



Meridium Enterprise APM Modules and Features

V4.1.5.0



Meridium Enterprise APM Modules and Features

V4.1.5.0

Copyright © Meridium, Inc. 2016

All rights reserved. Printed in the U.S.A.

This software/documentation contains proprietary information of Meridium, Inc.; it is provided under a license agreement containing restrictions on use and disclosure. All rights including reproduction by photographic or electronic process and translation into other languages of this material are fully reserved under copyright laws. Reproduction or use of this material in whole or in part in any manner without written permission from Meridium, Inc. is strictly prohibited.

Meridium is a registered trademark of Meridium, Inc.

All trade names referenced are the service mark, trademark or registered trademark of the respective manufacturer.

About This Document

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

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

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


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

Table of Contents

| | |
|--|-----------|
| Meridium Enterprise APM Modules and Features | 1 |
| Copyright and Legal | 2 |
| About This Document | 3 |
| Table of Contents | 4 |
| Deploying Modules and Features | 10 |
| Deploy AMS Analytics | 11 |
| Deploy AMS Analytics for the First Time | 12 |
| Upgrading AMS Analytics to V4.1.5.0 | 14 |
| Configure Oracle Specific Queries | 18 |
| Modify the AMS Analytics Overview Page for Oracle | 19 |
| About Defining the Criticality Value in AMS Asset Records | 20 |
| About Creating AMS Asset Data Source Records | 21 |
| AMS Analytics Security Groups and Roles | 22 |
| APM Connect | 24 |
| Deploying Asset Health Manager (AHM) | 25 |
| Deploying Asset Health Manager (AHM) for the First Time | 26 |
| Upgrading Asset Health Manager (AHM) to V4.1.5.0 | 28 |
| About the Asset Health Services | 37 |
| Configure the Meridium Notification Service for AHM | 40 |
| Asset Health Manager Security Groups and Roles | 41 |
| Deploying Asset Criticality Analysis (ACA) | 44 |
| Deploying Asset Criticality Analysis (ACA) for the First Time | 45 |
| Upgrading Asset Criticality Analysis (ACA) to V4.1.5.0 | 46 |
| About Associating an ACA with a Specific Site | 50 |
| Specify an Alternate Unmitigated Risk Label | 51 |
| ACA Security Groups and Roles | 52 |
| Deploying Asset Strategy Implementation (ASI) | 55 |
| Deploying Asset Strategy Implementation (ASI) for the First Time | 56 |

| | |
|--|-----|
| Upgrading Asset Strategy Implementation (ASI) to V4.1.5.0 | 58 |
| ASI Security Groups and Roles | 60 |
| Deploying Asset Strategy Management (ASM) | 66 |
| Deploying Asset Strategy Management (ASM) for the First Time | 67 |
| Upgrading Asset Strategy Management (ASM) to V4.1.5.0 | 68 |
| ASM Security Groups and Roles | 71 |
| Deploying Asset Strategy Optimization (ASO) | 81 |
| First-Time Deployment Workflow | 82 |
| Upgrading Asset Strategy Optimization (ASO) to V4.1.5.0 | 83 |
| Security Groups and Roles | 86 |
| Deploying Calibration Management | 87 |
| Deploying Calibration Management for the First Time | 88 |
| Upgrading Calibration Management to V4.1.5.0 | 89 |
| Install the Meridium Device Service | 91 |
| Calibration Management Security Groups and Roles | 93 |
| Deploying Failure Modes and Effects Analysis (FMEA) | 97 |
| Deploying Failure Modes and Effects Analysis (FMEA) for the First Time | 98 |
| Upgrading Failure Modes and Effects Analysis (FMEA) to V4.1.5.0 | 99 |
| Failure Modes and Effects Analysis (FMEA) Security Groups and Roles | 101 |
| Deploying Hazards Analysis | 105 |
| Deploying Hazards Analysis for the First Time | 106 |
| Upgrading Hazards Analysis to V4.1.5.0 | 108 |
| Hazards Analysis Security Groups and Roles | 111 |
| Deploying Inspection Management | 117 |
| Deploying Inspection Management for the First Time | 118 |
| Upgrading Inspection Management to V4.1.5.0 | 120 |
| Inspection Management Security Groups and Roles | 122 |
| Deploying Metrics and Scorecards | 125 |
| Deploying Metrics and Scorecards for the First Time | 126 |
| Upgrade Metrics and Scorecards to V4.1.5.0 | 130 |

