQL Server Analysis Server.	This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server in V3.5.1.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

Step	Task	Notes
1	On the Meridium Enterprise APM Server, import the required baseline rules.	⚠ **IMPORTANT:** This step is required and must be completed *before* upgrading the Meridium Enterprise APM Server and Add Ons software on the Meridium Enterprise APM Server(s). After completing this step, you should return to the upgrade Meridium Enterprise APM workflow. Then, after completing the remainder of the upgrade Meridium Enterprise 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 on the SQL Server Analysis Server.	This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube on 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	On the Meridium Enterprise APM Server, import the required baseline rules.	⚠ **IMPORTANT:** This step is required and must be completed *before* upgrading the Meridium Enterprise APM Server and Add Ons software on the Meridium Enterprise APM Server(s). After completing this step, you should return to the upgrade Meridium Enterprise APM workflow. Then, after completing the remainder of the upgrade Meridium Enterprise 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 on the SQL Server Analysis Server.	This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube on 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	On the Meridium Enterprise APM Server, import the required baseline rules.	⚠ **IMPORTANT:** This step is required and must be completed *before* upgrading the Meridium Enterprise APM Server and Add Ons software on the Meridium Enterprise APM Server(s). After completing this step, you should return to the upgrade Meridium Enterprise APM workflow. Then, after completing the remainder of the upgrade Meridium Enterprise 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 Code records instead of or in addition to the baseline OEE Code records that are provided in the Meridium Enterprise 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.

Step	Task	Notes
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 on the SQL Server Analysis Server.	This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server in V3.4.5.

Import Baseline Rules

> **Note:** If you are upgrading Production Loss Analysis from a starting version that is earlier than V4.0.0.0, 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 Meridium Enterprise APM and upgrade Production Loss Analysis workflows.
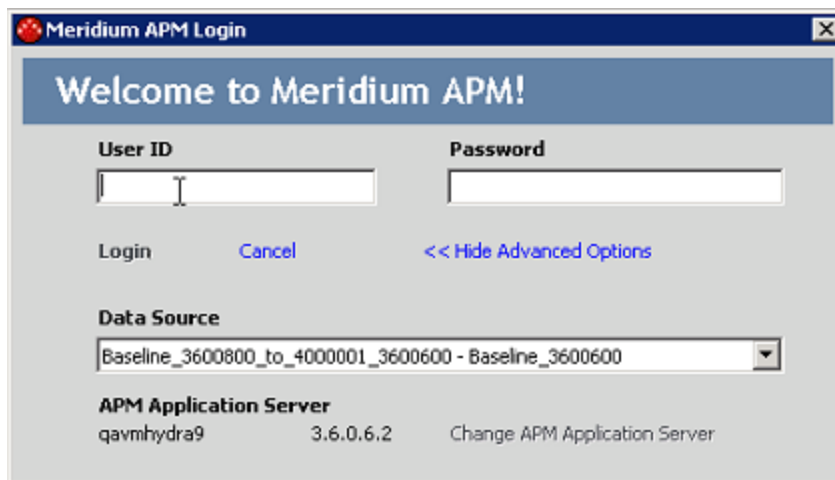
Before You Begin

- Acquire a copy of the baseline Meridium Enterprise 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 Meridium, Inc. Professional Services department.

Steps

1. On the Meridium Enterprise APM Server machine, 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 Meridium Enterprise 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.
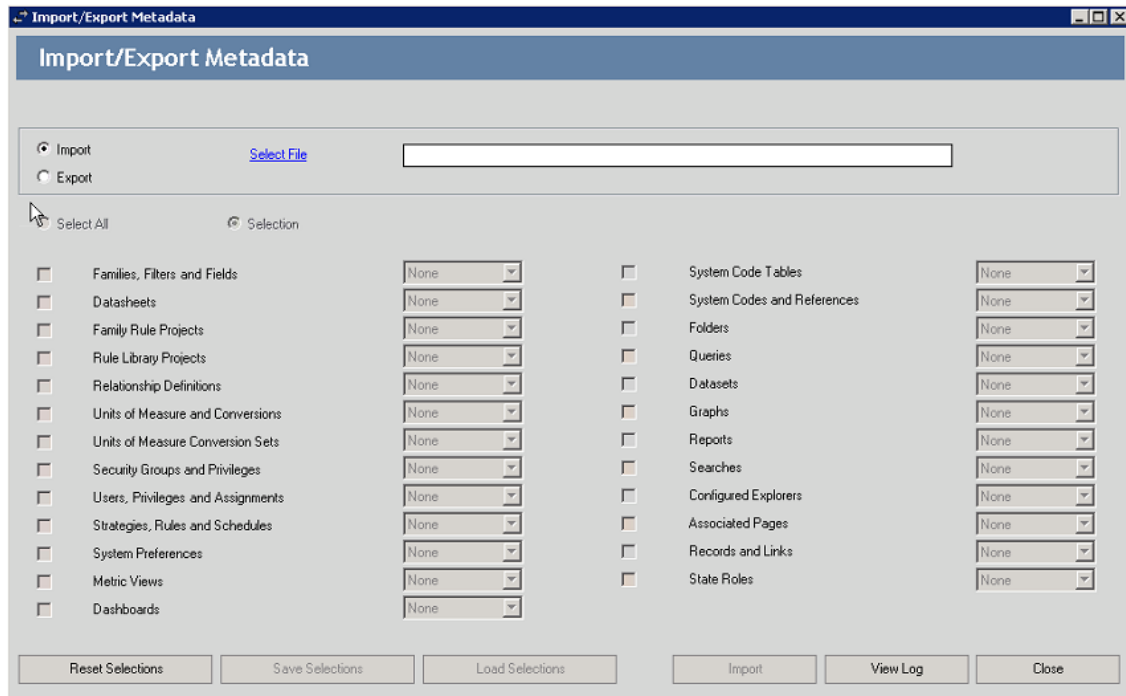
5. Select the **Export** check box, and then select **Select File**.

   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.
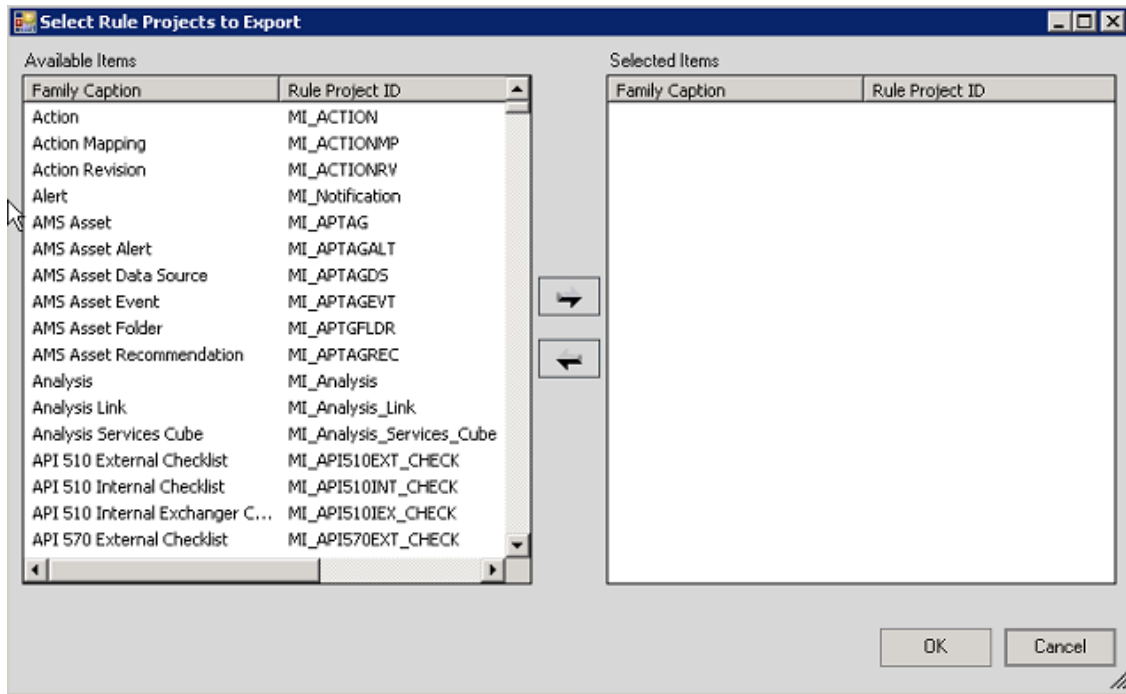
9. In the **Available Items** section, select the item whose Family Caption is Production Event, and then select ⟶ .

   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.
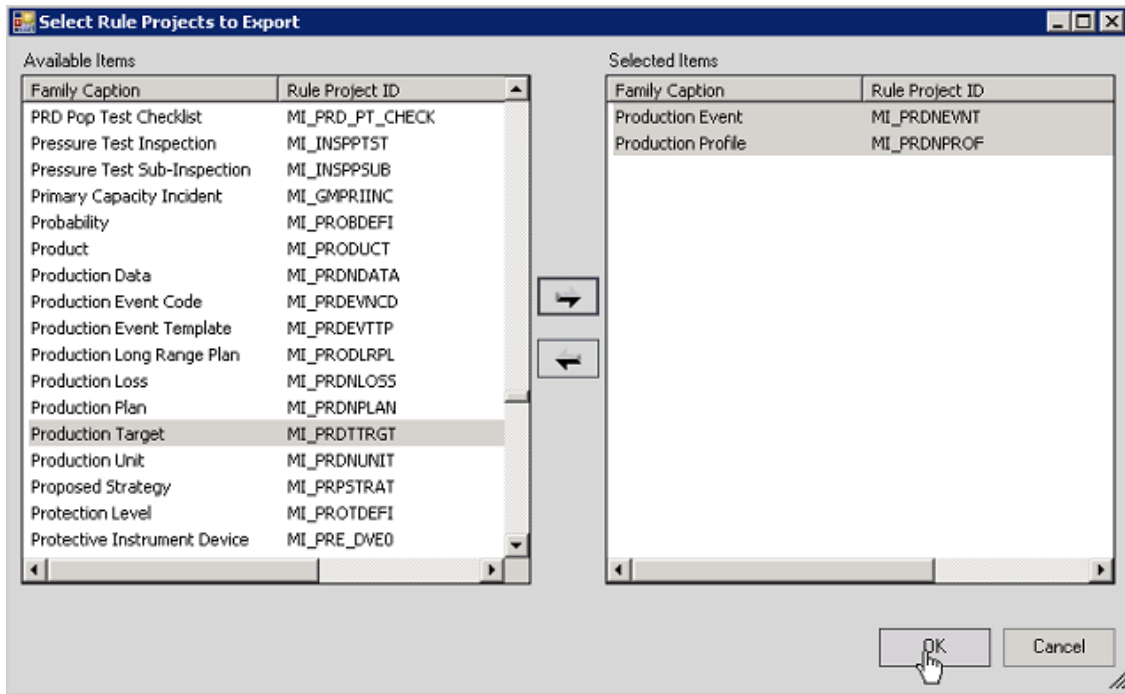
11. Select **OK**.

The **Select Rule Projects to Export** window closes, and, on the **Import/Export Metadata** window, the **Family Rule Projects** check box is selected automatically.
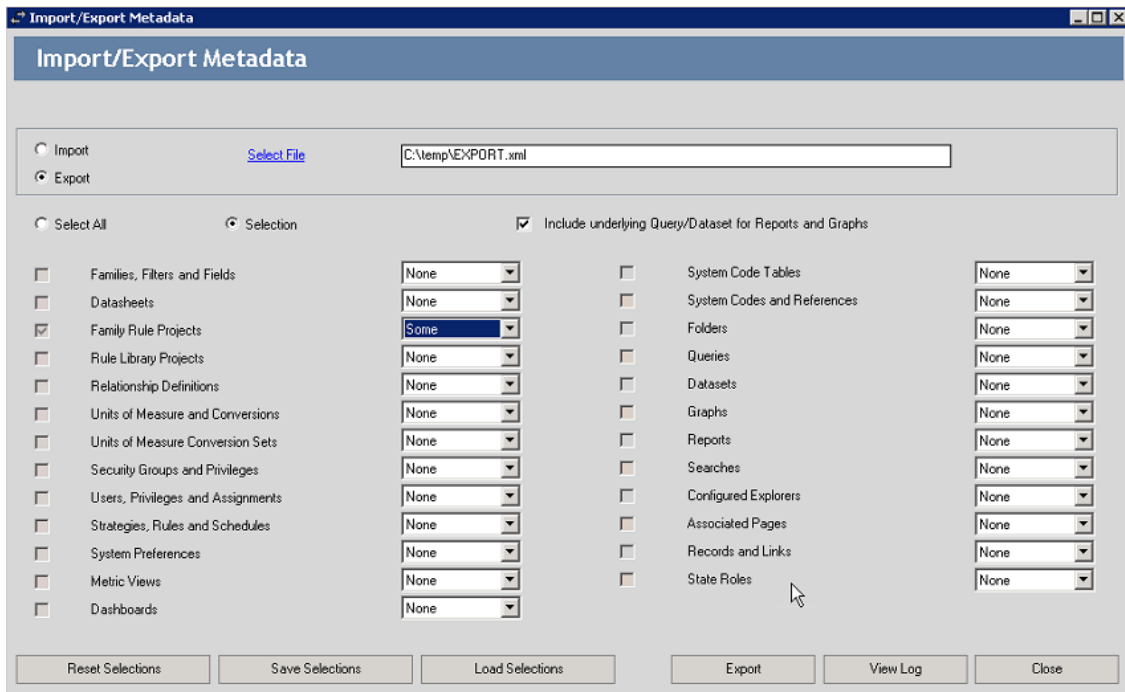
12. Select **Export**.

   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.
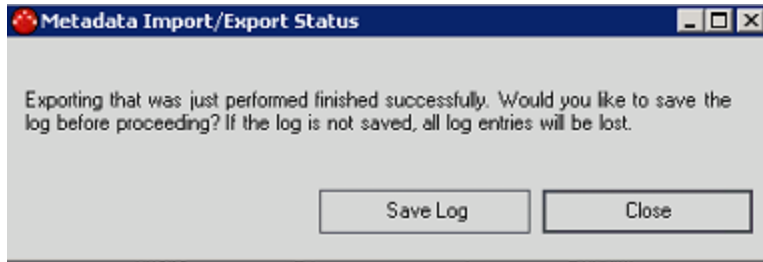
13. Select **Save Log**.

   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 Enterprise APM Server machine, via the Windows start button, access Configuration Manager.

   The **Meridium APM Login** window appears.
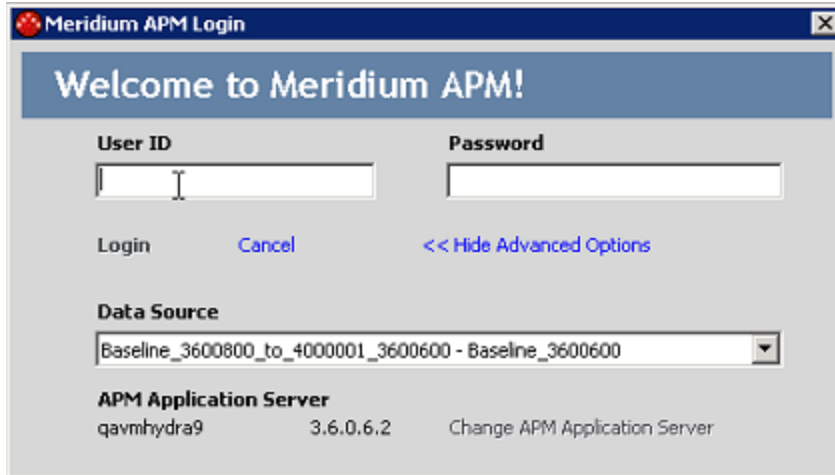
20. Enter your User ID and Password into the appropriate boxes, and then, in the **Data Source** box, select your current, pre-upgraded database.

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.
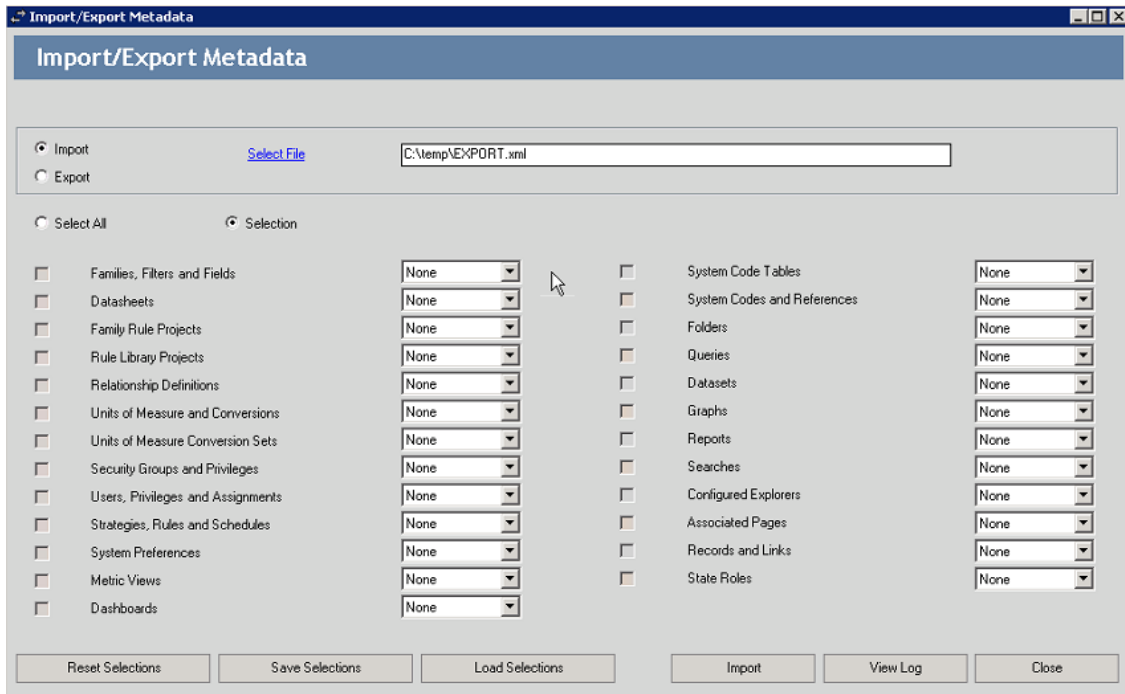
25. Select the **Selection** check box.

26. In the drop-down list box to the right of the **Family Rule Projects** check box, select **Some**.

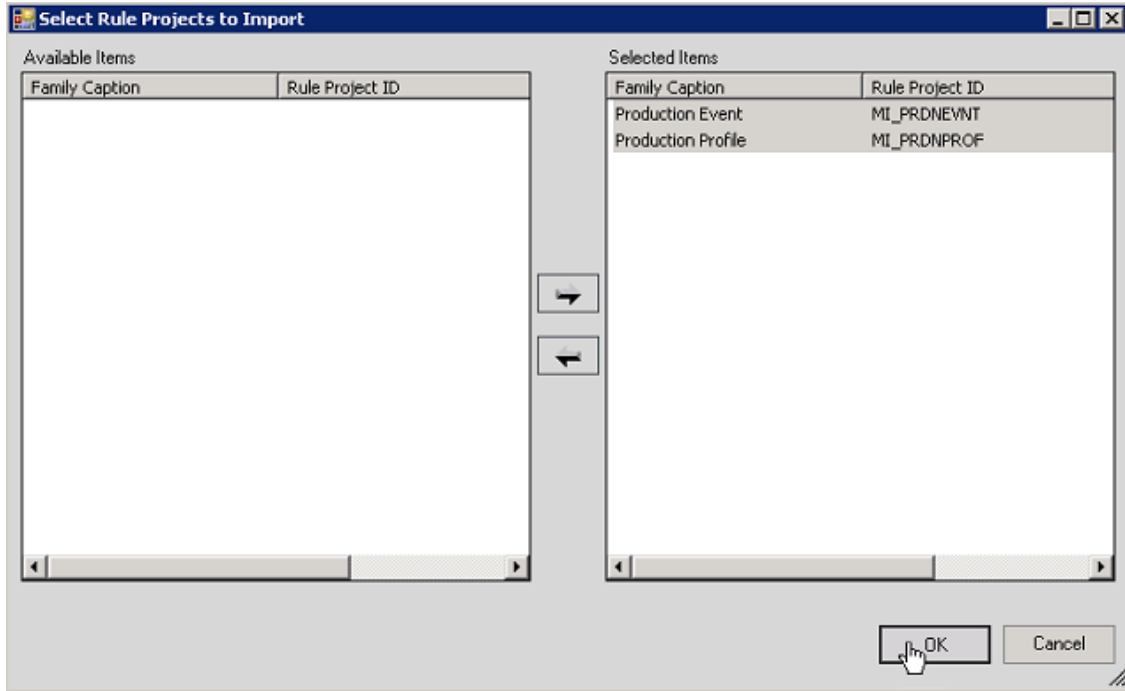The **Select Rule Projects to Import** window appears.
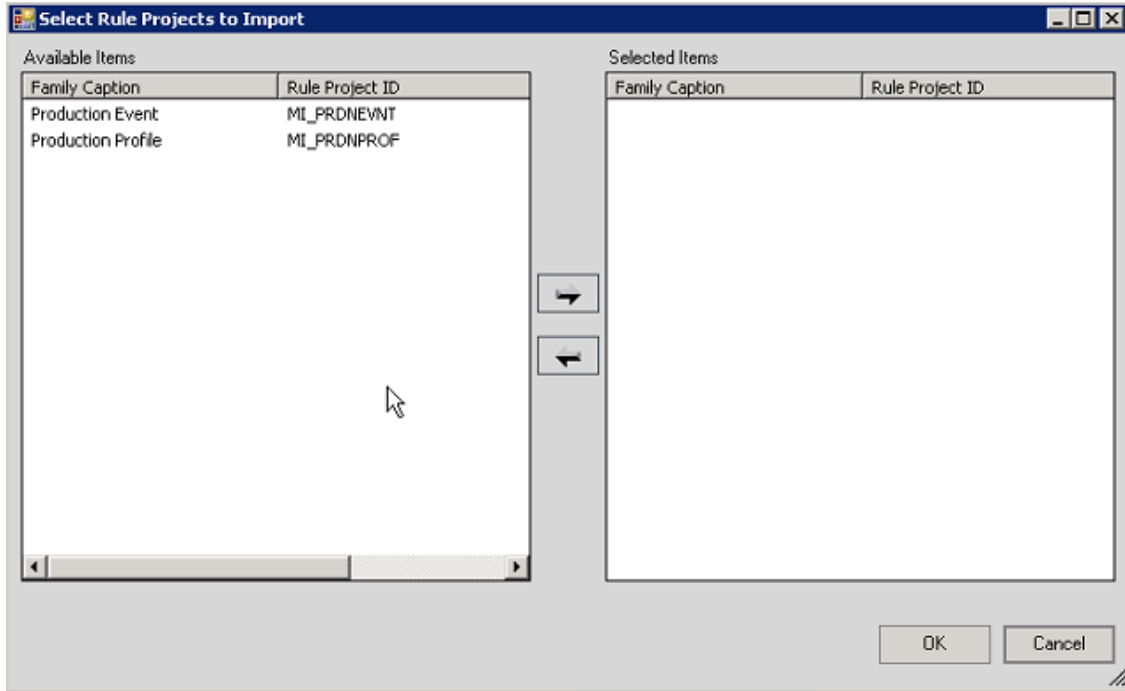
27. In the **Available Items** section, select the item whose Family Caption is Production Event, and then select [→].

