Meridium Enterprise APM Modules and Features Deployment

V4.0.1.0

Meridium Enterprise APM Modules and Features Deployment

V4.0.1.0

Table of Contents

⚠ **Important:** This document is utilizing a prototype PDF template. Links to external documents do not function correctly and should not be used. You will be prompted when you attempt to use a link to an external document. This template will continue to be updated.

Deploying 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.

Deploying 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.

Deploying 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. All steps are required unless otherwise noted.

Step	Task	Required?	Notes
1	Assign Security Users to the Asset Health Manager Security Groups.	Y	None
2	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for AHM.	Y	None
3	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	Y	None
4	On the Meridium Enterprise APM Server, modify the file *Meridium.AHI.Service.exe.config.* to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	
5	Start the Meridium AHM Service. **Note:** The Meridium AHM Service is referred to as the "Asset Health Indicator Service" throughout the Meridium Enterprise APM documentation.	Y	When you start the service, Health Indicator records are created or updated automatically based on health indicator and reading source records.
6	Review the AHM data model to determine which relationship definitions you will need to modify to include your custom asset families.	N	Required if you store asset information in families other than the baseline Equipment and Functional Location families.

Step	Task	Required?	Notes
7	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.	Y	If you are using custom asset families and relationships (see Step 5), make sure that the equivalent records and links exist in the database.
8	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.	Y	Baseline Health Indicator Mapping records exist for the following health indicator source families: • Measurement Location • KPI • OPC Tag • Health Indicator
9	Link each asset record to the record(s) that you want to use as a health indicator source records.	Y	None
10	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.	N	None
11	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.	N	Refer to the Asset Health Manager end user help for more information about events.

Upgrading Asset Health Manager (AHM) to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. 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. All steps are required unless otherwise noted.

V3.6.0.0.0

Step	Task	Required?	Notes
1	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for AHM.	Y	None
2	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	Y	None
3	On the Meridium Enterprise APM Server, modify the file *Meridium.AHI.Service.exe.config*. to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
4	Start or restart the Meridium AHM Service. **Note:** The Meridium AHM Service is referred to as the "Asset Health Indicator Service" throughout the Meridium Enterprise APM documentation.	Y	None

Step	Task	Required?	Notes
5	Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each.	Y	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 V4.0.1.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records.
6	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.	Y	None
7	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.	Y	None

V3.5.1

Step	Task	Required?	Notes
1	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for AHM.	Y	None

Step	Task	Required?	Notes
2	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	Y	None
3	On the Meridium Enterprise APM Server, modify the file *Meridium.AHI.Service.exe.config.* to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
4	Start or restart the Meridium AHM Service. **Note:** The Meridium AHM Service is referred to as the "Asset Health Indicator Service" throughout the Meridium Enterprise APM documentation.	Y	None
5	Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each.	Y	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 V4.0.1.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records.

Step	Task	Required?	Notes
6	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..	Y	None
7	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.	Y	None

V3.5.0 SP1 LP

Step	Task	Required?	Notes
1	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for AHM.	Y	None
2	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	Y	None
3	On the Meridium Enterprise APM Server, modify the file *Meridium.AHI.Service.exe.config*. to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
4	Start or restart the Meridium AHM Service. **Note:** The Meridium AHM Service is referred to as the "Asset Health Indicator Service" throughout the Meridium Enterprise APM documentation.	Y	None

Step	Task	Required?	Notes
5	Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each.	Y	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 V4.0.1.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records.

Step	Task	Required?	Notes
6	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.	Y	None
7	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.	Y	None

V3.5.0

Step	Task	Required?	Notes
1	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for AHM.	Y	None
2	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	Y	None
3	On the Meridium Enterprise APM Server, modify the file *Meridium.AHI.Service.exe.config.* to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
4	Start or restart the Meridium AHM Service. **Note:** The Meridium AHM Service is referred to as the "Asset Health Indicator Service" throughout the Meridium Enterprise APM documentation.	Y	None

Step	Task	Required?	Notes
5	Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each.	Y	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 V4.0.1.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records.
6	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.	Y	None
7	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.	Y	None

V3.4.5

Step	Task	Required?	Notes
1	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for AHM.	Y	None

Step	Task	Required?	Notes
2	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	Y	None
3	On the Meridium Enterprise APM Server, modify the file *Meridium.AHI.Service.exe.config.* to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
4	Start or restart the Meridium AHM Service. **Note:** The Meridium AHM Service is referred to as the "Asset Health Indicator Service" throughout the Meridium Enterprise APM documentation.	Y	None
5	Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each.	Y	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 V4.0.1.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records.

Step	Task	Required?	Notes
6	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.	Y	None
7	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.	Y	None

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

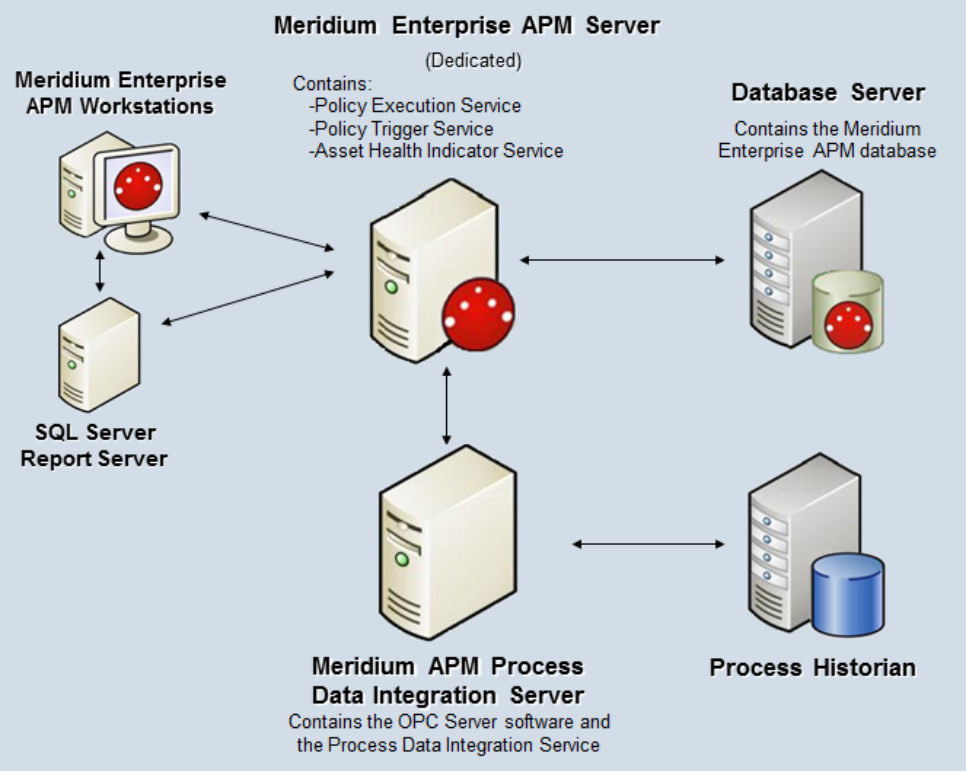
The following services are used by the Asset Health Manager, Process Data Integration, and Policy Designer modules:

- **Asset Health Indicator Service:** Automatically updates 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. 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.

The following table also includes an example of the database connection string that you must specify in the configuration file for each service used in your system architecture. For specific instructions on configuring each service, *including additional required configurations*, refer to the respective service configuration help topics.

Machine	Software Installed	Asset Health Service Installed Automatically with Service Software	Example Database Connection String
Meridium Enterprise APM Server	Meridium Enterprise APM Server software	Asset Health Indicator Service	<connection name="EXAMPLE_CONNECTION" applicationServer="" datasource="DATASOURCE_NAME" userId="SERVICE_USER_NAME " password="!PaSsWoRd" />
		Policy Trigger Service	<connection name="EXAMPLE_CONNECTION" applicationServer="" datasource="DATASOURCE_NAME" userId="SERVICE_USER_NAME " password="!PaSsWoRd" />
		Policy Execution Service	<connection name="EXAMPLE_CONNECTION" applicationServer="" datasource="DATASOURCE_NAME" userId="SERVICE_USER_NAME " password="!PaSsWoRd" />
Process Data Integration Server, which also acts as the OPC Server	Process Data Integration Service software	Process Data Integration Service	<connection name="EXAMPLE_CONNECTION" applicationServer="APPSERVER_NAME" datasource="DATASOURCE_NAME" userId="SERVICE_USER_NAME" password="!PaSsWoRd" xiServers="OPCSystem1" />
	OPC Server software	NA	NA
Process Historian	Process historian software	NA	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.

Configure the Asset Health Indicator Service

When you install the Meridium Enterprise APM Server, the Meridium AHM Service is installed automatically.

Note: The Meridium AHM Service is referred to as the "Asset Health Indicator Service" throughout the Meridium Enterprise APM documentation.

This service allows the values in the following Health Indicator record fields to be updated automatically when values change in the primary source record.

- 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. You must configure the Asset Health Indicator Service by modifying the file *Meridium.AHI.Service.exe.config.* These steps must be completed on all Meridium Enterprise APM Servers.

Steps

1. On the Meridium Enterprise APM Server, navigate to the folder where the Meridium Enterprise APM Server software is 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.AHI.Service.exe.config** in an application that you can use to modify XML script (e.g., Notepad).
3. Within the **<meridiumConnections>** tags, uncomment the example connection tag by deleting **<!--EXAMPLE:** and the corresponding **-->** from the beginning and end of the string.
4. 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.

Within this attribute...	Make this change	Notes
applicationServer	Specify the Meridium Enterprise APM Server on which the data source specified in the **datasource** attribute is configured. If the data source is configured on the Meridium Enterprise APM Server on which you are modifying this file, accept the default setting (i.e., an empty value). -or- If the data source is configured on a *remote* Meridium Enterprise APM Server, between the quotations, type the name or IP Address of that Meridium Enterprise APM Server.	If you want to create Health Indicator records from OPC Tag records, the Meridium Enterprise APM Server that you specify here must match the Meridium Enterprise APM Server that you specify in the Process Data Integration Service configuration file.
datasource	Replace **DATASOURCE_NAME** with the name of the Meridium Enterprise APM database that you will use to store your Health Indicator records.	If you want to create Health Indicator records from OPC Tag records, the data source that you specify here must match the data source that you specify in the Process Data Integration Service configuration file. 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.

Within this attribute...	Make this change	Notes
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 AHI User Security Group.
password	Replace **PaSsWoRd** with the password for the specified user.	You should 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.

5. Save and close the file.

   Your settings will be applied when the Meridium AHM Service is started or restarted.

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 each 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.

To do so, in each configuration file, complete the following steps for *each* required connection.

Steps

1. Configure the first connection by modifying the attributes within **<meridiumConnections>** tags, as described in the respective service configuration topic:
   - Configure the Policy Execution Service
   - Configure the Policy Trigger Service
   - Configure the Process Data Integration Service
   - Configure the Asset Health Indicator 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.

Asset Health Manager Security Groups and Roles

The following table lists the baseline Security Groups that represent the main types of users for this module, as well as the baseline roles assigned to each.

Security Group	Roles
MI AHI Administrator	MI Health Admin
MI AHI User	MI Health User MI Health Power

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

Family	MI AHI Administrator	MI AHI User
Entity Families		
Checkpoint Task	View, Update, Insert	View, Update, Insert
Event Mapping	View, Update, Insert, Delete	View
Health Indicator	View, Update, Insert, Delete	View, Update
Health Indicator Mapping	View, Update, Insert, Delete	View
Health Indicator Value	View, Update, Insert, Delete	View
Hierarchy Item Child Definition	View, Update, Insert, Delete	View
Hierarchy Item Definition	View, Update, Insert, Delete	View
Measurement Location	View	View
KPI	View	View
KPI Measurement	View	View
Measurement Location Template	View	View
Operator Rounds Allowable Values	View	View
Policy	View	View

Family	MI AHI Administrator	MI AHI User
Policy Instance	View	View
Reading	View	View
Recommendation	View, Update, Insert, Delete	View, Update, Insert, Delete
Timestamped Value	View, Update, Insert, Delete	View
OPC Reading	View	View
OPC System	View	View
OPC Tag	View	View
Relationship Families		
Has Checkpoint	View	View
Has Child Hierarchy Item	View, Update, Insert, Delete	View
Has Health Indicators	View, Update, Insert, Delete	View
Has Readings	View	View
Has Recommendations	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Timestamped Value	View, Update, Insert, Delete	View
Has OPC Reading	View	View
Has OPC Tag	View	View
Health Indicator Has Mapping	View, Update, Insert, Delete	View
Health Indicator Has Source	View, Update, Insert, Delete	View

Deploying 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.

Deploying Asset Criticality Analysis (ACA) for the First Time

The following table outlines the steps that you must complete to deploy and configure ACA 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. All steps are required unless otherwise noted.

Step	Task	Notes
1	Assign Security Users to one or more of the ACA Security Groups.	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.	Required if you will use equipment and location families other than the baseline Equipment and Functional Location families.
3	Define sites to associate with ACA Analyses.	None
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.	Required if you do not want to use the default label, *Unmitigated Risk*.
5	Lock the Risk Matrix.	Required if you do not want risk values to be specified manually via the Risk Matrix.

Upgrading Asset Criticality Analysis (ACA) to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. 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. All steps are required unless otherwise noted.

V3.6.0.0.0

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.	Required if you do not want to use the default label, *Unmitigated Risk*.
2	Lock the Risk Matrix.	Required 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.	Required if you want to update your SAP system to reflect the criticality value that is determined in ACA.

V3.5.1

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.	Required if you do not want to use the default label, *Unmitigated Risk*.
2	Lock the Risk Matrix.	Required 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.	Required if you want to update your SAP system to reflect the criticality value that is determined in ACA.

V3.5.0 SP1 LP

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.	Required if you do not want to use the default label, *Unmitigated Risk*.
2	Lock the Risk Matrix.	Required 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.	Required if you want to update your SAP system to reflect the criticality value that is determined in ACA.

V3.5.0

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.	Required if you do not want to use the default label, *Unmitigated Risk*.
2	Lock the Risk Matrix.	Required 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.	Required if you want to update your SAP system to reflect the criticality value that is determined in ACA.

V3.4.5

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.	Required if you do not want to use the default label, *Unmitigated Risk*.
2	Lock the Risk Matrix.	Required 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.	Required if you want to update your SAP system to reflect the criticality value that is determined in ACA.

ACA Security Groups

The following table lists the baseline Security Groups that represent the main types of users for this module, as well as the baseline roles assigned to each.

Security Group	Roles
MI ACA Administrator	
MI ACA Member	
MI ACA Owner	

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

Family	MI ACA Administrator	MI ACA Member	MI ACA Owner
Analysis Has Human Resource	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Asset Criticality Analysis	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Asset Criticality Analysis Has System	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Asset Criticality Analysis System	View, Update, Insert, Delete	View	View, Update, Insert, Delete
Consequence	View, Update, Insert, Delete	View	View
Consequence Modifier	View, Update, Insert, Delete	View	View
Criticality Mapping	View	View	View
Equipment	View	View	View
Equipment Has Equipment	View	View	View
Functional Location	View	View	View
Functional Location Has Equipment	View	View	View
Functional Location Has Functional Location	View	View	View
Has Criticality Mapping	View	View	View

Family	MI ACA Administrator	MI ACA Member	MI ACA Owner
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
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

Family	MI ACA Administrator	MI ACA Member	MI ACA Owner
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
System Strategy	View	None	None

About Associating an ACA with a Specific Site

Some companies that use the Meridium Enterprise APM software have facilities at multiple sites, or locations, around the world. Each site contains unique units, systems, and assets.

If desired, you can define these sites and associate equipment and locations with the site to which they belong. You can also associate risk matrices with specific sites. If a risk matrix is associated with a site, you can specify which site you want to associate with an ACA. You can associate a site with an ACA by selecting the ID of the desired Site Reference record in the Site ID field on the Analysis Definition datasheet for that ACA.

After an ACA is associated with a site, when you create a Risk Assessment record for an Asset Criticality Analysis System, Equipment, or Functional Location record associated with the ACA, rather than seeing the default risk matrix, you will see the risk matrix that is associated with the specified site.

You can add to an ACA an Equipment or Functional Location record that is already associated with a site even if the site is different than the one specified in the Asset Criticality Analysis record. If an Equipment or Functional Location record is already associated with a site and a risk rank value already exists for that record:

- The risk rank value that was determined using the risk matrix associated with the Equipment or Functional Location record will appear in the Analysis Summary pane beneath its parent system.
- When you try to view or modify the risk rank for the Equipment or Functional Location record, a message will appear, indicating that the risk rank was determined using a risk matrix other than the one that is currently associated with the analysis. When this message appears, you can choose to:
  - Accept the current risk rank value that was determined using a risk matrix other than the one that is associated with the current analysis. If you choose this option, you will not be able to modify the risk rank for the record.
  - Determine the risk rank for the Equipment or Functional Location record using the risk matrix that is associated with the current analysis.

Note: This information is also true if you specify a site for the ACA, and then later specify a different site.

If an Equipment or Functional Location record is associated with a site but a risk rank value has not been determined for that record, when you select the Risk Matrix link to define the risk rank for that record, the risk matrix that is currently associated with the ACA appears.

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 of the datasheet, select {pencil icon}.

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

6. Select {disk icon}.

   The Unmitigated Risk Label for that risk matrix is changed.

Deploying 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.

Deploying 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.

Steps are marked as *Required* in the **Required/Optional** column if you must perform the steps to take advantage of ASI functionality. This documentation assumes that, in addition to implementing the basic ASI functionality, that you also want to implement integration with SAP. Steps necessary for SAP integration are also designated as *Required* in the following table.

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. All steps are required unless otherwise noted.

Step	Task	Required/Optional	Notes
1	Install the ASI for SAP ABAP add-on on your SAP System.	Required	None
2	Review the ASI 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 the Configuration Manager application.	Optional	This task is necessary only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
3	Assign users to one or more of the Strategy Security Roles via the Security Manager application.	Required	Users will need permissions to the ASI families in order to use ASI.
4	Configure SAP permissions.	Required	None
5	Configure secured Maintenance Plants in your SAP System.	Optional	None
6	Configure Work Management Item Definition records via the ASI Application Settings.	Optional	This task is necessary only if you want to use Work Management Item Definition records beyond those provided with the baseline database.

Step	Task	Required/Optional	Notes
7	Define Implementation Roles via the ASI Application Settings.	Optional	None
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.	Required	None

Upgrading Asset Strategy Implementation (ASI) to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

V3.6.0.0.0

Step	Task	Required?	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	Y	None

V3.5.1

Step	Task	Required?	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	Y	None

V3.5.0 SP1 LP

Step	Task	Required?	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	Y	None

V3.5.0

Step	Task	Required?	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	Y	None

V3.4.5

Step	Task	Required?	Notes
1	Upgrade the ASI for SAP ABAP add-on in your SAP System.	Y	None

Security Groups and Roles in ASI

The following table lists the baseline Security Groups that represent the main types of users for this module, as well as the baseline roles assigned to each.

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

MI Strategy User: Users have access to default RCM/FMEA user privileges (view, create, edit), ASI user privileges, and ASM view privileges.

MI Strategy Power: Users have Strategy_Users access, plus ASM reviewer privileges (manage strategies, actions, tasks, and risks).

MI Strategy Admin: Users have Strategy_PowerUsers access, plus RCM/FMEA administrator privileges (configuring and maintaining), ASI administrator privileges, and ASM management administrator privileges.