| | |
|---|-----|
| About Configuring a Cube for Usage Metrics Tracking | 134 |
| About Scheduling Cubes for Processing | 135 |
| Install SQL Server Analysis Services on the Server | 136 |
| Migrate SQL Server Cubes | 137 |
| Deploy the Work History Cube | 139 |
| Metrics and Scorecard Security Groups and Roles | 140 |
| Deploying Policy Designer | 142 |
| Deploying Policy Designer for the First Time | 143 |
| Upgrading Policy Designer to V4.1.5.0 | 144 |
| About the Asset Health Services | 150 |
| About Configuring Policy Execution | 153 |
| Configure the Policy Trigger Service | 154 |
| Configure Multiple Meridium Enterprise APM Servers for Policy Execution | 155 |
| Policy Designer Security Groups and Roles | 158 |
| Deploying Process Data Integration (PDI) | 159 |
| Deploying Process Data Integration (PDI) for the First Time | 160 |
| Upgrading Process Data Integration (PDI) to V4.1.5.0 | 162 |
| Process Data Integration Server Roles | 169 |
| About the Asset Health Services | 170 |
| Install the Process Data Integration Service | 173 |
| Upgrade the Process Data Integration Service | 175 |
| Configure the Meridium Notification Service for PDI | 177 |
| Configure the Process Data Integration Service | 179 |
| Configure Multiple Data Sources | 183 |
| Configure Multiple Process Data Integration and OPC Servers | 184 |
| Process Data Integration Security Groups and Roles | 186 |
| Deploying Production Loss Analysis (PLA) | 187 |
| Deploying Production Loss Analysis (PLA) for the First Time | 188 |
| Upgrading Production Loss Analysis (PLA) to V4.1.5.0 | 192 |
| Import Baseline Rules | 197 |

| | |
|---|-----|
| Replace the Top 10 Bad Actors Query | 209 |
| Production Loss Analysis Security Groups and Roles | 212 |
| Deploying R Scripts | 216 |
| Deploying R Scripts for the First Time | 217 |
| Upgrading R Scripts to V4.1.5.0 | 218 |
| Upgrade R Script Metadata | 219 |
| Deploying Recommendation Management | 220 |
| Deploying Recommendation Management for the First Time | 221 |
| Upgrading Recommendation Management to V4.1.5.0 | 222 |
| About Asset Queries | 224 |
| Recommendation Management Security Groups and Roles | 226 |
| Deploying Reliability Analytics | 228 |
| Deploying Reliability Analytics for the First Time | 229 |
| Upgrading Reliability Analytics to V4.1.5.0 | 230 |
| Reliability Analytics Security Groups and Roles | 232 |
| Deploying Reliability Centered Maintenance (RCM) | 237 |
| Deploying Reliability Centered Maintenance (RCM) for the First Time | 238 |
| Upgrading Reliability Centered Maintenance (RCM) to V4.1.5.0 | 239 |
| Reliability Centered Maintenance (RCM) Security Groups and Roles | 241 |
| Reports | 246 |
| Deploying Reports for the First Time | 247 |
| Install the APM Reports Designer | 248 |
| Set Up the APM Report Designer | 257 |
| Deploying RBI 581 | 259 |
| Deploying RBI 581 for the First Time | 260 |
| Upgrading RBI 581 to V4.1.5.0 | 262 |
| Modify the Review Analyses for Asset Query | 267 |
| Add the 581 Tab to Criticality RBI Component Datasheets | 269 |
| RBI 581 Security Groups and Roles | 274 |
| Deploying Risk Based Inspection (RBI) | 275 |