   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.
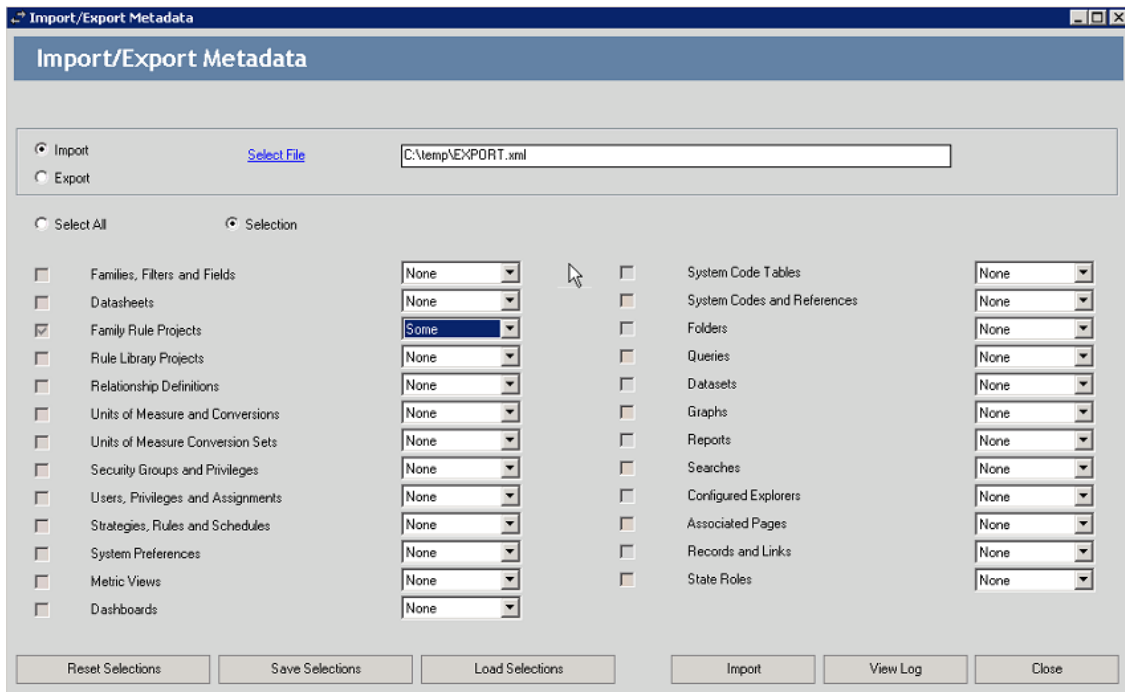
30. Select **Import**.

    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.
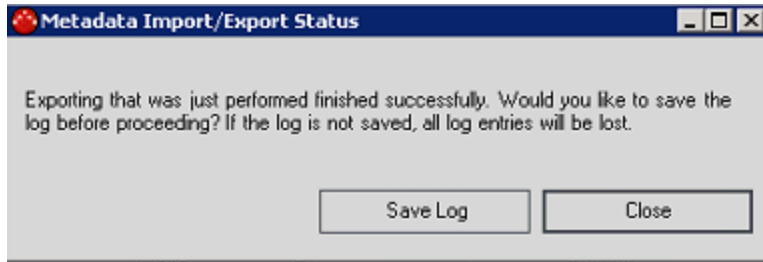
31. Select **Save Log**.

    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**.

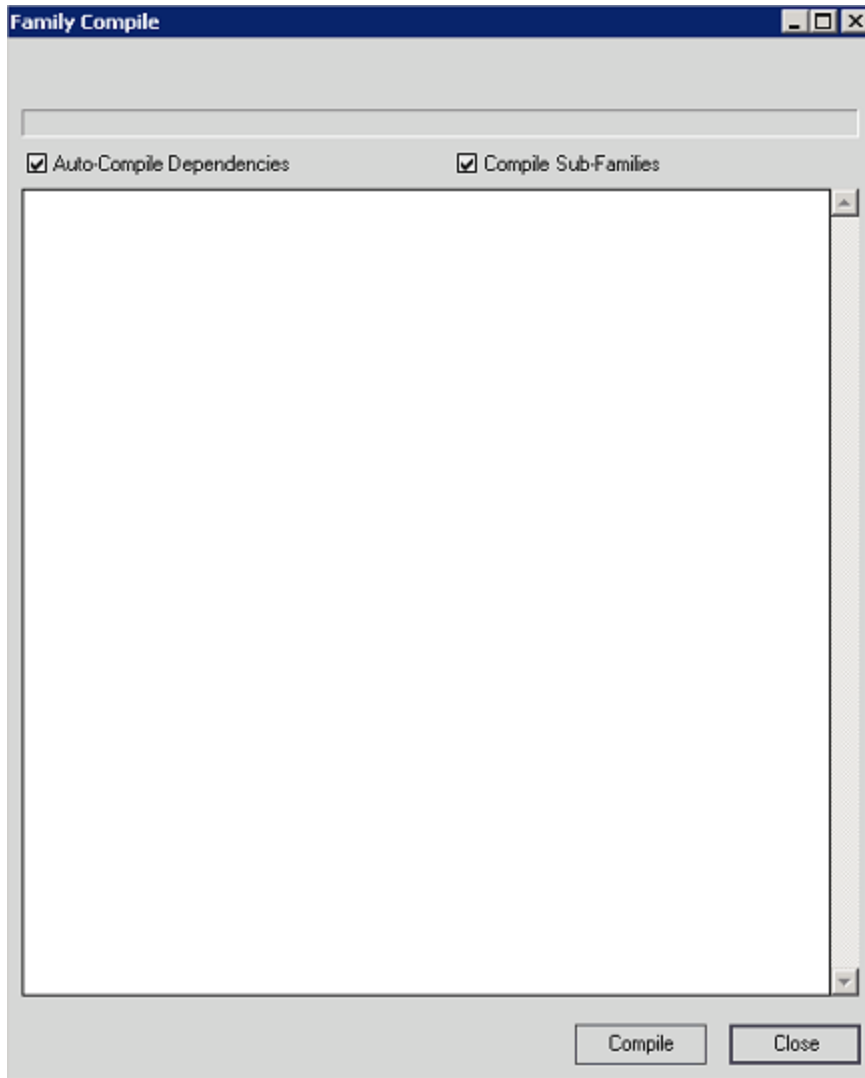   The **Metadata Import/Export Status** dialog box closes.

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.

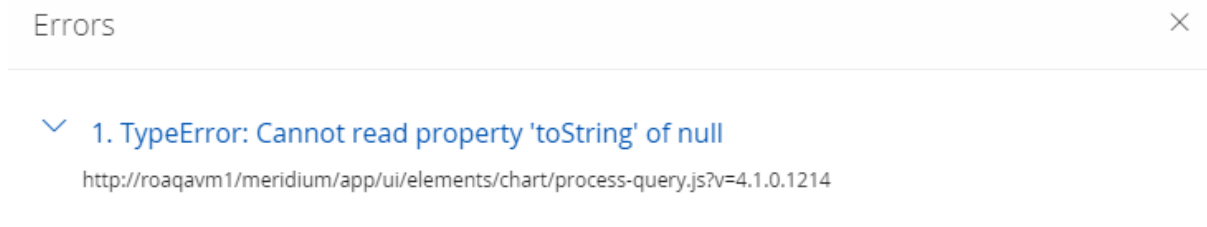38. When the progress bar reaches the end, select **Close**.

    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

The **Top 10 Bad Actors** query is used by Meridium Enterprise 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:

Errors   ✕

∨   1. TypeError: Cannot read property 'toString' of null
        http://roaqavm1/meridium/app/ui/elements/chart/process-query.js?v=4.1.0.1214

To implement the corrected query and to correct this error, complete the following steps.

Steps

1. Access the **Query** page .

2. In the heading of the **Query** page, select **Browse**.

   The **Select a query from the catalog** window appears.

   Select a query from the catalog

Catalog
⟨ 🔍 ⌃
Home ∨
Personal
Public
Baseline

   Open   Cancel
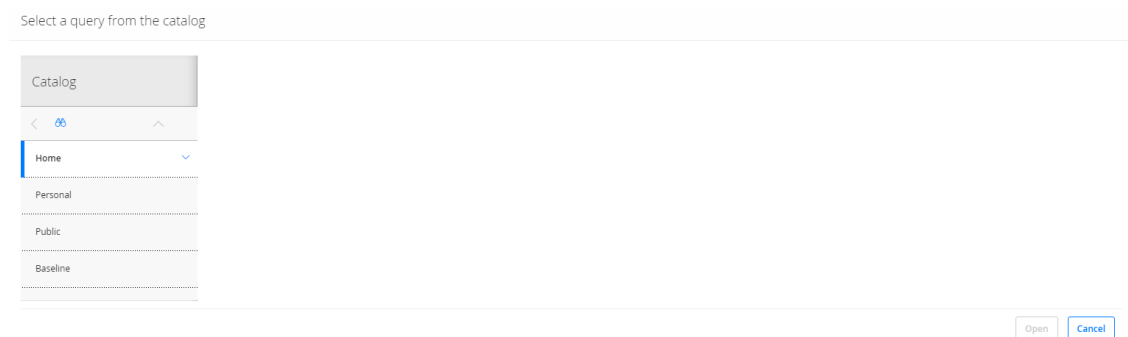
3. In the left pane, navigate the **Catalog** to*: Meridium/Public/Modules/PLA/Queries,* select the **Top10BadActors** query and then select **Open.**

   The **Enter Parameter Values** window appears.

4. Select **OK**.

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-
d=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**.

Production Loss Analysis 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 Production Loss Accounting Administrator	MI FE Admin
MI Production Loss Accounting Manager	MI FE Admin
	MI FE PowerUser
MI Production Loss Accounting Service	MI FE Admin
MI Production Loss Accounting User	MI FE Admin
	MI FE PowerUser
	MI FE User

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

Family	MI Production Loss Accounting Administrator	MI Production Loss Accounting Manager	MI Production Loss Accounting Service	MI Production Loss Accounting User
Entity Families				
Equipment	View, Update, Insert, Delete	View	View	View
Functional Location	View	View	View	View
Impact Code	View, Update, Insert, Delete	View	View	View
Interface Log	View, Update, Insert, Delete	View	View	View

Family	MI Production Loss Accounting Administrator	MI Production Loss Accounting Manager	MI Production Loss Accounting Service	MI Production Loss Accounting User
OEE Code	View, Update, Insert, Delete	View	View	View
Product	View, Update, Insert, Delete	View	View	View
Production Analysis	View, Update, Insert, Delete	View	View	View, Update, Insert, Delete
Production Data	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert
Production Event	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Production Event Code	View, Update, Insert, Delete	View	View	View
Production Event Template	View, Update, Insert, Delete	View	View	View, Update, Insert, Delete
Production Long Range Plan	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Production Loss	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Production Losses	View, Update, Insert, Delete	None	View, Update, Insert, Delete	View, Update, Insert, Delete
Production Plan	View, Update, Insert, Delete	View	View	View, Update, Insert, Delete
Production Target	View, Update, Insert, Delete	View	View	View, Update, Insert, Delete
Xi Reading	None	None	View	None
Xi Tag	View	None	View	None
Relationship Families				
Analysis Link	View, Update, Insert, Delete	View	View	View, Update, Insert, Delete

Family	MI Production Loss Accounting Administrator	MI Production Loss Accounting Manager	MI Production Loss Accounting Service	MI Production Loss Accounting User
Caused by Production Event	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Base Production Event Code	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Child Production Event Code	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Has Impact Code	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Losses	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has OEE Code	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Product	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Has Production Data	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Production Event	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Production Event Code	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Production Event Template	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Production Long Range Plan	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Production Plan	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Production Profile	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete

Family	MI Production Loss Accounting Administrator	MI Production Loss Accounting Manager	MI Production Loss Accounting Service	MI Production Loss Accounting User
Has Production Target	View, Update, Insert, Delete	View	View	View, Update, Insert, Delete
Has Production Unit	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Reference Documents	View, Update, Insert, Delete	View	View	View, Update, Insert, Delete
Has Reliability	View, Update, Insert, Delete	View	View	View, Update, Insert, Delete
Has Unit Profile	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Has Work History	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Production Event Has RCA Analysis	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Is Production Unit	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Xi Tag Has Production Event Template	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete

Deploy R Scripts

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 R Scripts 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 Meridium Enterprise 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.

Step	Task	Notes
1	Ensure that your R Server is configured according to the R scripts system requirements.	This step is required.
2	In Meridium Enterprise APM, specify the R Server credentials.	This step is required.

Upgrade or Update R Scripts to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

Step	Task	Notes
1	Ensure that your R Server is configured according to the R scripts system requirements.	This step is required.
2	In Meridium Enterprise 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 Meridium Enterprise 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 Meridium Enterprise APM, specify the R Server credentials.	This step is required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

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 Meridium Enterprise APM, specify the R Server credentials.	This step is required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

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 Meridium Enterprise APM, specify the R Server credentials.	This step is required.

Upgrade R Script Metadata

If you are upgrading *directly* from V3.6.0.8.0, after upgrading your database to 4.2.0.7.0, 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.

> ℹ **Note**: If you are unsure whether you need to complete this step, or if you would like assistance, please contact Meridium, Inc.

Steps

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.

Deploy Recommendation 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 module.

Deploy Recommendation Management 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 Meridium Enterprise 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.

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

Upgrade or Update Recommendation Management to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Recommendation 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.

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

Deploy Reliability Analytics

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 Reliability Analytics 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 Meridium Enterprise 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.

Step	Task	Notes
1	Review the Reliability Analytics data models 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 Reliability Analytics Security Groups and Roles.	This step is required.

Upgrade or Update Reliability Analytics to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.0

Reliability Analytics will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Reliability Analytics will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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	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.

Reliability Analytics 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 Reliability Administrator	MI FE Admin
MI Reliability User	MI FE Admin MI FE PowerUser MI FE User
MI Reliability Viewer	MI FE Admin MI FE PowerUser MI FE User

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

Family	MI Reliability Administrator	MI Reliability User	MI Reliability Viewer
Analysis	View	View	View
Distribution	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Exponential	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Growth Model	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Lognormal	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Normal	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI Reliability Administrator	MI Reliability User	MI Reliability Viewer
Production Analysis	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Production Losses	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Reliability Automation Rule	View, Update, Insert, Delete	View	View
Reliability Distribution	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Reliability Growth	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Reliability Recommendation	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Spare	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Spares Analysis	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Spare Analysis Chart	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Spare Application	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Spare Application Population	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Action	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Action Mapping	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Action Optimization	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Action Result	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Analysis	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI Reliability Admin-istrator	MI Reliability User	MI Reliability Viewer
System Asset	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Buffer	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Condition Monitor	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Element	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Element Result	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Global Event	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Inspection	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Link	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Preventative Main-tenance	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Resource	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Resource Result	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Resource Usage	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Risk	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Risk Assessment	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Scenario	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Sensor	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI Reliability Admin-istrator	MI Reliability User	MI Reliability Viewer
System Special Action	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Subsystem	View, Update, Insert, Delete	View, Update, Insert, Delete	View
System Switch	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Weibull	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Analysis Link	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Global Events	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Mitigated TTF Dis-tribution	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Planned Resource Usages	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Consolidated Recom-mendations	View	View	View
Has Recommendations	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Reliability	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Resource Usage	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Risk Assessments	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Root System	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Scenarios	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has System Actions	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI Reliability Admin-istrator	MI Reliability User	MI Reliability Viewer
Has System Elements	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has System Optimization	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has System Resources	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has System Results	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has System Risks	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has TTF Distribution	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Unplanned Resource Usages	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Deploy Reliability Centered Maintenance (RCM)

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 Reliability Centered Maintenance (RCM) 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 Meridium Enterprise 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.

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

Upgrade or Update Reliability Centered Maintenance (RCM) to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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.

Reliability Centered Maintenance (RCM) 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 RCM User MI RCM Viewer	MI Strategy User
MI RCM User MI RCM Viewer	MI Strategy Power
MI RCM User MI RCM Viewer	MI Strategy Admin

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

Family Caption	MI RCM User	MI RCM Viewer
Entity families		
Action	View	View
Asset Criticality Analysis System	View	None
Consequence Definition	View	View
Decision Tree Consequence	View	View
Decision Tree Response	View	View
Decision Tree Structure	View	View

Human Resource	View, Update, Insert, Delete	View
Mitigates Risk	View, Update, Insert, Delete	View
Probability Definition	View	View
Protection Level	View	View
RCM FMEA Analysis	View, Update, Insert, Delete	View
RCM FMEA Asset	View, Update, Insert, Delete	View
RCM Function	View, Update, Insert, Delete	View
RCM Functional Failure	View, Update, Insert, Delete	View
RCM FMEA Failure Mode	View, Update, Insert, Delete	View
RCM FMEA Failure Effect	View, Update, Insert, Delete	View
RCM FMEA Recommendation	View, Update, Insert, Delete	View
RCM FMEA Template	View, Update, Insert, Delete	View
RCM FMEA Task	View, Update, Insert, Delete	View
Reference Documents	View, Update, Insert, Delete	View
Risk Assessment	View, Update, Insert, Delete	View
Risk Category	View	View
Risk Matrix	View	View
Risk Rank	View, Update, Insert, Delete	View
Risk Threshold	View	View

Site Reference	View	View
Task History ℹ️ **Note:** The Task History relationship family is inactive in the baseline Meridium Enterprise APM database.	View, Update, Insert, Delete	View
Relationship Families		
Has Associated Recommendation	View	View
Has Consolidated Recommendations	View	View
Has Driving Recommendation	View	View
Has RCM FMEA Team Member	View, Update, Insert, Delete	View
Has RCM FMEA Analysis	View, Insert, Delete	None
Has RCM FMEA Asset	View, Update, Insert, Delete	View
Has RCM Function	View, Update, Insert, Delete	View
Has RCM Functional Failure	View, Update, Insert, Delete	View
Has RCM FMEA Failure Mode	View, Update, Insert, Delete	View
Has RCM FMEA Failure Effect	View, Update, Insert, Delete	View
Has RCM FMEA Recommendation	View, Update, Insert, Delete	View
Has Reference Values	View	View
Has Recommendations	View, Update, Insert, Delete	View
Has Reference Documents	View, Update, Insert, Delete	View
Has Risk	View	None
Has Risk Category	View, Update, Insert, Delete	View

Has Site Reference	View	View
Has Superseded Recommendations	View	View
Has Task History ℹ **Note:** The Has Task History relationship family is inactive in the baseline Meridium Enterprise APM database.	View, Update, Insert, Delete	View
Has Tasks	View, Update, Insert, Delete	View
Has Templates	View, Update, Insert, Delete	View
Is Based on RCM FMEA Failure Effect	View	View
Is RCM FMEA Asset	View, Update, Insert, Delete	View

With these privileges, any user who is a member of the MI RCM User Security Group will have access to ALL records involved in RCM Analyses. In addition to these baseline privileges, which you can grant by assigning users to the MI RCM User Security Group, you will need to grant RCM users permission to the Equipment or Functional Location family if it is related to the RCM FMEA Asset family through the Is RCM FMEA Asset relationship.

ℹ **Note:** You may also want to grant some users permission to modify the items in the following Catalog folders: \\Public\Meridium\Modules\RCM.

Reports

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 Reports 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 Meridium Enterprise 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.

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 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Install the APM Reports Designer

Before You Begin

- Install Microsoft SQL Server Data Tools - Business Intelligence for Visual Studio 2013 (available at the official Microsoft website).

Steps

1. On the machine that will serve as the APM Reports Designer, access the Meridium APM Enterprise APM Distribution package, and then navigate to the **Admin** folder.

2. Open the file **Setup.exe**.
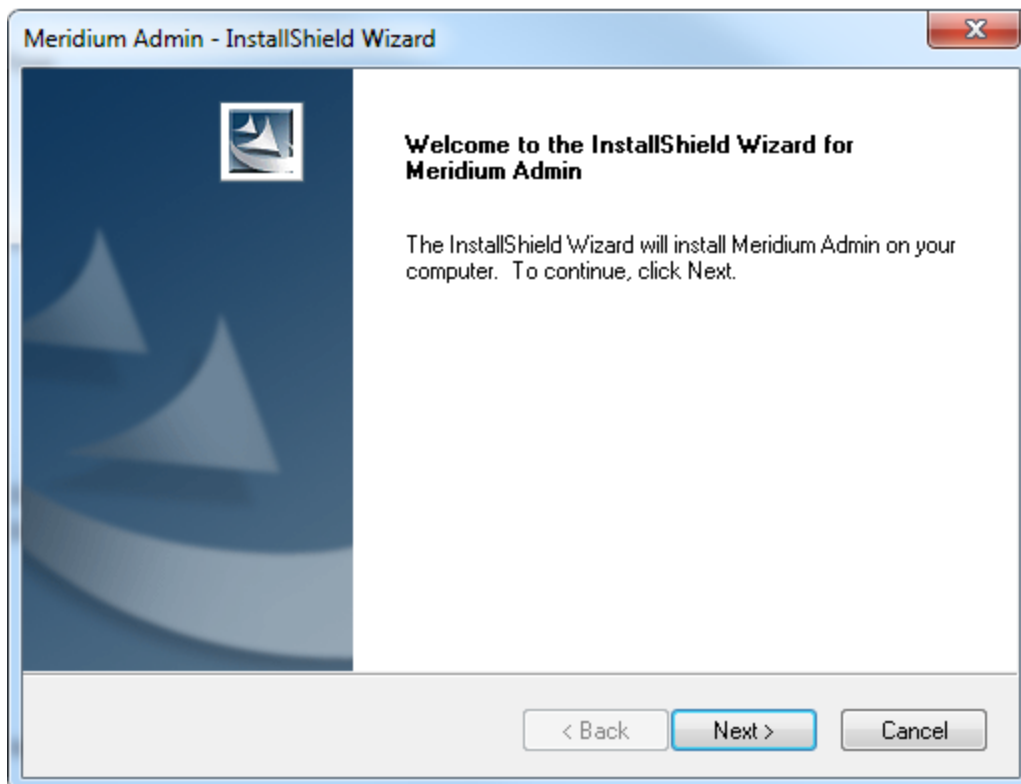
   The **Meridium Admin - InstallShield Wizard** screen appears.

3. Select **Next**.

   The **License Agreement** screen appears.
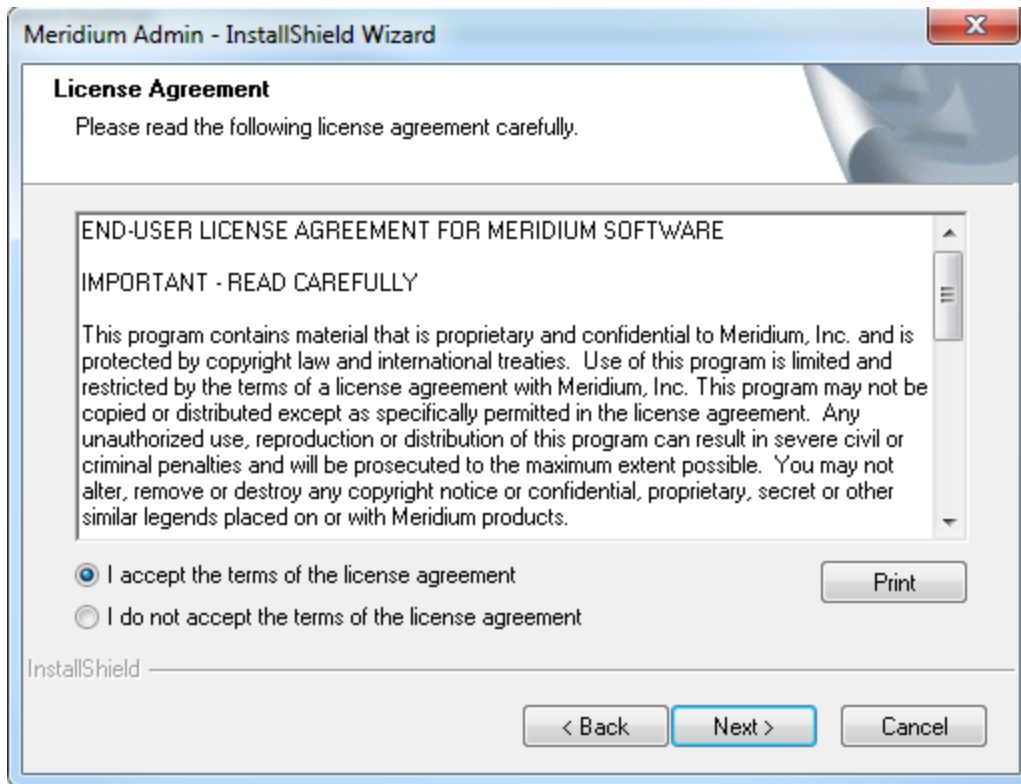
4. Read the License Agreement and, if you agree, select the **I accept the terms of the license agreement** check box. Then, select **Next**.