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
Action	None	View, Update
Action Mapping	View, Update, Insert, Delete	View
Active Strategy	None	View
Asset Strategy	None	View
Calibration Task	None	View, Update, Insert, Delete
Consequence	None	View
Equipment	View, Update, Insert, Delete	View, Update, Insert
Execution Mapping	View, Update, Insert, Delete	View

Functional Location	View, Update, Insert, Delete	View, Update, Insert
Health Indicator	None	View
Health Indicator Mapping	None	View
Hierarchy Item Child Definition	None	View
Hierarchy Item Definition	None	View
Implementation Authorization	View, Update, Insert, Delete	View
Implementation Package	None	View, Update, Insert, Delete
Implementation Role	View, Update, Insert, Delete	View
Inspection Task	None	View, Update, Insert, Delete
KPI	None	View
KPI Measurement	None	View
Maintenance Item	None	View, Update, Insert, Delete
Maintenance Package	None	View, Update, Insert, Delete
Maintenance Plan	None	View, Update, Insert, Delete
Material	None	View, Update, Insert, Delete
Measurement Location	None	View, Update, Insert, Delete
Measurement Location Group	None	View, Update, Insert, Delete
Measurement Location Template	View, Update, Insert, Delete	View, Update, Insert
Notification	None	View, Update, Insert, Delete
Object List Item	None	View, Update, Insert, Delete

Operation	None	View, Update, Insert, Delete
Operator Rounds Allowable Values	None	View
Probability	None	View
Proposed Strategy	None	View
Protection Level	None	View
PRT	None	View, Update, Insert, Delete
PRT Template	View, Update, Insert, Delete	View
RCM FMEA Asset	None	View
RCM FMEA Recommendation	None	View
Risk	None	View
Risk Assessment	None	View
Risk Category	None	View
Risk Matrix	None	View
Risk Rank	None	View
Risk Threshold	None	View
SAP System	View, Update, Insert, Delete	View
Site Reference	View	View
System Strategy	None	View
Task List	None	View, Update, Insert, Delete
Task Types	None	View
Thickness Monitoring Task	None	View, Update, Insert, Delete
Unit Strategy	None	View
Work Management Item Child Definition	View, Update, Insert, Delete	View

Work Management Item Definition	View, Update, Insert, Delete	View
Work Management Item Definition Configuration	View, Update, Insert, Delete	View
Relationship Families		
Authorized to Implement	View, Update, Insert, Delete	View
Documents Action	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Actions	None	View
Has Action Mapping	View, Update, Insert, Delete	View
Has Action Revisions	None	View
Has Active Strategy	None	View
Has Asset Strategy	None	View
Has Associated Recommendation	None	View
Has Checkpoint	None	View, Insert
Has Child Hierarchy Item	None	View
Has Child Work Management Item	View, Update, Insert, Delete	View
Has Driving Recommendation	None	View
Has Execution Mapping	View, Update, Insert, Delete	View
Has Health Indicators	View, Update, Insert, Delete	View, Update, Insert, Delete
Has KPI Measurement	None	View
Has Maintenance Item	None	View, Update, Insert, Delete
Has Maintenance Package	None	View, Update, Insert, Delete
Has Material	None	View, Update, Insert, Delete

Has Measurement Location Group	None	View, Update, Insert, Delete
Has Mitigation Revisions	None	View
Has Object List Item	None	View, Update, Insert, Delete
Has Operation	None	View, Update, Insert, Delete
Has Proposed Strategy	None	View
Has PRT	None	View, Update, Insert, Delete
Has Reference Values	None	View
Has Risk	None	View
Has Risk Category	None	View
Has Risk Revisions	None	View
Has SAP System	None	View, Update, Insert, Delete
Has Strategy	None	View
Has Strategy Revision	None	View
Has System Strategy	None	View
Has Tasks	None	View, Update, Insert, Delete
Has Task List	None	View, Update, Insert, Delete
Has Task Revision	None	View, Update, Insert, Delete
Has Work Management Item	None	View, Update, Insert, Delete
Has Work Management Item Definition Configuration	View, Update, Insert, Delete	View
Health Indicator Has Mapping	None	View, Update, Insert
Health Indicator Has Source	None	View, Update, Insert, Delete

Implements Action	None	View, Update, Insert, Delete
Implements Strategy	None	View, Update, Insert, Delete
Implements Secondary Strategy	None	View, Update, Insert, Delete
Is Mitigated	None	View
Master Template Has Asset Strategy	None	View
Mitigates Risk	None	View
Was Applied to Asset Strategy	View, Update, Insert, Delete	View, Update, Insert, Delete
Was Applied to PRT	View, Update, Insert, Delete	View, Update, Insert, Delete

Deploying 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.

Deploying 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. All steps are required unless otherwise noted.

Step	Task	Required/Optional	Notes
1	If you are using families outside of the baseline Equipment and Functional Location families, review the ASM data module 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 the Configuration Manager application.	Optional	This step is necessary only if you are using families outside the baseline Equipment and Functional Location families to store equipment and location data.
2	Assign users to one or more of the Strategy Security Roles via the Security Manager application.	Required	None

Upgrading Asset Strategy Management (ASM) to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

V3.6.0.0.0

ASM will be upgraded from V3.6.0.0.0 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.1

ASM will be upgraded from V3.5.1 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0 SP1 LP

Step	Task	Required?	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; Strategy Revision.	Y	None
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; Has Risk Category.	Y	None
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.	Y	None

V3.5.0

Step	Task	Required?	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 activation process: Action; Risk; Risk Assessment; Risk Rank; Action Revision; Risk Revision; Risk Assessment Revision; Strategy Revision.	Y	None

V3.4.5

Step	Task	Required?	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 activation process: Action; Risk; Risk Assessment; Risk Rank; Action Revision; Risk Revision; Risk Assessment Revision; Strategy Revision.	Y	None

ASM Security Groups

The following table lists the baseline Security Groups that represent the main types of users for this module, as well as the baseline roles assigned to each.

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

MI Strategy User: Users have access to default RCM/FMEA user privileges (view, create, edit), ASI user privileges, and ASM view privileges.

MI Strategy Power: Users have Strategy_Users access, plus ASM reviewer privileges (manage strategies, actions, tasks, and risks).

MI Strategy Admin: Users have Strategy_PowerUsers accesss, plus RCM/FMEA administrator privileges (configuring and maintaining), ASI administrator privileges, and ASM management administrator privileges.

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
Action	Insert, View, Update, and Delete	View	Insert, View, Update, and Delete	View
Action Mapping	View	None	None	None
Active Strategy	Insert, View, Update, and Delete	View	Insert, View, Update, and Delete	View
Analysis Link	View	View	View	View

Asset Criticality Analysis	View	View	View	View
Asset Criticality Analysis Has System	View	View	View	View
Asset Criticality Analysis System	View	View	View	View
Asset Strategy	Insert, View, Update, and Delete	View	View and Update	View
Calibration Task	View	None	View	None
Checkpoint Task	Insert, View and Update	Insert, View and Update	Insert, View and Update	Insert, View and Update
Consequence	View	Insert, View, Update, and Delete	View	View
Distribution	Insert, View, Update, and Delete	View	View	View
Execution Mapping	View	None	None	None
Growth Model	View	View	View	View
Has Action Driver	Insert, View, Update, and Delete	None	None	None
Has Action Mapping	View	None	None	None
Has Action Revisions	Insert, View, Update, and Delete	View	Insert, View, Update, and Delete	View
Has Actions	Insert, View, Update, and Delete	View	Insert, View, Update, and Delete	View
Has Active Strategy	Insert, View, Update, and Delete	View	Insert, View, Update, and Delete	View
Has Asset Strategy	Insert, View, Update, and Delete	View	View	View

Has Associated Recommendation	Insert, View, Update, and Delete	View	View	View
Has Associated Strategy	Insert, View, Update, and Delete	View	View	View
Has Checkpoint	View	None	None	None
Has Child Hierarchy Item	View	Insert, View, Update, and Delete	View	View
Has Child Work Management Item	View	None	None	None
Has Driving Recommendation	Insert, View, Update, and Delete	View	View and Delete	View
Has Execution Mapping	View	None	None	None
Has Functional Location	View	n/a	View	n/a
Has Global Events	Insert, View, Update, and Delete	View	View	View
Has Health Indicators	Insert, View, Update, and Delete	View	View	View
Has Measurement Location Group	Insert, View, Update, and Delete	None	None	None
Has Mitigated TTF Distribution	Insert, View, Update, and Delete	View	View	View
Has Mitigation Revisions	Insert, View, Update, and Delete	View	Insert, View, Update, and Delete	View
Has Planned Resource Usages	Insert, View, Update, and Delete	View	View	View
Has Proposed Strategy	Insert, View, Update, and Delete	View	Insert, View, Update, and Delete	View

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

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

Health Indicator Has Mapping	Insert, View, Update, and Delete	View	View	View
Health Indicator Has Source	Insert, View, Update, and Delete	View	View	View
Health Indicator Mapping	View	Insert, View, Update, and Delete	View	View
Hierarchy Item Child Definition	View	Insert, View, Update, and Delete	View	View
Hierarchy Item Definition	View	Insert, View, Update, and Delete	View	View
Implementation Package	View and Insert	None	None	None
Implementation Role	View	View	View	View
Implements Action	Insert, View and Update	None	None	None
Implements Strategy	View and Insert	None	None	None
Implements Secondary Strategy	View	None	None	None
Inspection Task	View	None	View	View
Is Based on RBI Degradation Mechanism	None	None	View and Delete	None
Is Based on RCM FMEA Failure Effect	Insert, View, Update, and Delete	None	None	None
Is Basis for Asset Strategy Template	Insert, View, Update, and Delete	View	View and Update	View
Is Mitigated	Insert, View, Update, and Delete	View	Insert, View, Update, and Delete	View
KPI	View	View	View	View
KPI Measurement	View	View	View	View

Master Template Has Asset Strategy	Insert, View, Update, and Delete	View	View and Update	View
Measurement Location	View	View	View	View
Measurement Location Group	Insert, View and Update	None	None	None
Measurement Location Template	View	View	View	View
Mitigates Risk	Insert, View, Update, and Delete	View	Insert, View, Update, and Delete	View
Operator Rounds Allowable Values	View	View	View	View
Probability	View	Insert, View, Update, and Delete	View	View
Proposed Strategy	Insert, View, Update, and Delete	View	View and Update	View
Protection Level	View	View	View	View
RBI Degradation Mechanisms	View and Update	None	None	None
RBI Recommendation	View and Update	None	None	None
RCM FMEA Asset	Insert, View, Update, and 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, and Delete	View	Insert, View, Update, and Delete	View
Risk Category	View	Insert, View, Update, and Delete	View	View

Risk Matrix	View	Insert, View, Update, and Delete	View	View
Risk Rank	Insert, View, Update, and Delete	View	Insert, View, Update, and Delete	View
Risk Threshold	View	Insert, View, Update, and Delete	View	View
Safety Analysis Has Equipment	View	n/a	View	n/a
Site Reference	View	View	View	View
System Action	Insert, View, Update, and Delete	View	View	View
System Action Mapping	View	Insert, View, Update, and Delete	View	View
System Action Optim-ization	Insert, View, Update, and Delete	View	View	View
System Action Result	Insert, View, Update, and Delete	View	View	View
System Analysis	Insert, View, Update, and Delete	View	View	View
System Element	Insert, View, Update, and Delete	View	View	View
System Element Result	Insert, View, Update, and Delete	View	View	View
System Global Event	Insert, View, Update, and Delete	View	View	View

System Resource	Insert, View, Update, and Delete	View	View	View
System Resource Result	Insert, View, Update, and Delete	View	View	View
System Resource Usage	Insert, View, Update, and Delete	View	View	View
System Risk Assessment	Insert, View, Update, and Delete	View	View	View
System Scenario	Insert, View, Update, and Delete	View	View	View
System Sensor	Insert, View, Update, and Delete	View	View	View
System Strategy	Insert, View, Update, and Delete	View	View and Update	View
Unit Strategy	Insert, View, Update, and Delete	View	View and Update	View
Was Applied to Asset Strategy	Insert, View, Update, and Delete	View	View and Update	View
Was Promoted to ASM Element	View	None	View	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

Associating a Strategy with a Specific Site

Some companies that use the Meridium Enterprise APM software have facilities at multiple sites, or locations, around the world. Each site contains unique locations and equipment.

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

Deploying 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.

Deploying 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. All steps are required unless otherwise noted.

Step	Task	Required/Optional	Notes
1	Review the Calibration Management data model to determine which relationship definitions you will need to modify to include your custom families.	Optional	Required 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.	Required	None
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.	Required	None
4	Define alternate search queries.	Optional	Required 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.	Required	None

Upgrading Calibration Management to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

V3.6.0.0.0

Calibration Management will be upgraded from V3.6.0.0 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.1

Calibration Management will be upgraded from V3.5.1 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0 SP1 LP

Calibration Management will be upgraded from V3.5.0 SP1 LP to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0

Calibration Management will be upgraded from V3.5.0 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.4.5

Calibration Management will be upgraded from V3.4.5 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Security Groups

The following table lists the baseline Security Groups that represent the main types of users for this module, as well as the baseline roles assigned to each.

Security Group	Roles
MI Calibration Administrator	MI Safety Admin
MI Calibration User	MI Safety Admin MI Safety Power MI Safety User

All Security Users who need to access Calibration Management functionality must be assigned to one of these two groups. Family-level privileges alone are not enough to allow a user to access Calibration Management.

The following table summarizes the baseline privileges for these Security Groups.

Family	MI Calibration Administrator	MI Calibration User
Entity Families		
Alert	View, Update, Insert, Delete	View, Update, Insert, Delete
Calibration Recommendation	View, Update, Insert, Delete	View, Update, Insert
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

Family	MI Calibration Administrator	MI Calibration User
Calibration (Event)	View, Update, Insert, Delete	View, Update, Insert, Delete
Calibration Result	View, Update, Insert, Delete	View, Update, Insert, Delete
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
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

Family	MI Calibration Administrator	MI Calibration User
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
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

Deploying 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.

Deploying Failure Modes and Effects Analysis (FMEA) for the First Time

Deploying and configuring FMEA for the first time includes completing multiple steps, which are outlined in the table in this topic. The steps in this section of the documentation provide all the information that you need to deploy and configure FMEA on top of the basic Meridium Enterprise APM system architecture.

Whether a step is required or optional is indicated in the **Required/Optional** cell. Steps are marked as *Required* if you must perform the step to take advantage of FMEA functionality.

The person responsible for completing each task may vary within your organization. We recommend, however, that the steps be performed in relatively the same order in which they are listed in the table.

Step	Task	Required/Optional	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.	Optional	This task is necessary only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign users to one or more of the Strategy Security Roles via the Security Manager application.	Required	None

Upgrading Failure Modes and Effects Analysis (FMEA) to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

V3.6.0.0.0

FMEA will be upgraded from V3.6.0.0.0 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.1

FMEA will be upgraded from V3.5.1 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0 SP1 LP

FMEA will be upgraded from V3.5.0 SP1 LP to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0

FMEA will be upgraded from V3.5.0 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.4.5

Step	Task	Required?	Notes
1	Assign Security Users to the MI RCM Viewer Security Group.	Y	None
2	Add values to the Recommended Resource System Code Table.	Y	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

The following table lists the baseline Security Groups that represent the main types of users for this module, as well as the baseline roles assigned to each.

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 FMEA module uses the following baseline Security Groups:

- **MI RCM Administrator**: The MI RCM Administrator Security Group has no family-level privileges configured for it in the baseline Meridium Enterprise APM database. Users who are members of this group will see the **Administration** link on the **RCM Start Page** in the Meridium Enterprise APM Framework application and will, therefore, have access to administrative functions in FMEA. Users who do not belong to this Security Group will not see this link and, therefore, will not be able to access the administrative functions.

  Because the MI RCM Administrator Security Group has no family-level privileges assigned to it by default, to access features and functions in FMEA, members of the MI RCM Administrator Security Group will also need to be assigned to the MI RCM User or MI RCM Viewer Security Group.
- **MI RCM User**: The MI RCM User Security Group has access to all features in FMEA.
- **MI RCM Viewer**: The MI RCM Viewer Security Group has view-only access to FMEA. Users belonging to the MI RCM Viewer Security Group will not have access to features that result in the creation, update, or deletion of records or links between records.

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.

Deploying 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.

Deploying 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. All steps are required unless otherwise noted.

Step	Task	Required/Optional	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.	Optional	Required 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.	Required	Users will not be able to access Hazards Analysis unless they have permissions to the Hazards Analysis families.
3	Define alternate search queries.	Optional	Required 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.	Optional	Required 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.	Optional	Required if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

Step	Task	Required/Optional	Notes
6	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group.	Optional	Required if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

Upgrading Hazards Analysis to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. 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. All steps are required unless otherwise noted.

V3.6.0.0.0

Step	Task	Required?	Notes
1	Activate the SIS Management license.	No	Required 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.	No	Required if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

V3.5.1

Step	Task	Required?	Notes
1	Activate the SIS Management license.	No	Required 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.	No	Required if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

V3.5.0 SP1 LP

Step	Task	Required?	Notes
1	Activate the SIS Management license.	No	Required if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

Step	Task	Required?	Notes
2	Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group.	No	Required if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

V3.5.0

Step	Task	Required?	Notes
1	Activate the SIS Management license.	No	Required 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.	No	Required if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

V3.4.5

Step	Task	Required?	Notes
1	Activate the SIS Management license.	No	Required 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.	No	Required if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

Security Groups and Privileges

The following table lists the baseline Security Groups that represent the main types of users for this module, as well as the baseline roles assigned to each.

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

These groups are intended to support the three main types of users who will use Hazards Analysis. Each of these groups has privileges assigned to it by default. The baseline family-level privileges 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
Functional Location	View	View	View	View
Hazards Analysis	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI HA Administrator	MI HA Owner	MI HA Facilitator	MI HA Member
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 Protection Layer	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Instrumented Function	View	View	View	View
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

Family	MI HA Administrator	MI HA Owner	MI HA Facilitator	MI HA Member
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				
Analysis Has Human Resource	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Cause Has Consequence	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI HA Administrator	MI HA Owner	MI HA Facilitator	MI HA Member
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 Safeguard 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 Location Has Equipment	View	View	View	View
Functional Location Has Functional Location	View	View	View	View
Has Hazards Analysis Revision	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has HAZOP Reference	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI HA Administrator	MI HA Owner	MI HA Facilitator	MI HA Member
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 Recommendations	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 Values	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
Has Site Reference	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

Family	MI HA Administrator	MI HA Owner	MI HA Facilitator	MI HA Member
Hazards Analysis Revision Has Systems/Nodes Revision	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Is Independent Protection 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 Revision Has IPL Revision	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

Deploying 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.

- Meridium Enterprise APM Installation and Upgrade

Deploying 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. All steps are required unless otherwise noted.

Step	Task	Required?	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. Modify any relationship definitions as needed via Configuration Manager.	N	Required 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.	Y	Security Users will need permissions to the Inspection Management families before they can use the Inspection Management features.
3	Set the Asset Query Path setting to the baseline Asset Query.	Y	In the baseline database, this setting is not defined. The documentation assumes that you are using the product according to the Meridium Enterprise APM Best Practice. Therefore, we assume that you will set the Asset Query Path setting to the baseline Asset Query.
4	Modify baseline Application Configuration settings.	N	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. You can modify these Application Configurations if you want.

5	Assign roles to users who should be able to complete tasks in Inspection Management.	Y	None
6	Define the Inspection Profile for each piece of equipment that you will inspect.	N	Required if you plan to create Inspection records in baseline families other than the *Checklists* subfamilies.
7	Modify the baseline Asset query.	N	Required if you want Inspection records to be linked to records in a family other than the *Equipment* family.
8	Define Event Configurations for any new Inspection families that you have created.	N	Required if you have created custom Inspection families that you want to use within Inspection Management.
9	Assign certifications to users.	N	None
10	Group inspection work into Work Packs.	N	None
11	Define Time-Based Inspection settings.	N	None

Upgrading Inspection Management to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

V3.6.0.0.0

Inspection Management will be upgraded from V3.6.0.0.0 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.1

Inspection Management will be upgraded from V3.5.1 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0 SP1 LP

Step	Task	Required?	Notes
1	Define Time-Based Inspection settings.	N	None

V3.5.0

Step	Task	Required?	Notes
1	Define Time-Based Inspection settings.	N	None

V3.4.5

Step	Task	Required?	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 set the value in the Reference field to *Inspection*.	N	Required if you have added System Codes to the MI_INSPECTION_TYPE System Code table.
2	Define Time-Based Inspection settings.	N	None

Inspection Management Security Groups

The baseline Inspection Management module contains one Security Group, *MI Inspection*. The MI Inspection Security Group has the following roles:

- MI Inspection User
- MI Inspection Power
- MI Inspection Admin

The following table lists the default privileges that members of the MI Inspection Security Group have to the Inspection entity and relationship families.