| | |
|---|-----|
| Deploying Risk Based Inspection (RBI) for the First Time | 276 |
| Upgrading Risk Based Inspection (RBI) to V4.1.5.0 | 279 |
| Modify the Review Analyses for Asset Query | 291 |
| Risk Based Inspection Security Groups and Roles | 293 |
| Deploying Root Cause Analysis (RCA) | 299 |
| Deploying Root Cause Analysis (RCA) for the First Time | 300 |
| Upgrading Root Cause Analysis (RCA) to V4.1.5.0 | 301 |
| Root Cause Analysis Security Groups and Roles | 303 |
| Deploying Rounds | 306 |
| Deploying Rounds for the First Time | 307 |
| Upgrading Rounds to V4.1.5.0 | 312 |
| Manage the Measurement Location Template Mappings | 319 |
| Meridium APM Sync Services Tasks | 320 |
| Install Meridium APM Sync Services | 321 |
| Verify Installation of Meridium APM Sync Services | 329 |
| Install Microsoft Sync Framework | 330 |
| Modify the Web.config for An Oracle Sync Services Database Connection | 331 |
| Modify the Web.config for An SQL Sync Services Database Connection | 333 |
| Modify Meridium Sync Config | 335 |
| Configure Security for Meridium Sync Service | 337 |
| Windows Mobile Handheld Devices | 338 |
| Install the .NET Compact Framework on Windows Mobile Device | 339 |
| Install Microsoft SQL CE on Windows Mobile Device | 340 |
| Install Microsoft Sync Services for ADO.NET on Windows Mobile Device | 341 |
| Install the Meridium APM Mobile Framework on Windows Mobile Device | 342 |
| Access Device Settings Screen on Windows Mobile Device | 343 |
| Identify the Sync Server Within the APM Mobile Framework on Windows Mobile Device | 344 |
| Specify the Security Query on Windows Mobile Device | 345 |
| Modify User Time-out Value on Windows Mobile Device | 346 |

| | |
|---|-----|
| Install Operator Rounds on Windows Mobile Device | 347 |
| Install the Barcode Add-on on Windows Mobile Device | 348 |
| Enable Barcode Scanning on Windows Mobile Device | 350 |
| Install the RFID Add-on on Windows Mobile Device | 351 |
| Enable RFID Tag Scanning on Windows Mobile Device | 353 |
| Install Translations for Operator Rounds on Windows Mobile Device | 355 |
| Uninstall Meridium APM Mobile Framework on Windows Mobile Device | 356 |
| Uninstall then RFID Add-on on Windows Mobile Device | 357 |
| Uninstall the Barcode Add-on on Windows Mobile Device | 360 |
| Uninstall Translations for Operator Rounds on Windows Mobile Device | 363 |
| Uninstall Operator Rounds on Windows Mobile Device | 366 |
| Upgrade Windows Mobile Handheld Device | 369 |
| Security Groups and Privileges In Rounds | 370 |
| Deploying Rules | 374 |
| Install the Meridium Rules Editor | 375 |
| Deploying SIS Management | 383 |
| Deploying SIS Management for the First Time | 384 |
| Upgrading SIS Management to V4.1.5.0 | 386 |
| SIS Management Security Groups and Roles | 389 |
| Deploying Thickness Monitoring (TM) | 396 |
| Deploying Thickness Monitoring (TM) for the First Time | 397 |
| Upgrading Thickness Monitoring (TM) to V4.1.5.0 | 400 |
| Use Custom TML Analysis Types | 406 |
| Install the Meridium Device Service | 408 |
| Configure the Meridium Device Service | 409 |
| Thickness Monitoring Functional Security Privileges | 410 |
| Thickness Monitoring Security Groups and Roles | 412 |

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.

Deploy AMS Analytics

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

Deploy AMS Analytics for the First Time

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

| Step | Task | Notes |
|------|--|---|
| 1 | On the Meridium APM Web Server, run the Meridium APM Server and Add-ons installer, selecting the Meridium Integration Services check box on the Select the features you want to install screen . | None |
| 2 | Create one AMS Asset Data Source record per AMS Analytics data source whose data you want to transfer into Meridium Enterprise APM. | None |
| 3 | Test the connection to each AMS Analytics data source. | None |
| 4 | Link each AMS Asset record to the Equipment or Functional record that represents the piece of equipment or location for which the AMS Asset record exists. | <p>You can link AMS Tag records to Equipment or Functional Location records using one of the following:</p> <ul style="list-style-type: none"> • Record Manager • System and Tags • Tags Data Loader |
| 5 | If you are using Asset Criticality Analysis, define the criticality field in the AMS Asset records for the equipment or location linked to each AMS Asset record. | None |
| 6 | For Oracle users only, configure AMS Analytics to use Oracle-specific queries . | This task is necessary only if you are using an Oracle Meridium Enterprise APM database. If you are using a SQL Server database, the baseline queries will work without any manual configuration. |

| | | |
|---|---|--|
| 7 | For Oracle users only, in Meridium Enterprise APM, modify the AMS Analytics Overview page . | This task is necessary only if you are using an Oracle Meridium Enterprise APM database. If you are using a SQL Server database, the overview page will work without any manual configuration. |
| 8 | Assign the needed Security Users to one or more AMS Analytics Security Groups . | None |