The **Select Installation Location** screen appears.
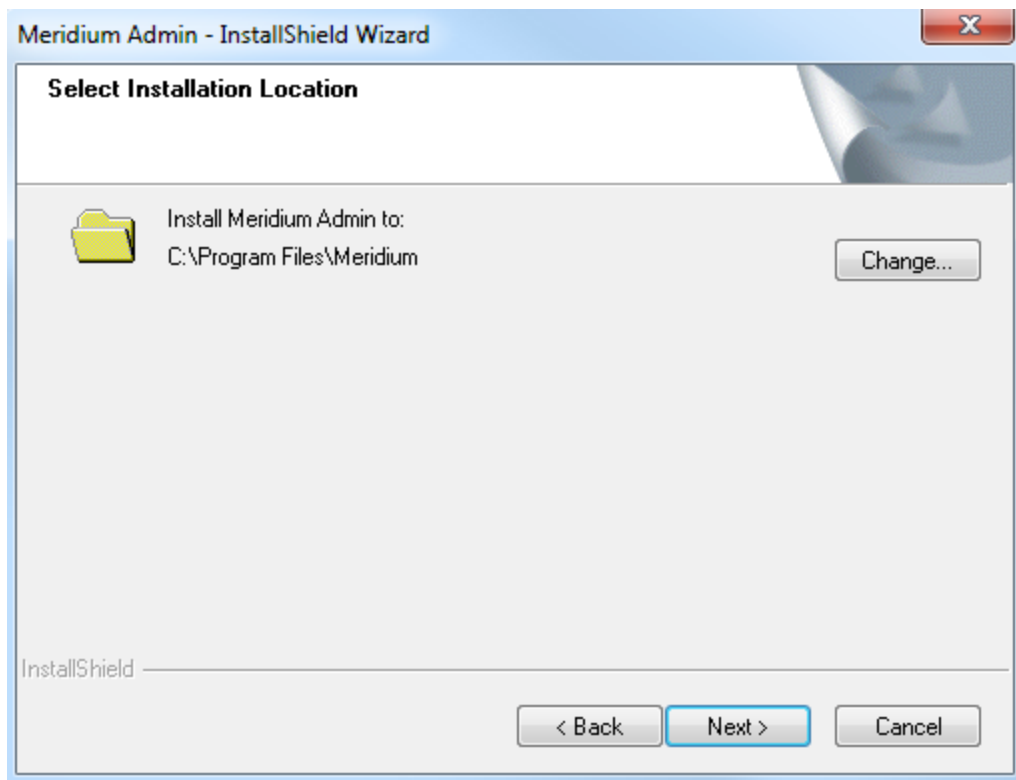
5. Select **Next** to accept the default location.

   The **Select the features you want to install** screen appears.
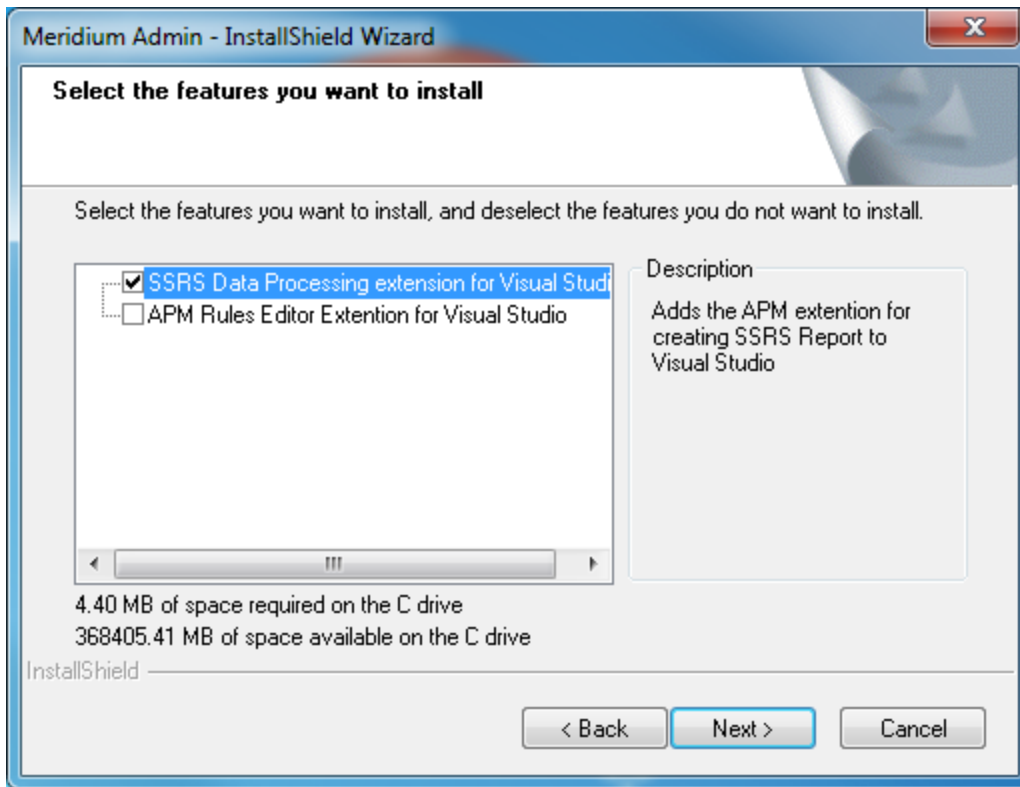
6. Select **SSRS Data Processing Extension for Visual Studio**, and then select **Next**.

   The **Complete the Installation** screen appears.
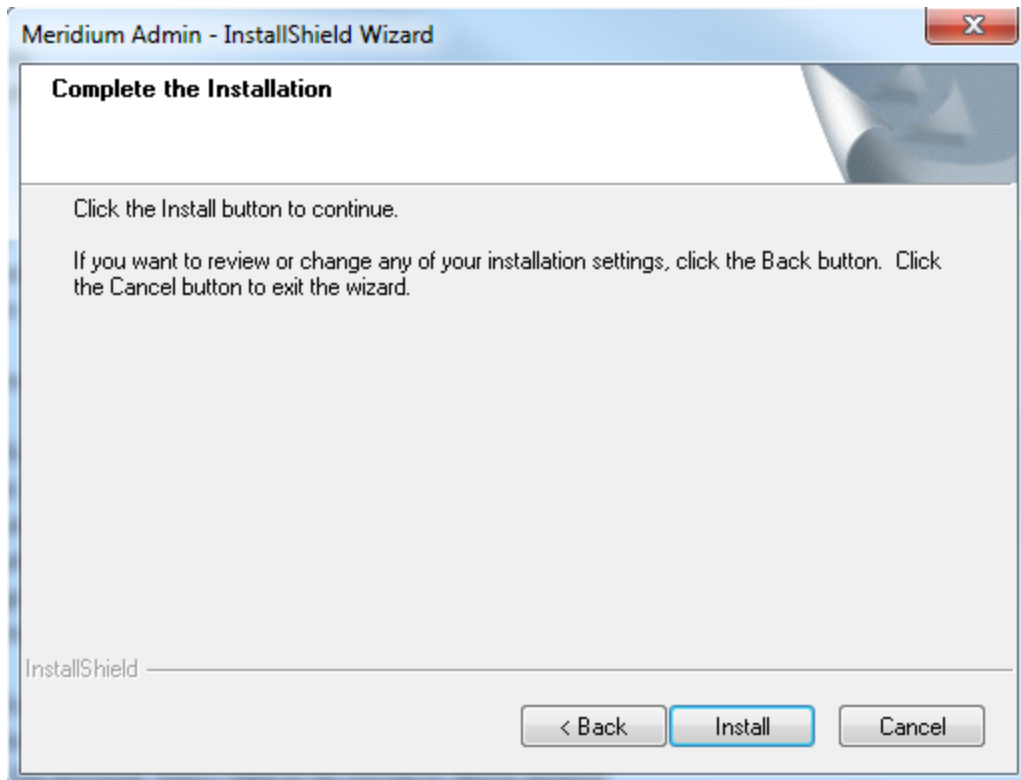
7. Select **Install**.

The **Setup Status** screen appears, which displays a progress bar that shows the progress of the installation process. After the progress bar reaches the end, a message appears, indicating that the installation was successful.
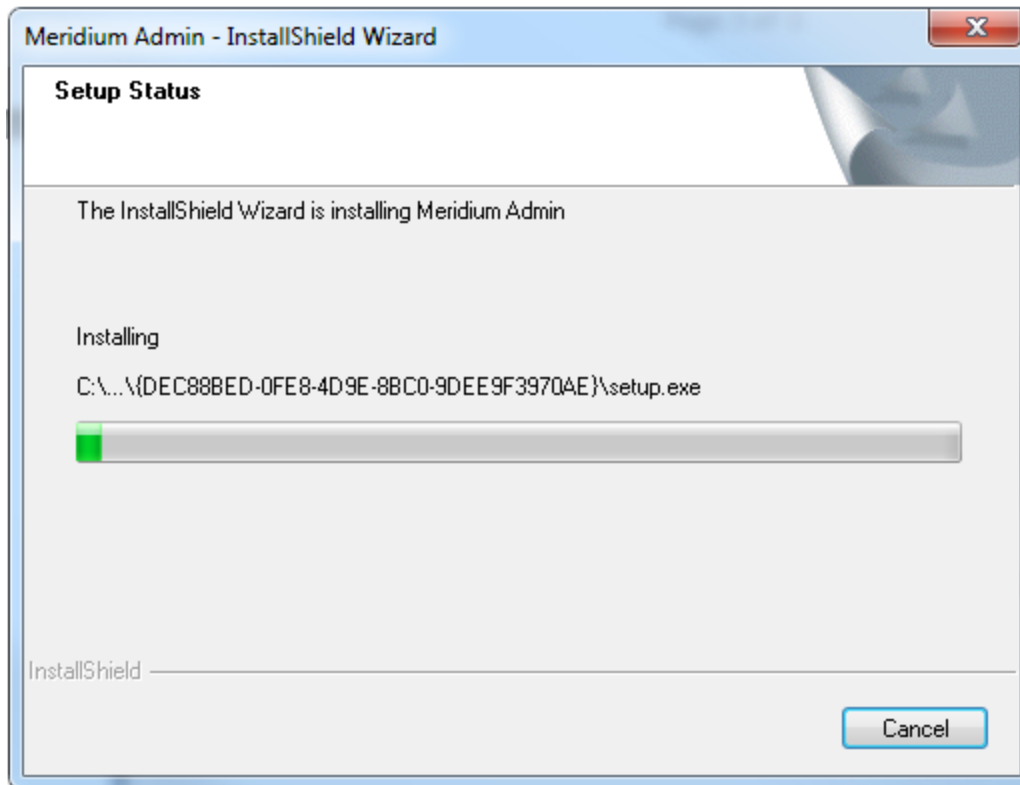
8. Clear the **Launch APM System Administration now** box, and then select **Finish**.
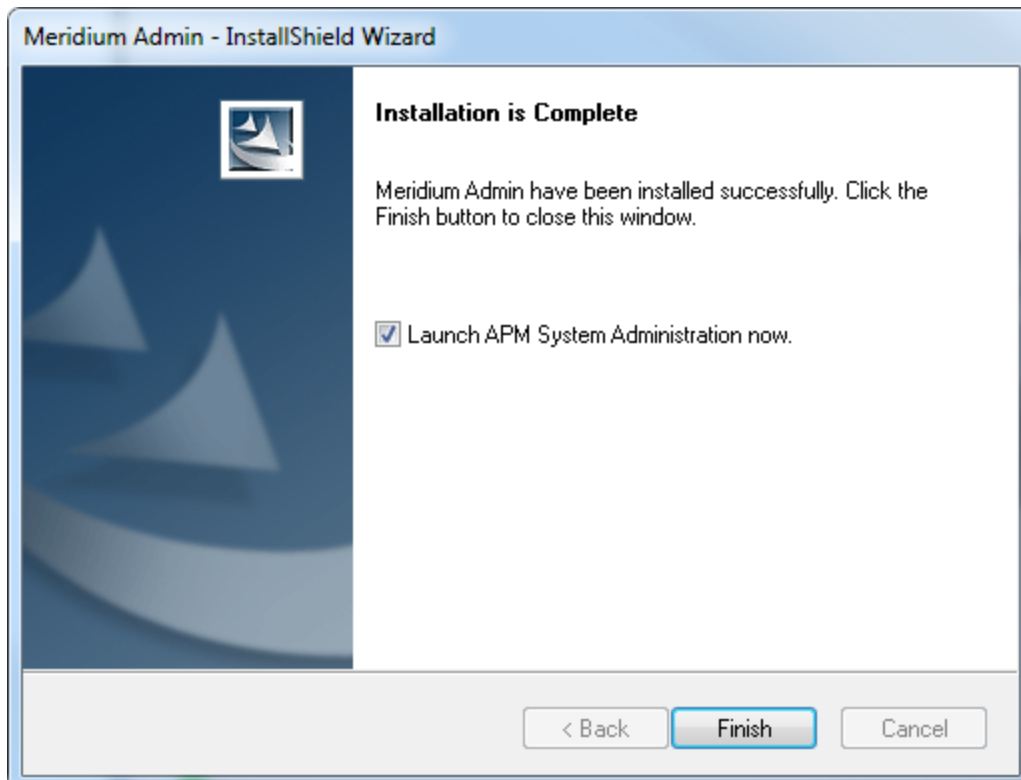
> ℹ **Note:** You may be asked to restart your system for the changes to take effect.

The **APM System Administration** window appears.
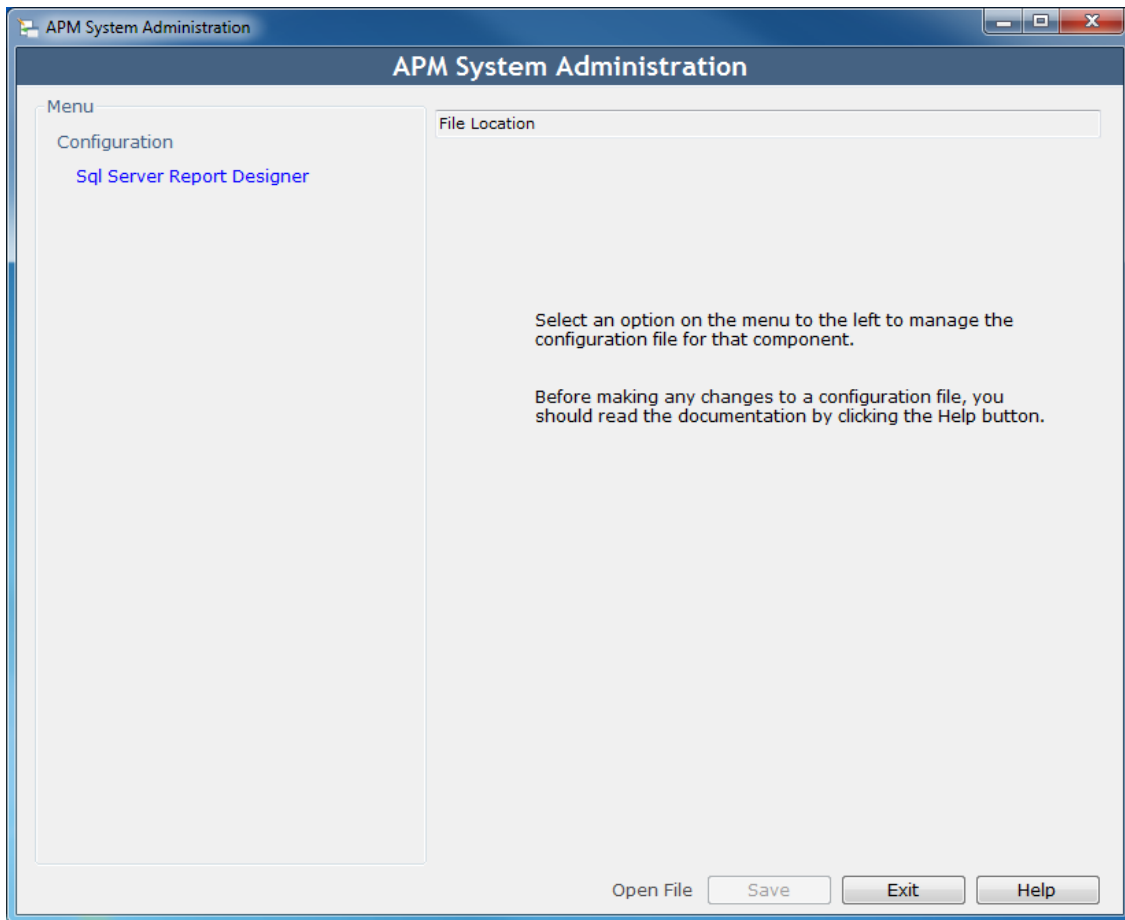
9. Select **Sql Server Report Designer**.

    The **Add Meridium URL to SSRS Designer** box appears.
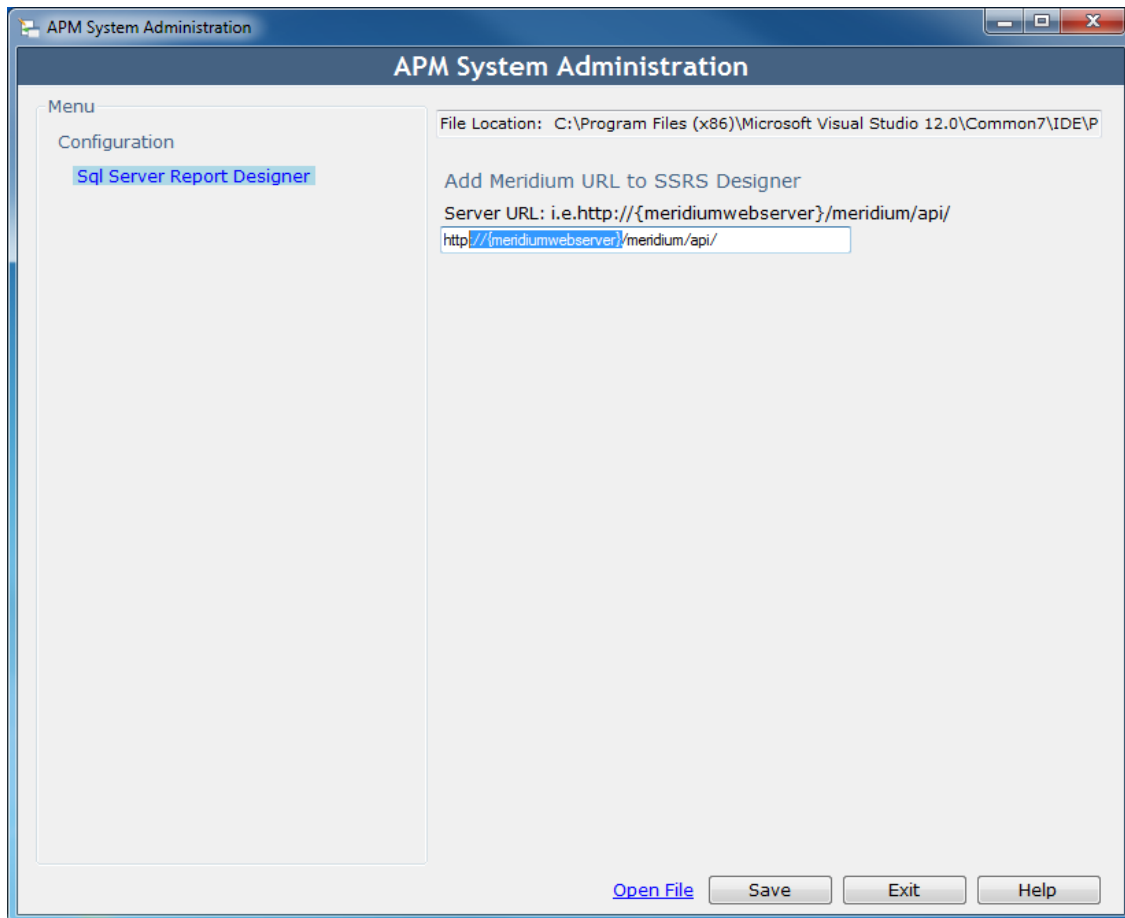
10. Enter the server URL in the **Add Meridium URL to SSRS Designer** box.

11. Select **Save**.

    The Meridium Server URL is added.

12. Select **Exit**.

Results

APM Report Designer is now installed.

What's Next?

- Set Up the APM Report Designer

Set Up the APM Report Designer

After installing the APM Report Designer plugin, you must set up APM Report Designer to interact with Meridium Enterprise APM Server.

Before You Begin

- [Install the APM Report Designer](#).

Steps

1. On the Meridium Enterprise APM Server, open Microsoft Visual Studio.

2. On the **Tools** menu, select **Options**.

   The **Options** window appears.
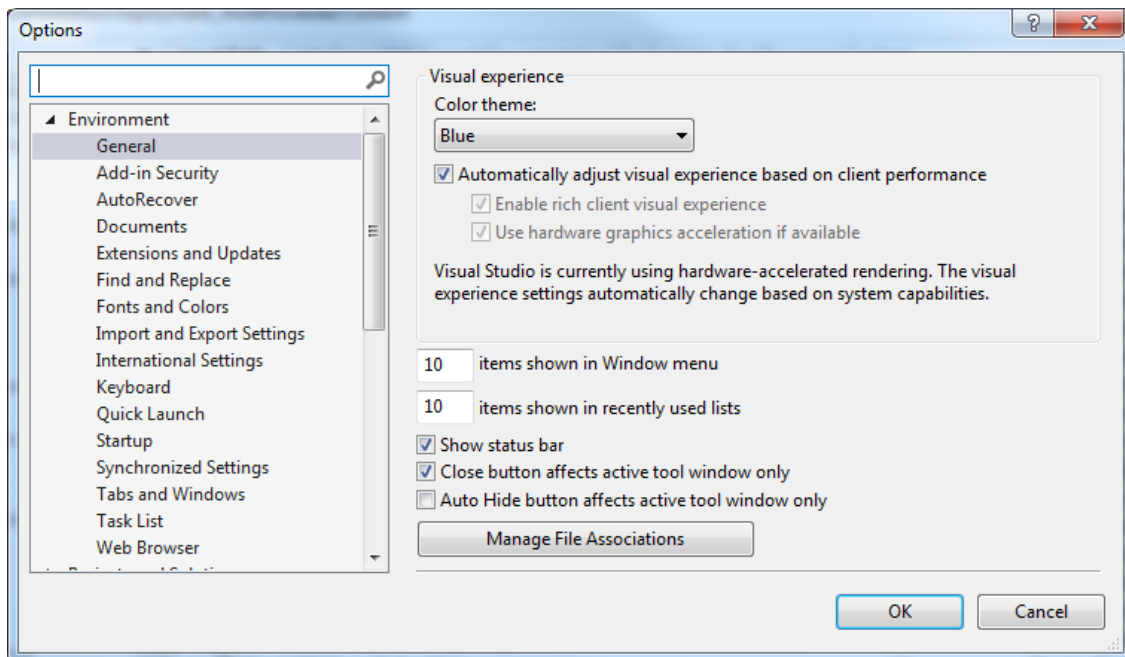
3. On the **Options** window, in the left section, select **APM Report Designer**, and then select **General**.