Family	Privileges
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
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

Family	Privileges
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
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

Family	Privileges
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.

Deploying 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.

Deploying 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. All steps are required unless otherwise noted.

Step	Task	Required?	Notes
1	Deploy SQL Server Analysis Services on the SQL Server Analysis Server (Version 12 or Version 14) machine. Deploying SQL Server Analysis Services on the SQL Server Analysis Server machine includes the following steps: 1. Install SQL Server Analysis Services. 2. Deploy Work History Analysis Services database. This is a replacement of *Meridium_Event_Analysis* database, and *Equipment and Functional Location Work History* cubes delivered as packaged solution. 3. Create a Windows User on the Analysis Server or in your organization's Active Directory. The user name requires minimum privileges and will only be used by the Meridium Enterprise Application 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 4. Add the user created in Step 3 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. Work History database already has a *View* role defined, you should add the user to this role. For more information, con-	Y	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	Required?	Notes
	sult the MSDN documentation regarding Roles and Permissions for Analysis Services. 5. Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication. HTTPS is recommended with basic authentication. For more information, consult the MSDN documentation regarding configuring the HTTP access to Analysis Services on Internet Information Service (IIS).		
2	Configure a cube for usage metrics tracking on the SQL Server Analysis Server.	N	Required if you will use Metrics and Scorecards to view the usage metrics in a cube.
3	Schedule cubes for processing on the SQL Server Analysis Server.	Y	None
4	If needed, migrate SQL Server cubes from one version of SQL Server Analysis Services to another.	Y	None
5	Assign Security Users to the Metrics and Scorecards Security Groups.	Y	None
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, with server address you need to provide credentials of the user created in Step 1 Task 3.	Y	None
7	Grant Security Users and Groups access rights to Analysis Services Cube records.	Y	None
8	Configure privileges for KPI.	Y	None
9	Configure privileges for Scorecards.	Y	None

Upgrading Metrics and Scorecards to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

V3.6.0.0.0

The DBUMS utility will upgrade existing Scorecards and KPIs seamlessly. However, to upgrade metric views, ensure that the user running the upgrade utility has read permissions on the cubes associated to metric views and the cubes are active.

V3.5.1

Metrics and Scorecards will be upgraded from V3.5.1 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0 SP1 LP

Step	Task	Required?	Notes
1	Migrate your SQL Server Analysis Services database and cubes to SQL Server Analysis Services 2012.	N	Required if you were previously using SQL Server Analysis Services 2008 R2 and want to use SQL Server Analysis Services 2012 instead.

V3.5.0

Step	Task	Required?	Notes
1	Migrate your SQL Server Analysis Services database and cubes to SQL Server Analysis Services 2012.	N	Required if you were previously using SQL Server Analysis Services 2008 R2 and want to use SQL Server Analysis Services 2012 instead.

V3.4.5

Step	Task	Required?	Notes
1	Migrate your SQL Server Analysis Services database and cubes to either of the following supported SQL Server Analysis Services versions: • 2008 R2 • 2012	N	Required if you were previously using SQL Server Analysis Services 2005. This step is optional if you were previously using SQL Server Analysis Services 2008 R2 and want to use SQL Server Analysis Services 2012 instead.
2	Create a master scheduled item for managing automatic KPI updates.	Y	This step is necessary for supporting automatic KPI updates.

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.

Metrics and Scorecard Security Groups

The following baseline Security Groups are provided for the Metrics and Scorecards module:

- MI Metrics Administrator: Provides users with full access to all Metrics and Scorecards features and functions.
- MI Metrics User: Provides users with view-only access to Metrics and Scorecards functionality, provided that they have been granted the necessary entity-level permissions.

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

Family	MI Metrics Administrator	MI Metrics User
Analysis Services Cube	View, Update, Insert, Delete	View
KPI	View, Update, Insert, Delete	View, Update, Insert, Delete
KPI Measurement	View, Update, Insert, Delete	View, Update, Insert, Delete
Scorecard	View, Update, Insert, Delete	View, Update, Insert, Delete
Has KPI Measurement	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Privileges	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Sub Indicators	View, Update, Insert, Delete	View, Update, Insert, Delete
Is Used By Scorecard	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 see the **Manage Cubes** button on the **Metrics and Scorecards** page in the Meridium Enterprise APM.
- Can manage privileges for all KPIs in the Meridium Enterprise APM.
- Can manage privileges for all Scorecards in the Meridium Enterprise APM.
- Has full access to all KPIs, Scorecards, and Cubes without needing to be granted additional privileges via the Meridium Enterprise APM.

Deploying 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.

Deploying 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. All steps are required unless otherwise noted.

Note: These steps assume that your system architecture contains only one Meridium Enterprise APM Server which is also used for policy execution. If your system architecture contains more than one Meridium Enterprise APM Server, you must complete certain steps on multiple machines.

Step	Task	Required?	Notes
1	Assign the needed Security Users to one or more Policy Designer Security Groups.	Y	None
2	On the Meridium Enterprise APM Server, modify the Policy Execution Service configuration file to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
3	Start the Policy Execution Service.	Y	None
4	On the Meridium Enterprise APM Server, modify the Policy Trigger Service configuration file to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
5	Start the Policy Trigger Service.	Y	None
6	On the Meridium Enterprise APM Server, reset IIS.	Y	None
7	On the Meridium Process Data Integration Server, start or restart the Process Data Integration Service.	Y	Required *only* if you want to use OPC Tag records in your policies.

Upgrading Policy Designer to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

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.

V3.6.0.0.0

Step	Task	Required?	Notes
1	On the Meridium Enterprise APM Server, modify the Policy Execution Service configuration file to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
2	Start or restart the Policy Execution Service.	Y	None
3	On the Meridium Enterprise APM Server, modify the Policy Trigger Service configuration file to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
4	Start or restart the Policy Trigger Service.	Y	None
5	On the Meridium Enterprise APM Server, reset IIS.	Y	None
6	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	Y	Required *only* if you want to use OPC Tag records in your policies.

V3.5.1

Step	Task	Required?	Notes
1	On the Meridium Enterprise APM Server, modify the Policy Execution Service configuration file to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
2	Start or restart the Policy Execution Service.	Y	None

Step	Task	Required?	Notes
3	On the Meridium Enterprise APM Server, modify the Policy Trigger Service configuration file to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
4	Start or restart the Policy Trigger Service.	Y	None
5	On the Meridium Enterprise APM Server, reset IIS.	Y	None
6	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	Y	Required *only* if you want to use OPC Tag records in your policies.

V3.5.0 SP1 LP

Step	Task	Required?	Notes
1	On the Meridium Enterprise APM Server, modify the Policy Execution Service configuration file to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
2	Start or restart the Policy Execution Service.	Y	None
3	On the Meridium Enterprise APM Server, modify the Policy Trigger Service configuration file to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
4	Start or restart the Policy Trigger Service.	Y	None
5	On the Meridium Enterprise APM Server, reset IIS.	Y	None
6	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	Y	Required *only* if you want to use OPC Tag records in your policies.

V3.5.0

Step	Task	Required?	Notes
1	On the Meridium Enterprise APM Server, modify the Policy Execution Service configuration file to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
2	Start or restart the Policy Execution Service.	Y	None
3	On the Meridium Enterprise APM Server, modify the Policy Trigger Service configuration file to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
4	Start or restart the Policy Trigger Service.	Y	None
5	On the Meridium Enterprise APM Server, reset IIS.	Y	None
6	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	Y	Required *only* if you want to use OPC Tag records in your policies.

V3.4.5

Step	Task	Required?	Notes
1	On the Meridium Enterprise APM Server, modify the Policy Execution Service configuration file to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
2	Start or restart the Policy Execution Service.	Y	None
3	On the Meridium Enterprise APM Server, modify the Policy Trigger Service configuration file to specify the Meridium Enterprise APM Server, Meridium Enterprise APM database, and login credentials.	Y	None
4	Start or restart the Policy Trigger Service.	Y	None
5	On the Meridium Enterprise APM Server, reset IIS.	Y	None

Step	Task	Required?	Notes
6	On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service.	Y	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

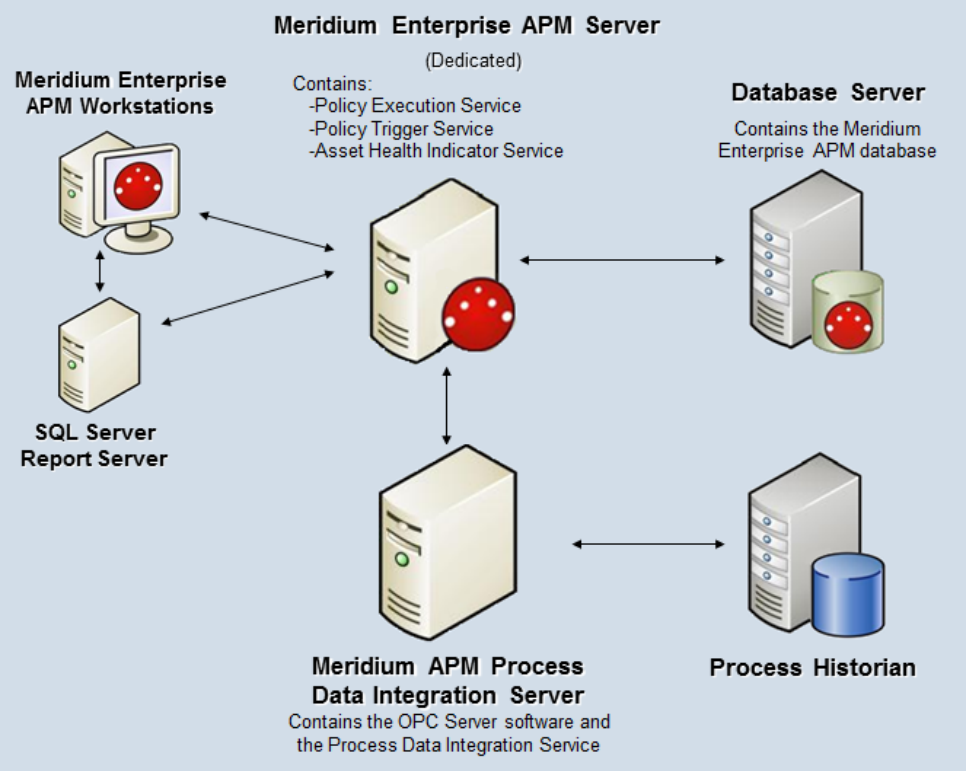
The following services are used by the Asset Health Manager, Process Data Integration, and Policy Designer modules:

- **Asset Health Indicator Service:** Automatically updates 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. 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.

The following table also includes an example of the database connection string that you must specify in the configuration file for each service used in your system architecture. For specific instructions on configuring each service, *including additional required configurations*, refer to the respective service configuration help topics.

Machine	Software Installed	Asset Health Service Installed Automatically with Service Software	Example Database Connection String
Meridium Enterprise APM Server	Meridium Enterprise APM Server software	Asset Health Indicator Service	<connection name="EXAMPLE_ CONNECTION" applicationServer="" data-source="DATASOURCE_NAME" userId=" SERVICE_USER_NAME " pass-word="!PaSsWoRd" />
		Policy Trigger Service	<connection name="EXAMPLE_ CONNECTION" applicationServer="" data-source="DATASOURCE_NAME" userId=" SERVICE_USER_NAME " pass-word="!PaSsWoRd" />
		Policy Execution Service	<connection name="EXAMPLE_ CONNECTION" applicationServer="" data-source="DATASOURCE_NAME" userId=" SERVICE_USER_NAME " pass-word="!PaSsWoRd" />
Process Data Integration Server, which also acts as the OPC Server	Process Data Integration Service software	Process Data Integration Service	<connection name="EXAMPLE_ CONNECTION" applic-ationServer="APPSERVER_NAME" data-source="DATASOURCE_NAME" userId=" SERVICE_USER_NAME" pass-word="!PaSsWoRd" xiServer-s="OPCSystem1" />
	OPC Server software	NA	NA
Process Historian	Process historian software	NA	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 Execution Service

The Policy Execution Service is installed automatically on the Meridium Enterprise APM Server when you select the Meridium Enterprise APM Application Server option in the Meridium Enterprise APM Server and Add-ons installer.

In order to execute policies, you must configure the Policy Execution Service by modifying the file *Meridium.Policies.ExecutionService.exe.config* on each Meridium Enterprise APM Server that will be used for policy execution. If your system architecture contains more than one of these machines, you must configure each one.

Steps

1. On the Meridium Enterprise APM Server machine, navigate to the folder where the Policy Execution 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.ExecutionService.exe.config** in an application that you can use to modify XML script (e.g., Notepad).
3. Within the **<meridiumConnections>** tags, uncomment the example connection tag by deleting **<!--EXAMPLE:** and the corresponding **-->** from the beginning and end of the string.
4. 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.

Within this attribute...	Make this change	Notes
applicationServer	Specify the Meridium Enterprise APM Server on which the data source specified in the **data-source** attribute is configured. If the data source is configured on the Meridium Enterprise APM Server on which you are modifying this file, accept the default setting (i.e., an empty value). -or- If the data source is configured on a *remote* Meridium Enterprise APM Server, between the quotations, type the name or IP Address of that Meridium Enterprise APM Server.	If you have more than one Meridium Enterprise APM Server in your system architecture, the value that you specify here depends on the load-balancing option you are using.

Within this attribute...	Make this change	Notes
datasource	Replace **DATASOURCE_NAME** with the name of the Meridium Enterprise APM database that you will use to store your policies.	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. To ensure that policies are triggered as expected, the data source name configured for a Meridium Enterprise APM database should be the same on all machines in your system architecture (i.e., Meridium Enterprise APM Servers and PDI Servers). As a result, the data source value that you specify here will match the data source value that you specify when you configure corresponding services (i.e., the Policy Trigger Service, the Process Data Integration Service, and the Asset Health Indicator Service).
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 that you specify must have privileges to all Policy Designer families and any other families that will be associated with a policy. Therefore, we recommend that you specify a user that is a Super User. In order for policies to be able to send email messages, there must be an email address associated with the user that you specify.
password	Replace **PaSsWoRd** with the password for the specified user.	You should 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.

5. Save and close the file.

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

Configure the Policy Trigger Service

The Policy Trigger Service is installed automatically on the Meridium Enterprise APM Server when you select the Meridium Enterprise APM Application Server option in the Meridium Enterprise APM Server and Add-ons installer.

In order to execute policies, you must configure the Policy Trigger Service by modifying the file *Meridium.Policies.Service.exe.config*. These steps must be completed on *all* Meridium Enterprise APM Servers.

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, uncomment the example connection tag by deleting **<!--EXAMPLE:** and the corresponding **-->** from the beginning and end of the string.
4. Within the **add url** attribute:
   - If you have only one Meridium Enterprise APM Server in your system architecture, replace **EXECUTION_SERVER_NAME** with *localhost*.

     -or-

   - If you have more than one Meridium Enterprise APM Server in your system architecture, replace **EXECUTION_SERVER_NAME** with the name of the cluster used for policy executions.
5. In the file, within the **<meridiumConnections>** tags, uncomment the example connection tag by deleting **<!--EXAMPLE:** and the corresponding **-->** from the beginning and end of the string.
6. 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.

Within this attribute...	Make this change	Notes
applicationServer	Specify the Meridium Enterprise APM Server on which the data source specified in the **data-source** attribute is configured. If the data source is configured on the Meridium Enterprise APM Server on which you are modifying this file, accept the default setting (i.e., an empty value). -or- If the data source is configured on a *remote* Meridium Enterprise APM Server, between the quotations, type the name or IP Address of that Meridium Enterprise APM Server.	None

Within this attribute...	Make this change	Notes
datasource	Replace **DATASOURCE_NAME** with the name of the Meridium Enterprise APM database that you will use to store your policies.	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. To ensure that policies are triggered as expected, the data source name configured for a Meridium Enterprise APM database should be the same on all machines in your system architecture (i.e., Meridium Enterprise APM Servers and PDI Servers). As a result, the data source value that you specify here will match the data source value that you specify when you configure corresponding services (i.e., the Policy Execution Service, the Process Data Integration Service, and the Asset Health Indicator Service).
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 that you specify must have privileges to all Policy Designer families and any other families that will be associated with a policy. Therefore, we recommend that you specify a user that is a Super User. In order for policies to be able to send email messages, there must be an email address associated with the user that you specify.
password	Replace **PaSsWoRd** with the password for the specified user.	You should 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.

7. Save and close the file.

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

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 each 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.

To do so, in each configuration file, complete the following steps for *each* required connection.

Steps

1. Configure the first connection by modifying the attributes within **<meridiumConnections>** tags, as described in the respective service configuration topic:
   - Configure the Policy Execution Service
   - Configure the Policy Trigger Service
   - Configure the Process Data Integration Service
   - Configure the Asset Health Indicator 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.

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. When you complete the first-time deployment steps for Policy Designer, you must complete certain steps on each machine. Specifically:

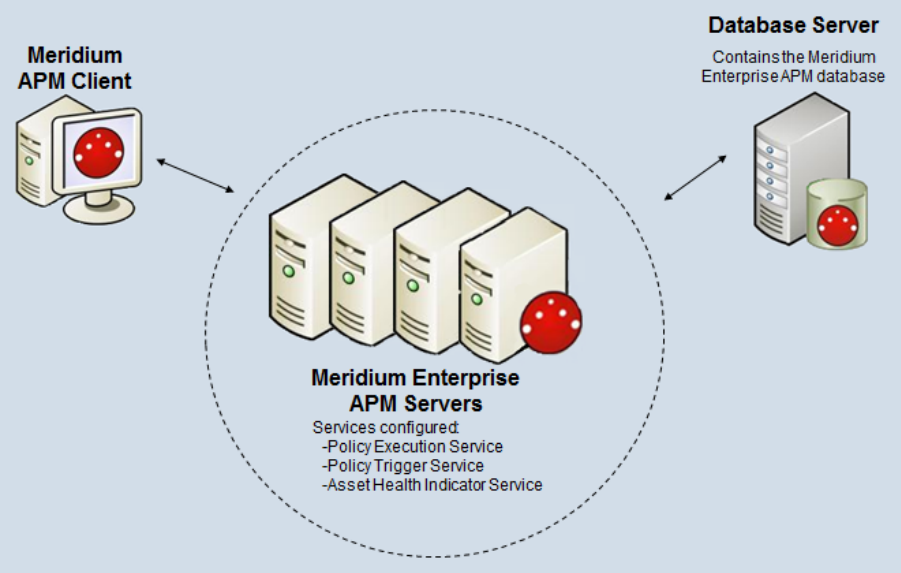
1. On *all* Meridium Enterprise APM Server machines, configure and start the Policy Trigger Service.
2. On *all* Meridium Enterprise APM Server machines, configure and start the Asset Health Indicator Service.
3. On each Meridium Enterprise APM Server machine *used for policy execution*, configure and start the Policy Execution Service. The value that you specify in the **<meridiumConnections>** tags depends on the server load-balancing option you are using. See below for details.

Server Load-Balancing Options

Depending on your company's preference for server load-balancing, you can configure your Meridium Enterprise APM System Architecture in one of two basic ways:

- **Global load-balancing**: 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 Execution Service on all Meridium Enterprise APM Server. When you do so, in the **applicationServer** attribute within the **<meridiumConnections>** tags, you should specify the name of the cluster.