Upgrading AMS Analytics to V4.1.5.0

The following table outlines the steps that you must complete to upgrade this module to V4.1.5.0. 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.

Upgrade from any version V4.1.0.0 through V4.1.1.1

| Step | Task | Notes |
|------|---|-------|
| 1 | If you are not using Equipment and Functional Location records and you want to view AMS Asset Folders and AMS Assets in a hierarchy, modify the application-wide Asset Hierarchy configuration in order to include the Asset Folder and AMS Asset families. | None |
| 2 | If you are using message queues to receive data from an AMS server, you must configure the message queue section in the Web Service Details tab of the AMS Data Source Configuration UI page | None |
| 3 | If you want to use the AMS Asset Tag Data Loader to create relationships between tags and assets, you must run the following update query <code>UPDATE [MI_APTAG] SET [MI_APTAG].[MI_TAG_SYSTEM_ID_C] = [MI_APTAG].[MI_TAG_PATH_C]</code> | None |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| Step | Task | Notes |
|------|---|-------|
| 1 | If you are not using Equipment and Functional Location records and you want to view AMS Asset Folders and AMS Assets in a hierarchy, modify the application-wide Asset Hierarchy configuration in order to include the Asset Folder and AMS Asset families. | None |
| 2 | If you are using message queues to receive data from an AMS server, you must configure the message queue section in the Web Service Details tab of the AMS Data Source Configuration UI page | None |
| 3 | If you want to use the AMS Asset Tag Data Loader to create relationships between tags and assets, you must run the following update query <code>UPDATE [MI_APTAG] SET [MI_APTAG].[MI_TAG_SYSTEM_ID_C] = [MI_APTAG].[MI_TAG_PATH_C]</code> | None |

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

| Step | Task | Notes |
|------|---|-------|
| 1 | If you are not using Equipment and Functional Location records and you want to view AMS Asset Folders and AMS Assets in a hierarchy, modify the application-wide Asset Hierarchy configuration in order to include the Asset Folder and AMS Asset families. | None |
| 2 | If you are using message queues to receive data from an AMS server, you must configure the message queue section in the Web Service Details tab of the AMS Data Source Configuration UI page | None |
| 3 | If you want to use the AMS Asset Tag Data Loader to create relationships between tags and assets, you must run the following update query <code>UPDATE [MI_APTAG] SET [MI_APTAG].[MI_TAG_SYSTEM_ID_C] = [MI_APTAG].[MI_TAG_PATH_C]</code> | None |

Upgrade from any version V3.5.1 through V3.5.1.10.0

| Step | Task | Notes |
|------|---|-------|
| 1 | If you are not using Equipment and Functional Location records and you want to view AMS Asset Folders and AMS Assets in a hierarchy, modify the application-wide Asset Hierarchy configuration in order to include the Asset Folder and AMS Asset families. | None |
| 2 | If you are using message queues to receive data from an AMS server, you must configure the message queue section in the Web Service Details tab of the AMS Data Source Configuration UI page | None |
| 3 | If you want to use the AMS Asset Tag Data Loader to create relationships between tags and assets, you must run the following update query <code>UPDATE [MI_APTAG] SET [MI_APTAG].[MI_TAG_SYSTEM_ID_C] = [MI_APTAG].[MI_TAG_PATH_C]</code> | None |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

| Step | Task | Notes |
|------|---|-------|
| 1 | If you are not using Equipment and Functional Location records and you want to view AMS Asset Folders and AMS Assets in a hierarchy, modify the application-wide Asset Hierarchy configuration in order to include the Asset Folder and AMS Asset families. | None |

| Step | Task | Notes |
|------|---|-------|
| 2 | If you are using message queues to receive data from an AMS server, you must configure the message queue section in the Web Service Details tab of the AMS Data Source Configuration UI page | None |
| 3 | If you want to use the AMS Asset Tag Data Loader to create relationships between tags and assets, you must run the following update query <code>UPDATE [MI_APTAG] SET [MI_APTAG].[MI_TAG_SYSTEM_ID_C] = [MI_APTAG].[MI_TAG_PATH_C]</code> | None |