   The **MeridiumServerURL** box appears in the right section.
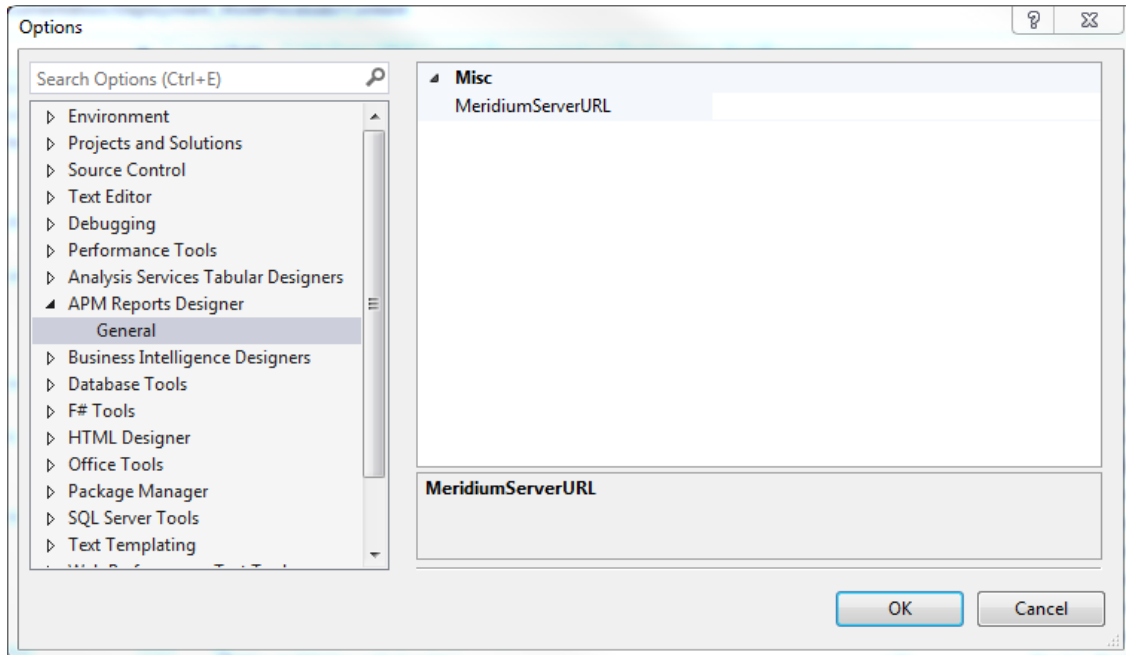
4. In the **MeridiumServerURL** box, enter the Meridium Web Services URL in the following format:

   http://<server_name>//meridium/api/
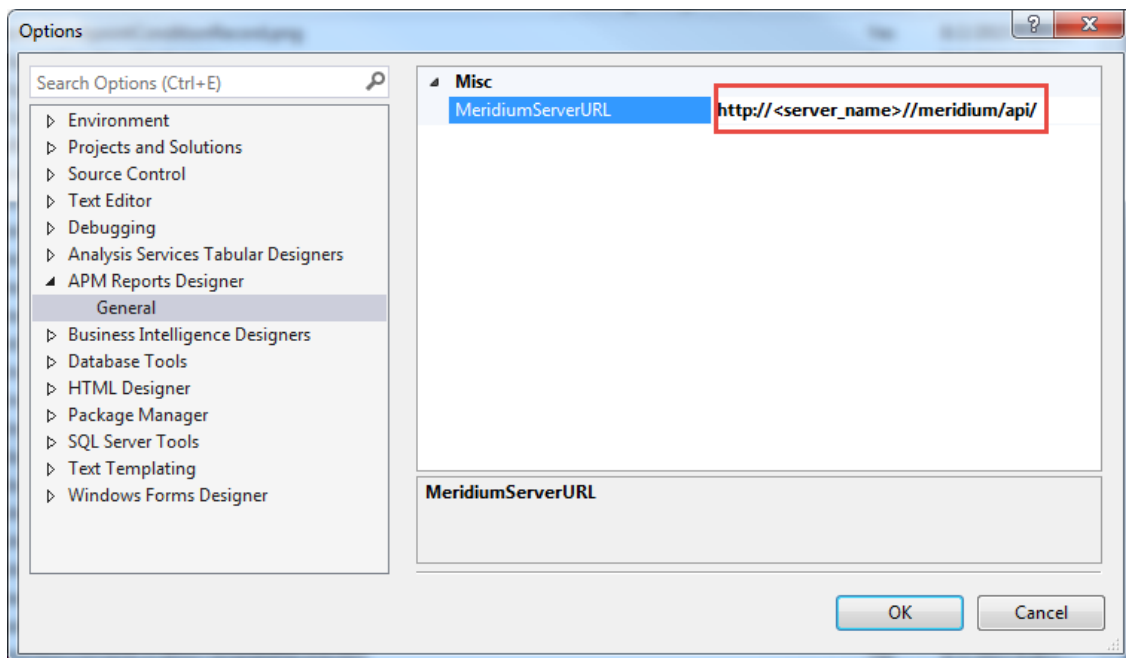
The APM Report Designer setup is now complete.

Deploy RBI 581

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 RBI 581 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 Meridium Enterprise 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.

Step	Task	Notes
1	Review and complete the steps required for deploying R Scripts.	This step is required. This will install R Scripts and other third-party software that is used by the RBI 581 module.
2	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.
3	Assign Security Users to one or more of the RBI Security Groups and Roles.	This step is required.
4	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.
5	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.

Step	Task	Notes
6	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.
7	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.
8	Using Configuration Management, import the **MI_REPFLUID_581.xml** file from the **C:\Meridium\DbUpg\MI_DB_MASTER_4020000\4020000_IEU_ManualImports** folder.	This step is required to import the Representative Fluids that are used in RBI 581. If you want to use *only* RBI 581 (i.e., you do *not* want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 representative fluids. If you want to verify that the file has been imported successfully, run the following query: `SELECT Count( [MI_REPFLUID].[MI_REPFLUID_FLUID_C]) "Fluid" FROM [MI_REPFLUID]` This will return a list of 30 records. If you want to use *both* RBI 580 and RBI 581, import these files *without* deleting the existing content. In this case, the aforementioned query returns a list of 111 records.

Step	Task	Notes
| 9 | Using Configuration Management, import the **MI_CMT_FLE0.xml** file from the **C:\Meridium\DbUpg\MI_DB_MASTER_4020000\4020000\_IEU_Manu-alImports** folder. | This step is required to import the Component Damage Flammable records.<br><br>If you want to use only RBI 581 (i.e., you do not want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Component Damage Flammable records. This will ensure that the content in this table is as per API 3rd Edition table 4.8.<br><br>If you want to verify that the file has been imported successfully, run the following query:<br><br>```
SELECT Count( [MI_CMT_FLE0].[MI_CMT_FLE0_
FLUID_C]) "Fluid" FROM [MI_CMT_FLE0]
```<br><br>This will return a list of 64 records. If you want to use *both* RBI 580 and RBI 581, import these files *without* deleting the existing content. |
| 10 | Using Configuration Management, import the **MI_FLD_VSCY_581.xml** file from the **C:\Meridi-um\DbUpg\MI_DB_MASTER_4020000\4020000\_IEU_Manu-alImports** folder. | This step is required to import the Fluid Viscosity records.<br><br>If you want to use *only* RBI 581 (i.e., you do *not* want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Fluid Viscosity tables. This will ensure that the content in this table is as per API 3rd Edition table 6.1.<br><br>If you want to verify that the file has been imported successfully, run the following query:<br><br>```
SELECT Count( [MI_FLD_VSCY].[MI_FLD_VSCY_
FLUID_C]) "Fluid" FROM [MI_FLD_VSCY]
```<br><br>This will return a list of 5 records. If you want to use *both* RBI 580 and RBI 581, import these files *without* deleting the existing content. In this case, the aforementioned query returns a list of 10 records. |

Step	Task	Notes
11	Using Configuration Management, import the **MI_PRL_CNS0.xml** file from the **C:\Meridium\DbUpg\MI_DB_MASTER_4020000\4020000_IEU_ManualImports** folder.	This step is required to import the Personal Injury Flammable CE Constants records. If you want to use *only* RBI 581 (i.e., you do not want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Fluid Viscosity records. This will ensure that the content in this table is as per API 3rd Edition table 4.9. If you want to verify that the file has been imported successfully, run the following query: `SELECT Count( [MI_PRL_CNS0].[MI_PRL_CNS0_FLUID_C]) "Fluid" FROM [MI_PRL_CNS0]` This will return a list of 62 records. If you want to use *both* RBI 580 and RBI 581, import these files *without* deleting the existing content. In this case, the aforementioned query returns a list of 62 records.
12	On the Meridium Enterprise APM Server, restart Redis.	This step is required, and has to be performed after you complete all the aforementioned steps.
13	On the Meridium Enterprise APM Server, reset IIS.	This step is required, and has to be performed after you complete all the aforementioned steps.

Upgrade or Update RBI 581 to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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	Using Configuration Management, import the **MI_REPFLUID_581.xml** file from the **C:\Meridium\DbUpg\MI_DB_MASTER_4020000\4020000_IEU_ManualImports** folder.	This step is required to import the Representative Fluids that are used in RBI 581. If you want to use *only* RBI 581 (i.e., you do *not* want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 representative fluids. If you want to verify that the file has been imported successfully, run the following query: ```SELECT Count([MI_REPFLUID].[MI_REPFLUID_FLUID_C]) "Fluid" FROM [MI_REPFLUID]``` This will return a list of 30 records. If you want to use both RBI 580 and RBI 581, import these files *without* deleting the existing content. In this case, the aforementioned query returns a list of 111 records.

Step	Task	Notes
2	Using Configuration Management, import the **MI_ CMT_FLE0.xml** file from the **C:\Meridi- um\DbUpg\MI_DB_ MASTER_ 4020000\4020000_IEU_ ManualImports** folder.	This step is required to import the Component Damage Flammable records. If you want to use only RBI 581 (i.e., you do not want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Component Damage Flammable records. This will ensure that the content in this table is as per API 3rd Edition table 4.8. If you want to verify that the file has been imported successfully, run the following query: ```SELECT Count([MI_CMT_FLE0].[MI_CMT_FLE0_FLUID_C]) "Fluid" FROM [MI_CMT_FLE0]``` This will return a list of 64 records. If you want to use both RBI 580 and RBI 581, import these files *without* deleting the existing content.
3	Using Configuration Management, import the **MI_ FLD_VSCY_581.xml** file from the **C:\Meridi- um\DbUpg\MI_DB_ MASTER_ 4020000\4020000_IEU_ ManualImports** folder.	This step is required to import the Fluid Viscosity records. If you want to use *only* RBI 581 (i.e., you do *not* want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Fluid Viscosity tables. This will ensure that the content in this table is as per API 3rd Edition table 6.1. If you want to verify that the file has been imported successfully, run the following query: ```SELECT Count([MI_FLD_VSCY].[MI_FLD_VSCY_FLUID_C]) "Fluid" FROM [MI_FLD_VSCY]``` This will return a list of 5 records. If you want to use both RBI 580 and RBI 581, import these files without deleting the existing content. In this case, the aforementioned query returns a list of 10 records.

Step	Task	Notes
4	Using Configuration Management, import the **MI_ PRL_CNS0.xml** file from the **C:\Meridium\DbUpg\MI_DB_ MASTER_ 4020000\4020000_IEU_ ManualImports** folder.	This step is required to import the Personal Injury Flammable CE Constants records. If you want to use *only* RBI 581 (i.e., you do not want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Fluid Viscosity records. This will ensure that the content in this table is as per API 3rd Edition table 4.9. If you want to verify that the file has been imported successfully, run the following query: ```SELECT Count([MI_PRL_CNS0].[MI_PRL_CNS0_FLUID_C]) "Fluid" FROM [MI_PRL_CNS0]``` This will return a list of 62 records. If you want to use both RBI 580 and RBI 581, import these files without deleting the existing content. In this case, the aforementioned query returns a list of 62 records.
5	Using Configuration Management, import the following files located in the **C:\Meridium\DbUpg\MI_ DB_MASTER_ 4020000\4020000\20_ IEU\50_Other\2_Records-Links** 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 581 *and* 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.

Step	Task	Notes
6	Using Configuration Management, import the following files located in the **C:\Meridium\DbUpg\MI_DB_MASTER_4020000\4020000\20_IEU\50_Other\2_RecordsLinks** folder: • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml	This step is required only if you have not performed it while deploying Risk Based Inspection. This will update the RBI Strategy Mapping Composite entities, overwriting the existing ones.
7	[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.

Step	Task	Notes
8	Review and complete the steps required for deploying R Scripts.	This step is required. This will install R-Script and other third-party software that is used by the RBI 581 module.
9	On the Meridium Enterprise APM Server, reset IIS.	This step is required, and has to be performed after you complete all the aforementioned steps.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

RBI 581 has been introduced in Meridium Enterprise APM V3.6.0.8.0. Therefore, if you have an earlier version of Meridium Enterprise APM, then you must follow the steps in the first-time deployment of RBI 581. If you have deployed RBI 581 in Meridium Enterprise APM V3.6.0.8.0 or later, you must follow the steps outlined in the following table.

Step	Task	Notes
1	Review and complete the steps required for deploying R Scripts.	This step is required. This will install R-Script and other third-party software that is used by the RBI 581 module.
2	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.

Step	Task	Notes
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.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

RBI 581 has been introduced in Meridium Enterprise APM V3.6.0.8.0. Therefore, if you have an earlier version of Meridium Enterprise APM, then you must follow the steps in the first-time deployment of RBI 581. If you have deployed RBI 581 in Meridium Enterprise APM V3.6.0.8.0 or later, you must follow the steps outlined in the following table.

Step	Task	Notes
1	Review and complete the steps required for deploying R Scripts.	This step is required. This will install R-Script and other third-party software that is used by the RBI 581 module.
2	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.

Step	Task	Notes
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.

Add the RBI-581 Tab to Criticality RBI Component Datasheets

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** tab to those customized datasheets. The following table indicates the fields that should appear on each datasheet.

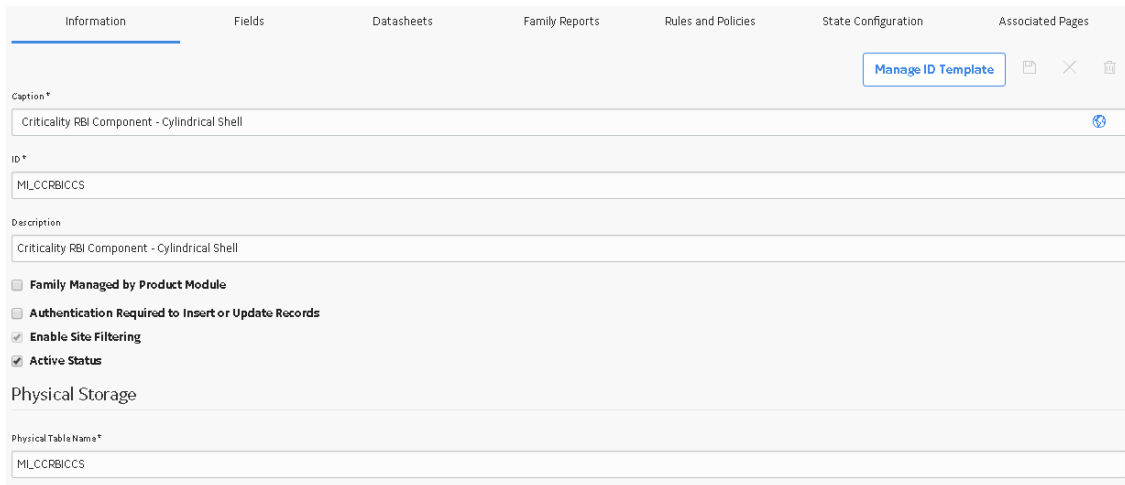| Caption	Field ID	Criticality RBI Component - Cylindrical Shell	Criticality RBI Component - Exchanger Bundle	Criticality RBI Component - Exchanger - Header	Criticality RBI Component - Exchanger Tube	Criticality RBI Component - Piping	Criticality RBI Component - Tank Bottom
Coefficient Y Material	MI_CCRBIC-OM_COEFFI-CNT_Y_MTRL_C	✕	✕	✕	✕	✓	✕
Percent Liquid Volume	MI_RBICOM-PO_PER_LIQ_VOL_N	✓	✓	✓	✓	✓	✓
Cladding Present	MI_CCRBIC-OM_CLADDI-NG_PRESE-NT_L	✓	✓	✓	✓	✓	✓

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
Detection System	MI_CCRBICOM_DETECTION_SYSTEM_C	✓	✓	✓	✓	✓	✓
Mitigation System	MI_CCRBICOM_MITIGATION_SYSTM_C	✓	✓	✓	✓	✓	✓
Fluid Velocity	MI_CCRBICOM_FLUID_VELOCITY_N	✓	✓	✓	✓	✓	✓
Isolation System	MI_CCRBICOM_ISOLA_SYSTE_CHR	✓	✓	✓	✓	✓	✓
Geometry Type	MI_CCRBICOM_GEOMETRY_TYPE_C	✓	✓	✓	✓	✓	✓

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
GFF Component Type	MI_CCRBICOM_GFF_COMPO_O_TYPE_CHR	✓	✓	✓	✓	✓	✓
Minimum Structural Thickness	MI_CCRBICOM_MNMM_STRCTRL_THS_N	✓	✓	✓	✓	✓	✓
Furnished Cladding Thk	MI_CCRBICOM_FRNSHD_CLDDG_THK_N	✓	✓	✓	✓	✓	✓
Liner Present	MI_CCRBICOM_LINER_PRESE_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
Liner Type	MI_ CCRBIC- OM_ LINER_ TP_C	✓	✓	✓	✓	✓	✓
Has Release Prevention - Barrier?	MI_ CCRBIC- TB_ HAS_ RELEA_ PREVE_ F	✕	✕	✕	✕	✕	✓
CM Corrosion Rate	MI_ CCRBIC- OM_ CM_ COR_ RT_C	✓	✓	✓	✓	✓	✓
Corrosion Allow	MI_ RBICOM- PO_ CORR- O_ ALLOW_ N	✓	✓	✓	✓	✓	✓
pH of Water	MI_ CCRBIC- OM_ PH_OF_ WATE- R_N	✓	✓	✓	✓	✓	✓

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
Specified Tmin	MI_CCRBIC-OM_SPECIFI-ED_TMIN_N	✓	✓	✓	✓	✓	✓
Cladding Material	MI_CCRBIC-OM_CLADDI-NG_MATERI-L_C	✓	✓	✓	✓	✓	✓
Is Intrusive?	MI_RBICOM-PO_IS_INTRU_CHR	✓	✓	✓	✓	✓	✓
Base Material	Base Material MI_CCRBIC-OM_BASE_MATE-R_C	✓	✓	✓	✓	✓	✓
Total Acid Number	MI_CCRBIC-OM_TOTAL_ACID_NUMB-R_N	✓	✓	✓	✓	✓	✓

Steps

> **Note:** You must repeat this procedure for each Criticality RBI Component datasheet that you have customized.

1. Access the **Family Management** page.

2. In the left pane, locate 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. At the top of 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. In the new tab, rename *new section* to *RBI-581*.

6. In the **RBI-581** section, select **Table Layout**.

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 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 Coefficent Y Material field to the **Value(s)** column, then enter *Coefficient Y Material* into the corresponding cell in the left column.

10. At the top of the workspace, select ≡+.

    In the **RBI-581** section, in the table, a new row appears.

11. Repeat steps 9 to 11 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 you selected in step 2 is saved, and the **RBI-581** tab will now appear on the selected Criticality RBI Component datasheet.

RBI 581 Security Groups and Roles

[RBI 581 shares the same security groups as Risk Based Inspection](). Any existing RBI user will be able to access RBI 581, after the module is activated.

Deploy Risk Based Inspection (RBI)

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 Risk Based Inspection (RBI) 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 Meridium Enterprise 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.

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 RBI Security Groups and Roles.	This step is required.
3	Add 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.
4	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.
5	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 rather want to use the Asset Strategy Management (ASM) module to recommend actions and manage mitigated risk. This check box is selected by default.
6	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.

Step	Task	Notes
7	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.
8	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.
9	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.
10	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.
11	Configure the Meridium Enterprise APM system to generate RBI Recommendation records automatically.	This step is optional.
12	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 Meridium Enterprise APM database.
13	Assign a ranking to all Qualatative 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.

Upgrade or Update Risk Based Inspection (RBI) to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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	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
2	On the Meridium Enterprise 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_4200000\4200000\20_IEU\50_Other\2_RecordsLinks**. You must extract the **4200000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.
3	On the Meridium Enterprise 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_4020000\4020000\20_IEU\50_Other\2_RecordsLinks**. You must extract the **4020000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required only if you have not completed it while upgrading RBI 581. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in this KBA.

Upgrade from any version V4.0.0.0 through V4.0.1.0

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 Meridium Enterprise 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_4200000\4200000\20_IEU\50_Other\2_RecordsLinks**. You must extract the **4200000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.

Step	Task	Notes
3	On the Meridium Enterprise APM Server, using Configuration Manager, import the following files: • Select Protected Assets • Unlinked Corrosion Loops These files should be located in the following folder: **C:\Meridi-um\DbUpg\MI_DB_MASTER_4200000\4200000_IEU_Cata-logItems_Queries**. You must zip any files together that you need to import into the system. You must extract the **4200000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required only if you have modified the queries that were delivered in baseline. After you complete this step, Site Filtering is enabled.
4	On the Meridium Enterprise APM Application 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:\Meridi-um\DbUpg\MI_DB_MASTER_4020000\4020000\20_IEU\50_Other\2_RecordsLinks**. You must extract the **4020000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required only if you have not completed it while [upgrading RBI 581](#). This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in this [KBA](#).

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

Step	Task	Notes
1	[Import Policy records](#) that Meridium, Inc. modified in order to fix issues in the [associated policy diagrams](#). This includes the following Policy records: Appendix_G; Appendix_H; Appendix_I.	This step is required only if you use Policy records to generate RBI Recommendations.
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 Meridium Enterprise 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_4200000\4200000\20_IEU\50_Other\2_RecordsLinks**. You must extract the **4200000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.
4	On the Meridium Enterprise 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_4020000\4020000\20_IEU\50_Other\2_RecordsLinks**. You must extract the **4020000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required only if you have not completed it while upgrading RBI 581. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in this KBA.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

Step	Task	Notes
1	[Import Policy records](#) that Meridium, Inc. modified in order to fix issues in the [associated policy diagrams](#). This includes the following Policy records: Appendix_G; Appendix_H; Appendix_I.	This step is required only if you use Policy records to generate RBI Recommendations.
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 Meridium Enterprise 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_4200000\4200000\20_IEU\50_Other\2_RecordsLinks**. You must extract the **4200000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.
4	On the Meridium Enterprise 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_4020000\4020000\20_IEU\50_Other\2_RecordsLinks**. You must extract the **4020000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required only if you have not completed it while [upgrading RBI 581](). This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in this [KBA]().

Upgrade from any version V3.5.1 through V3.5.1.12.0

Step	Task	Notes
1	Import Policy records that Meridium, Inc. modified in order to fix issues in the associated policy diagrams. This includes the following Policy records: Appendix_G; Appendix_H; Appendix_I.	This step is required only if you use Policy records to generate RBI Recommendations.
2	Import the Inspection Strategy records that Meridium, Inc. 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 Meridium Enterprise APM Server machine: **C:\Meridium\DbUpg\MI_DB_Master_3600000\3600000\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 Meridium Enterprise 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_4200000\4200000\20_IEU\50_Other\2_RecordsLinks**. You must extract the **4200000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.