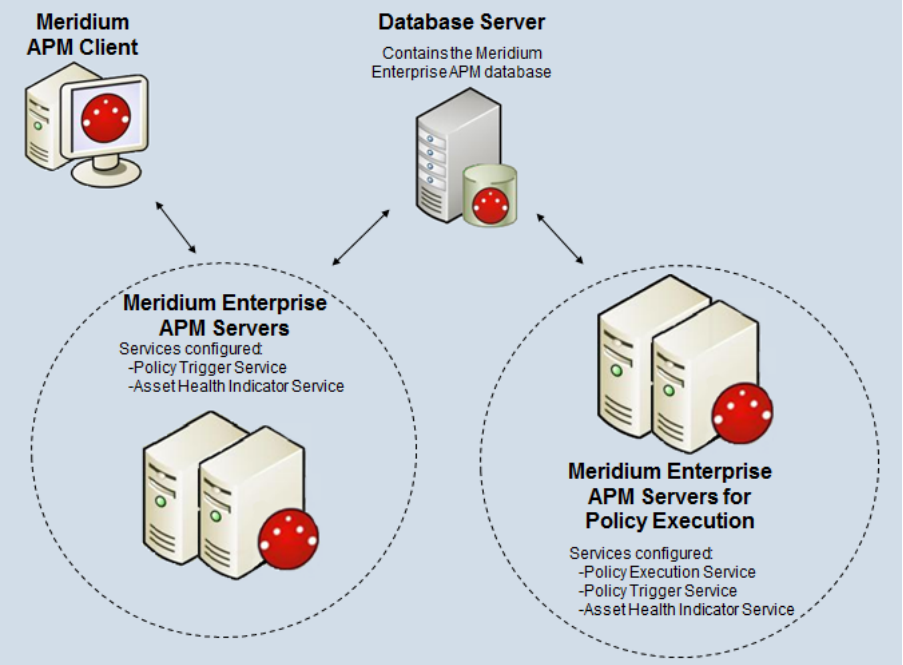


-or-

- **Isolated load-balancing**: 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 Execution Service on only the machines in the cluster for policy executions. When you do so, in the **applicationServer** attribute within the **<meridiumConnections>** tags, you should accept the default setting (i.e., an empty value) to use the local machine.

  IMPORTANT: When using isolated load-balancing, when you configure the Policy Execution, Policy Trigger, and Asset Health Indicator Services on the Meridium Enterprise APM Servers, the values that you specify in the **<meridiumConnections>** tags should not reference a machine or cluster outside of the cluster within which you are configuring the service.


Meridium
APM Client
Database Server
Contains the Meridium
Enterprise APM database
Meridium Enterprise
APM Servers
Services configured:
-Policy Trigger Service
-Asset Health Indicator Service
Meridium Enterprise
APM Servers for
Policy Execution
Services configured:
-Policy Execution Service
-Policy Trigger Service
-Asset Health Indicator Service

Policy Designer Security Groups and Roles

The following table lists the baseline Security Groups that represent the main types of users for this module, as well as the baseline roles assigned to each.

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

Deploying 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.

Deploying 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 already configured the Meridium Enterprise APM Server on a separate machine.

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. All steps are required unless otherwise noted.

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	Required?	Notes
1	Ensure that your OPC Server and process historian are configured according to the PDI system requirements.	Y	None
2	Review the server roles that are configured for the Process Data Integration Server in the Meridium Enterprise APM testing environment, and configure roles on your Process Data Integration Server accordingly.	Y	None
3	Assign Security Users to one or more of the Process Data Integration Security Groups.	Y	None
4	In Meridium Enterprise APM, create an OPC System record to represent the OPC-compliant system from which you want to retrieve data.	Y	None
5	On the Process Data Integration Server, install the Process Data Integration Service.	Y	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	Required?	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.	Y	None
7	On the Process Data Integration Server, start the Process Data Integration Service.	Y	When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records.
8	On the Meridium Enterprise APM Server, configure the Meridium Notification Service for PDI.	Y	None
9	On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service.	Y	None
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.	N	Required if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
11	In Meridium APM, link OPC Tag records to related asset records.	Y	None

Upgrading Process Data Integration (PDI) to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

V3.6.0.0.0

Step	Task	Required?	Notes
1	On the Process Data Integration Server, upgrade the Process Data Integration Service.	Y	None
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.	Y	None
3	On the Process Data Integration Server, start or restart the Process Data Integration Service.	Y	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.	Y	None
5	On the Meridium Enterprise APM Server, restart the Meridium Notification Service.	Y	None
6	In Meridium Enterprise APM, link any new OPC Tag records to related asset records.	Y	None

V3.5.1

Step	Task	Required?	Notes
1	On the Process Data Integration Server, upgrade the Process Data Integration Service.	Y	None
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.	Y	None
3	On the Process Data Integration Server, start or restart the Process Data Integration Service.	Y	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.	Y	None
5	On the Meridium Enterprise APM Server, restart the Meridium Notification Service.	Y	None
6	In Meridium Enterprise APM, link any new OPC Tag records to related asset records.	Y	None

V3.5.0 SP1 LP

Step	Task	Required?	Notes
1	On the Process Data Integration Server, upgrade the Process Data Integration Service.	Y	None

Step	Task	Required?	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.	Y	None
3	On the Process Data Integration Server, start or restart the Process Data Integration Service.	Y	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.	Y	None
5	On the Meridium Enterprise APM Server, restart the Meridium Notification Service.	Y	None
6	In Meridium APM, link any new OPC Tag records to related asset records.	Y	None

V3.5.0

Step	Task	Required?	Notes
1	On the Process Data Integration Server, upgrade the Process Data Integration Service.	Y	None
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.	Y	None

Step	Task	Required?	Notes
3	On the Process Data Integration Server, start or restart the Process Data Integration Service.	Y	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.	Y	None
5	On the Meridium Enterprise APM Server, restart the Meridium Notification Service.	Y	None
6	In Meridium APM, link any new OPC Tag records to related asset records.	Y	None

V3.4.5

Step	Task	Required?	Notes
1	On the Process Data Integration Server, upgrade the Process Data Integration Service.	Y	None
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.	Y	None

Step	Task	Required?	Notes
3	On the Process Data Integration Server, start or restart the Process Data Integration Service.	Y	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.	Y	None
5	On the Meridium Enterprise APM Server, restart the Meridium Notification Service.	Y	None
6	In Meridium APM, link any new OPC Tag records to related asset records.	Y	None

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

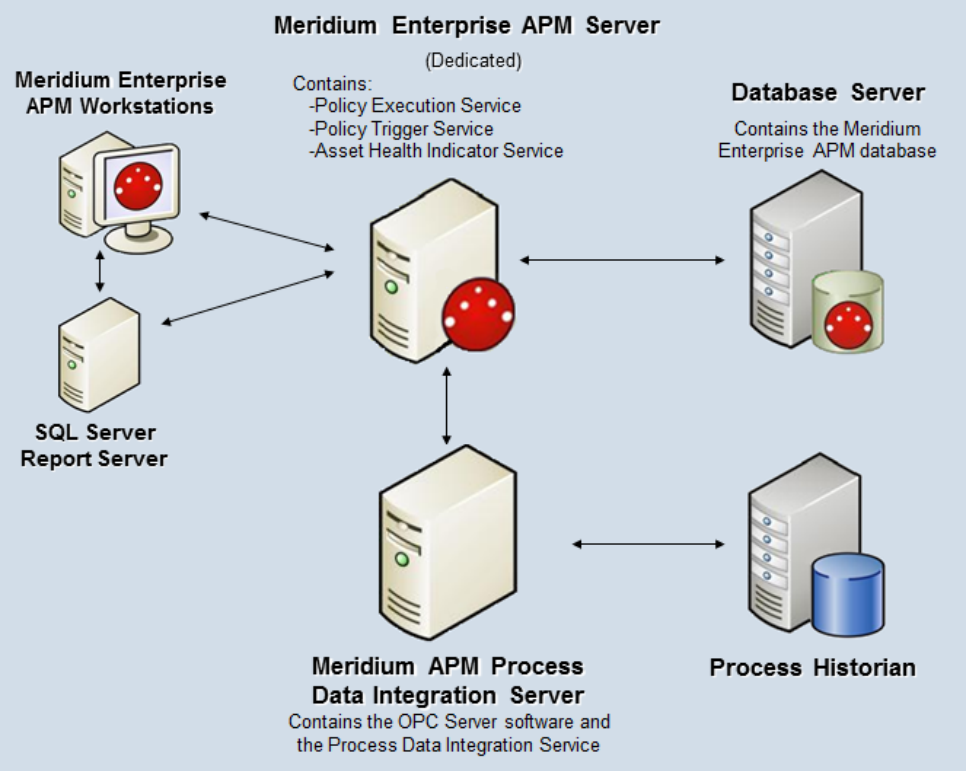
The following services are used by the Asset Health Manager, Process Data Integration, and Policy Designer modules:

- **Asset Health Indicator Service:** Automatically updates 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. 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.

The following table also includes an example of the database connection string that you must specify in the configuration file for each service used in your system architecture. For specific instructions on configuring each service, *including additional required configurations*, refer to the respective service configuration help topics.

Machine	Software Installed	Asset Health Service Installed Automatically with Service Software	Example Database Connection String
Meridium Enterprise APM Server	Meridium Enterprise APM Server software	Asset Health Indicator Service	<connection name="EXAMPLE_ CONNECTION" applicationServer="" data-source="DATASOURCE_NAME" userId=" SERVICE_USER_NAME " pass-word="!PaSsWoRd" />
		Policy Trigger Service	<connection name="EXAMPLE_ CONNECTION" applicationServer="" data-source="DATASOURCE_NAME" userId=" SERVICE_USER_NAME " pass-word="!PaSsWoRd" />
		Policy Execution Service	<connection name="EXAMPLE_ CONNECTION" applicationServer="" data-source="DATASOURCE_NAME" userId=" SERVICE_USER_NAME " pass-word="!PaSsWoRd" />
Process Data Integration Server, which also acts as the OPC Server	Process Data Integration Service software	Process Data Integration Service	<connection name="EXAMPLE_ CONNECTION" applic-ationServer="APPSERVER_NAME" data-source="DATASOURCE_NAME" userId=" SERVICE_USER_NAME" pass-word="!PaSsWoRd" xiServer-s="OPCSystem1" />
	OPC Server software	NA	NA
Process Historian	Process historian software	NA	NA

Installing 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

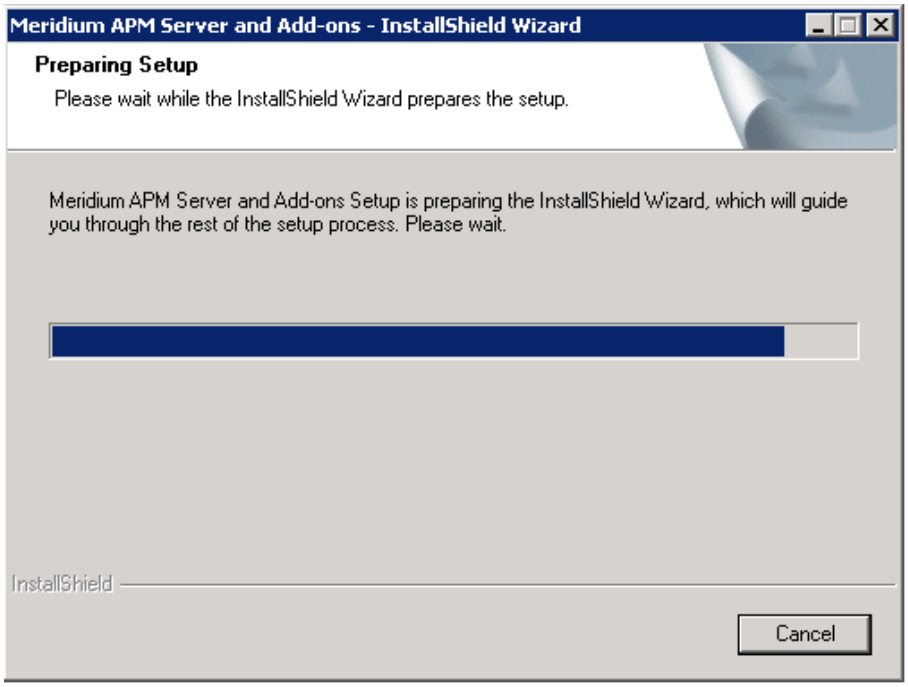
The following instructions provide details on upgrading the Process Data Integration Service on the Process Data Integration Server. These instructions assume that you are an Administrator with full access to the Meridium Process Data Integration server machine.

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.

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.
password	Replace **PaSsWoRd** with the password for the specified user.	You should 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.
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 each 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.

To do so, in each configuration file, complete the following steps for *each* required connection.

Steps

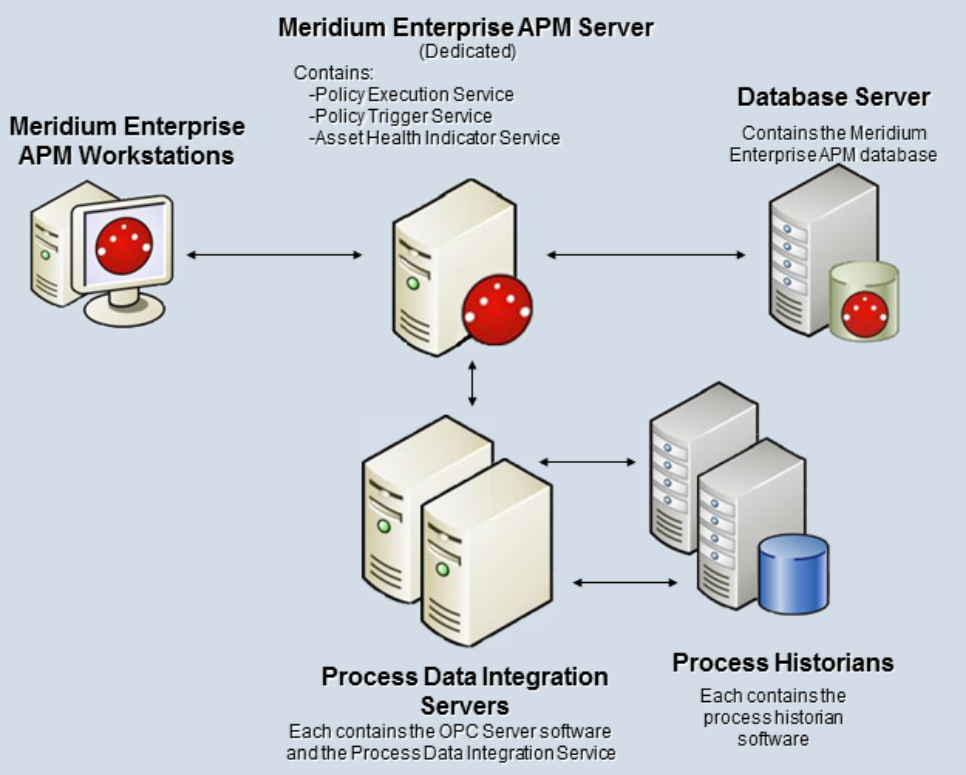
1. Configure the first connection by modifying the attributes within **<meridiumConnections>** tags, as described in the respective service configuration topic:
   - Configure the Policy Execution Service
   - Configure the Policy Trigger Service
   - Configure the Process Data Integration Service
   - Configure the Asset Health Indicator 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.

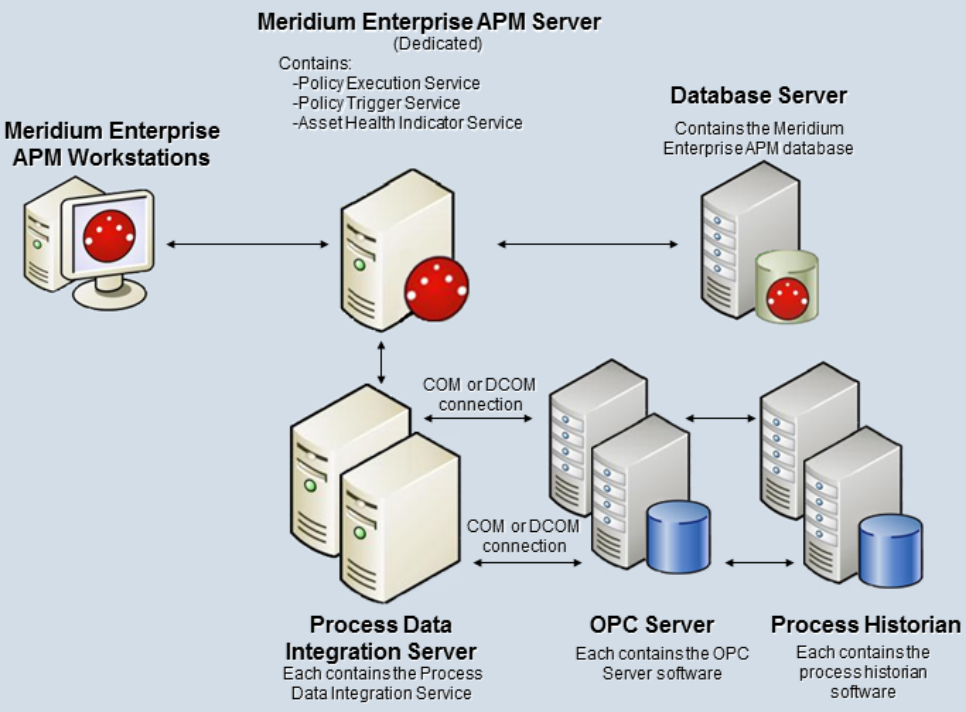
Configure Multiple Process Data Integration and OPC Servers

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" datasource="DATASOURCE_NAME" userId=" SERVICE_USER_NAME" password="!PaSsWoRd" xiServers="OPCSystem1" />`
- On the second Process Data Integration Server: `<connection name="EXAMPLE_CONNECTION" applicationServer="APPSERVER_NAME" datasource="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 that represent the main types of users for this module, as well as the baseline roles assigned to each.

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

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

Deploying 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.

Deploying 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. All steps are required unless otherwise noted.

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. Modify any relationship definitions as needed via Configuration Manager.	This task is required 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 PLA Security Groups.	This task is required. Users must have permissions to the PLA families to use the PLA functionality.
3	Change the default currency symbol.	The currency symbol is set by default to $ and displayed in the following places: • Default Margin field on the Production Profile datasheet. • Production Summary tab of the Production Loss Analysis Details page.
4	Define all products.	This task 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 task 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 task is required. For each production unit that you defined in the previous task, you must identify all the products 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.

Step	Task	Notes
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.
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.

Step	Task	Notes
10	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. 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: • Define production event templates. • Link Production Profile records to OPC Tag records.	This task is required if you want to use the integration between PLA and the Process Data Integration feature where Production Event records are created automatically.

Upgrading Production Loss Analysis (PLA) to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

V3.6.0.0.0

Step	Task	Notes
1	Confirm the deployment of the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server.	If you deployed the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server in V3.6.0.0.0, you do not need to configure these again.

V3.5.1

Step	Task	Notes
1	Confirm the deployment of the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server.	If you deployed the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server in V3.5.1, you do not need to configure these again.

V3.5.0 SP1 LP

Step	Task	Notes
1	Confirm the deployment of the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server.	If you deployed the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server in V3.5.0. SP1 LP, you do not need to configure these again.

V3.5.0

Step	Task	Notes
1	Confirm the deployment of the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server.	If you deployed the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server in V3.5.0, you do not need to configure these again.

V3.4.5

Step	Task	Notes
1	Define OEE codes.	You can use the baseline OEE Code records that are provided in the Meridium Enterprise APM database. If you do not want to use the OEE Code records that are provided, 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.
2	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. If you want to map different or additional PLA values, you can do so by modifying the All Production Data query.
3	Confirm the deployment of the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server.	If you deployed the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server in V3.4.5, you do not need to configure these again.

Production Loss Analysis Security Groups and Roles

The following table lists the baseline Security Groups that represent the main types of users for this module, as well as the baseline roles assigned to each.

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 following table lists the default privileges that members of each group have to the PLA entity and relationship families.