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

| Step | Task | Notes |
|------|---|-------|
| 1 | If you are not using Equipment and Functional Location records and you want to view AMS Asset Folders and AMS Assets in a hierarchy, modify the application-wide Asset Hierarchy configuration in order to include the Asset Folder and AMS Asset families. | None |
| 2 | If you are using message queues to receive data from an AMS server, you must configure the message queue section in the Web Service Details tab of the AMS Data Source Configuration UI page | None |
| 3 | If you want to use the AMS Asset Tag Data Loader to create relationships between tags and assets, you must run the following update query <code>UPDATE [MI_APTAG] SET [MI_APTAG].[MI_TAG_SYSTEM_ID_C] = [MI_APTAG].[MI_TAG_PATH_C]</code> | None |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Notes |
|------|---|-------|
| 1 | If you are not using Equipment and Functional Location records and you want to view AMS Asset Folders and AMS Assets in a hierarchy, modify the application-wide Asset Hierarchy configuration in order to include the Asset Folder and AMS Asset families. | None |
| 2 | If you are using message queues to receive data from an AMS server, you must configure the message queue section in the Web Service Details tab of the AMS Data Source Configuration UI page | None |

| Step | Task | Notes |
|------|--|-------|
| 3 | If you want to use the AMS Asset Tag Data Loader to create relationships between tags and assets, you must run the following update query UPDATE [MI_APTAG] SET [MI_APTAG].[MI_TAG_SYSTEM_ID_C] = [MI_APTAG].[MI_TAG_PATH_C] | None |

Configure Oracle Specific Queries

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

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

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

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

Steps


1. Rename the SQL Server versions of the queries. For example, you might want to rename the Event Trend Daily query `Event Trend Daily_SQL`.
2. In the Oracle versions of the queries, remove the text `_Oracle` from the name.

Queries are configured for Oracle users.

Modify the AMS Analytics Overview Page for Oracle

Steps

1. In Meridium Enterprise APM, access the **Dashboard** page.
2. Open the AMS Analytics Overview Widget Dashboard stored in the Catalog folder **\\Public\Meridium\Modules\AMS Asset Portal\Dashboard**.

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

3. Using the options to hide and display widgets:
 - a. Hide the **AMS Active Alerts by Duration** widget.
 - b. Display the **AMS Active Alerts by Duration (Oracle)** widget.
4. Arrange the widgets at each screen size as necessary.

About Defining the Criticality Value in AMS Asset Records

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

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

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

About Creating AMS Asset Data Source Records

AMS Asset Data Source records store connection information that the Meridium Enterprise APM system uses to import data from AMS Analytics data sources

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

AMS Analytics Security Groups and Roles

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

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

| Security Group | Roles |
|--------------------------------|-----------------|
| MI AMS Suite APM Administrator | MI Health Admin |
| MI AMS Suite APM Power User | MI Health Power |
| MI AMS Suite APM User | MI Health User |

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

| Family | MI AMS Suite APM User | MI AMS Suite APM Power User | MI AMS Suite APM Administrator |
|--------------------------|-----------------------|-----------------------------|--------------------------------|
| Entity Families | | | |
| Tag | View | View, Update | View, Update, Insert, Delete |
| Tag Alert | View | View, Update | View, Update, Insert, Delete |
| Tag Data Source | View | View | View, Update, Insert, Delete |
| Tag Event | View | View, Update | View, Update, Insert, Delete |
| AMS Asset Recommendation | View, Update, Insert | View, Update, Insert | View, Update, Insert, Delete |