Step	Task	Notes
4	On the Meridium Enterprise 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_4020000\4020000\20_ IEU\50_Other\2_RecordsLinks**. You must extract the **4020000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required only if you have not completed it while upgrading RBI 581. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in this KBA.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

Step	Task	Notes
1	Import Policy records that Meridium, Inc. modified in order to fix issues in the associated policy diagrams. This includes the following Policy records: Appendix_G; Appendix_H; Appendix_I.	This step is required only if you use Policy records to generate RBI Recommendations.
2	Import the Inspection Strategy records that Meridium, Inc. 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 Meridium Enterprise APM Server machine: **C:\Meridium\DbUpg\MI_DB_Master_ 3600000\3600000\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.

Step	Task	Notes
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.
6	On the Meridium Enterprise 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_4200000\4200000\20_IEU\50_Other\2_RecordsLinks**. You must extract the **4200000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.

Step	Task	Notes
7	On the Meridium Enterprise 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_4020000\4020000\20_IEU\50_Other\2_RecordsLinks**. You must extract the **4020000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required only if you have not completed it while upgrading RBI 581. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in this KBA.

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	Import Policy records that Meridium, Inc. modified in order to fix issues in the associated policy diagrams. This includes the following Policy records: Appendix_G; Appendix_H; Appendix_I.	This step is required only if you use Policy records to generate RBI Recommendations.

Step	Task	Notes
2	Import the Inspection Strategy records that Meridium, Inc. 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 Meridium Enterprise APM Server machine: **C:\Meridium\DbUpg\MI_DB_Master_3600000\3600000\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 Meridium Enterprise 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_4200000\4200000\20_IEU\50_Other\2_RecordsLinks**. You must extract the **4200000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.
7	On the Meridium Enterprise 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_4020000\4020000\20_IEU\50_Other\2_RecordsLinks**. You must extract the **4020000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required only if you have not completed it while upgrading RBI 581. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in this KBA.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	Import Policy records that Meridium, Inc. modified in order to fix issues in the associated policy diagrams. This includes the following Policy records: Appendix_G; Appendix_H; Appendix_I.	This step is required only if you use Policy records to generate RBI Recommendations.

Step	Task	Notes
2	Import the Inspection Strategy records that Meridium, Inc. 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 Meridium Enterprise APM Server machine: **C:\Meridium\DbUpg\MI_DB_Master_3600000\3600000\20_IEU\50_Other\2_RecordsLinks** 2. Import the file **MI_INSP_STRAT.xml** from the afore-mentioned 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 Meridium Enterprise 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_4200000\4200000\20_ IEU\50_Other\2_RecordsLinks**. You must extract the **4200000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required. This will overwrite the existing Strategy Mapping Composite Entities.
7	On the Meridium Enterprise 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_4020000\4020000\20_ IEU\50_Other\2_RecordsLinks**. You must extract the **4020000** archive from the **MI_DB_MASTER_4200000** archive.	This step is required only if you have not completed it while upgrading RBI 581. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in this KBA.

Risk Based Inspection 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
RBI Security Groups	
MI RBI Administrator	MI Mechanical Integrity Administrator
MI RBI Analyst	MI Mechanical Integrity Administrator
	MI Mechanical Integrity Power
RBI Policy Security Groups	
MI RBI Calculation Policy Designer	None
MI RBI Calculation Policy Viewer	MI Mechanical Integrity Administrator
	MI Mechanical Integrity Power
MI RBI Recommendation Policy Designer	None
MI RBI Recommendation Policy Viewer	MI Mechanical Integrity Administrator
	MI Mechanical Integrity Power
MI RBI Risk Mapping Policy Designer	None
MI RBI Risk Mapping Policy Viewer	MI Mechanical Integrity Administrator
	MI Mechanical Integrity Power

The baseline privileges that exist for the RBI Policy Security Groups to access the Policy family are summarized in the following table.

Security Group	Privileges to the Policy Family
MI RBI Calculation Policy Designer	View, Update, Insert, Delete
MI RBI Calculation Policy Viewer	View

Security Group	Privileges to the Policy Family
MI RBI Recommendation Policy Designer	View, Update, Insert, Delete
MI RBI Recommendation Policy Viewer	View
MI RBI Risk Mapping Policy Designer	View, Update, Insert
MI RBI Risk Mapping Policy Viewer	View

The baseline family-level privileges that exist for the MI RBI Administrator and MI RBI Analyst Security Groups are summarized in the following table.

Family	MI RBI Administrator	MI RBI Analyst
Entity Families		
Asset Group	View, Update, Insert, Delete	View, Update, Insert, Delete
Consequence Evaluation Factors	View, Update, Insert, Delete	View
Corrosion	View	View
Corrosion Analysis Settings	View	View
Criticality Consequence Evaluation	View, Update, Insert, Delete	View, Update, Insert, Delete
Criticality Env. Crack. Deg. Mech. Eval.	View, Update, Insert, Delete	View, Update, Insert, Delete
Criticality Ext. Corr. Deg. Mech. Eval.	View, Update, Insert, Delete	View, Update, Insert, Delete
Criticality Int. Corr. Deg. Mech. Eval.	View, Update, Insert, Delete	View, Update, Insert, Delete
Criticality Other Damage Mech. Eval.	View, Update, Insert, Delete	View, Update, Insert, Delete
Criticality RBI Component - Cylindrical Shell	View, Update, Insert, Delete	View, Update, Insert, Delete
Criticality RBI Component - Exchanger Bundle	View, Update, Insert, Delete	View, Update, Insert, Delete
Criticality RBI Component - Exchanger Header	View, Update, Insert, Delete	View, Update, Insert, Delete

Family	MI RBI Administrator	MI RBI Analyst
Criticality RBI Component - Exchanger Tube	View, Update, Insert, Delete	View, Update, Insert, Delete
Criticality RBI Component - Piping	View, Update, Insert, Delete	View, Update, Insert, Delete
Criticality RBI Component - Tank Bottom	View, Update, Insert, Delete	View, Update, Insert, Delete
Data Mapping Column-Field Pair	View, Update, Insert, Delete	View
Data Mapping Group	View, Update, Insert, Delete	View
Data Mapping Query	View, Update, Insert, Delete	View
Degradation Mechanisms Evaluation Factors	View, Update, Insert, Delete	View, Update, Insert, Delete
Equipment	View, Update, Insert, Delete	View, Update, Insert, Delete
Functional Location	View, Update, Insert, Delete	View, Update, Insert, Delete
Grouping Element	View, Update, Insert, Delete	View, Update, Insert, Delete
Inspection Task	View, Update, Insert, Delete	View, Update, Insert, Delete
Meridium General Recommendation	View	View, Update, Insert, Delete
Meridium Reference Tables	View, Update, Insert, Delete	View
Policy	View	View
Potential Degradation Mechanisms	View, Update, Insert, Delete	View
RBI Criticality Analysis	View, Update, Insert, Delete	View, Update, Insert, Delete
RBI Custom DM Evaluation Configuration	View, Update, Insert, Delete	View

Family	MI RBI Administrator	MI RBI Analyst
RBI Custom DM Evaluation Configuration Details	View, Update, Insert, Delete	View
RBI Custom DM Evaluation Validation	View, Update, Insert, Delete	View
RBI Custom DM Evaluation Validation Details	View, Update, Insert, Delete	View
RBI Degradation Mechanisms	View, Update, Insert, Delete	View, Update, Insert, Delete
RBI Recommendation	View, Update, Insert, Delete	View, Update, Insert, Delete
RBI Risk Matrix Mapping	View, Update, Insert, Delete	View, Update, Insert, Delete
RBI Strategy Mapping Configuration	View, Update, Insert, Delete	View, Update, Insert, Delete
RBI Strategy Mapping Details	View, Update, Insert, Delete	View, Update, Insert, Delete
RBI System	View, Update, Insert, Delete	View, Update, Insert, Delete
Reference Document	View, Update, Insert, Delete	View, Update, Insert, Delete
Risk Assessment	View, Update, Insert, Delete	View, Update, Insert, Delete
Risk Rank	View, Update, Insert, Delete	View, Update, Insert, Delete
Risk Translation	View, Update, Insert, Delete	View, Update, Insert, Delete
SAP System	View	View
Strategy Logic Case	View, Update, Insert, Delete	View
Strategy Reference Table	View, Update, Insert, Delete	View, Update, Insert, Delete
Task Type	View, Update, Insert, Delete	View, Update, Insert, Delete

Family	MI RBI Administrator	MI RBI Analyst
Time Based Inspection Interval	View, Update, Insert, Delete	View, Update, Insert, Delete
Time Based Inspection Setting	View, Update, Insert, Delete	View, Update, Insert, Delete
Relationship Families		
Belongs to a Unit	View, Update, Insert, Delete	View, Update, Insert, Delete
Data Mapping has Column-Field Pair	View, Update, Insert, Delete	View
Data Mapping has Query	View, Update, Insert, Delete	View
Data Mapping has Subgroup	View, Update, Insert, Delete	View
Has Asset Group	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Child RBI Criticality Analysis	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Consequence Evaluation	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Consolidated Recommendations	View	View, Update, Insert, Delete
Has Corrosion Analyses	View	View
Has Corrosion Analysis Settings	View	View
Has Datapoints	View	View
Has Degradation Mechanisms	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Inspections	View	View, Update, Insert, Delete
Has Inspection Scope	View	View
Has Potential Degradation Mechanisms	View, Update, Insert, Delete	View, Update, Insert, Delete

Family	MI RBI Administrator	MI RBI Analyst
Has RBI Components	View, Update, Insert, Delete	View, Update, Insert, Delete
Has RBI Criticality Analysis	View, Update, Insert, Delete	View, Update, Insert, Delete
Has RBI Custom DME Configuration	View, Update, Insert, Delete	View, Update, Insert, Delete
Has RBI Custom DME Validation	View, Update, Insert, Delete	View
Has RBI Degradation Mechanisms Evaluation	View, Update, Insert, Delete	View, Update, Insert, Delete
Has RBI Strategy Mapping Configuration	View, Update, Insert, Delete	View, Update, Insert, Delete
Has RBI Systems	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Recommendations	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Reference Documents	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Reference Values	View	View
Has SAP System	View	View
Has Superseded Recommendations	View	View, Update, Insert, Delete
Has Task Revision	View	View, Update, Insert, Delete
Has Tasks	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Time Based Inspection Interval	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Unmitigated Risk	View, Update, Insert, Delete	View, Update, Insert, Delete
Is Based on RBI Degradation Mechanisms	View, Update, Insert, Delete	View, Update, Insert, Delete

Family	MI RBI Administrator	MI RBI Analyst
Is Mitigated	View, Update, Insert, Delete	View, Update, Insert, Delete
Is Part of Group	View, Update, Insert, Delete	View, Update, Insert, Delete
Mapped to RBI Component	View, Update, Insert, Delete	View, Update, Insert, Delete
Represents Inspections	View, Update, Insert, Delete	View, Update, Insert, Delete

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

These families are *not* used elsewhere in the RBI module.

- Privileges to the following entity and relationship families support integration with the Inspection Management module:
    - Has Inspection Scope
    - Has Time Based Inspection Interval
    - Time Based Inspection Interval
    - Time Based Inspection Setting

Specifically, certain features of the Time-Based Inspection Settings functionality, which you can use if the Inspection Management license is active, are facilitated by these privileges.

Deploy Root Cause Analysis (RCA)

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 Root Cause Analysis (RCA) 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 Meridium Enterprise 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.

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 Meridium Enterprise 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 Meridium Enterprise APM database. You can select one or more default Critical Success Factors or define your own.
5	Define the Tracking Evaluation Query.	This step is required only if you do not want to use the baseline query, which is defined by default.

Upgrade or Update Root Cause Analysis (RCA) to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Root Cause Analysis 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 PROACT Administrator	MI FE Admin
MI PROACT Team Member	MI FE Admin MI FE PowerUser MI FE User
MI PROACT Viewer	MI FE Admin MI FE PowerUser MI FE User

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

> 📄 **Note:** Access to RCA is not granted through these privileges but through *membership* in these Security Groups and the privileges associated with them.

Family	MI PROACT Administrator	MI PROACT Team Member	MI PROACT Viewer
Entity Families			
Equipment	View	View	View
Functional Location	View	View	View
Human Resource	View, Update, Insert	View, Update, Insert	View
Notification	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI PROACT Administrator	MI PROACT Team Member	MI PROACT Viewer
RCA Analysis	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Build List Item	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Critical Success Factor	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Event	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Failure Mode	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Hypothesis	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Image	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Logic Gate	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Preserve Item	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Recommendation	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Sequence Node	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Team Member	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Tracking Item	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Verification	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Reference Document	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Security User	View	View	View
Relationship Families			

Family	MI PROACT Administrator	MI PROACT Team Member	MI PROACT Viewer
Has Consolidated Recommendations	View	View	View
Has Recommendations	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Reference Documents	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Is a User	View, Update, Insert	View, Update, Insert	View
Group Assignment	View, Update, Insert	View, Update, Insert	View
Production Event Has RCA Analysis	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Analysis Has Asset	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Analysis Relationships	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA System Relationships	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Tracking Item Relationships	View, Update, Insert, Delete	View, Update, Insert, Delete	View
User Assignment	View, Update, Insert	View, Update, Insert	View
Equipment Has Equipment	View	View	View
Functional Location Has Equipment	View	View	View
Functional Location Has Functional Location(s)	View	View	View

Deploy Rounds

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 Rounds 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 Meridium Enterprise 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.

Meridium APM Sync Server

> ☐ **Note:** Meridium APM Sync Server is only required if you want to use Operator Rounds on Windows Mobile handheld devices.

Step	Task	Notes
1	Configure the Meridium APM Sync Server. Configuring the Meridium APM Sync Server includes completing the following steps. a. Install Meridium APM Sync Services. b. Install the Microsoft Sync Framework. c. Modify the file web.config depending on Oracle database provider or SQL database provider. d. Modify the file MeridiumSync.config.	This step is required only if you want to use Operator Rounds on Windows Mobile handheld devices.
2	Configure security for the MeridiumSyncService Service.	This step is required only if you want to use Operator Rounds on Windows Mobile handheld devices.

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.	This step is required only if you have asset data in families outside of the baseline Equipment and Functional Location families.

Step	Task	Notes
2	Assign the desired 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 Meridium Enterprise 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.

Step	Task	Notes
4	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 created an asset family that you want to link to a Measurement Location or a Lubrication Requirement using the *Has Checkpoint* relationship family.
5	Create a relationship definition as follows: • Relationship family: Has OPR Recommendation • Predecessor: Lubrication Requirement or Measurement Location family • Successor: Operator Rounds Recommendation • Cardinality: One to Many	This step is required only if you want to create OPR Recommendations with photographs in mobile devices.
6	Install the Meridium Enterprise APM application on the mobile device that you plan to use for data collection.	This step is required only if you want to use a mobile device for data collection.
7	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.
8	Set up the Scheduled Compliance task.	This step is required. The scheduled compliance task starts as soon as the Rounds module is deployed, and is set to run continuously as long as Rounds in use.

> 🛈 **Note:** It is important that in addition to the above tasks, you compile the database and reset IIS on the Meridium APM Server.

Windows Mobile Handheld Device

The following tasks need to be performed on each Windows Mobile handheld device that you want to use with Operator Rounds.

Step	Task	Notes
1	Ensure that all the Windows Mobile handheld devices that you want to use with Operator Rounds meet the software requirements.	This step is required.
2	Install the .NET Compact Framework.	This step is required.
3	Install Microsoft SQL CE. Install Microsoft SQL CE.	This step is required.
4	Install Microsoft Sync Services for ADO.NET.	This step is required.
5	Install the Meridium APM Mobile Framework.	This step is required.
6	Access Device Settings Screen.	This step is required.
7	Identify the Sync Server within the Meridium Enterprise APM Mobile Framework.	This step is required.
8	Specify the security query to be used with the Meridium APM Mobile Framework.	This step is required.
9	Modify the user time-out value.	This step is required.
10	Install Operator Rounds.	This step is required.
11	Configure barcode scanning. Configuring barcode scanning includes the followings steps: • Install the Barcode add-on. • Enable barcode scanning.	This step is required only if you will use an Barcode scanner with Operator Rounds.

Step	Task	Notes
12	Configure RFID tag scanning. Configuring RFID scanning includes the following steps: • Install the RFID add-on. • Enable RFID tag scanning.	This step is required only if you will use an RFID scanner with Operator Rounds.
13	Install translations for Operator Rounds.	This step is required only if you are using translations.

Upgrade or Update Rounds to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Before You Begin

> **Note:** The steps in this Before You Begin section are required only if you are upgrading from a version of Meridium Enterprise APM prior to V4.0.0.0.

In Meridium Enterprise APM 4.2.0.7.0, a Checkpoint can be linked to *one* asset. During upgrade from versions V3.x to 4.2.0.7.0, the related asset entity key is added to a field on the Checkpoint family. Hence, if you have Checkpoints that are linked to more than one asset, then you must remove the linkage to the additional assets prior to the upgrade. To do so, perform the following steps.

1. Using an appropriate database management tool, run the following query in the database configured with the current version of Meridium Enterprise APM that you will configure to work with Meridium Enterprise APM 4.2.0.7.0.

   For example, run the following query:

   For Measurement Location in the database:

   ```
   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
```

For Lubrication Requirement in the database:

```
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 Meridium 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 (e.g., either a Functional Location *or* an Equipment if you are using the default asset families).

Update from version V4.2.0.0 through V4.2.0.6.0

Step	Task	Notes
1	Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework, 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.
2	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.
3	Confirm the assignment of Security Users for the existing route subscriptions and make additional assignments if needed.	This step is required.

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

Step	Task	Notes
1	Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework, 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.
2	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.
3	Confirm the assignment of Security Users for the existing route subscriptions and make additional assignments if needed.	This step is required.

Upgrade from any version V4.0.0.0 through V4.0.1.0

Step	Task	Notes
1	Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework, 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.
2	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.
3	Confirm the assignment of Security Users for the existing route subscriptions and make additional assignments if needed.	This step is required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

Step	Task	Notes
1	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.
2	Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework, 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.

Step	Task	Notes
3	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.
4	Confirm the assignment of Security Users for the existing route subscriptions and make additional assignments if needed.	This step is required. Routes that were subscribed to by a user via the Meridium Enterprise APM mobile application will be assigned to the user automatically through the database upgrade process.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

Step	Task	Notes
1	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.
2	Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework, 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.
3	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.
4	Confirm the assignment of Security Users for the existing route subscriptions and make additional assignments if needed.	This step is required. Routes that were subscribed to by a user via the Meridium Enterprise APM mobile application will be assigned to the user automatically through the database upgrade process.

Upgrade from any version V3.5.1 through V3.5.1.12.0

Step	Task	Notes
1	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.
2	Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework, 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.
3	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.
4	Assign mobile device users to Routes.	This step is required only if you will use a mobile device for data collection.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

Step	Task	Notes
1	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.
2	Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework, 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.
3	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.
4	Assign mobile device users to Routes.	This step is required only if you will use a mobile device for data collection.

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Step	Task	Notes
1	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.
2	Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework, 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.
3	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.

Step	Task	Notes
4	Assign mobile device users to Routes.	This step is required only if you will use a mobile device for data collection.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Step	Task	Notes
1	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.
2	Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework, 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.
3	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.
4	Assign mobile device users to Routes.	This step is required only if you will use a mobile device for data collection.

Manage the Measurement Location Template Mappings

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 Meridium Enterprise 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:

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.

Meridium APM Sync Services Tasks

Meridium APM Sync Services is a solution provided for Meridium Enterprise APM handheld applications (e.g., Operator Rounds) that is built upon the Microsoft Sync Framework. The Meridium APM Mobile Sync Server provides a connection between handheld devices and the Meridium APM Application Server so that data can be synchronized between the windows mobile devices and the Meridium Enterprise APM database.

Install Meridium APM Sync Services

Before You Begin

- You must be logged in as the administrator for the system.

- IIS must be reset before installation.

- [Install Microsoft Sync Framework](#).

Steps

1. On the Meridium APM Sync Server machine, access the Meridium Enterprise APM distribution package, and then navigate to the **Meridium APM Server and Add-ons** folder.

2. Open the file **Setup.exe**.

   The **Meridium APM Server and Add-ons** installer screen 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** option. Then, select **Next** button.

   The **Select Installation Location** screen appears.

5. Select **Next** to accept the default location.

    The **Select the features you want to install** screen appears.

> **Note:** The **Select the features you want to install** screen lets you select which features and languages you want to install on the Meridium APM Sync Server machine.

6. Select the **Meridium APM Application Server** and **Meridium APM Sync Services with Operator Rounds** check boxes. All the subnodes that appear below these nodes become selected automatically.

> **Note:** The **Default Language (English)** check box cannot be cleared. English is the default language for Meridium Enterprise APM and will always be installed.

7. Select **Next**.

The **websites** screen appears.

8. Select the website where you want to create a virtual directory for Meridium APM Sync Ser-
   vices.

   > Note: You can accept the default selection.

9. Select **Next**.

   The **Complete the Installation** screen appears.

10. Select **Install**.

The **Setup Status** screen appears.

After the progress bar reaches the end, the **Installation is Complete** screen appears.

11. Select **Finish**.

The **Meridium APM Server and Add-ons** installer closes.

> ☐ **Note**: If the **Launch APM System Administration now** check box was selected, the **APM System Administration** window appears.

Verify Installation of Meridium APM Sync Services

Steps

1. On the Meridium APM Sync Server machine, open Internet Explorer.

2. Navigate to the URL **http://<Sync_Server_Name>.me-ridium.com/MeridiumSyncService/MeridiumSyncService.svc**,

   where **<Sync_Server_Name>** is the name or IP address of the server, on which Meridium APM Sync Services is installed.

   The following page appears, indicating that Meridium APM Sync Services is successfully installed.

SyncService Service

You have created a service.

To test this service, you will need to create a client and use it to call the service. You can do this using the svcutil.exe tool from the command line with the following syntax:

```
svcutil.exe http://docvm.meridium.com/MeridiumSyncService/MeridiumSyncService.svc?wsdl
```

This will generate a configuration file and a code file that contains the client class. Add the two files to your client application and use the generated client class to call the Service. For example:

C#

```csharp
class Test
{
    static void Main()
    {
        SyncServiceClient client = new SyncServiceClient();

        // Use the 'client' variable to call operations on the service.

        // Always close the client.
        client.Close();
    }
}
```

Visual Basic

```vb
Class Test
    Shared Sub Main()
        Dim client As SyncServiceClient = New SyncServiceClient()
        ' Use the 'client' variable to call operations on the service.