Family	MI Production Loss Accounting Administrator	MI Production Loss Account-ing Manager	MI Production Loss Account-ing Service	MI Pro-duction Loss Accounting User
Entity Families				
Equipment	View, Update, Insert, Delete	View	View	View
Functional Loca-tion	View	View	View	View
Impact Code	View, Update, Insert, Delete	View	View	View
Interface Log	View, Update, Insert, Delete	View	View	View
OEE Code	View, Update, Insert, Delete	View	View	View
Product	View, Update, Insert, Delete	View	View	View
Production Ana-lysis	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
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
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

Family	MI Production Loss Accounting Administrator	MI Production Loss Account-ing Manager	MI Production Loss Account-ing Service	MI Pro-duction Loss Accounting User
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
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

Family	MI Production Loss Accounting Administrator	MI Production Loss Accounting Manager	MI Production Loss Accounting Service	MI Production Loss Accounting User
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

Deploying 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.

Deploying 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. All steps are required unless otherwise noted.

Step	Task	Required?	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.	N	Required if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to the Recommendation Management Security Group via the Configuration Manager.	Y	None
3	Modify the asset queries used by Recommendation Management.	N	Required if you store equipment and location information in families other than the baseline Equipment and Functional Location families.

Upgrading Recommendation Management to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

V3.6.0.0.0

Recommendation Management will be upgraded from V3.6.0.0.0 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.1

Recommendation Management will be upgraded from V3.5.1 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0 SP1 LP

Recommendation Management will be upgraded from V3.5.0 SP1 LP to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0

Recommendation Management will be upgraded from V3.5.0 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.4.5

Recommendation Management will be upgraded from V3.4.5 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Recommendation Management Security Groups

One baseline Security Group is provided for Recommendation Management: MI Recommendation Management User. The following table lists the baseline privileges that are granted to this Security Group.

Entity Families

Family	Privileges
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

Family	Privileges
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 RMC FMEA Recommendation	View, Update, Insert, Delete
Has Strategy	View, Update, Insert, Delete
Has Superseded Recommendations	View, Update, Insert, Delete

Family	Privileges
Is RCM FMEA Asset	View, Update, Insert, Delete
Production Event Has RCA Analysis	View
RCA Analysis Relationships	View

About Asset Queries

To identify the Equipment or Functional Location record that will be used to complete an operation, the Meridium Enterprise APM system runs the following queries, which are stored in the Catalog folder **\\Public\Meridium\Modules\Core\Queries:**

- **Equipment Asset Query**: After providing a prompt for an Entity Key, the Equipment Asset Query returns the record with the provided Entity Key. In the baseline Meridium Enterprise APM database, the query returns records in the Equipment family.
- **Location Asset Query**: After providing a prompt for an Entity Key, the Location Asset Query returns the record with the provided Entity Key. In the baseline Meridium Enterprise APM database, the query returns records in the Functional Location family.

The Equipment Asset Query is always run first. If it returns a record, that record is assumed to be the correct predecessor record, and the Location Asset Query is not run. This means that if a Recommendation record is linked to an Equipment record and a Functional Location record, the Equipment record will always be assumed to be the correct predecessor record.

You will need to modify the baseline queries only if your Recommendation records are linked to records in a family other than the Equipment family or the Functional Location family. When you modify the queries, keep in mind that they must contain the Entity Key field from the source family whose records you want to return. A prompt must exist on the Entity Key field, but the prompt can be a simple prompt with no valid values.

Both of these queries should query at the highest level necessary to include all equipment or location subfamilies. This means that if all of your customer-defined equipment and location families are structured in a hierarchy under a single parent family, such as Asset, you should modify only the Equipment Asset Query to include this parent family. In this case, the Location Asset Query will never be run because all customer-defined equipment and location records will be returned by the Equipment Asset Query.

When These Queries are Run

The Equipment Asset Query and Location Asset Query are not meant to be run on their own. Instead, the Meridium Enterprise APM system runs these queries when you promote a Recommendation record to an Action record.

When these queries are run, the Meridium Enterprise APM system supplies the prompt with the Entity Keys of the predecessor records that are linked to the selected Recommendation record using the following workflow.

- The Meridium Enterprise APM system first runs the Equipment Asset Query. If any of the predecessor Entity Keys identify a record that belongs to the Equipment Asset Query's source family, the Asset Strategy record will be linked to the record that is returned by the query.
- If none of the predecessor Entity Keys identify a record that belongs to the Equipment Asset Query's source family, the Meridium Enterprise APM system runs the Location

Asset Query. If any of the Entity Keys identify a record that belongs to this query source's family, the Asset Strategy record will be linked to the record that is returned by this query.

- If none of the predecessor Entity Keys identify a record that belongs to the Location Asset Query's source family, the Recommendation record will be promoted to an Action record, but the Asset Strategy will not be linked to an Equipment or Functional Location record.

Example: Asset Query

Suppose a Recommendation record is linked to the Equipment record HX-112 and the RBI Criticality Analysis record Analysis 101. If you promote that Recommendation record to an Action record, the Meridium Enterprise APM system will:

- Identify the Entity Key of the Equipment record HX-112 and the RBI Criticality Analysis record Analysis 101.
- Supply these Entity Keys to the prompt in the Equipment Asset Query.
- Identify the record that is returned by the query. Because the source family is the Equipment family, the Equipment record HX-112 will be returned by the query.
- Link the new Asset Strategy record to the Equipment record HX-112.

Deploying 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.

Deploying 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. All steps are required unless otherwise noted.

Step	Task	Required?	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. Modify any relationship definitions as required.	N	Required 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.	Y	Users will not be able to access Reliability Analytics unless they have permissions to the Reliability Analytics families.

Upgrading Reliability Analytics to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

V3.6.0.0.0

Reliability Analytics will be upgraded from V3.6.0.0 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.1

Reliability Analytics will be upgraded from V3.5.1 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0 SP1 LP

Reliability Analytics will be upgraded from V3.5.0 SP1 LP to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0

Reliability Analytics will be upgraded from V3.5.0 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.4.5

Step	Task	Required?	Notes
1	Configure the ability for users to create Reliability Distribution and Reliability Growth Analyses from Associated Pages.	N	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 task, however, only if you want to implement this functionality.

Reliability Analytics Security Groups

The following Security Groups are provided for Reliability Analytics:

- MI Reliability Viewer
- MI Reliability User
- MI Reliability Administrator

These Security Groups are provided as part of the baseline Meridium Enterprise APM database. In addition to assigning Security Users to the appropriate Security Group, you must assign the appropriate family privileges to any Security User or Security Group who should be able to perform Reliability Analytics tasks. Specifically, you must set family privileges for any custom-defined families that will be used in Reliability Analytics.

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

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

Family	MI Reliability Viewer	MI Reliability User	MI Reliability Administrator
Reliability Recommendation	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Spare	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Spares Analysis	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Spare Analysis Chart	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Spare Application	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Spare Application Population	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Action	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Action Mapping	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Action Optimization	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Action Result	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Analysis	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Asset	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Buffer	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Condition Monitor	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Element	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Element Result	View	View, Update, Insert, Delete	View, Update, Insert, Delete

Family	MI Reliability Viewer	MI Reliability User	MI Reliability Administrator
System Global Event	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Inspection	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Link	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Preventative Maintenance	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Resource	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Resource Result	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Resource Usage	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Risk	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Risk Assessment	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Scenario	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Sensor	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Special Action	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Subsystem	View	View, Update, Insert, Delete	View, Update, Insert, Delete
System Switch	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Weibull	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Analysis Link	View	View, Update, Insert, Delete	View, Update, Insert, Delete

Family	MI Reliability Viewer	MI Reliability User	MI Reliability Administrator
Has Global Events	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Mitigated TTF Distribution	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Planned Resource Usages	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Consolidated Recommendations	View	View	View
Has Recommendations	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Reliability	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Resource Usage	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Risk Assessments	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Root System	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Scenarios	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has System Actions	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has System Elements	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has System Optimization	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has System Resources	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has System Results	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has System Risks	View	View, Update, Insert, Delete	View, Update, Insert, Delete

Family	MI Reliability Viewer	MI Reliability User	MI Reliability Administrator
Has TTF Distribution	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Unplanned Resource Usages	View	View, Update, Insert, Delete	View, Update, Insert, Delete

Deploying 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.

Deploying 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. All steps are required unless otherwise noted.

Step	Task	Required/Optional	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.	Optional	This task is necessary only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign users to one or more of the Strategy Security Roles via the Security Manager application.	Required	None

Upgrading Reliability Centered Maintenance (RCM) to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

V3.6.0.0.0

RCM will be upgraded from V3.6.0.0.0 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.1

RCM will be upgraded from V3.5.1 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0 SP1 LP

RCM will be upgraded from V3.5.0 SP1 LP to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0

RCM will be upgraded from V3.5.0 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.4.5

Step	Task	Required?	Notes
1	Assign Security Users to the MI RCM Viewer Security Group.	Y	None
2	Add values to the Recommended Resource System Code Table.	Y	This System Code Table is used to populate the Recommended Resource field in RCM FMEA Recommendation records.

Reliability Centered Maintenance (RCM) Security Groups

The following table lists the baseline Security Groups that represent the main types of users for this module, as well as the baseline roles assigned to each.

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

MI Strategy User: Users have access to default RCM/FMEA user privileges (view, create, edit), ASI user privileges, and ASM view privileges.

MI Strategy Power: Users have Strategy_Users access, plus ASM reviewer privileges (manage strategies, actions, tasks, and risks).

MI Strategy Admin: Users have Strategy_PowerUsers accesss, plus RCM/FMEA administrator privileges (configuring and maintaining), ASI administrator privileges, and ASM management administrator privileges.

Associating RCM Analyses with a Specific Site

Some companies that use the Meridium Enterprise APM software have facilities at multiple sites, or locations, where each site contains unique equipment and locations. If desired, you can define the sites in your organization and associate equipment and locations with the site to which they belong. When you create RCM Analyses for those pieces of equipment and locations, you will need to select the appropriate site on the Analysis datasheet of the RCM Analysis.

To help streamline the analysis-creation process, after you select a site on the Analysis datasheet, the Meridium Enterprise APM system will allow you to add Equipment and Functional Location records to the RCM Analysis only if those pieces of equipment and locations belong to that site.

You can also associate Risk Matrices with specific sites. If a Risk Matrix is associated with a site and an RCM Analysis is associated with the same site, when you define the unmitigated risk for a failure effect, rather than seeing the default Risk Matrix, you will see the Risk Matrix that is associated with that site.

RCM Security Groups

The RCM module uses the following baseline Security Groups:

- **MI RCM Administrator:** The MI RCM Administrator Security Group has *no* family-level privileges configured for it in the baseline Meridium Enterprise APM database. Users who are members of this group will see the **Administration** link on the **RCM Start Page** in the Meridium Enterprise APM Framework application and will, therefore, have access to administrative functions in RCM. Users who do not belong to this Security Group will not see this link and, therefore, will not be able to access the administrative functions.
- Because the MI RCM Administrator Security Group has *no* family-level privileges assigned to it by default, to access features and functions in RCM, members of the MI RCM Administrator Security Group will also need to be assigned to the MI RCM User or MI RCM Viewer Security Group.
- **MI RCM User:** The MI RCM User Security Group has access to *all* features in RCM.
- **MI RCM Viewer:** The MI RCM Viewer Security Group has view-only access to RCM. Users belonging to the MI RCM Viewer Security Group will not have access to features that result in the creation, update, or deletion of records or links between records.

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

Family Caption	MI RCM User	MI RCM Viewer
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		

Family Caption	MI RCM User	MI RCM Viewer
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

Family Caption	MI RCM User	MI RCM Viewer
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 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.

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.

Deploying 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. All steps are required unless otherwise noted.

Step	Task	Required/Optional	Notes
1	Install the Reports Designer.	Required	None
2	Set Up the Reports Designer.	Required	None

Install the APM Reports Designer

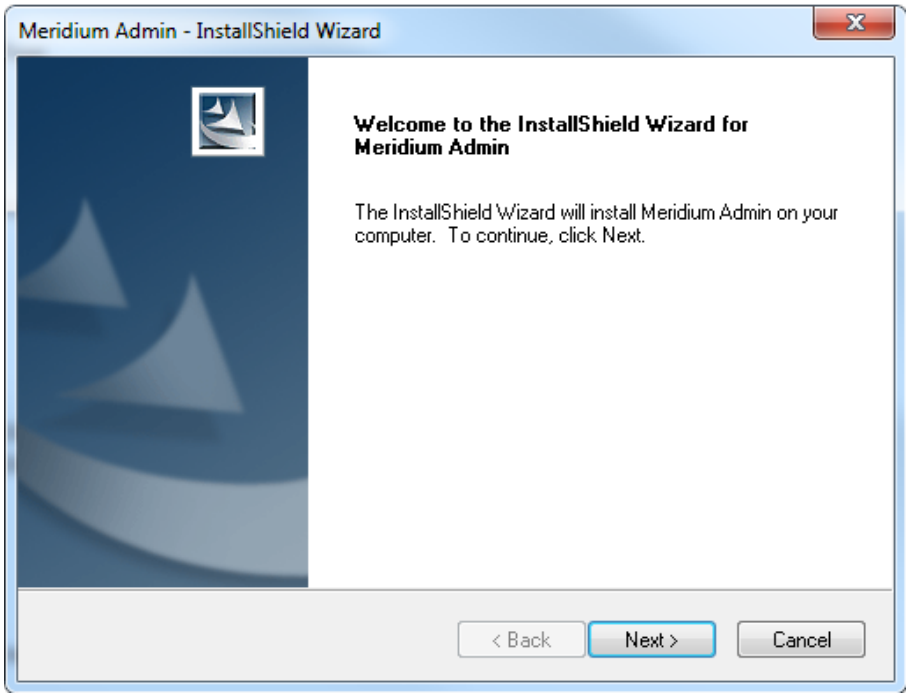
Before You Begin

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

Steps

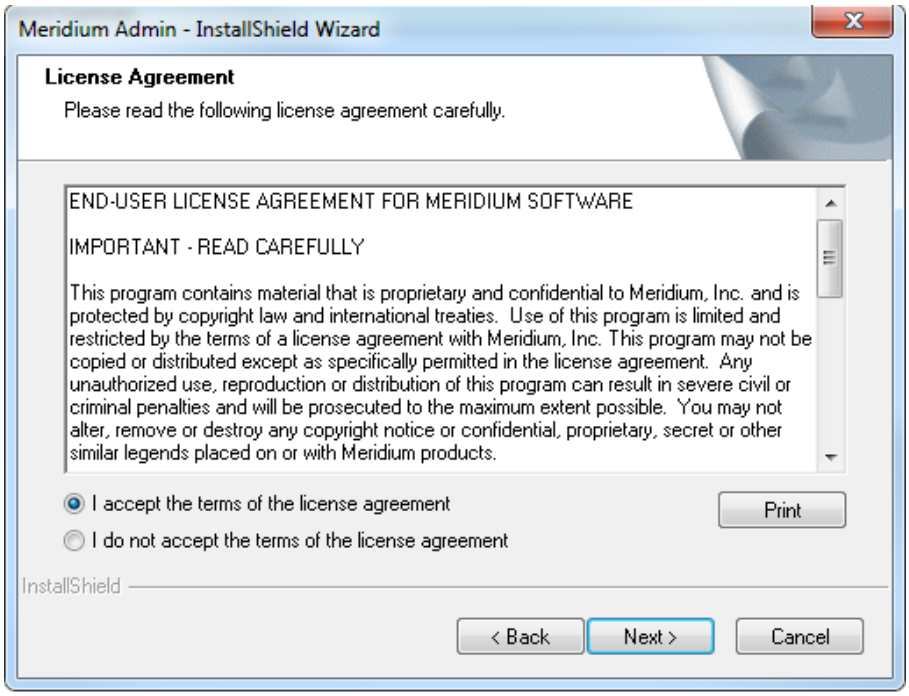
1. On the machine that will serve as the APM Reports Designer, access the Meridium APM Enterprise APM Distribution package, and navigate to the **Admin** folder.
2. Double-click the file **Setup.exe**.

   The **Meridium Admin - InstallShield Wizard** appears.



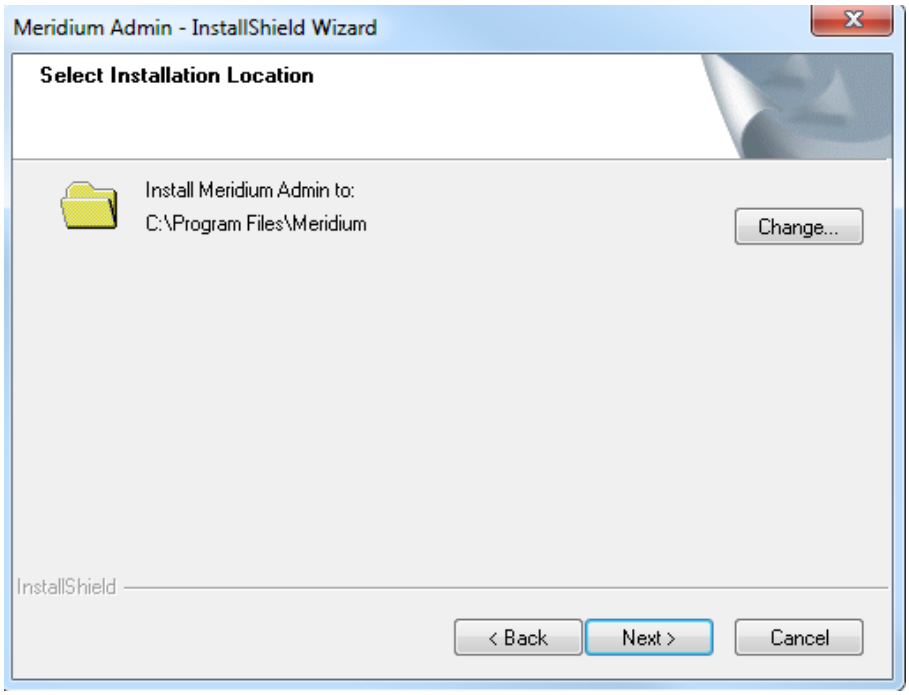
3. Select **Next**.

   The **License Agreement** screen appears.



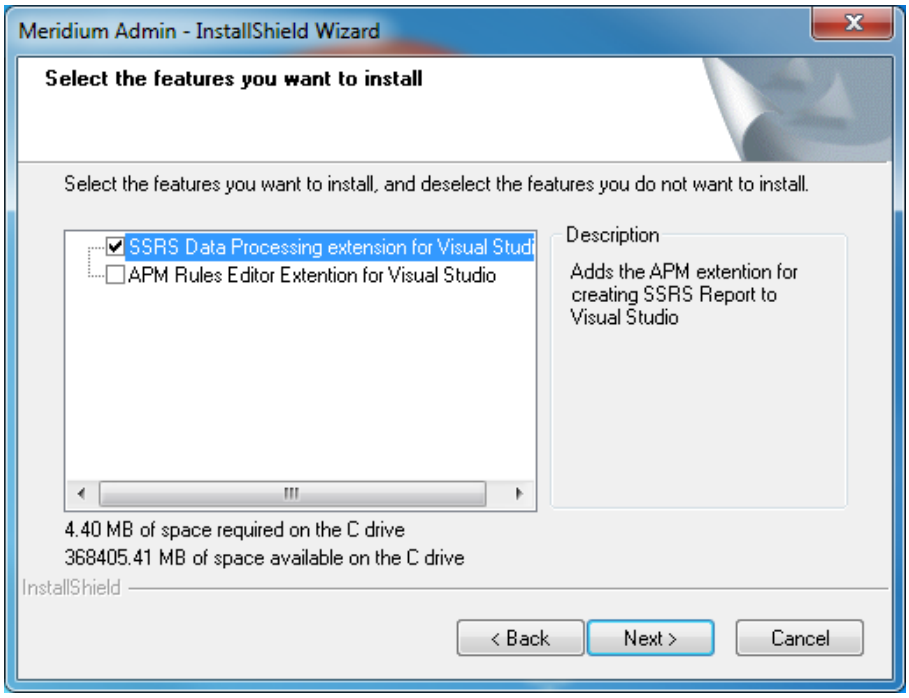
4. Read the License Agreement and, if you agree, select the **I accept the terms of the license agreement** check box. Then, select **Next**.

   The **Select Installation Location** screen appears.