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

APM Connect

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

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

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 | You may review the log files for this service at C:\ProgramData\Meridium . |
| 4 | On the Meridium Enterprise APM Server, start the Meridium AHI Service (Asset Health Indicator Service). | Y | When you start the service, Health Indicator records are created or updated automatically based on health indicator and reading source records. You may review the log files for this service at C:\Program Files\Meridium\Logs . |
| 5 | Review the AHM data model to determine which relationship definitions you will need to modify to include your custom asset families. | N | Required if you store asset information in families other than the baseline Equipment and Functional Location families. |

| Step | Task | Required? | Notes |
|------|---|-----------|--|
| 6 | Determine the equipment or location whose overall health you want to evaluate, and make sure that an asset record exists in the database for this equipment or location and is included in the Asset Hierarchy configuration. | 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. |
| 7 | Configure Health Indicator Mapping records for each family that you want to use as a health indicator source, for which a baseline Health Indicator Mapping record does not already exist. | Y | Baseline Health Indicator Mapping records exist for the following health indicator source families: <ul style="list-style-type: none"> • Measurement Location • KPI • OPC Tag • Health Indicator |
| 8 | Link each asset record to the record(s) that you want to use as a health indicator source records. | Y | None |
| 9 | For any specific records in a health indicator source family for which you <i>do not</i> want health indicators to be created, exclude these records from the automatic health indicator creation. | N | None |
| 10 | Review the baseline event mappings and modify or create new mappings as necessary to customize the information that is displayed in the Events section in Asset Health Manager. | N | Refer to the Asset Health Manager end user help for more information about events . |

Upgrading Asset Health Manager (AHM) to V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

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.

Upgrade from any version V4.1.0.0 through V4.1.1.1

| 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 | Start or restart the Meridium AHI Service (Asset Health Indicator Service). | Y | None |
| 4 | On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service. | N | Required only if you are using OPC Tag records as health indicators sources. |


Upgrade from any version V4.0.0.0 through V4.0.1.0

| Step | Task | 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 |


| Step | Task | Required? | Notes |
|------|--|-----------|--|
| 3 | Start or restart the Meridium AHI Service (Asset Health Indicator Service). | Y | None |
| 4 | On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service. | N | Required only if you are using OPC Tag records as health indicators sources. |

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

| 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 | You may review the log files for this service at C:\ProgramData\Meridium . |
| 3 | Start or restart the Meridium AHI Service (Asset Health Indicator Service). | Y | You may review the log files for this service at C:\Program Files\Meridium\Logs . |

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 4 | Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each. | Y | <p>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 <i>excluded</i> from the automatic health indicator creation by default.</p> <div>  Note: Alternatively, prior to upgrading to V4.1.5.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records. </div> |
| 5 | If you previously used the Hierarchy Item Definition family to create a custom hierarchy for Asset Health Manager, ensure that the relevant asset families are included in the application-wide Asset Hierarchy configuration. | Y | None |
| 6 | If you are using custom Health Indicator Mapping records, specify values in the Type Field and Type Value fields to ensure that the mappings are used for the appropriate reading type. | Y | None |
| 7 | On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service. | N | Required only if you are using OPC Tag records as health indicators sources. |


Upgrade from any version V3.5.1 through V3.5.1.10.0

| 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 | You may review the log files for this service at C:\ProgramData\Meridium . |
| 3 | Start or restart the Meridium AHL Service (Asset Health Indicator Service). | Y | You may review the log files for this service at C:\Program Files\Meridium\Logs . |
| 4 | Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each. | Y | <p>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 <i>excluded</i> from the automatic health indicator creation by default.</p> <div>  Note: Alternatively, prior to upgrading to V4.1.5.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records. </div> |
| 5 | If you previously used the Hierarchy Item Definition family to create a custom hierarchy for Asset Health Manager, ensure that the relevant asset families are included in the application-wide Asset Hierarchy configuration.. | Y | None |


| Step | Task | Required? | Notes |
|------|---|-----------|--|
| 6 | If you are using custom Health Indicator Mapping records, specify values in the Type Field and Type Value fields to ensure that the mappings are used for the appropriate reading type. | Y | None |
| 7 | On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service. | N | Required only if you are using OPC Tag records as health indicators sources. |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

| 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 | You may review the log files for this service at C:\ProgramData\Meridium . |
| 3 | Start or restart the Meridium AHl Service (Asset Health Indicator Service). | Y | You may review the log files for this service at C:\Program Files\Meridium\Logs . |