        ' Always close the client.
        client.Close()
    End Sub
End Class
```

> **Note**: If an error message appears or this page cannot be displayed, review the installation and configuration steps.

Install Microsoft Sync Framework

Before You Begin

- You must be logged in as the administrator for the system.

- IIS must be reset before installation.

- Install .NET Framework 3.5 SP1.

Steps

1. On the Meridium APM Sync Server machine, access the Meridium Enterprise APM distribution package, and then navigate to the **Microsoft Sync Framework x86_en** folder.

2. Open the file **Setup.exe**.

   The Installation process begins and the **License Agreement** screen appears. Read the License Agreement and, if you agree, select the **I accept the terms of the license agreement** option.

3. Select **Next**.

   > ⚠ **Note**: During the installation, an error message appears, indicating that the installer was unable to locate the file **SyncSDK.msi**. This error is seen because Meridium, Inc. does not distribute the folder **Microsoft Sync Framework SDK** with the **Microsoft Sync Framework** installation package. When you see this error message, select **Close** to proceed with the installation. This error message will not interfere with a successful installation of the required components.

3. Select **Finish**.

   Microsoft Sync Framework is now installed.

Modify the Web.config for An Oracle Sync Services Database Connection
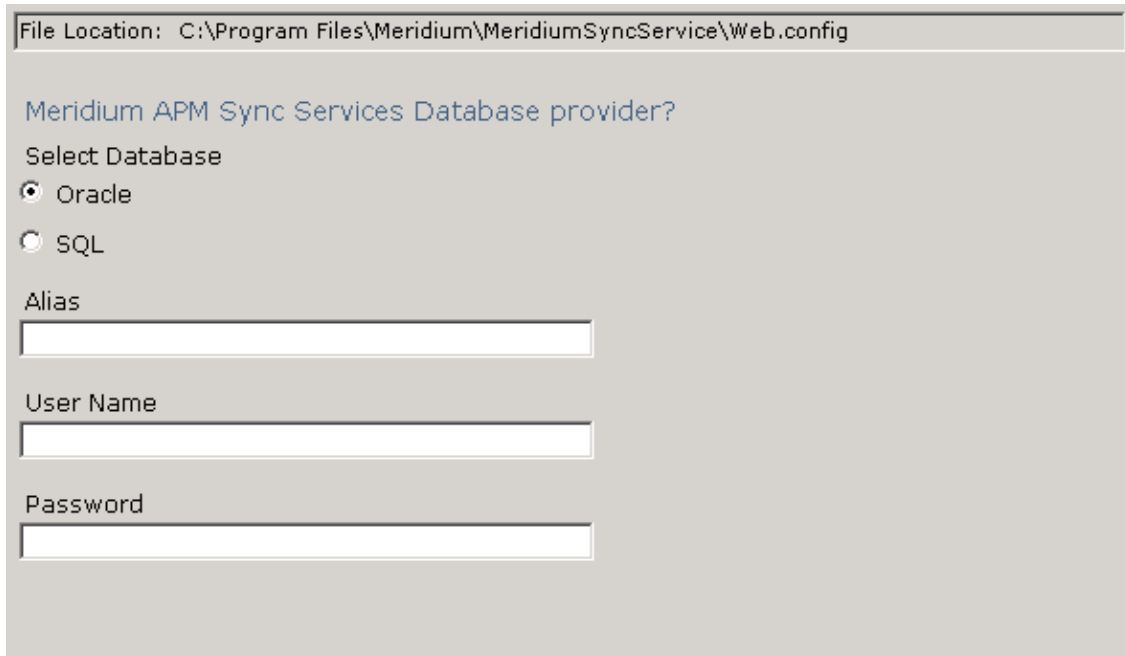
These instructions assume that:
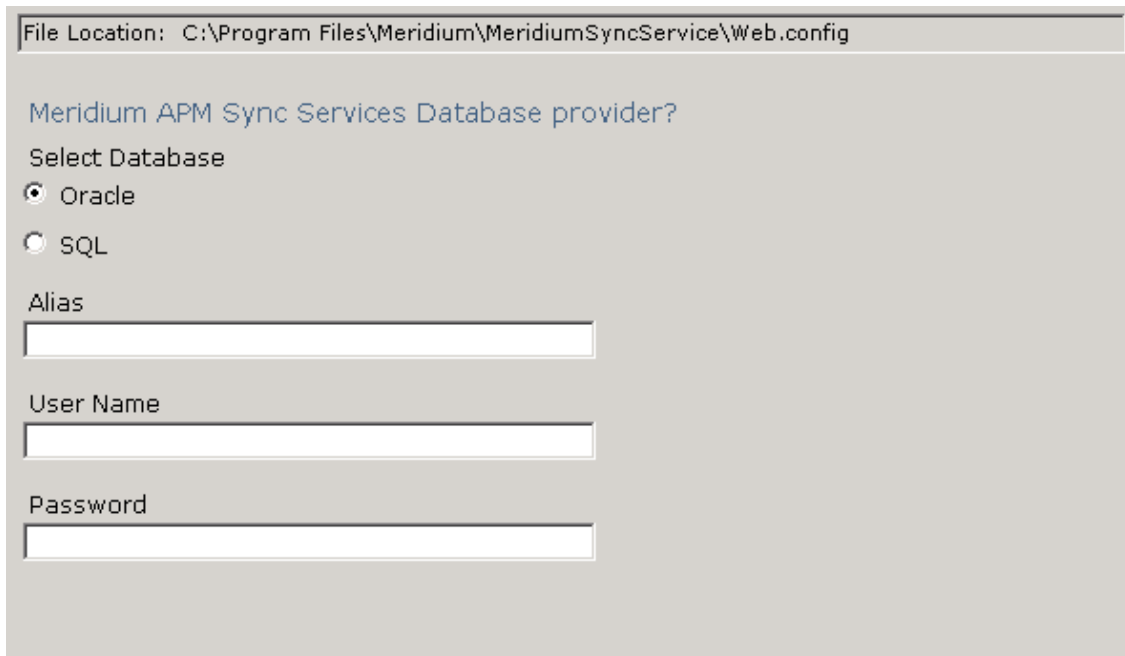
- The Oracle database that will contain the database tables for the Meridium APM Sync Services already exists.
- You have accessed the APM System Administration tool on the Meridium APM Sync Server machine.

> ⓘ **Note**: If you are changing the Sync Services database, we recommend that you first create a back-up of the original database.

Steps

1. Access the Meridium Enterprise APM System Administration Tool.

2. In the **Configuration** section, select **Sync Services Database** link.

   The content of the web.config file appears in the **Meridium APM Sync Services Database provider** section. These settings specify connection information to the database that contains the database tables that are used by the Meridium APM Sync Services.

3. In the **Select Database** section, accept the default selection, **Oracle**.

4. In the **Alias** box, enter the database alias. This value is case-sensitive.

5. In the **User Name** box, enter the user name that you want to use to connect to the database.

6. In the **Password** box, enter the password associated with the user name you entered in the **User Name** box. This setting is case-sensitive.

7. At the bottom of the APM System Administration window, select **Save**.

    Your changes are saved to the web.config file.

Modify the Web.config for An SQL Sync Services Database Connection

These instructions assume that:

- The SQL database that will contain the database tables for the Meridium APM Sync Services already exists.
- You have accessed the APM System Administration tool on the Meridium APM Sync Server machine.

> ℹ **Note**: If you are changing the Sync Services database, we recommend that you first create a back-up of the original database.

Steps

1. Access the Meridium Enterprise APM System Administration Tool.

2. In the **Configuration** section, select **Sync Services Database**.

   The content of the web.config file appears in the Meridium APM Sync Services Database provider section. These settings specify connection information to the database that contains the database tables that are used by the Meridium APM Sync Services.

   File Location: C:\Program Files\Meridium\MeridiumSyncService\Web.config

   Meridium APM Sync Services Database provider?
   Select Database
   ⦿ Oracle
   ○ SQL

   Alias

   User Name

   Password

3. For the **Select Database** setting, select **SQL**.

   The SQL settings appear and replace the Oracle settings.

File Location: C:\Program Files\Meridium\MeridiumSyncService\Web.config

Meridium APM Sync Services Database provider?

Select Database

○ Oracle

◉ SQL

DB Server

DB Name

User Name

Password

4. In the **DB Server** box, enter the name of the Database Server that contains the database.

5. In the **DB Name** box, enter the database name.

6. In the **User Name** box, enter the user name that you want to use to connect to the database.

7. In the **Password** box, enter the password associated with the user name you entered in the **User Name** box. This setting is case-sensitive.

8. At the bottom of the **APM System Administration** window, select **Save**.

Modify Meridium Sync Config

When you perform a sync operation in the Meridium APM Mobile Framework, the device connects to the Meridium APM Sync Server, which in turn connects to the specified Meridium APM Application Server and logs in to the data source defined in the file MeridiumSync.config. Security User credentials are required for logging in to the data source.

Before you can perform a sync operation, you will need to define the following settings on the Meridium APM Sync Server:

- The Meridium Enterprise APM Server

- The Meridium Enterprise APM data source

- The Meridium APM Sync Services Security User credentials that will be used to connect the Meridium APM Sync Server to the Meridium Enterprise APM database

  The user you specify must have the family-level privileges required to access all data that needs to be downloaded to the Windows Mobile Device for a given application. The MI Operator Rounds Administrator and MI Operator Rounds Mobile User Security Groups, which are provided with the baseline Operator Rounds product, have these privileges. Therefore, you can create your own Security User and assign it to either one of these Security Groups for this purpose.

To specify these settings, you will need to modify the MeridiumSync.Config file via the APM System Administration tool on the Meridium APM Sync Server machine.
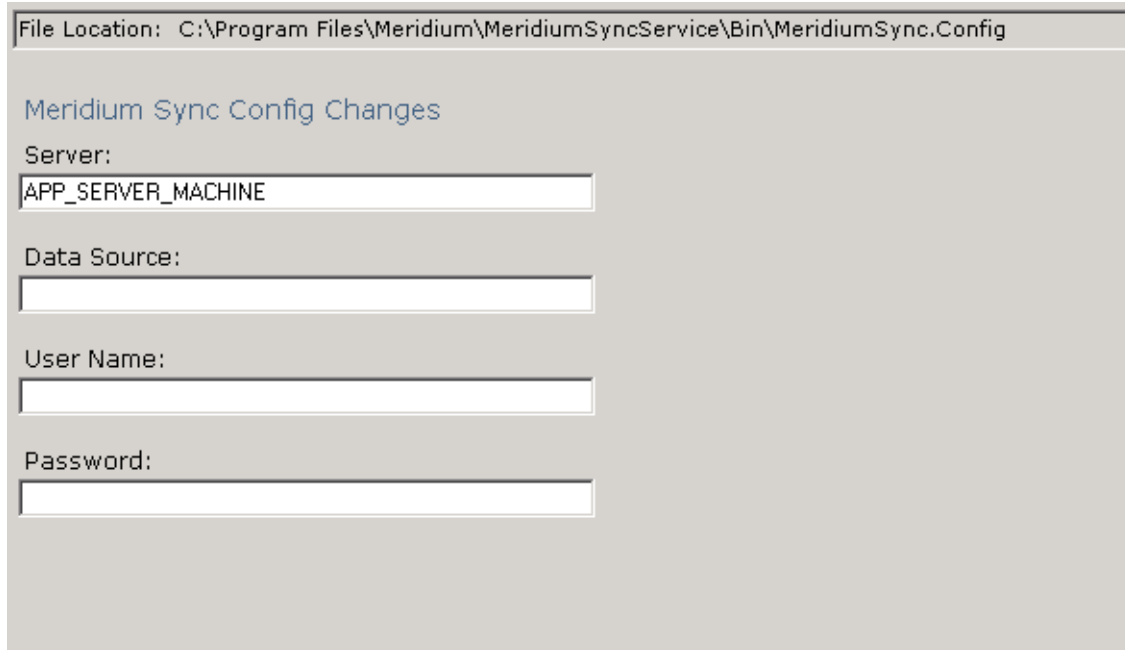
The following instructions provide details on defining the Meridium Enterprise APM Server, data source, and Sync Services Security User credentials in the MeridiumSync.config file. These instructions assume that you have:

- Created the Security User whose credentials you will enter in the configuration file and granted them the appropriate permissions to Operator Rounds families.

- Accessed the APM System Administration tool on the Meridium APM Sync Services server machine.

Steps

1. Access the Meridium Enterprise APM System Administration Tool.

2. In the **Configuration** section, select **Meridium Sync Config** link.

   The contents of the MeridiumSync.Config file appear in the Meridium Sync Config Changes section.

```
File Location:  C:\Program Files\Meridium\MeridiumSyncService\Bin\MeridiumSync.Config

Meridium Sync Config Changes
Server:
APP_SERVER_MACHINE

Data Source:


User Name:


Password:

```

By default, the **Server** box contains the name of the machine on which you are currently working.

3. In the **Server** box, enter the name of the Meridium Enterprise APM Server machine that you want to use with Sync Services.

4. In the **Data Source** box, enter the name of the Meridium Enterprise APM data source to which you want to log in. This data source must be configured on the Application Server machine defined in the **Server** box.

> Note: This value is case-sensitive. You must define the data source name using the same case that is used in Data Source Manager.

5. In the **User Name** box, enter the User ID of the Meridium APM Security User that you want to use for logging in to the data source identified in the **Data Source** box.

6. In the **Password** box, enter the password associated with the Meridium Enterprise APM Security User identified in the **User Name** box. This password will be encrypted in the file.

7. At the bottom of the **APM System Administration** window, select **Save**.

Your changes are saved to the MeridiumSync.config file.

Configure Security for Meridium Sync Service

When you install Meridium APM Sync Services, the service MeridiumSyncService is created under the Default Web Site in IIS on the Meridium APM Sync Server machine. The Windows user account that is configured at the Default Web Site level to be used for anonymous access is granted permission to the following folder:

<root>\MeridiumSyncService

Where <root> is the drive and root folder where the Meridium APM Sync Services was installed (e.g., **C:\Program Files\Meridium**).

If you configure a different Windows user account to be used for anonymous access at the MeridiumSyncService level, you must grant that user the following permissions to the folder **<root>\MeridiumSyncService**:

- Modify
- Read & Execute
- List Folder Contents
- Read
- Write

If these permissions are not granted, when any user attempts to perform a sync operation in the Meridium APM Mobile Framework, an error message will be displayed, and synchronization will fail. For details on granting these permissions, see the Microsoft documentation.

Windows Mobile Handheld Devices

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.

Install the .NET Compact Framework on Windows Mobile Device

Before You Begin

- You must be logged in as the administrator on the Windows Mobile device.

- [Install Microsoft Sync Framework](#).

- [Install Meridum APM Sync Services](#)

Steps

1. On the Windows Mobile handheld device, open Internet Explorer, and navigate to the URL **http://<machine>/MeridiumSyncService**, where **<machine>** is the name or IP address of the server on which Meridium APM Sync Services is installed.

   You are redirected automatically to one of the following URLs, and then a download screen appears:

   - For Windows Mobile devices: **http://<machine>/MeridiumSyncService/winmodownload.aspx**.

2. If the device is running Windows Mobile 2003, select **PPC2003\NETCFv35.PPC.ARMV4.CAB**.

   or

   If the device is running Windows Mobile 5.0 or later, select **WCE500\NETCFv35.WM.ARMV4i.CAB**.

   A message appears, asking if you really want to download the file.

3. Select **Yes**.

   The file is downloaded, and the .NET Compact Framework is installed. When the installation is complete, a message will appear indicating that the installation is successful and instructing you to restart the device.

Install Microsoft SQL CE on Windows Mobile Device

Steps

1. On the Windows Mobile handheld device, open Internet Explorer, and then navigate to the URL **http://<machine>/MeridiumSyncService**, where **<machine>** is the name or IP address of the server on which Meridium APM Sync Services is installed.

   You are redirected automatically to one of the following URLs, and then a download screen appears:

   - For Windows Mobile devices: **http://<ma-chine>/MeridiumSyncService/winmodownload.aspx**.

2. If the device is running Windows Mobile 2003, select **PPC2003\SQLCE.PPC.ARM4.CAB**.

   or

   If the device is running Windows Mobile 5.0 or later, select **WCE500\SQLCE.WCE5.ARMV4i.CAB**.

   A message appears, asking if you really want to download the file.

3. Select **Yes**.

   The file is downloaded, and the Microsoft SQL CE is installed. When the installation is complete, a message will appear, indicating that the installation is successful.

Install Microsoft Sync Services for ADO.NET on Windows Mobile Device

Steps

1. On the Windows Mobile handheld device, open Internet Explorer, and then navigate to the URL **http://<machine>/MeridiumSyncService**, where **<machine>** is the name or IP address of the server on which Meridium APM Sync Services is installed.

   You are redirected automatically to one of the following URLs, and then a download screen appears:

   - For Windows Mobile devices: **http://<machine>/MeridiumSyncService/winmodownload.aspx**.

2. If the device is running Windows Mobile 2003, select **PPC2003\SYNCSERVICES.WCE.CAB**.

   or

   If the device is running Windows Mobile 5.0 or later, select **WCE500\SQLCE.WCE5.ARMV4i.CAB**.

   A message appears, asking if you really want to download the file.

3. Select **Yes**.

   The file is downloaded, and the **Microsoft Sync Services for ADO.NET** is installed. When the installation is complete, a message will appear, indicating that the installation is successful.

Install the Meridium APM Mobile Framework on Windows Mobile Device

Steps

1. On the Windows Mobile handheld device, open Internet Explorer, and then navigate to the URL **http://<machine>/MeridiumSyncService**, where **<machine>** is the name or IP address of the server on which Meridium Enterprise APM Sync Services is installed.

   You are redirected automatically to one of the following URLs, and then a download screen appears:

   - For Windows Mobile devices: **http://<machine>/MeridiumSyncService/winmodownload.aspx**.

2. Select **MFX.APM.<version>.ARM4.CAB**, where <version> is the corresponding version of Meridium Enterprise APM.

   A message appears, asking if you really want to download the file.

3. Select **Yes**.

   The file is downloaded, and the Meridium APM Mobile Framework is installed. When the installation is complete, a message will appear, indicating that the installation is successful.

   The **Meridium APM Mobile Framework** screen appears, indicating that no users are available on the Windows Mobile device yet.

Access Device Settings Screen on Windows Mobile Device

Steps

1. On the Windows Start menu, select **Programs**.

    The **Programs** screen appears.

2. Select **APM Mobile Framework**.

    The **Meridium APM Mobile Framework** screen appears.

3. Select **Settings**.

    The **Device Settings** screen appears.
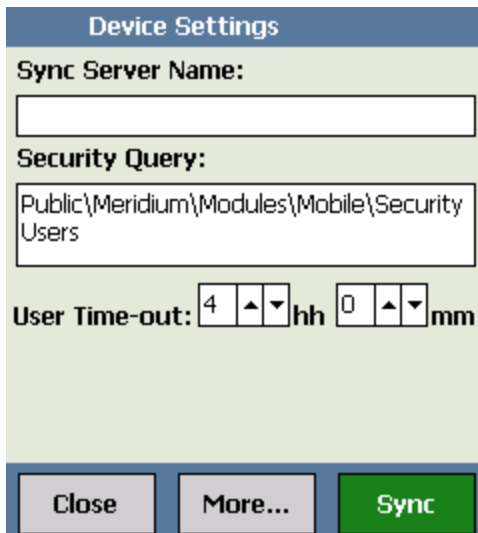
Identify the Sync Server Within the APM Mobile Framework on Windows Mobile Device

Steps

1. On the Windows Start menu, select **Programs**.

   The **Programs** screen appears.

2. Select **APM Mobile Framework**.

   The **Meridium APM Mobile Framework** screen appears.

3. Select **Settings**.

   The **Device Settings** screen appears.
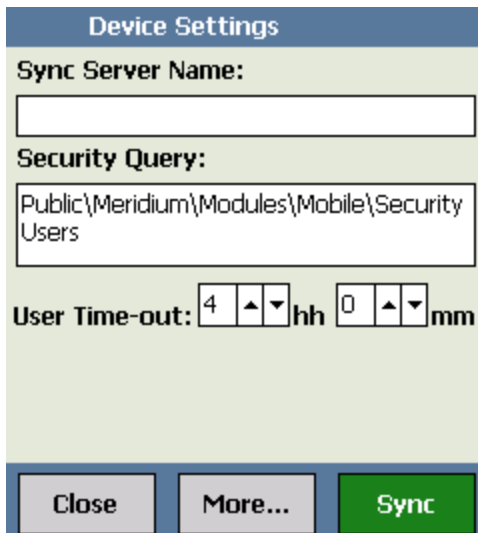
4. In the **Sync Server Name** box, type the name or IP address of the server on which Meridium APM Sync Services is installed.

   > 📄 **Note**: At this point, you can also specify the security query.

5. Select **Sync**.

   The **Synchronizer** screen appears, displaying the progress of the synchronization process. When the synchronization process is complete, a message will appear, indicating whether or not the process was successful.

6. When the process is complete, select **Close**.

Specify the Security Query on Windows Mobile Device

Steps

1. On the Windows Start menu, select **Programs**.

   The **Programs** screen appears.

2. Select **APM Mobile Framework**.

   The **Meridium APM Mobile Framework** screen appears.

3. Select **Settings**.

   The **Device Settings** screen appears, displaying the **Sync Server Name** and **Security Query** boxes. The **Security Query** box is used to store the path to the query that determines who can log into Operator Rounds on the device. Note that the default security query is Security Users, which is stored in the Meridium APM Catalog folder *Public\Meridium\Modules\Mobile*.

4. In the **Security Query** box, enter the path to the query that you want to use to determine who can log into Operator Rounds on the device.

   If the query is stored in the Meridium APM Catalog folder *Public\Meridium\Modules\Operator Rounds\Queries\Download Queries*, type the name of the query. If the query is stored in a subfolder of the Meridium APM Catalog folder *Public\Meridium\Modules\Operator Rounds\Queries\Download Queries*, type the path to the query, starting with the first subfolder name.

   For example, if the Chicago Users query is stored in the Meridium APM Catalog folder *Public\Meridium\Modules\Operator Rounds\Queries\Download Queries*, enter Chicago Users.

   Likewise, if the Chicago Users query is stored in the Meridium APM Catalog folder *Public\Meridium\Modules\Operator Rounds\Queries\Download Queries\Users\Chicago*, enter Users\Chicago\Chicago Users.

5. Select **Sync**.

   The **Synchronizer** screen appears, displaying the progress of the synchronization process.

Modify User Time-out Value on Windows Mobile Device

By default, if the Windows Mobile Device is left idle for four hours or longe,r and is not in the process of downloading data, the current Security User will be logged out of the Meridium APM Mobile Framework automatically, and the log in screen will be displayed. You can change the default user time-out value via the **Device Settings** screen to decrease or increase the amount of time a use should remain logged in to the Meridium APM Mobile Framework if the device is left idle and is not in the process of downloading data.

Steps

1. Access the **Device Settings** screen.

2. Use the **User Time-out** boxes to select or type the value that represents the amount of time a user should remain logged in to the Meridium APM Mobile Framework, if the device is left idle and is not in the process of downloading data.

3. Select **Close**.

   The **login** screen is highlighted, and your changes to the time-out value are applied.

Install Operator Rounds on Windows Mobile Device

Before You Begin

- You must be logged in as the administrator for the system.

- [Install Meridium APM Mobile Framework](#).
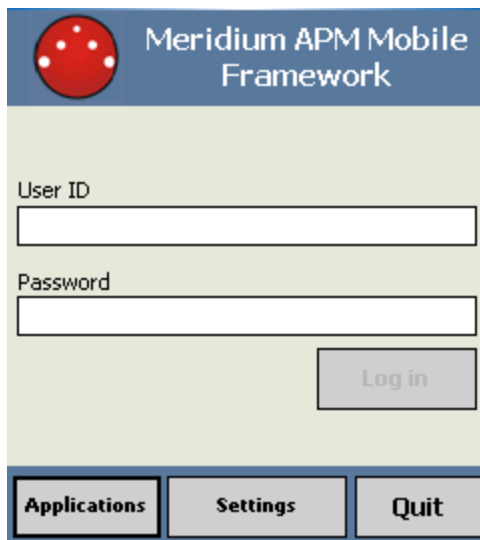
Steps

1. On the Windows Start menu, select **Programs**.

   The **Programs** screen appears.

2. Select **APM Mobile Framework**.

   The **Meridium APM Mobile Framework** screen appears.

3. Select **Applications**.

   The **Add/Remove Applications** screen appears.

4. In the list of available applications, select the **Install** button that appears to the right of **Operator Rounds**.

   A message appears, asking if you want to install Operator Rounds.

5. Select **Yes**.

   The installation process begins. The **Meridium APM Mobile Framework** closes, and the **Operator Rounds** application is installed.

   > ⓘ **Note**: After the installation is complete, the Meridium APM Mobile Framework will reopen automatically and return you to the **Meridium APM Mobile Framework** screen.

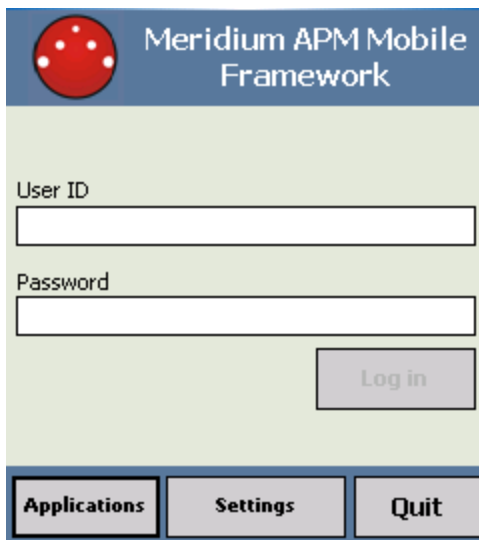# Install the Barcode Add-on on Windows Mobile Device

Steps

1. On the Windows Start menu, select **Programs**.

   The **Programs** window appears.

2. Select **APM Mobile Framework**.

   The **Meridium APM Mobile Framework** window appears.

3. Select **Applications**.

   The **Add/Remove Applications** window appears.

4. In the list of available applications, select the **Install** button that appears to the right of **Barcode**.

   A message appears, asking if you want to install the Barcode add-on.

5. Select **Yes**.

   The installation process begins. The Meridium APM Mobile Framework closes, and the Barcode add-on is installed.

   > **Note**: After the installation is complete, the Meridium APM Mobile Framework will reopen automatically, and the Meridium APM Mobile Framework screen appears and you can enable Barcode scanning.

Enable Barcode Scanning on Windows Mobile Device

Before You Begin

- Install the **Barcode** add-on.

Steps

1. On the Windows Mobile device, access the Device Settings screen.

2. Select **More**.

3. Select **Barcode**.

    The **Barcode Settings** screen appears.
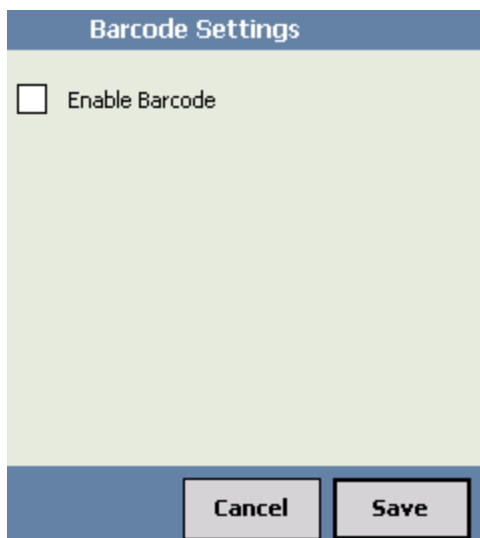
4. Select the **Enable Barcode** check box.

5. Select **Save**.

    Barcode scanning is enabled, and the Device Settings screen is highlighted.

6. Select **Close**.

    You are returned to the **login** page.

Install the RFID Add-on on Windows Mobile Device

Steps

1. On the Windows Start menu, select **Programs**.

    The **Programs** screen appears.

2. Select **APM Mobile Framework**.

    The **Meridium APM Mobile Framework** screen appears.

3. Select **Applications**.

    The **Add/Remove Applications** screen appears.

4. In the list of applications, select the **Install** button that appears to the right of **RFID**.

   A message appears, asking if you want to install the RFID add-on.

5. Select **Yes**.

   The installation process begins. During this process, the **Meridium APM Mobile Framework** closes, and the RFID add-on is installed.

   > ℹ **Note**: After the installation process is complete, the **Meridium APM Mobile Framework** reopens automatically, and the Meridium APM Mobile Framework screen appears.

Enable RFID Tag Scanning on Windows Mobile Device

Before You Begin

- Install the **RFID** add-on.

Steps

1. Access the **Device Settings** screen.
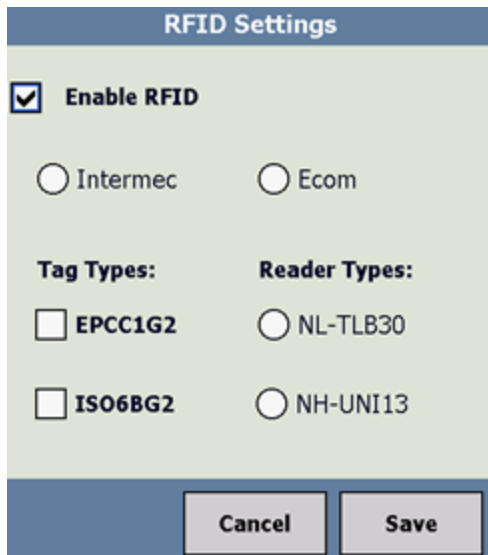

2. Select **More**.

   A menu appears, displaying additional buttons that are conditionally enabled according to the add-ons that you have installed.

3. Select **RFID**.

   The **RFID Settings** screen appears.

4. Select the **Enable RFID** check box.

5. Select the type of **RFID reader** (i.e., Intermec or Ecom) that you will use.

6. If you selected Intermec, select the check box that corresponds with the classification of RFID tags that you will use:

   - **EPCC1G2**: Select this check box if your RFID tags are classified as Electronic Product Code Class 1 Generation 2 tags.

   - **ISO6BG2**: Select this check box if your RFID tags are classified as International Standards Organization 18000-6B Generation 2 tags.

7. If you select Ecom, select the check box that corresponds with the classification of RFID types that you will use:

   - **NL-TLB30**: Select this check box if your RFID reader types are classified as Low Frequency.

   - **NH-UNI13**: Select this check box if your RFID reader types are classified as High Frequency.

8. Select **Save**.

   RFID scanning is enabled, and you are returned to the **Device Settings** screen.

9. Select **Close**.

Install Translations for Operator Rounds on Windows Mobile Device

Before You Begin

- You must be logged in as the administrator for the system.

- [Install Meridium APM Mobile Framework](#).

> ⓘ **Note**: To deploy translations for Operator Rounds, in addition to completing the following steps, you will also need to ensure that the regional setting on the device is set to the corresponding language.

Steps

1. On the Windows Start menu, select **Programs**.

   The **Programs** screen appears.

2. Select **APM Mobile Framework**.

   The **Meridium APM Mobile Framework** screen appears.

3. Select **Applications**.

   The Add/Remove Applications screen appears.

4. In the list of available applications, select the **Install** button that appears to the right of the application that you want to install.

   A message appears, asking if you are sure that you want to install translations for the selected language.

5. Select **Yes**.

   The installation process begins. **Meridium APM Mobile Framework** closes, and the translations are installed.

   > ⓘ **Note**: After the installation is complete, the Meridium APM Mobile Framework will reopen automatically and return you to the Meridium APM Mobile Framework screen.

Uninstall Meridium APM Mobile Framework on Windows Mobile Device

Steps

1. On the Windows Mobile handheld device, access the **Remove Programs** feature supplied via the operating system.

2. In the list of installed programs, select **MFX APM Mobile Framework**, and then select **Remove**.

   A message appears, asking if you really want to remove the program.

3. Select **Yes**.

   The Meridium APM Mobile Framework is removed from the Windows Mobile handheld device.

Uninstall then RFID Add-on on Windows Mobile Device

Steps

1. On the Windows Start menu, select **Programs**.

   The **Programs** screen appears.

2. Select **APM Mobile Framework**.

   The **Meridium APM Mobile Framework** screen appears.

3. Select **Applications**.

   The **Add/Remove Applications** screen appears. This following image shows an example of the **Add/Remove Applications** screen.

4. In the list of available applications, to the right of **RFID** , select **Uninstall**.

    The **Uninstall** screen appears, prompting you to enter your username and password.

5. In the **User ID** box, enter your username.

    The **Uninstall** button is enabled.

6. In the **Password** box, enter your password.

    > ℹ **Note**: If the credentials that you enter are not associated with a Security User who is a Super User or member of the MI Operator Rounds Administrator Security Group, a message will appear, indicating that you do not have the privileges required to uninstall the application.

7. Select **Uninstall**.

The uninstallation process begins. The Meridium APM Mobile Framework closes, and the **RFID** add-on is uninstalled.

Uninstall the Barcode Add-on on Windows Mobile Device

Steps

1. On the Windows Start menu, select **Programs**.

   The **Programs** screen appears.

2. Select **APM Mobile Framework**.

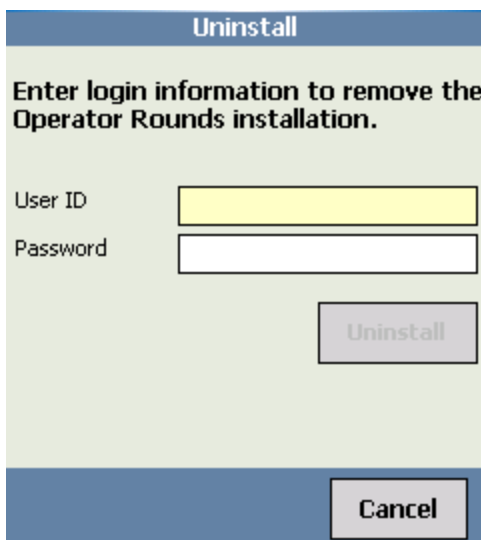   The **Meridium APM Mobile Framework** screen appears.
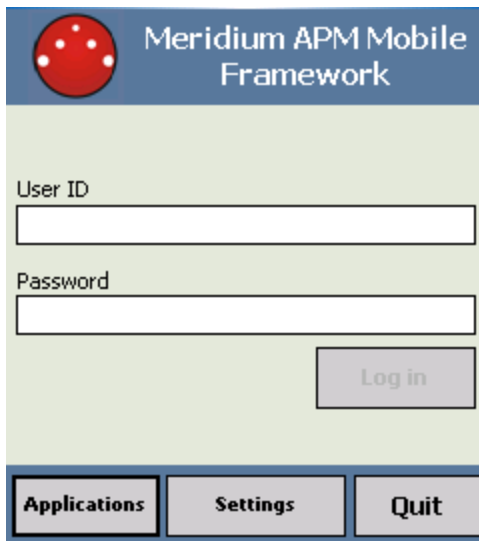
3. Select **Applications**.

   The **Add/Remove Applications** screen appears. This following image shows an example of the **Add/Remove Applications** screen.

4. In the list of available applications, to the right of **Barcode**, select **Uninstall**.

    The **Uninstall** screen appears, prompting you to enter your username and password.

5. In the **User ID** box, enter your username.

    The **Uninstall** button is enabled.

6. In the **Password** box, enter your password.

    > ⓘ **Note**: If the credentials that you enter are not associated with a Security User who is a Super User or member of the MI Operator Rounds Administrator Security Group, a message will appear, indicating that you do not have the privileges required to uninstall the application.

7. Select **Uninstall**.

The uninstallation process begins. The Meridium APM Mobile Framework closes, and the Barcode add-on is uninstalled.

Uninstall Translations for Operator Rounds on Windows Mobile Device

Steps

1. On the Windows Start menu, select **Programs**.

   The **Programs** screen appears.

2. Select **APM Mobile Framework**.

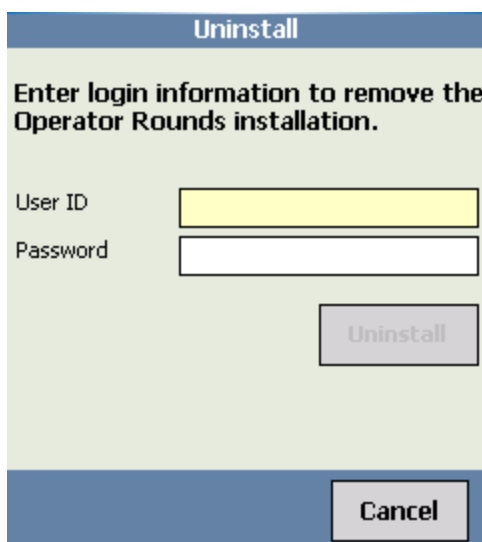   The **Meridium APM Mobile Framework** screen appears.
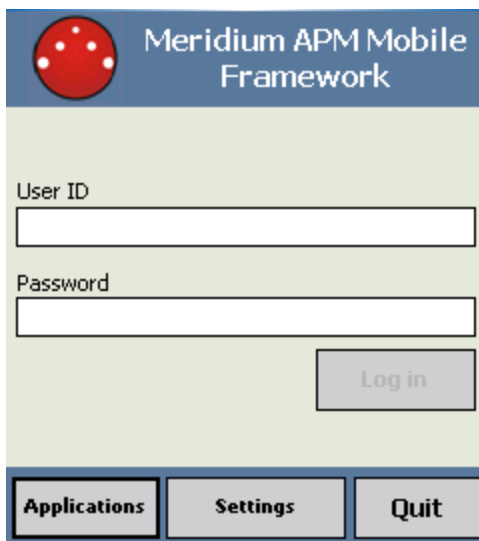
3. Select **Applications**.

   The **Add/Remove Applications** screen appears. This following image shows an example of the **Add/Remove Applications** screen.

4. In the list of available applications, to the right of the language whose translation you want to uninstall, select **Uninstall**.

   The **Uninstall** screen appears, prompting you to enter your username and password.

5. In the **User ID** box, enter your username.

   The **Uninstall** button is enabled.

6. In the **Password** box, enter your password.

   > ⓘ **Note**: If the credentials that you enter are not associated with a Security User who is a Super User or member of the MI Operator Rounds Administrator Security Group, a mes-

sage will appear, indicating that you do not have the privileges required to uninstall the application.

7. Select **Uninstall**.

The uninstallation process begins. The Meridium APM Mobile Framework closes, and the translations add-on for a language is uninstalled.

# Uninstall Operator Rounds on Windows Mobile Device

Steps

1. On the Windows Start menu, select **Programs**.

   The **Programs** screen appears.

2. Select **APM Mobile Framework**.

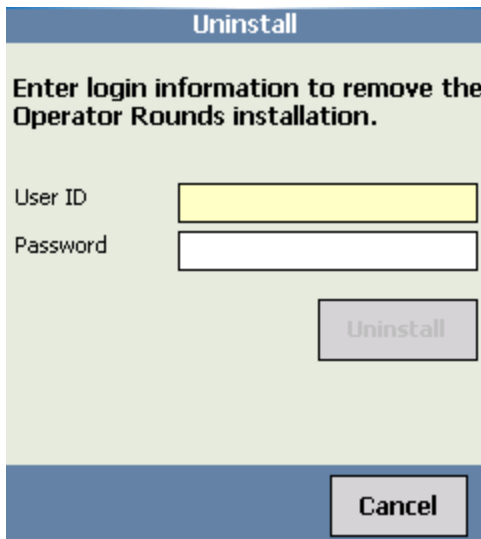   The **Meridium APM Mobile Framework** screen appears.

3. Select **Applications**.

   The **Add/Remove Applications** screen appears. This following image shows an example of the **Add/Remove Applications** screen.

4. In the list of available applications, to the right of the **Operator Rounds**, select **Uninstall**.

    The **Uninstall** screen appears, prompting you to enter your username and password.

5. In the **User ID** box, enter your username.

    The **Uninstall** button is enabled.

6. In the **Password** box, enter your password.

    > ℹ **Note**: If the credentials that you enter are not associated with a Security User who is a Super User or member of the MI Operator Rounds Administrator Security Group, a message will appear, indicating that you do not have the privileges required to uninstall the application.

7. Select **Uninstall**.

The uninstallation process begins. The Meridium APM Mobile Framework closes, and the **Operator Rounds** is uninstalled.

Upgrade Windows Mobile Handheld Device

After you upgrade the Meridium APM Sync Server, you will need to upgrade each Windows Mobile Device that connects to that server. This can be done by initiating a synchronization operation from within the Meridium APM Mobile Framework or from within Operator Rounds on each device that needs to be upgraded. After any updated data has been transferred to the server, a message will appear in the synchronization log, indicating that the server has been updated and that an update of the handheld components needs to be performed. The update will begin automatically.

During the update process, depending upon the device's operating system, messages may appear indicating that the Meridium APM components are already installed and that they need to be reinstalled. if you see these messages, you must select the **Yes** button. One message will appear for each component that is installed (i.e., Meridium APM Mobile Framework, Operator Rounds, and the Barcode and/or RFID add-ons). On other device operating systems, however, these messages do not appear, and the Meridium APM Mobile Framework closes automatically to allow the upgrade process to be completed.

When the upgrade process is complete, all applications that were previously installed will be reinstalled and updated automatically to the version to which you upgraded. In addition, any settings that were previously configured will be retained (e.g., the name of the security query). You will be redirected to the Operator Rounds login screen, where you can log in and begin using the Operator Rounds application.

> **Note**: You are not required to update Windows Mobile Devices all at once or within a specific timeframe after upgrading the Meridium APM Sync Server. If desired, you can simply allow the update to occur automatically the next time users synchronize with the server.

Upgrade Records with Schedules Containing End Dates

When upgrading from any V3.x version to V4.2.0.0, 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.

Steps

Prior to Upgrading

1. Review the affected record types to determine if there are any schedules containing end dates.

   You can use the following queries to locate these records:

   - Checkpoint Templates (i.e., 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 (i.e., 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.

After upgrading:

1. In Meridium Enterprise APM, locate the records you noted in the previous section.

2. In each record, update the schedule to set the required end date.

Rounds 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 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	None

The following table lists the default privileges that members of each group have to the Rounds entity and relationship families.

> 🗒 **Notes:**
>
> - 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

Family	MI Operator Rounds Administrator	MI Operator Rounds Mobile User	MAP-M Security Group	MI Rounds Designer Viewer	MI Lubrication Management Administrator	MI Lubrication Management User
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
Operator Rounds Allowable Values (Deprecated)	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

Family	MI Operator Rounds Administrator	MI Operator Rounds Mobile User	MAP-M Security Group	MI Rounds Designer Viewer	MI Lubrication Management Administrator	MI Lubrication Management User
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
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

Family	MI Operator Rounds Administrator	MI Operator Rounds Mobile User	MAP-M Security Group	MI Rounds Designer Viewer	MI Lubrication Management Administrator	MI Lubrication Management User
Has Checkpoint	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
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

Family	MI Operator Rounds Administrator	MI Operator Rounds Mobile User	MAP-M Security Group	MI Rounds Designer Viewer	MI Lubrication Management Administrator	MI Lubrication Management User
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
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

Family	MI Operator Rounds Administrator	MI Operator Rounds Mobile User	MAP-M Security Group	MI Rounds Designer Viewer	MI Lubrication Management Administrator	MI Lubrication Management User
Template Has Checkpoint	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View

Deploy Rules

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.

Install the Meridium Rules Editor

Before You Begin

- Microsoft Visual Studio 2013 Professional or Microsoft Visual Studio 2015 Professional must be installed on every workstation where you want to work with Meridium, Inc. rules in the Meridium Enterprise APM system.

- If you are using Microsoft Visual Studio 2013 Professional, then, after Microsoft Visual Studio 2013 Professional is installed, on the same machine, access the Meridium Enterprise APM third-party software distribution package, then navigate to the folder **\\Microsoft VS2015 Shell**, then run the installer **vs_isoshell.exe**, and then run the installer **vs_int-shelladditional.exe**. These installers must be run in the order prescribed. This operation is required only if you are using Microsoft Visual Studio 2013 Professional.

- MSXML must also be installed on these workstations.

- You must be logged in as the administrator for the system.

Steps

1. On the machine that will serve as the Meridium rules editor, access the Meridium Enterprise APM distribution package, and then navigate to the folder **\\General Release\Meridium APM Setup\Setup\Admin**.

2. Open the file **Setup.exe**.
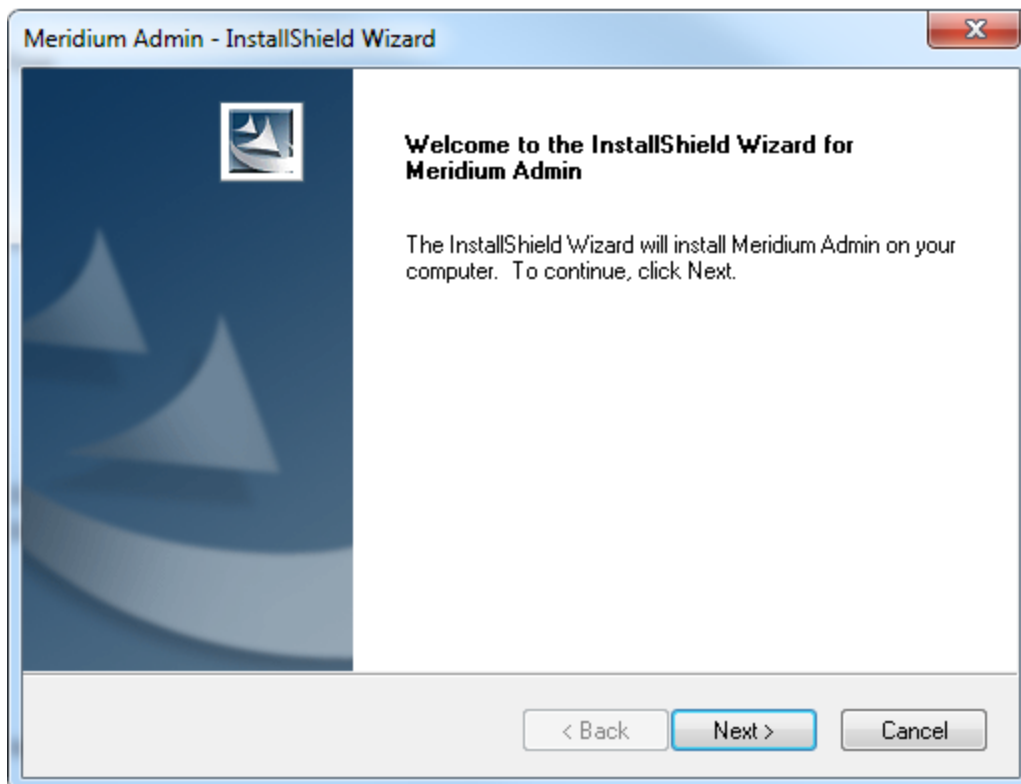
   The **Meridium Admin - InstallShield Wizard** screen appears.

3. Select **Next**.

   The **License Agreement** screen appears.
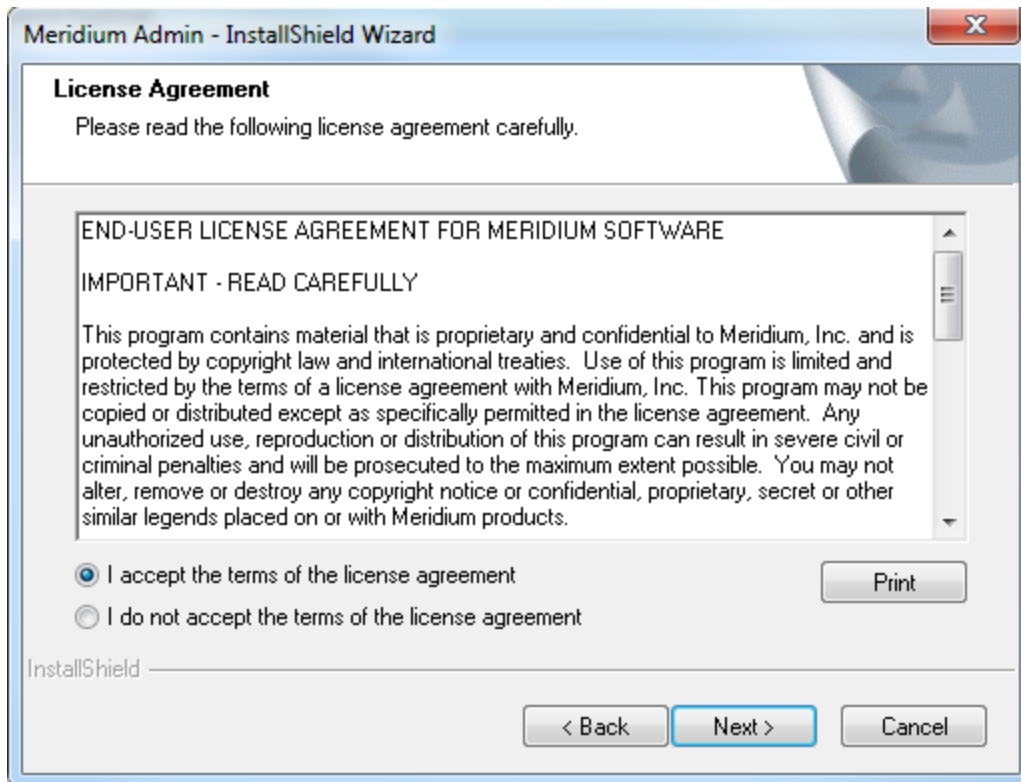
4. Read the License Agreement and, if you agree, select the **I accept the terms of the license agreement** option. Then, select **Next** button.

   The **Select Installation Location** screen appears.

5. Select **Next** to accept the default location.

    The **Select the features you want to install** screen appears.
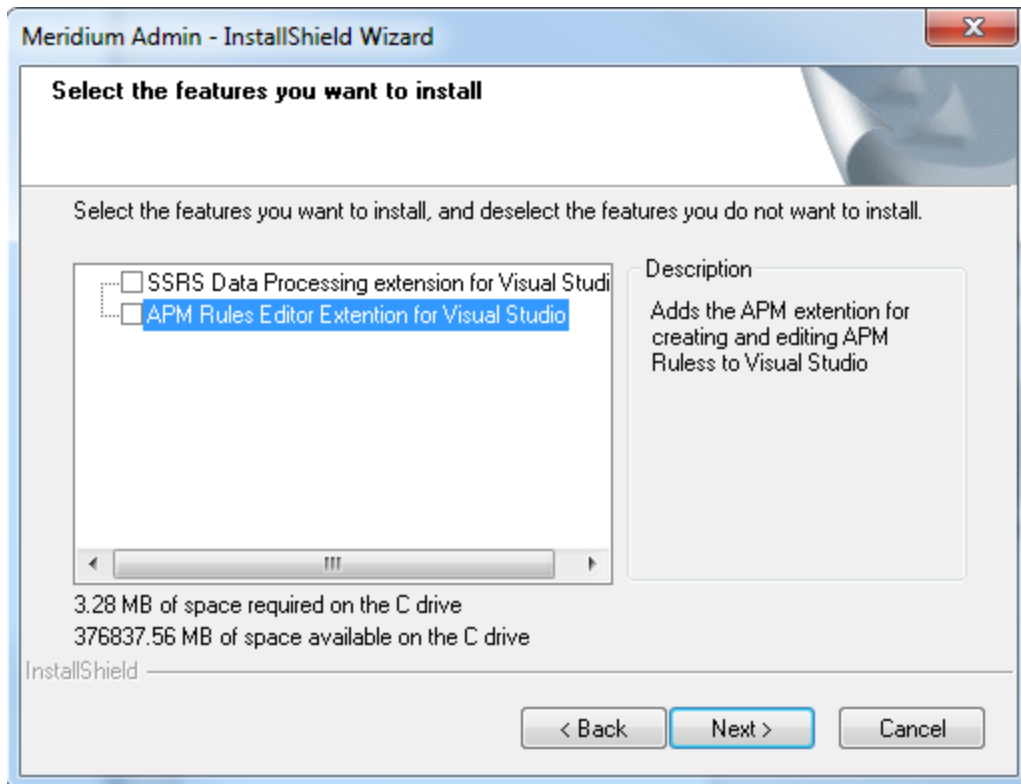
6. Select the **APM Rules Editor Extension for Visual Studio** option.

   Meridium Enterprise APM performs a check to make sure that your machine contains the required prerequisites for the features that you want to install. If one or more prerequisites are missing or there is not enough space on the machine, a dialog box will appear, explaining which prerequisites are missing or asking to free up space. If this occurs, close the installer, install the missing prerequisite or free up some space, and then run the installer again.

7. Select **Next**.

   The **Complete the Installation** screen appears.
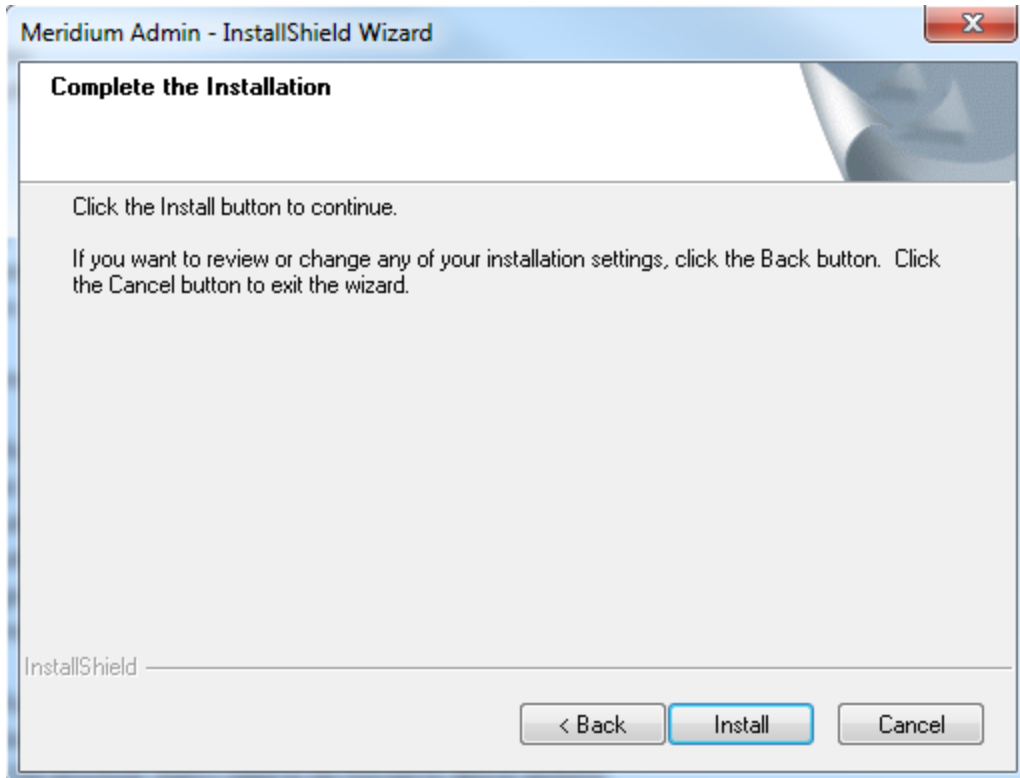
8. Select **Install**.

   The **Setup Status** screen appears, which displays a progress bar that shows the progress of the installation process. After the progress bar reaches the end, a message appears, indicating that Meridium Admin is installed successfully. Optionally, you can select to launch the APM System Administration tool when the installer window closes.
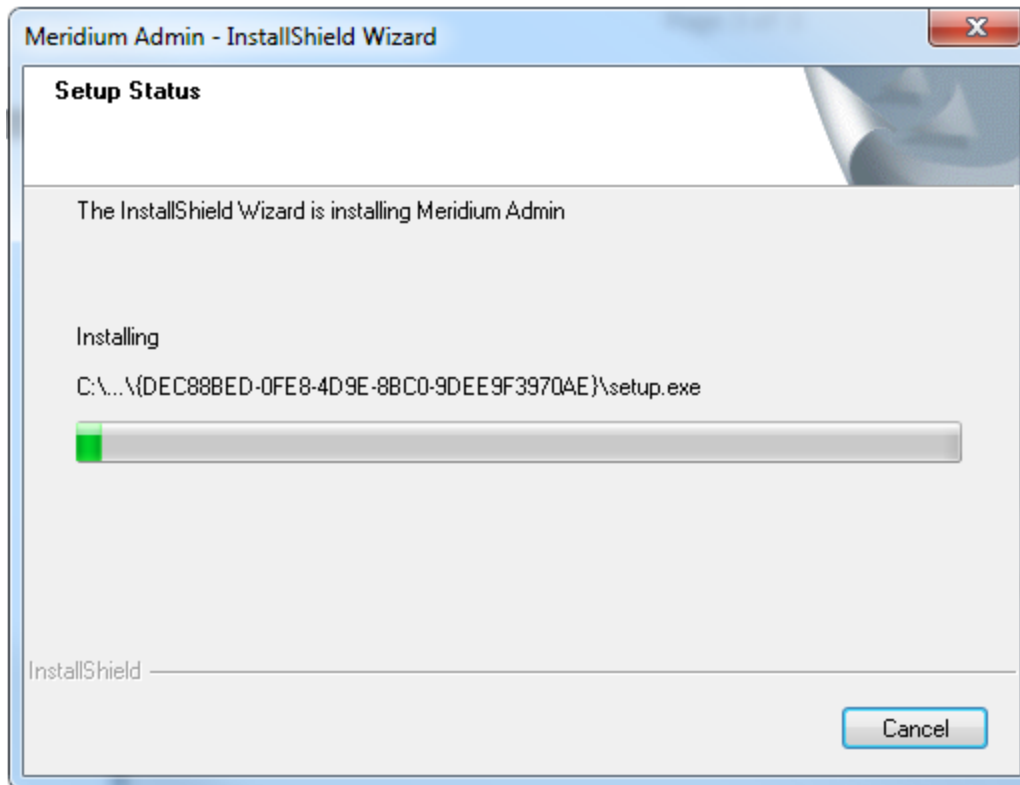
9. Clear the **Launch APM System Administration now** box, and then select **Finish**.
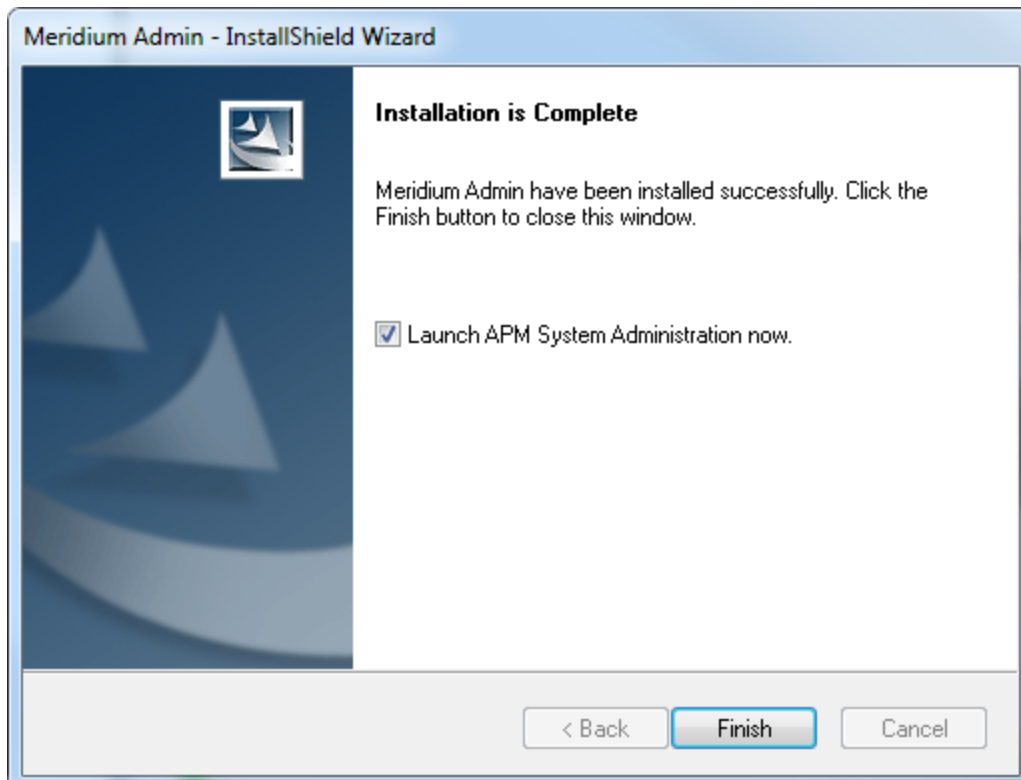
Results

- The Meridium Rules Editor is installed.

What's Next?

- Access the Meridium Rules Editor .

Deploy SIS 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 module.

Deploy SIS Management 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 Meridium Enterprise 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.

Step	Task	Notes
1	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 or location information in families other than the baseline Equipment and Functional Location families.
2	Assign the desired Security Users to one or more SIS Management Security Groups using the Configuration Manager.	This step is required. Users will not be able to access SIS Management unless they have permissions to the SIS Management families.
3	Define alternate search queries.	This step is required only if you do not want to use the baseline search queries.
4	Import data from an Exida project file.	This step is required only if you want to create SIL Analyses using an Exida project file.
5	Export data from an Exida project file.	This step is optional.
6	Manage the types of independent layers of protection that will be used to populate the Type list in an Independent Layer of Protection record. To do so, add a code to the MI_IPL_TYPE system code table.	This step is required only if you want to add another value to the list of default values in the Type list in the Independent Layer of Protection datasheet.

Step	Task	Notes
7	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.
8	Assign at least view permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager.	This step is required only for Security Groups that will be used in the integration between the SIS Management module and Hazards Analysis.

Upgrade or Update SIS Management to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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	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 at least View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager.	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 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 at least View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager.	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 V3.6.1.2.0

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 at least View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager.	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 V3.6.0.12.4

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 at least View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager.	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 V3.5.1.12.0

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 at least View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager.	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 V3.5.0.1.9.0

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 at least View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager.	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 at least View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager.	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 at least View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager.	This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

SIS 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 SIS Administrator	MI Safety Admin
MI SIS Engineer	MI Safety Admin MI Safety Power MI Safety User
MI SIS User	MI Safety Admin MI Safety Power MI Safety User

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

Family	MI SIS Administrator	MI SIS Engineer	MI SIS User
Entity Families			
Asset Criticality Analysis	View	None	None
Asset Criticality Analysis System	View	None	None
Consequence	View, Update, Insert, Delete	View	View
Consequence Modifier	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Equipment	View	View	View

Family	MI SIS Administrator	MI SIS Engineer	MI SIS User
External Assessment	View, Update, Insert, Delete	View, Update, Insert, Delete	None
Functional Location	View	View	View
Functional Systems	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Functional Test Detail	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Human Resource	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Independent Layer of Protection	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Instrumented Function	View, Update, Insert, Delete	View, Update, Insert, Delete	View
IPL Type	View, Update, Insert, Delete	View, Update, Insert, Delete	View
LOPA	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Notification	View, Update, Insert, Delete	View, Update, Insert, Delete	None
PHA Internal Assessment	View, Update, Insert, Delete	View, Update, Insert, Delete	None
Probability	View, Update, Insert, Delete	View	View
Protection Level	View, Update, Insert, Delete	View, Insert	View
Protective Instrument Loop	View, Update, Insert, Delete	View, Insert	View
Protective Instrument Loop Element	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Proven In Use Justification	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI SIS Administrator	MI SIS Engineer	MI SIS User
RBI Components	View, Update, Insert, Delete	View, Update, Insert, Delete	None
Reference Document	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Risk	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Risk Assessment	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Risk Assessment Recommendation	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Risk Category	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Risk Matrix	View, Update, Insert, Delete	View	View
Risk Matrix Internal Assessment	View, Update, Insert, Delete	View, Update, Insert, Delete	None
Risk Threshold	View, Update, Insert, Delete	View	View
Safety Instrumented System	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Safety Integrity Level	View, Update, Insert, Delete	View	View
SIF Common Cause Failure	View, Update, Insert, Delete	View, Update, Insert, Delete	View
SIL Analysis	View, Update, Insert, Delete	View, Update, Insert, Delete	View
SIL Threshold	View, Update, Insert, Delete	View	View
SIS Proof Test	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
SIS Proof Test Template	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI SIS Administrator	MI SIS Engineer	MI SIS User
SIS Proof Test Template Detail	View, Update, Insert, Delete	View, Update, Insert, Delete	View
SIS Trip Report	View, Update, Insert, Delete	View, Update, Insert, Delete	View
SIS Trip Report Detail	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Site Reference	View	View	View
Task	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Time Based Inspection Interval	View	View	View
Time Based Inspection Setting	View	View	View
Relationship Families			
Analysis Has Human Resource	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Asset Criticality Analysis Has System	View	None	View
Equipment Has Equipment	View	View	View
Functional Location Has Equipment	View	View	View
Functional Location Has Functional Location	View	View	View
Has Consequence Modifier	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Equipment	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Functional Location	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Functional Location Detail	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI SIS Administrator	MI SIS Engineer	MI SIS User
Has Functional Test	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Functional Test Detail	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Hazard Event	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has HAZOP Reference	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Has IF	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Independent Protection Layer	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Instrumented Function Revision	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Instrument Loop	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Instrument Loop Revision	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has LOPA	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has LOPA Revision	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has PIL Device	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has PIL Device Revision	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has PIL Group	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has PIL Group Revision	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has PIL Subsystem	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI SIS Administrator	MI SIS Engineer	MI SIS User
Has PIL Subsystem Revision	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Proven In Use Justification	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has RBI Components	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Recommendations	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Reference Documents	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Insert
Has Reference Values	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Risk	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Risk Category	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Risk Matrix	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has SIF Common Cause Failures	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has SIL Assessment	View, Update, Insert, Delete	View, Update, Insert, Delete	None
Has SIS Analysis Revision	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has SIS Revision	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has SIS Trip Report Detail	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Site Reference	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Task History	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Insert

Family	MI SIS Administrator	MI SIS Engineer	MI SIS User
Has Tasks	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Task Revision	View	View	View
Has Template Detail	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Templates	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Time Based Inspection Interval	View	View	View
Migrates Risk	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Was Promoted to ASM	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Deploy Thickness Monitoring (TM)

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 Thickness Monitoring (TM) 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 Meridium Enterprise 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.

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 TM Security Groups and Roles.	This step is required. User must have permissions to the TM families in order to use the TM functionality.
3	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*.

Step	Task	Notes
4	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 Meridium Enterprise APM database.
5	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.
6	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.
7	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 Meridium Enterprise APM database. You can specify that additional fields be displayed in the header section of these pages.
8	Disable the Auto Manage Tasks setting.	This step is required only if you are using both the RBI and the TM modules.
9	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.
10	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 (TM) to 4.2.0.7.0

The following tables outline the steps that you must complete to upgrade this module to 4.2.0.7.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise 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.

Update from version V4.2.0.0 through V4.2.0.6.0

This module will be updated to 4.2.0.7.0 automatically when you update the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise 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 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.2.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.4

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.9.0

This module will be upgraded to 4.2.0.7.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

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: a. 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) b. 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_	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
	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. c. Run the Bulk Analyze tool using your custom records.	

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 4.2.0.7.0. To do so: a. 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. b. Use the Bulk Analyze tool to update TM Analyses that are associated with TML Corrosion Analyses returned by the query you created in step a.	This step is required.

Step	Task	Notes
2	Manually update TM Analyses for which you used custom corrosion rates. To do so: a. 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) b. Use the Bulk Analyze tool to update TM Analyses associated with the Equipment and TML Group records returned by this query. ℹ **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_	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
	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. c. Run the Bulk Analyze tool using your custom records.	

Use Custom TML Analysis Types

The baseline Meridium Enterprise 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 Meridium Enterprise 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
```