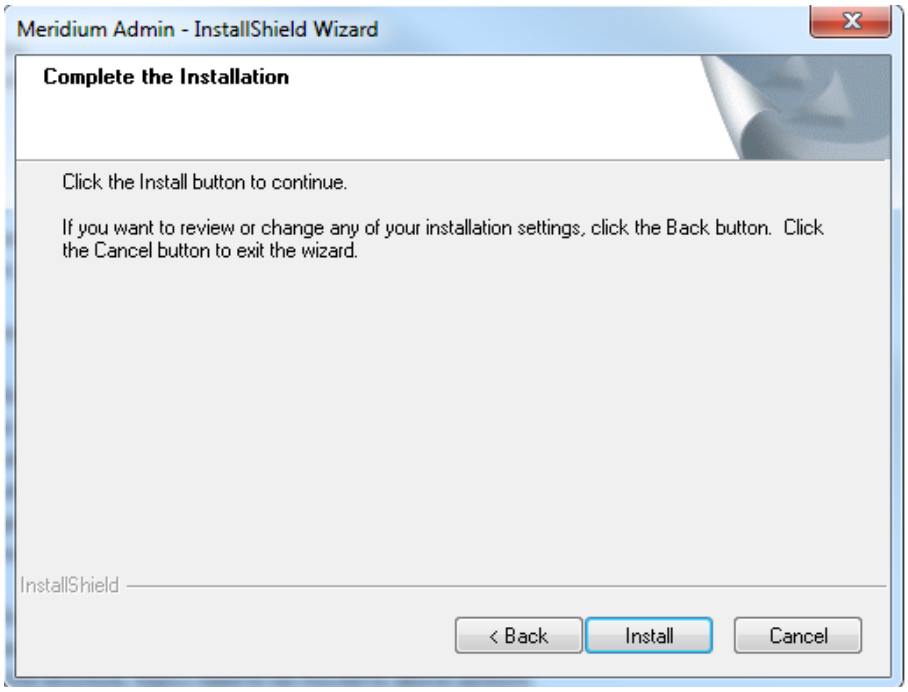
5. Select **Next** to accept the default location.

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



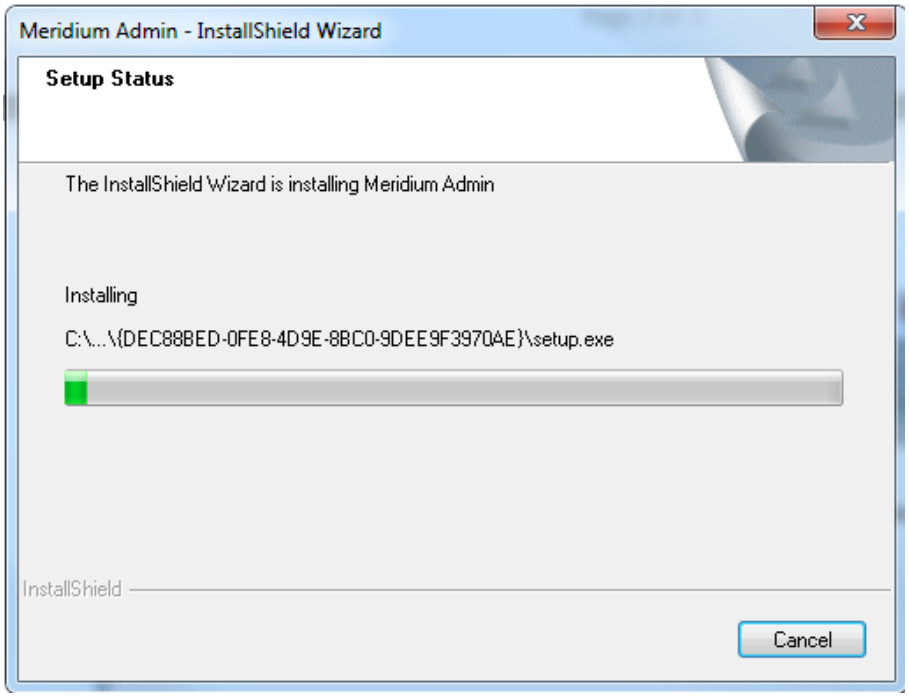
6. Select **SSRS Data Processing Extension for Visual Studio**, and then select **Next**.

   The **Complete the Installation** screen appears.

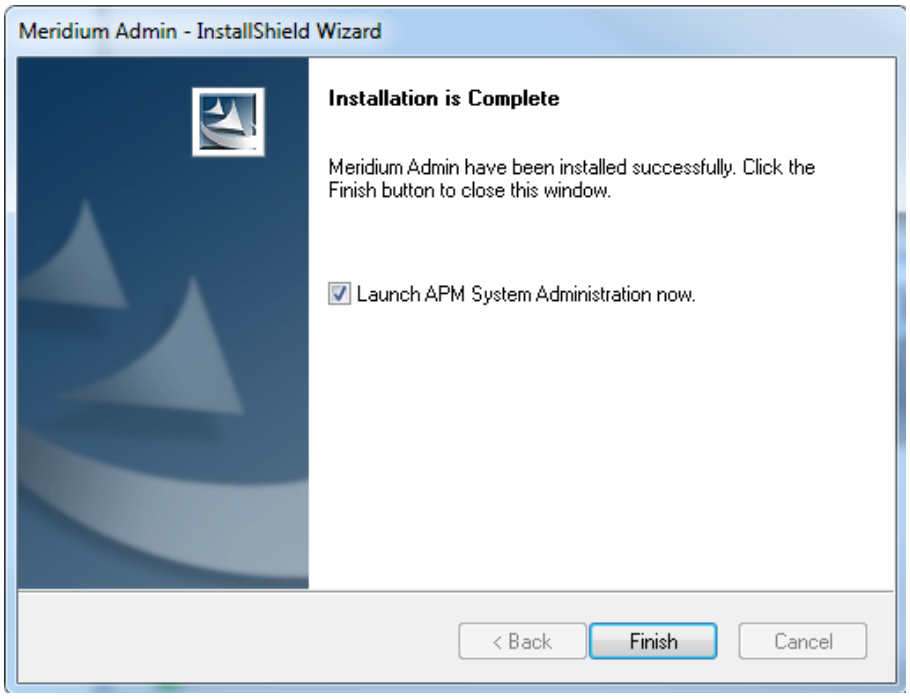


7. Select **Install**.

   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 Meridium Admin is installed successfully. Optionally, you can select to launch the APM System Administration tool when the installer window closes.

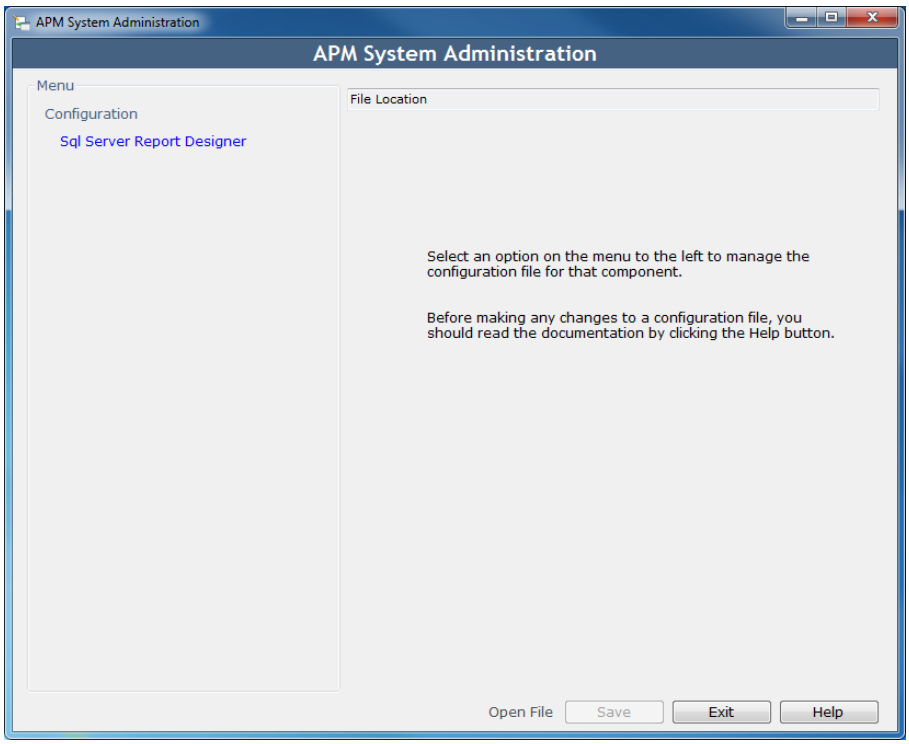


8. Clear the **Launch APM System Administration now** box, and then select **Finish**.



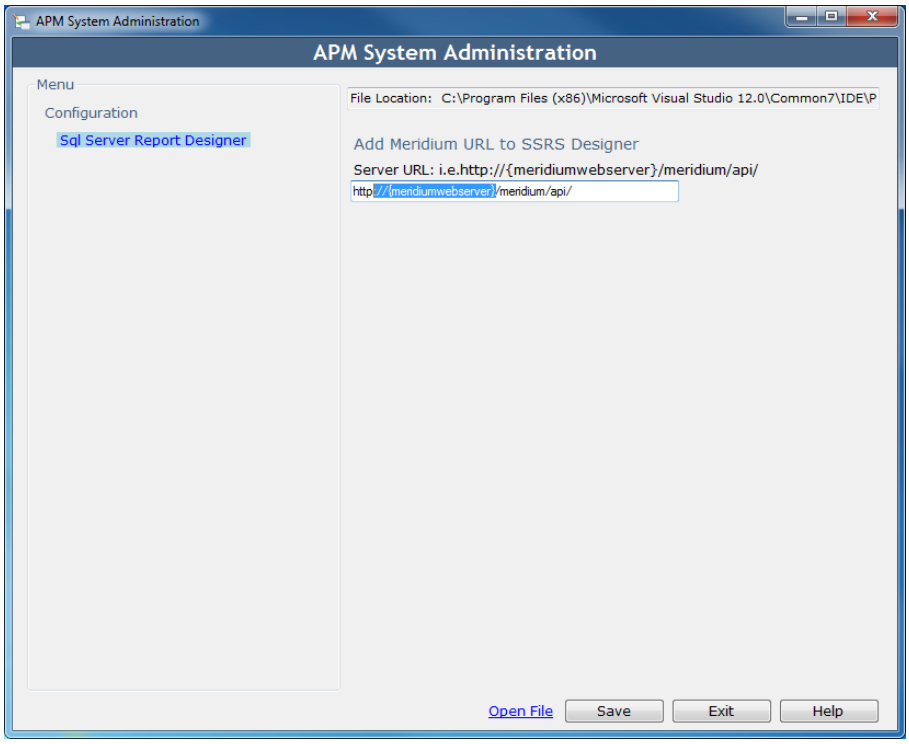
Note: You may be asked to restart your system for the changes to take effect.

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.

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.

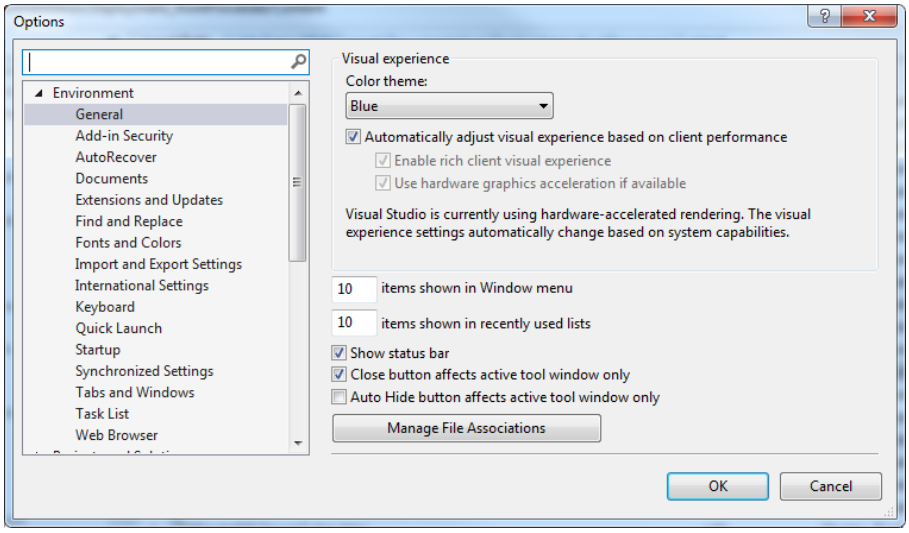
Before You Begin

- Install the APM Report Designer.

Steps

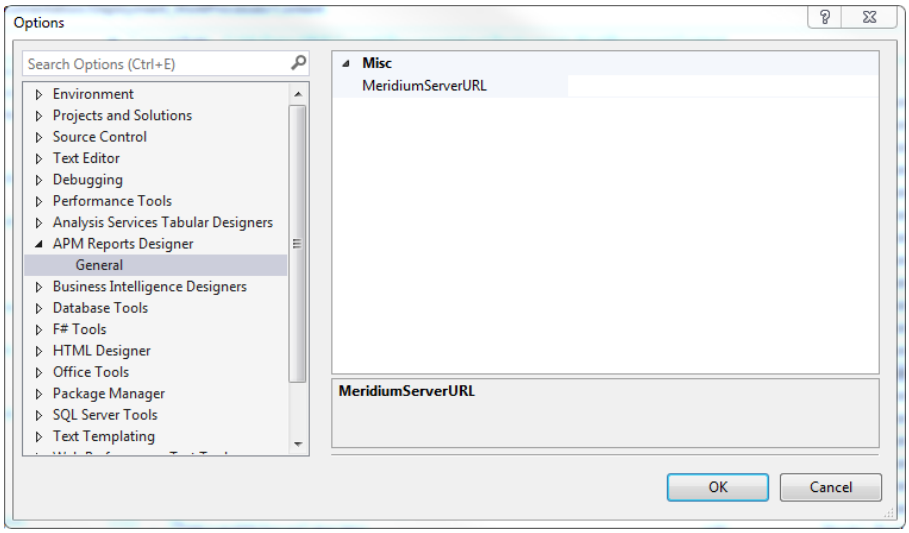
1. On the Meridium Enterprise APM Server, open Microsoft Visual Studio.
2. On the **Tools** menu, select **Options**.

   The **Options** window appears.



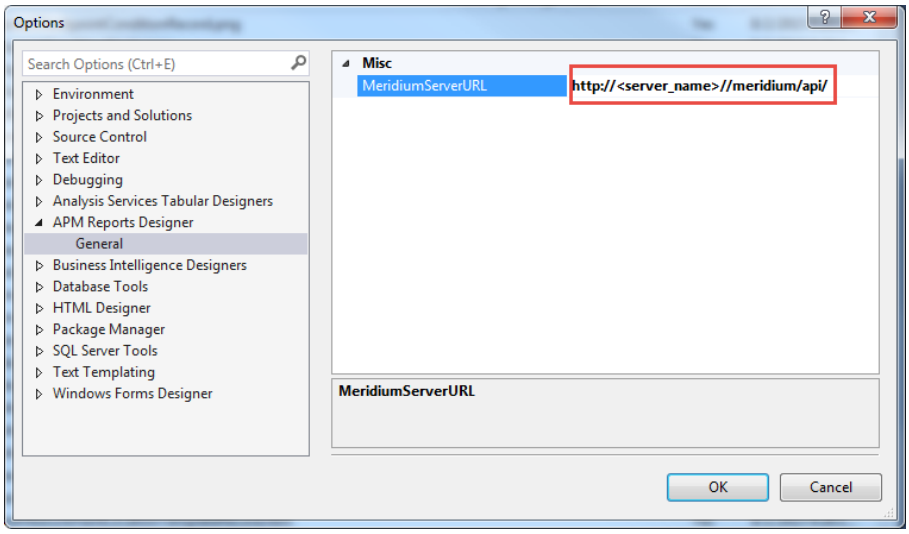
3. On the **Options** window, in the left section, select **APM Report Designer**, and then select **General**.

   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.

Deploying 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.

Deploying 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. All steps are required unless otherwise noted.

Step	Task	Required?	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. .	N	Required 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.	Y	Users will need permissions to the RBI families in order to use the RBI functionality.
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 corrosion rates. • Users who should be able to navigate to TM via RBI.	N	Required if you are using the integration between the RBI and TM modules.
4	If you plan to create your own Potential Degradation Mechanisms records, modify the MI_DEGRADATION_MECHANISM_TYPES System Code Table by adding the desired System Code values.	N	

Step	Task	Required?	Notes
5	Modify the *Recommendation Creation Enabled* setting in the RBI **Global Preferences** workspace.	N	This setting is enabled by default. This task is necessary only if you want to disable this setting because you use the Asset Strategy Management (ASM) module to recommend actions and manage mitigated risk.
6	Modify the *Enable Recommendations to be Generated at Created State* setting in the RBI **Global Preferences** workspace.	N	This setting is disabled by default. This task is necessary only if you want to create RBI Recommendation records while RBI Criticality Analysis records are in the *Created* state.
7	Modify the *Allow Override of Calculated Unmitigated Risk Values* setting in the RBI **Global Preferences** workspace.	N	This setting is disabled by default. This task is necessary only if you want to want to enable this setting because you use a custom calculator.
8	Modify the *Consider Half-Life when Determining Inspection Task Interval* setting in the RBI **Global Preferences** workspace.	None	This setting is disabled by default. If you are following the Meridium Enterprise APM RBI Best Practice, you should enable this setting so that additional values will be considered when determining the Desired Interval value in certain Inspection Task records.
9	Select the **Is a Unit?** check box in Functional Location records that represent units in your facility.	Y	This field is used throughout RBI to distinguish these Functional Location records from those that represent other levels in the location hierarchy.
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 field **Is a Unit?** contains the value True).	Y	
11	Configure the Meridium Enterprise APM system to generate RBI Recommendation records automatically.	N	You can complete this task only if certain conditions exist.

Step	Task	Required?	Notes
12	Create Potential Degradation Mechanisms records.	N	Required if you want to use additional Potential Degradation Mechanism records that are not provided in the baseline Meridium Enterprise APM database.
13	Assign a ranking to all Potential Degradation Mechanisms records.	N	Required if you want the Probability Category field in certain Criticality Degradation Mech Evaluation records to be populated automatically based upon this ranking.

Upgrading Risk Based Inspection (RBI) to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

V3.6.0.0.0

Step	Task	Required?	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.	N	Required if you use Policy records to generate RBI Recommendation records.

V3.5.1

Step	Task	Required?	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_B; Appendix D; Appendix E; Appendix F; Appendix G; Appendix H; Appendix I; PRD Strategies.	N	Required if you use Policy records to generate RBI Recommendation records.
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 this location. The file is imported, and the associated Inspection Strategy records are created, replacing the previous ones.	Y	

V3.5.0 SP1 LP

Step	Task	Required?	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_B; Appendix D; Appendix E; Appendix F; Appendix G; Appendix H; Appendix I; PRD Strategies.	N	Required if you use Policy records to generate RBI Recommendation records.
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 this location. The file is imported, and the associated Inspection Strategy records are created, replacing the previous ones.	Y	
3	Import Policy records that are new to V3.5.1. The XML files that you will need to import are: Int Corrosion Insp Grouping Policy.xml; CUI Insp Grouping Policy.xml.	N	Required if you want to use Inspection Grouping functionality.
4	In Functional Location records that represent units in your facility, select the **Is a Unit?** check box.	Y	This step will ensure that queries used by RBI modules function correctly when returning results.

Step	Task	Required?	Notes
5	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*).	Y	
6	Modify the *Enable Recommendations to be Generated at Created State* setting on the **Global Preferences workspace.**	N	This setting is disabled by default. This task is necessary only if you want to create RBI Recommendation records while RBI Criticality Analysis records are in the *Created* state.

V3.5.0

Step	Task	Required?	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_B; Appendix D; Appendix E; Appendix F; Appendix G; Appendix H; Appendix I; PRD Strategies.	N	Required if you use Policy records to generate RBI Recommendation records.