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 4 | Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each. | Y | <p>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 <i>excluded</i> from the automatic health indicator creation by default.</p> <div>  Note: Alternatively, prior to upgrading to V4.1.5.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records. </div> |
| 5 | If you previously used the Hierarchy Item Definition family to create a custom hierarchy for Asset Health Manager, ensure that the relevant asset families are included in the application-wide Asset Hierarchy configuration. | Y | None |
| 6 | If you are using custom Health Indicator Mapping records, specify values in the Type Field and Type Value fields to ensure that the mappings are used for the appropriate reading type. | Y | None |
| 7 | On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service. | N | Required only if you are using OPC Tag records as health indicators sources. |


Upgrade from any version V3.5.0 through V3.5.0.0.7.2

| 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 | You may review the log files for this service at C:\ProgramData\Meridium . |
| 3 | Start or restart the Meridium AHL Service (Asset Health Indicator Service). | Y | You may review the log files for this service at C:\Program Files\Meridium\Logs . |
| 4 | Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each. | Y | <p>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 <i>excluded</i> from the automatic health indicator creation by default.</p> <div>  Note: Alternatively, prior to upgrading to V4.1.5.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records. </div> |
| 5 | If you previously used the Hierarchy Item Definition family to create a custom hierarchy for Asset Health Manager, ensure that the relevant asset families are included in the application-wide Asset Hierarchy configuration. | Y | None |

| Step | Task | Required? | Notes |
|------|---|-----------|--|
| 6 | If you are using custom Health Indicator Mapping records, specify values in the Type Field and Type Value fields to ensure that the mappings are used for the appropriate reading type. | Y | None |
| 7 | On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service. | N | Required only if you are using OPC Tag records as health indicators sources. |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | 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 | You may review the log files for this service at C:\ProgramData\Meridium . |
| 3 | Start or restart the Meridium AHM Service (Asset Health Indicator Service). | Y | You may review the log files for this service at C:\Program Files\Meridium\Logs . |

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 4 | Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each. | Y | <p>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 <i>excluded</i> from the automatic health indicator creation by default.</p> <div>  Note: Alternatively, prior to upgrading to V4.1.5.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records. </div> |
| 5 | If you previously used the Hierarchy Item Definition family to create a custom hierarchy for Asset Health Manager, ensure that the relevant asset families are included in the application-wide Asset Hierarchy configuration. | Y | None |
| 6 | If you are using custom Health Indicator Mapping records, specify values in the Type Field and Type Value fields to ensure that the mappings are used for the appropriate reading type. | Y | None |
| 7 | On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service. | N | Required only if you are using OPC Tag records as health indicators sources. |