More information on customizing baseline rules is available here.

Install the Meridium Device Service

> ⚠ **IMPORTANT:** This procedure needs to be repeated on every machine to which a data-logger will be connected.
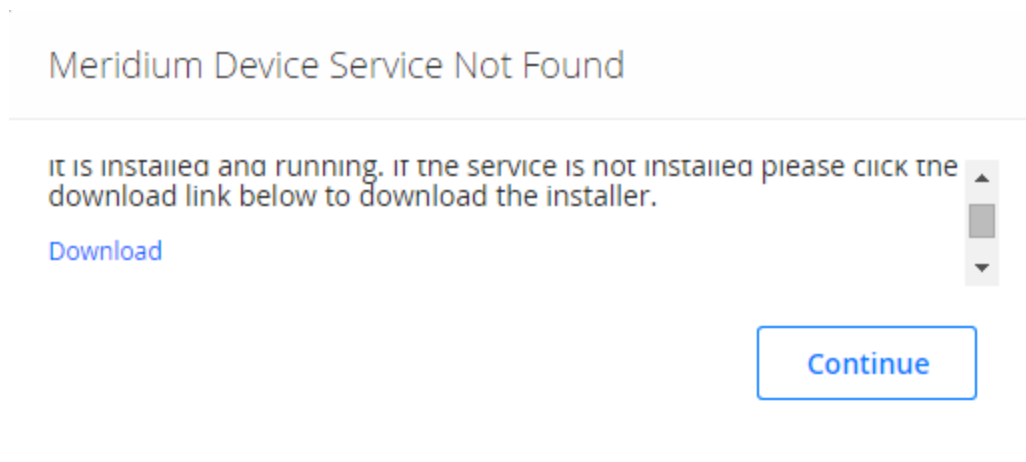
The Meridium Device Service can be installed in the normal workflow when using dataloggers with Thickness Monitoring.

Steps

1. Access Dataloggers for the any asset or TML Group.

2. Select **Send**.

   > 📄 **Note:** A datalogger does not need to be connected.

   The **Meridium Device Service Not Found** window appears.

   Meridium Device Service Not Found

   It is installed and running. If the service is not installed please click the download link below to download the installer.

   Download

   Continue

3. Select the **Download** link.

   MeridiumDevices.exe is downloaded.

4. Run **MeridiumDevices.exe** and follow the instructions in the installer.

   The Meridium Device Service is installed.

5. In the **Meridium Device Service Not Found** window, select **Continue**.

   Dataloggers can now be used with Thickness Monitoring.

Configure the Meridium Device Service

After installing the Meridium Device Service, you can make changes to certain configuration settings. The Meridium Device Service is designed to function out of the box. Generally, you will only make changes to the configuration if you need to increase the client timeout period, or change the port the service uses (by default, port 2014).

Steps

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 Meridium Enterprise 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 Monitoring Functional Security Privileges

Meridium Enterprise 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 Meridium Enterprise 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

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?
Exclude TMLs	No	Yes	No
Renew TMLs	No	Yes	No
Reset User Preferences	Yes	No	No

Thickness Monitoring 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 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

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
Entity Families			
Corrosion	View, Update, Insert	View, Update, Insert	View, Update, Insert
Datapoint	View, Update, Insert	View, Update, Insert	View, Update, Insert
Datapoint Measurement	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert
Equipment	View	View	View
Human Resource	View, Update, Insert, Delete	View	View
Inspection Task	View	View, Update	View

Family	MI Thickness Monitoring Administrator	MI Thickness Monitoring Inspector	MI Thickness Monitoring User
Materials of Construction	View	View	View
Meridium Reference Tables	View, Update, Insert, Delete	View	View
Resource Role	View, Update, Insert, Delete	View	View
Security Group	View	View	View
Security User	View	View	View
Settings	View, Update, Insert	View, Update, Insert	View
Task Execution	View, Insert	View, Insert	View
Thickness Monitoring Task	View, Update, Insert, Delete	View, Update, Insert	View, Update, Insert
TML Group	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Relationship Families			
Belongs to a Unit	View, Update, Insert, Delete	View, Update, Insert	View, Update, Insert
Equipment Has Equipment	View	View	View
Group Assignment	View	View	View
Has Archived Corrosion Analyses	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Archived Corrosion Analysis Settings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Archived Subcomponent Analysis Settings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete

Family	MI Thickness Monitoring Administrator	MI Thickness Monitoring Inspector	MI Thickness Monitoring User
Has Archived Subcomponent Corrosion Analyses	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Corrosion Analyses	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Corrosion Analysis Settings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Datapoints	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Measurements	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Roles	View, Update, Insert, Delete	View	View
Has Task Execution	View, Insert	View, Insert	View
Has Task Revision	View, Insert	View, Insert	View
Has Tasks	View, Insert	View, Insert	View, Insert
Has TML Group	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Is a User	View	View	View
User Assignment	View	View	View