Step	Task	Required?	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 this location. The file is imported, and the associated Inspection Strategy records are created, replacing the previous ones.	Y	
3	Import Policy records that are new to V3.5.1. The XML files that you will need to import are: Int Corrosion Insp Grouping Policy.xml; CUI Insp Grouping Policy.xml.	N	Required if you want to use Inspection Grouping functionality.
4	In Functional Location records that represent units in your facility, select the **Is a Unit?** check box.	Y	This step will ensure that queries used by RBI modules function correctly when returning results.
5	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*).	Y	

Step	Task	Required?	Notes
6	Modify the *Enable Recommendations to be Generated at Created State* setting on the **Global Preferences workspace.**	N	This setting is disabled by default. This task is necessary only if you want to create RBI Recommendation records while RBI Criticality Analysis records are in the *Created* state.

V3.4.5

Step	Task	Required?	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_B; Appendix D; Appendix E; Appendix F; Appendix G; Appendix H; Appendix I; PRD Strategies.	N	Required if you use Policy records to generate RBI Recommendation records.
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 this location. The file is imported, and the associated Inspection Strategy records are created, replacing the previous ones.	Y	

Step	Task	Required?	Notes
3	Import Policy records that are new to V3.5.1. The XML files that you will need to import are: Int Corrosion Insp Grouping Policy.xml; CUI Insp Grouping Policy.xml.	N	Required if you want to use Inspection Grouping functionality.
4	In Functional Location records that represent units in your facility, select the **Is a Unit?** check box.	Y	This step will ensure that queries used by RBI modules function correctly when returning results.
5	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*).	Y	
6	Modify the *Enable Recommendations to be Generated at Created State* setting on the **Global Preferences workspace.**	N	This setting is disabled by default. This task is necessary only if you want to create RBI Recommendation records while RBI Criticality Analysis records are in the *Created* state.

Risk Based Inspection Security Groups

The following table lists the baseline Security Groups that represent the main types of users for this module, as well as the baseline roles assigned to each.

Security Group	Roles
MI RBI Administrator	MI RBI Admin
MI RBI Analyst	MI RBI Power MI RBI Admin

The baseline family-level privileges that exist for these 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, Update, Insert, Delete
Corrosion	View	View
Corrosion Analysis Settings	View	View
Criticality Consequence Evaluation	View, Update, Insert, Delete	View, Update, Insert, Delete
Criticality Other Damage Mech. Eval.	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 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

Family	MI RBI Administrator	MI RBI Analyst
Criticality RBI Component - Exchanger Header	View, Update, Insert, Delete	View, Update, Insert, Delete
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

Family	MI RBI Administrator	MI RBI Analyst
RBI Degradation Mechanisms	View, Update, Insert, Delete	View, Update, Insert, Delete
RBI Recommendation	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
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

Family	MI RBI Administrator	MI RBI Analyst
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
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 Degradation Mechanisms Evaluation	View, Update, Insert, Delete	View, Update, Insert, Delete
Has RBI Strategy Mapping Con-figuration	View, Update, Insert, Delete	View, Update, Insert, Delete
Has RBI Systems	View, Update, Insert, Delete	View, Update, Insert, Delete

Family	MI RBI Administrator	MI RBI Analyst
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
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.

Deploying 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.

Deploying 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. All steps are required unless otherwise noted.

Step	Task	Required?	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.	N	Required 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 RCA Security Groups.	Y	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.	N	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.	N	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.	N	Required only if you do not want to use the baseline query, which is defined by default.

Upgrading Root Cause Analysis (RCA) to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

V3.6.0.0.0

RCA will be upgraded from V3.6.0.0 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.1

RCA will be upgraded from V3.5.1 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0 SP1 LP

RCA will be upgraded from V3.5.0 SP1 LP to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0

RCA will be upgraded from V3.5.0 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.4.5

RCA will be upgraded from V3.4.5 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

About RCA Security

To use RCA, a Meridium Enterprise APM Security User must be a Super User or a member of one of the following Security Groups:

- **MI PROACT Administrator:** Allows access to ALL RCA features, including administrative features.
- **MI PROACT Team Member:** Allows access to all RCA features, except the administrative features.
- **MI PROACT Viewer:** Allows view-only access to the RCA module. Members of the MI PROACT Viewer Security Group will be able to view existing analyses but will not be able to create or modify them.

Each of these Security Groups has a set of family-level privileges associated with it, which are needed to provide access to the records used throughout RCA. Access to RCA features, however, is not granted through privileges alone but through *membership in these groups* and the privileges associated with them. Granting RCA family-level privileges at the Security User level or through a custom Security Group will not provide access to RCA.

Throughout the RCA documentation, when we explain how to perform a certain task, we assume that the user is a member of the Security Group that allows access to that task.

Note: In addition to assigning Security Users to these Security Groups, you will need to grant users family-level privileges to any custom family that participates in a relationship with a baseline RCA family.

RCA Security Groups

The following Security Groups are provided for RCA:

- MI PROACT Administrator
- MI PROACT Team Member
- MI PROACT Viewer

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

Note: The access to RCA is not granted through these privileges but through membership in these Security Groups.

Family	MI PROACT Administrator	MI PROACT Team Member	MI PROACT Viewer
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
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 Logic Gate	View, Update, Insert, Delete	View, Update, Insert, Delete	View
RCA Preserve Item	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI PROACT Administrator	MI PROACT Team Member	MI PROACT Viewer
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
RCA Image	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Security User	View	View	View
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

Family	MI PROACT Administrator	MI PROACT Team Member	MI PROACT Viewer
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

Deploying 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.

Deploying 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. All steps are required unless otherwise noted.

Step	Task	Required/Optional	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.	Optional	Required if you have asset data in families outside of the baseline Equipment and Functional Location families.
2	Assign the desired Security Users to the following Security Groups: • MI Operator Rounds Administrator • MI Operator Rounds Mobile User **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.	Required	None
3	Manage Measurement Location Template mappings.	Optional	Required if you added fields to the Measurement Location Template family via Configuration Manager.

Step	Task	Required/Optional	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 • Cardinality: ONE to MANY	Optional	Required if you created an asset family that you want to link to a Measurement Location using the *Has Checkpoint* relationship family.
5	Install the Meridium Enterprise APM application on the mobile device that you plan to use for data collection.	Optional	Required only if you want to use a mobile device for data collection.
6	Set the local time zone on the mobile device that you will use for data collection, typically the user time zone.	Optional	Required if you will use a mobile device for data collection.

Upgrading Rounds to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. 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. All steps are required unless otherwise noted.

Before You Begin

In Meridium Enterprise APM V4.0.1.0, a Measurement Location can be linked to *one* asset. During upgrade from earlier versions to V4.0.1.0, the related asset entity key is added to a field on the Measurement Location family. Hence, if you have Measurement Locations that are linked to more than one asset, then you must remove the linkage to the additional assets prior to the uprgrade.

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 V4.0.1.0:

```
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
```

A list of Measurement Locations that are linked to multiple assets appears, providing the Measurement Location key, Measurement Location ID, and the Asset Key of the assets linked to the Measurement Location.

2. Access each Measurement Location in Record Manager in the current version of Meridium APM.

   The left pane displays the records that are related to the Measurement Location.

3. Unlink the additional assets from the Measurement Location such 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).

V3.6.0.0.0

Step	Task	Required?	Notes
1	Install Meridium Enterprise APM V4.0.1.0 on the mobile device that you will use for data collection.	No	Required 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.	No	Required if you will use a mobile device for data collection.

V3.5.1

Step	Task	Required?	Notes
1	Install Meridium Enterprise APM V4.0.1.0 on the mobile device that you will use for data collection.	No	Required 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.	No	Required if you will use a mobile device for data collection.

V3.5.0 SP1 LP

Step	Task	Required?	Notes
1	Install Meridium Enterprise APM V4.0.1.0 on the mobile device that you will use for data collection.	No	Required if you will use a mobile device for data collection.

Step	Task	Required?	Notes
2	Set the local time zone on the mobile device that you will use for data collection.	No	Required if you will use a mobile device for data collection.

V3.5.0

Step	Task	Required?	Notes
1	Install Meridium Enterprise APM V4.0.1.0 on the mobile device that you will use for data collection.	No	Required 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.	No	Required if you will use a mobile device for data collection.

V3.4.5

Step	Task	Required?	Notes
1	Install Meridium Enterprise APM V4.0.1.0 on the mobile device that you will use for data collection.	No	Required 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.	No	Required if you will use a mobile device for data collection.

Security Groups and Privileges In Rounds

The following table lists the baseline Security Groups that represent the main types of users for this module, as well as the baseline roles assigned to each.

Security Group	Roles
MI Operator Rounds Administrator	MI Health Admin
MI Operator Rounds Mobile User	MI Health Admin MI Health Power MI Health User

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.

Note: 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. However, we recommend that you use the MI Operator Rounds User Security Group instead of the MAPM Security Group.

The following table lists the default privileges that members of each group have to the Rounds entity and relationship families.

Family Entity Families	MI Operator Rounds Administrator	MI Operator Rounds Mobile User	MAPM Security Group
Checkpoint Condition	View, Update, Insert, Delete	View	View
Checkpoint Task	View, Update, Insert, Delete	View, Update	View, Update
Health Indicator	View	View	View
Health Indicator Mapping	View, Update, Insert, Delete	View	View

Family	MI Operator Rounds Administrator	MI Operator Rounds Mobile User	MAPM Security Group
Hierarchy Item Child Definition	View, Update, Insert, Delete	View	View
Hierarchy Item Definition	View, Update, Insert, Delete	View	View
Measurement Location	View, Update, Insert, Delete	View	View
Measurement Location Template	View, Update, Insert, Delete	View	View
Operator Rounds Allowable Values	View, Update, Insert, Delete	View	View
Operator Rounds Recommendation	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Reading	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Reference Document	View, Update, Insert, Delete	View	View
Route	View, Update, Insert, Delete	View, Update	View, Update
Route History	View, Update, Insert, Delete	View, Insert, Update, Delete	View, Insert
Task	None	View, Update	View, Update
Template Group	View, Update, Insert, Delete	View	View
Relationship Families			
Condition Has ML	View, Update, Insert, Delete	View	View
Has Checkpoint	View, Update, Insert, Delete	View	View
Has Checkpoint Template	View, Update, Insert, Delete	View	View

Family	MI Operator Rounds Administrator	MI Operator Rounds Mobile User	MAPM Security Group
Has Health Indicator	View	View	View
Has History	View, Update, Insert, Delete	View, Insert, Delete	View, Insert
Has Readings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Recommendations	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Reference Documents	View, Update, Insert, Delete	View	View
Has Route	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Has Tasks	View, Update, Insert, Delete	View	View
Health Indicator Has Mapping	View, Update, Insert, Delete	View	View
Health Indicator Has Source	View	View	View
ML Has Condition	View, Update, Insert, Delete	View	View
ML Has OPR Recommendation	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete
Route Has Checkpoint	View, Update, Insert, Delete	View	View
Route Has Human Resource	View, Update, Insert, Delete	Insert	Insert
Template Has Checkpoint	View, Update, Insert, Delete	View	View

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.

Deploying 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

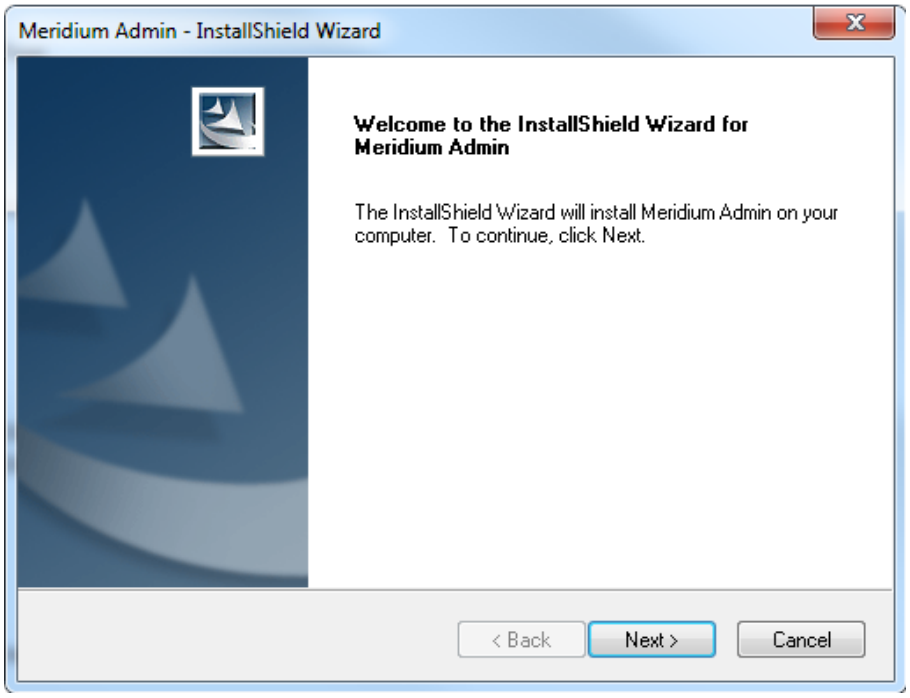
Before You Begin

- Microsoft Visual Studio 2012 or 2013 Professional must be installed on every workstation where you want to work with Meridium rules in the Meridium Enterprise APM system.
- MSXML must also be installed on these workstations.
- You must be logged in as the administrator for the system.

Steps

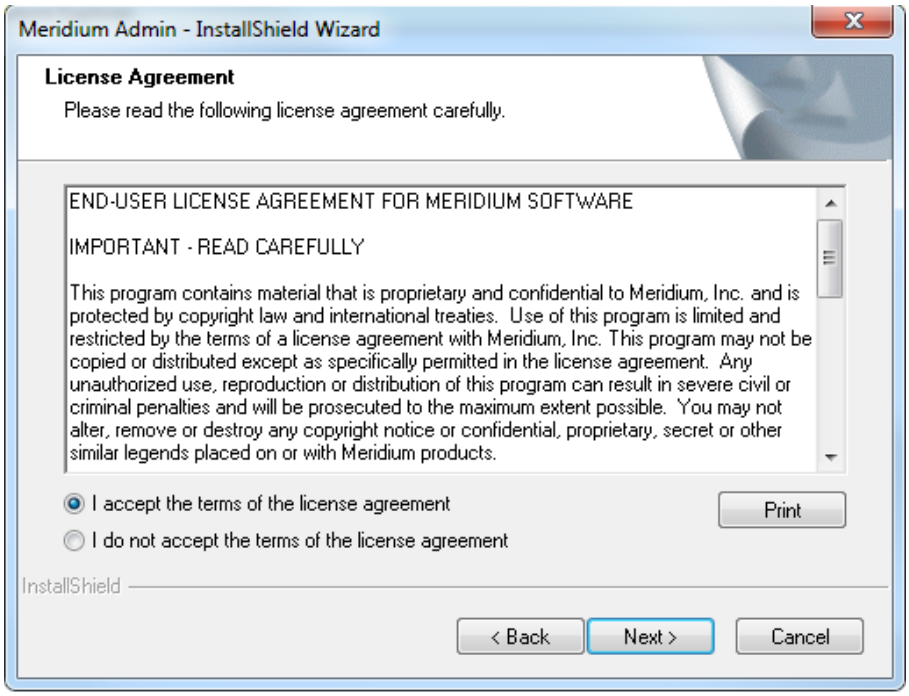
1. On the machine that will serve as the Meridium rules editor, insert the Meridium Enterprise APM Framework and Server Setup DVD, and navigate to the **Admin** folder.
2. Double-click the file **Setup.exe**.

   The **Meridium Admin - InstallShield Wizard** screen appears.



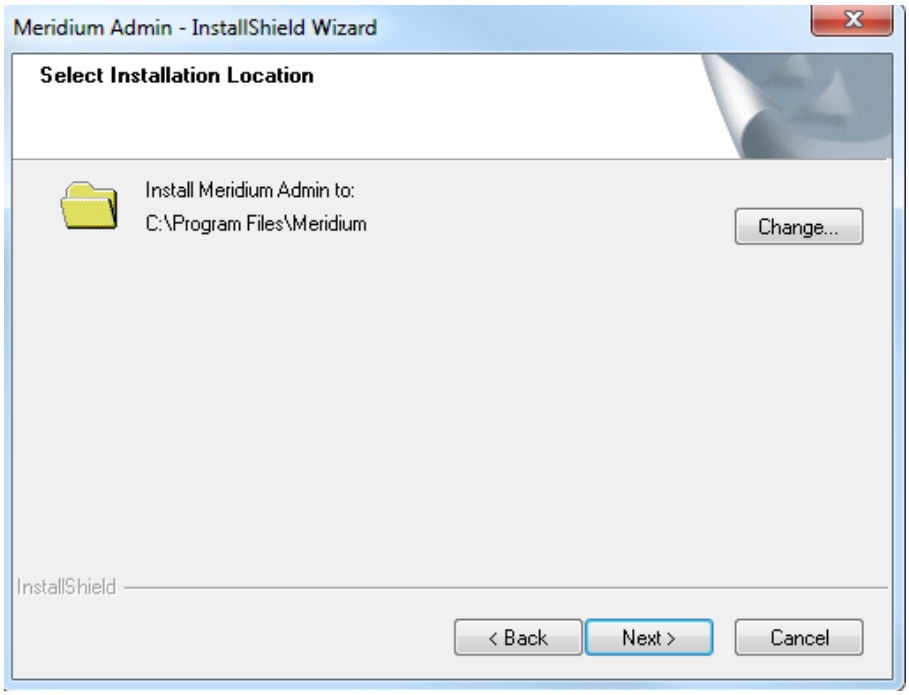
3. Select **Next**.

   The **License Agreement** screen appears.



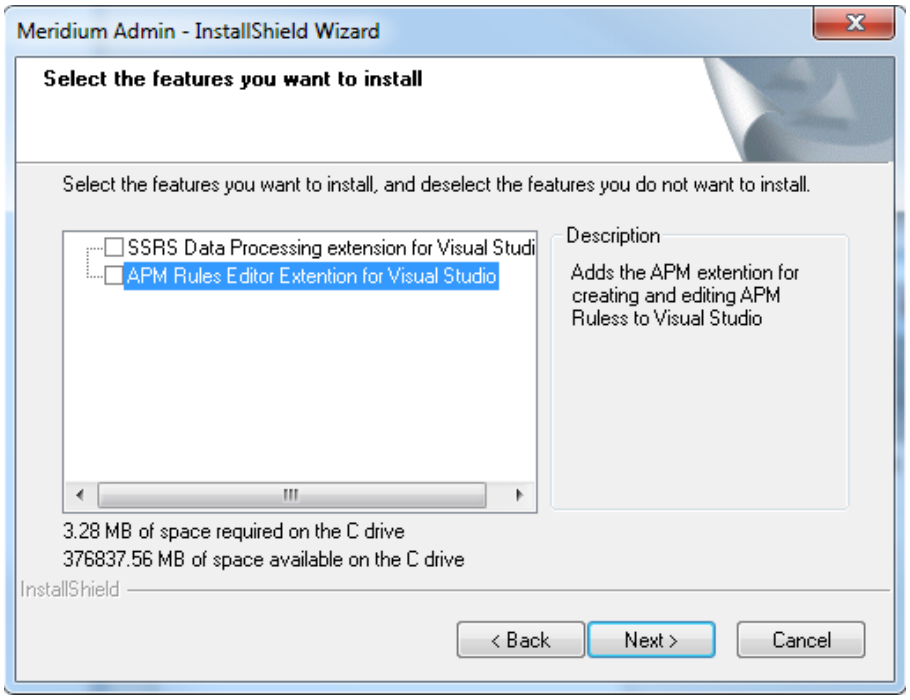
4. Read the License Agreement and, if you agree, select the **I accept the terms of the license agreement** option. Then, select **Next** button.

   The **Select Installation Location** screen appears.



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

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

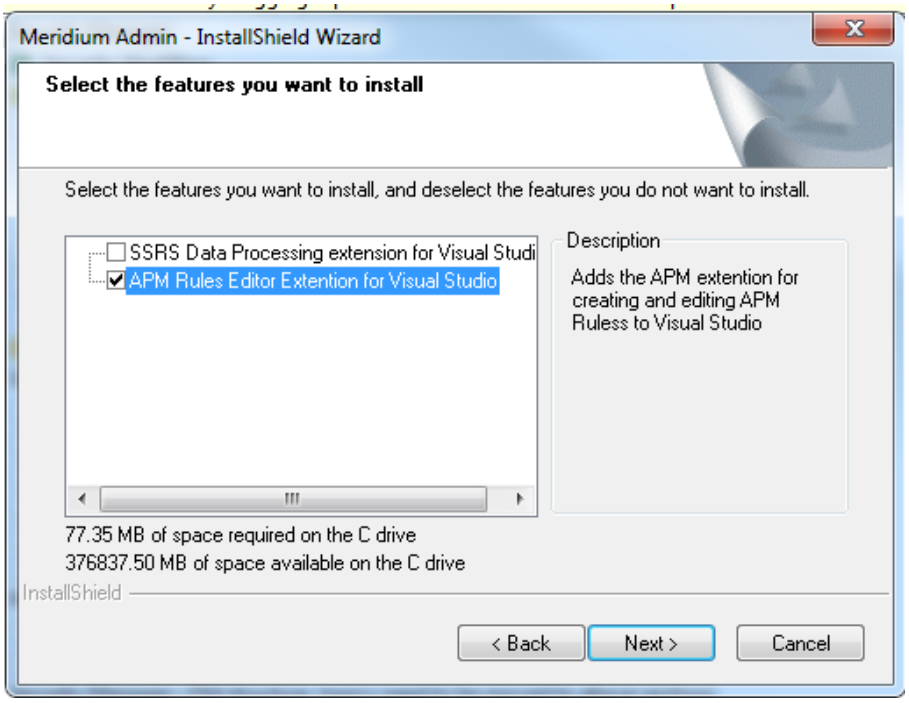


6. Select the **APM Rules Editor Extension for Visual Studio** option.

   Note: There are additional options available for selection. You may select these options depending on the requirement.

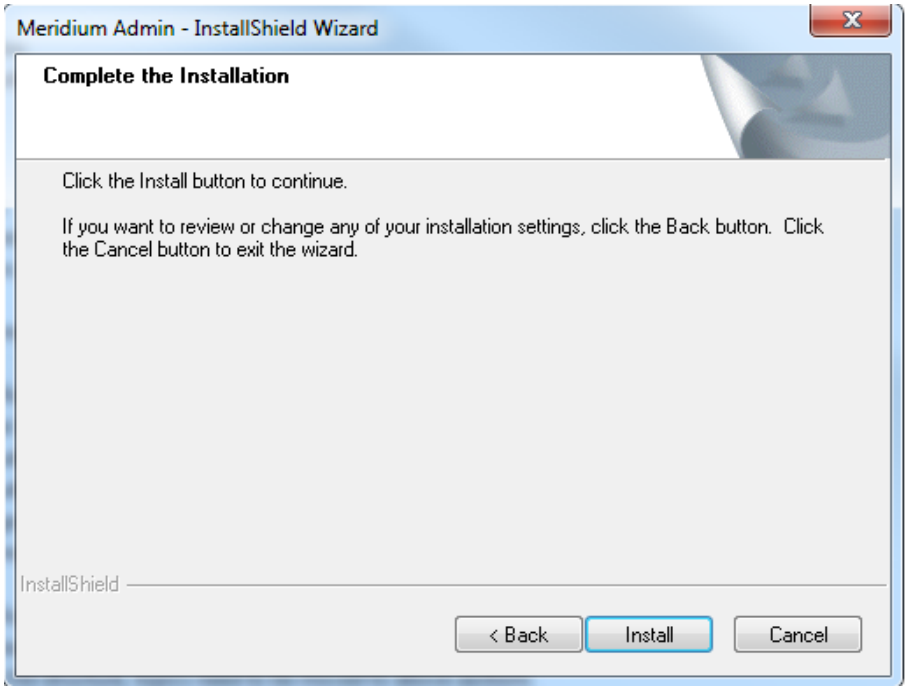
   Meridium Enterprise APM performs a check to make sure that your machine contains the required prerequisites for the features that you want to install.

   - 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.



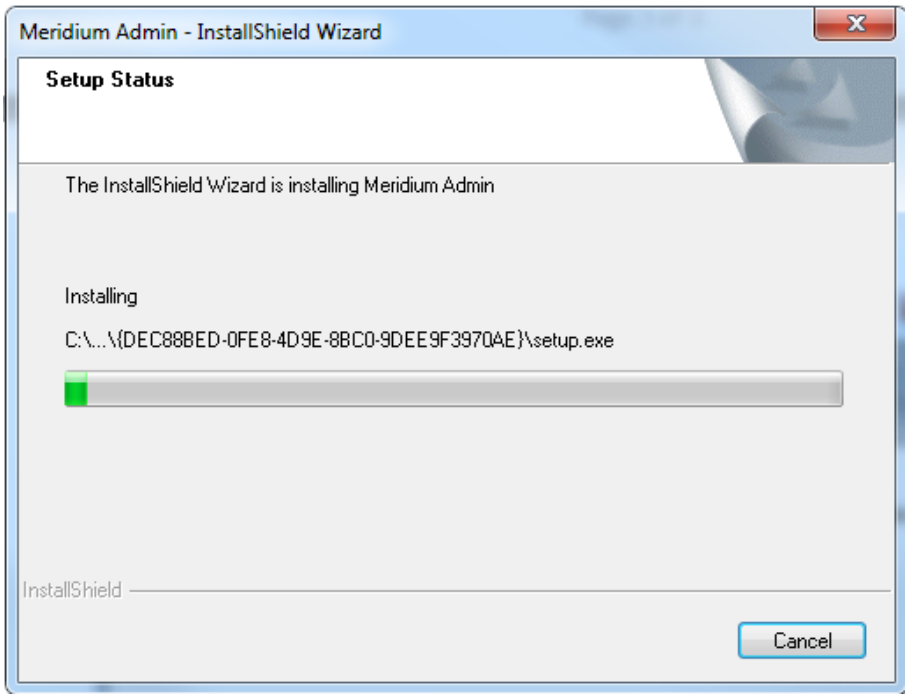
7. Select **Next**.

   The **Complete the Installation** screen appears.

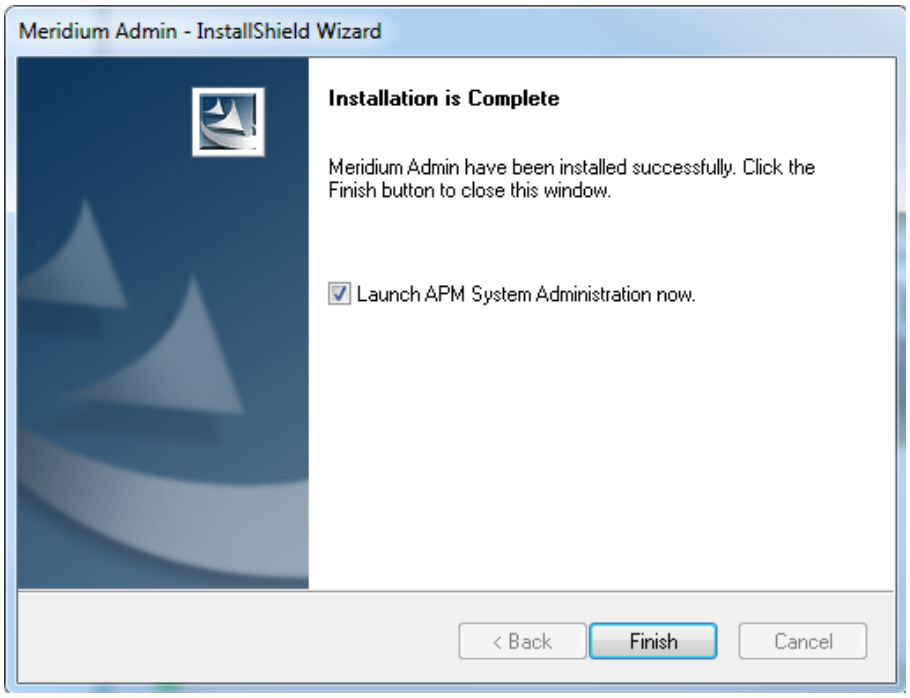


8. Select **Install**.

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?

- Open the Meridium Rules Editor

Deploying 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.

Deploying 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. All steps are required unless otherwise noted.

Step	Task	Required/Optional	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.	Optional	This task is necessary 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.	Required	Users will not be able to accesss SIS Management unless they have permissions to the SIS Management families.
3	Define alternate search queries.	Optional	Required if you do not want to use the baseline search queries.
4	Import data from an Exida project file.	Optional	This is necessary only if you want to create SIL Analyses using an Exida project file.
5	Export data from an Exida project file.	Optional	None

Step	Task	Required/Optional	Notes
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.	Optional	Required if you want to add another value to the list of default values in the Type list in the Independent Layer of Protection datasheet.
7	Activate the Hazards Analysis license.	Optional	This is necessary 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.	Optional	This is necessary only for Security Groups that will be used in the integration between the SIS Management module and Hazards Analysis.

Upgrade Workflow

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. 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. All steps are required unless otherwise noted.

V3.6.0.0.0

Step	Task	Required?	Notes
1	Activate the Hazards Analysis license.	No	Required 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.	No	Required if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

V3.5.1

Step	Task	Required?	Notes
1	Activate the Hazards Analysis license.	No	Required 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.	No	Required if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

V3.5.0 SP1 LP

Step	Task	Required?	Notes
1	Activate the Hazards Analysis license.	No	Required if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

Step	Task	Required?	Notes
2	Assign at least View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager.	No	Required if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

V3.5.0

Step	Task	Required?	Notes
1	Activate the Hazards Analysis license.	No	Required 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.	No	Required if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

V3.4.5

Step	Task	Required?	Notes
1	Activate the Hazards Analysis license.	No	Required 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.	No	Required if you want to take advantage of the integration between the SIS Management module and Hazards Analysis.

Security Groups and Privileges

The following table lists the baseline Security Groups that represent the main types of users for this module, as well as the baseline roles assigned to each.

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

These groups are intended to support the three main types of users who will use Hazards Analysis. Each of these groups has privileges assigned to it by default. The baseline family-level privileges 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
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

Family	MI SIS Administrator	MI SIS Engineer	MI SIS User
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
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

Family	MI SIS Administrator	MI SIS Engineer	MI SIS User
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
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

Family	MI SIS Administrator	MI SIS Engineer	MI SIS User
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
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

Family	MI SIS Administrator	MI SIS Engineer	MI SIS User
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
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

Family	MI SIS Administrator	MI SIS Engineer	MI SIS User
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
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

Family	MI SIS Administrator	MI SIS Engineer	MI SIS User
Migrates_Risk	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Was_Promoted_to_ASM	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Deploying 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.

Deploying 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. All steps are required unless otherwise noted.

Step	Task	Required?	Notes
1	Review the TM data model to determine which relationship definitions you will need to modify to include your custom equipment families. Modify any relationship definitions as needed. Modify any relationship definitions as needed.	N	Required if you store equipment information in families other than the baseline Equipment and TML Group families.
2	Assign the desired Security Users to one or more TM Security Groups.	Y	User must have permissions to the TM families in order to use the TM functionality.

Step	Task	Required?	Notes
3	Configure settings for the Equipment and TML Group families.	Y	Required regardless of whether or not you follow the TM Best Practice. If you do not follow the TM Best Practice, you must configure settings for the families that will be used to store equipment data in Thickness Monitoring. The following relationships *must* be defined regardless of whether you follow TM Best Practice: • For the *Equipment* family, the **Asset to Subcomponent Relationship** box must be set to **Has TML Group**, and the **Component ID** field must be set to **Equipment ID**. The **Subcomponent to Asset Relationship** box should be left *blank*. • For the *TML Group* family, the **Subcomponent to Asset Relationship** box must be set to **Has TML Group**, and the **Component ID** field must be set to **TML Group ID**. The **Asset to Subcomponent Relationship** box should be left *blank*.
4	Configure global settings.	N	Default reading preferences and Nominal T-Min preferences exist in the baseline Meridium Enterprise APM database. These 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.	N	Default TML Types exist in the baseline Meridium Enterprise APM database. You can define additional TML Types to use in your Corrosion Analyses.

Step	Task	Required?	Notes
6	Manage Thickness Monitoring Rules Lookup records.	N	You can complete this task 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.	N	Default Thickness Measurement fields are displayed in the header section 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.	N	Required if 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.	N	Required 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.	N	Required if you will use these devices to collect data that you transfer to Thickness Monitoring.

Upgrading Thickness Monitoring (TM) to V4.0.1.0

The following table outlines the steps that you must complete to upgrade this module to V4.0.1.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

V3.6.0.0.0

Thickness Monitoring will be upgraded from V3.6.0.0.0 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.1

TM will be upgraded from V3.5.1 to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0 SP1 LP

TM will be upgraded from V3.5.0 SP1 LP to V4.0.1.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

V3.5.0

Step	Task	Required?	Notes
1	Manually update TM Analyses for which you used custom corrosion rates. To do so: 1. Locate the records that you will need to update by running the following query: SELECT [MI_EQUIP000].[MI_EQUIP000_EQUIP_ID_C] "Equipment ID", [MI_TMLGROUP].[MI_TMLGROUP_ID_C] "TML Group ID", [MI Thickness Measurement Location].[MI_DP_ASSET_ID_CHR] "TML Asset ID", [MI Thickness Measurement Location].[MI_DP_ID_CHR] "TML ID", [MI TML Corrosion Analysis].[MI_TML_CA_A_CR_N] "Custom Calculation A Corros", [MI TML Corrosion Analysis].[MI_TML_CA_B_CR_N] "Custom Calculation B Corros" FROM [MI_EQUIP000] JOIN_SUCC [MI_TMLGROUP] JOIN_SUCC [MI Thickness Measurement Location] JOIN_SUCC [MI TML Corrosion Analysis] ON {MI Has Corrosion Analyses} ON {MI Has Datapoints} ON {MIR_HSTMLGP} WHERE ([MI TML Corrosion Analysis].[MI_TML_CA_A_CR_N] > 0 AND [MI TML Corrosion Analysis].[MI_TML_CA_B_CR_N] > 0) 2. Use the Bulk Analyze tool to update TM Analyses associated with the Equipment and TML Group records returned by this query. Note that 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	N	In previous versions of Meridium APM, if you used custom corrosion rates in your TM Analyses, 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. In order 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	Required?	Notes
	identify the records requiring update: • MI_EQUIP000 and MI_TMLGROUP with your custom family IDs. • MI_EQUIP000_EQUIP_ID_C and MI_TMLGROUP_ID_C with the field IDs used to identify these custom equipment records. Then, run the Bulk Analyze tool using your custom records.		

V3.4.5

Step	Task	Required?	Notes
1	Update certain TM Analyses to correct TML Corrosion Analyses for which you performed measurement variance evaluation prior to V4.0.1.0. To do so: 1. Locate the records that you will need to update by creating a query that returns TML Corrosion Analyses whose: • Short Term Corrosion Rate field contains the value 0 (zero). • Allowable Measurement Variance Applied field is set to True. 2. Use the Bulk Analyze tool to update TM Analyses that are associated with TML Corrosion Analyses returned by the query you created in step 1.	N	In previous versions of Meridium APM, in certain circumstances, TML Corrosion Analyses for which you performed measurement variance evaluation contained incorrect values in the Short Term Corrosion Rate and Allowable Measurement Variance Applied fields. In order to correct this issue in existing records, you must perform this step to manually update TM Analyses.

Step	Task	Required?	Notes
2	Manually update TM Analyses for which you used custom corrosion rates. To do so: 1. Locate the records that you will need to update by running the following query: SELECT [MI_EQUIP000].[MI_EQUIP000_EQUIP_ID_C] "Equipment ID", [MI_TMLGROUP].[MI_TMLGROUP_ID_C] "TML Group ID", [MI Thickness Measurement Location].[MI_DP_ASSET_ID_CHR] "TML Asset ID", [MI Thickness Measurement Location].[MI_DP_ID_CHR] "TML ID", [MI TML Corrosion Analysis].[MI_TML_CA_A_CR_N] "Custom Calculation A Corros", [MI TML Corrosion Analysis].[MI_TML_CA_B_CR_N] "Custom Calculation B Corros" FROM [MI_EQUIP000] JOIN_SUCC [MI_TMLGROUP] JOIN_SUCC [MI Thickness Measurement Location] JOIN_SUCC [MI TML Corrosion Analysis] ON {MI Has Corrosion Analyses} ON {MI Has Datapoints} ON {MIR_HSTMLGP} WHERE ([MI TML Corrosion Analysis].[MI_TML_CA_A_CR_N] > 0 AND [MI TML Corrosion Analysis].[MI_TML_CA_B_CR_N] > 0) 2. Use the Bulk Analyze tool to update TM Analyses associated with the Equipment and TML Group records returned by this query. Note that 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	N	In previous versions of Meridium APM, if you used custom corrosion rates in your TM Analyses, certain fields in the associated TML Corrosion Analyses 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. In order 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	Required?	Notes
	the records requiring update: • MI_EQUIP000 and MI_TMLGROUP with your custom family IDs. • MI_EQUIP000_EQUIP_ID_C and MI_TMLGROUP_ID_C with the field IDs used to identify these custom equipment records. Then, 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.

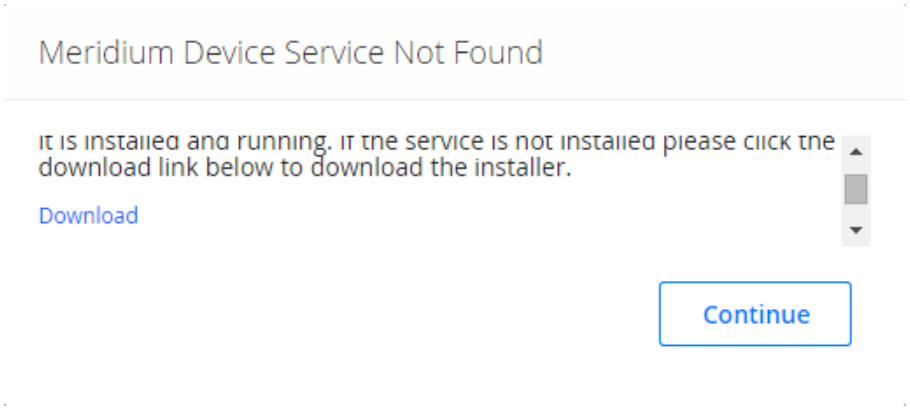
The Meridium Device Service can be installed in the normal workflow when using dataloggers with Thickness Monitoring.

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.



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 Caluclator	No	Yes	No
Archive Corrosion Rates	No	Yes	No
Reset the Maximum Historical Corrosion Rate	Yes	No	No
Exclude TMLs	No	Yes	No

Function	Can be done by members of the MI Thickness Monitoring Administrator Group?	Can be done by members of the MI Thickness Monitoring Inspector Group?	Can be done by members of the MI Thickness Monitoring User Group?
Renew TMLs	No	Yes	No
Reset User Preferences	Yes	No	No
Set Color Coding Preferences	Yes	No	No

Thickness Monitoring Security Groups

The baseline Meridium Enterprise APM database contains three Security Groups specifically for Thickness Monitoring:

Security Group	Roles
MI Thickness Monitoring Administrator	MI MechInt Admin
MI Thickness Monitoring Inspector	MI MechInt Admin MI MechInt Power MI MechInt User
MI Thickness Monitoring User	MI MechInt Admin MI MechInt Power MI MechInt User

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

Family	MI Thickness Monitoring Administrator	MI Thickness Monitoring Inspector	MI Thickness Monitoring User
Entity Family			
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
Materials of Construction	View	View	View
Meridium Reference Tables	View, Update, Insert, Delete	View	View
Resource Role	View, Update, Insert, Delete	View	View

Family	MI Thickness Monitoring Administrator	MI Thickness Monitoring Inspector	MI Thickness Monitoring User
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 Family			
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
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

Family	MI Thickness Monitoring Administrator	MI Thickness Monitoring Inspector	MI Thickness Monitoring User
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