About the Asset Health Services

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

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

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

Services Summary

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

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

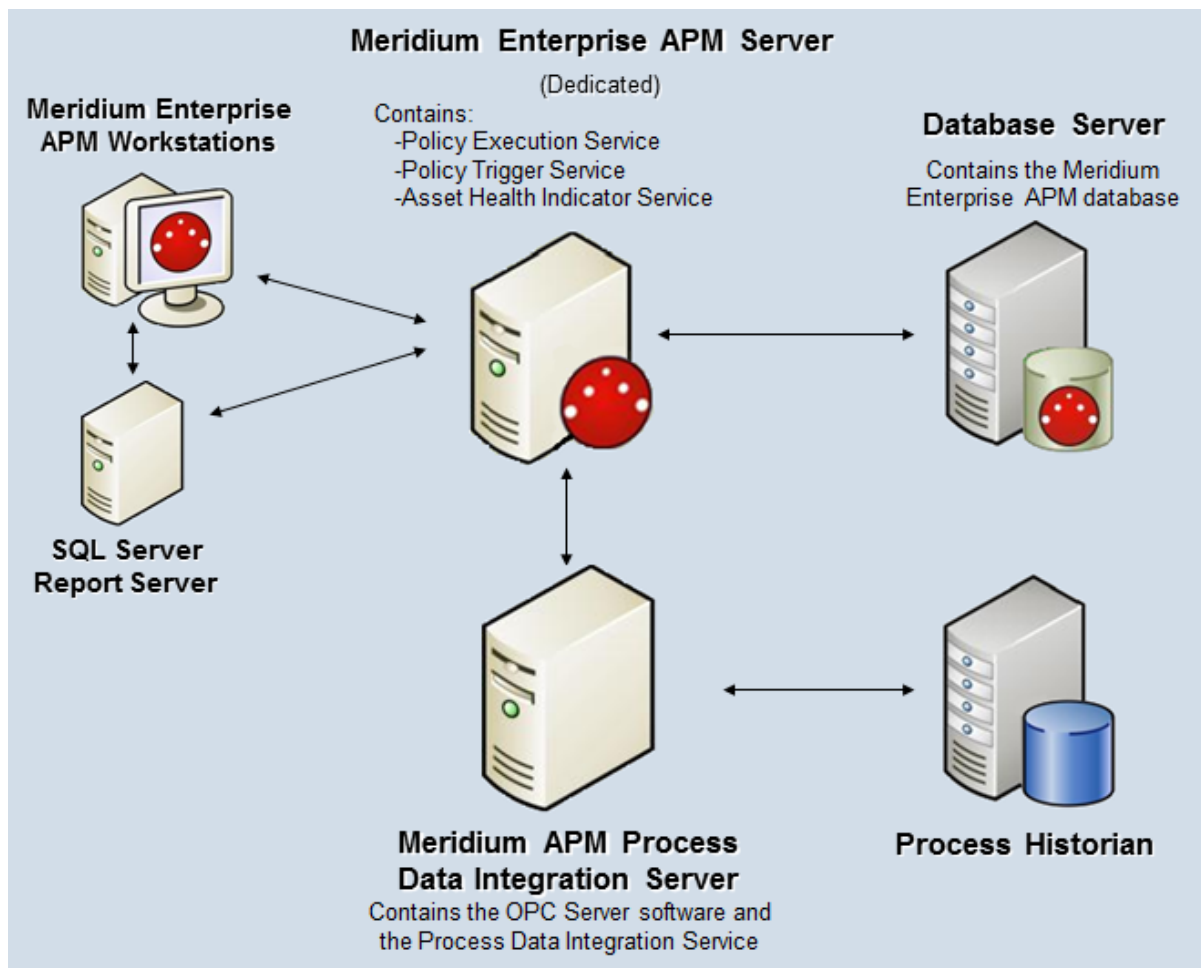
This service also facilitates the automatic creation of Health Indicator records for configured sources.

- **Policy Trigger Service:** When an input to a policy (i.e., an associated record in the Meridium Enterprise APM database or reading value in the process historian) changes or when a policy schedule is due, a message is added to the policy trigger queue. The Policy Trigger Service monitors this queue and sends these messages to an appropriate policy execution queue.
- **Policy Execution Service:** The Meridium Enterprise APM Policy Execution Service handles the execution of policies. Specifically, the Policy Execution Service monitors a corresponding policy execution queue and executes the policies that are added to it.
- **Process Data Integration (PDI) Service:** Monitors the subscribed tags (i.e., tags that are used in policies and health indicators or tags for which readings are being stored in the Meridium database) and, when data changes occur on these tags, adds messages to the appropriate queues. This service also facilitates the automatic import and synchronization of tags from a configured process historian.

Example: Standard System Architecture Configuration

The following diagram illustrates the machines in the Meridium Enterprise APM system architecture when the Policy Designer, Process Data Integration (PDI), and Asset Health Manager (AHM) modules are used together. This image depicts the standard configuration, where the OPC Server software and the Process Data Integration Service are on the *same* machine.

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



The following table summarizes the machines illustrated in this diagram and the software and services that you will install when you complete the first-time deployment steps for [Asset Health Manager](#), [Policy Designer](#), and [Process Data Integration](#).

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

Configure the Meridium Notification Service for AHM

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

Steps

1. On the Meridium Enterprise APM Server, navigate to the folder where the Meridium Notification Service files are installed. If you installed the software in the default location, you can locate these files in the folder **C:\Program Files\Meridium\Services**.
2. Open the file **Meridium.Service.Notification.exe.config** in an application that you can use to modify XML script (e.g., Notepad).
3. If you have not done so already, complete any necessary basic configuration for the Meridium Notification Service.
4. Within the **<notification>** tags, within the **<notificationSettings>** tags, uncomment the following text string (i.e., delete the **<!--** and **-->**):

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

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

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

6. Save and close the file.
7. Start or restart the Meridium Notification Service.

Asset Health Manager Security Groups and Roles

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

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

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

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 |

| Family | MI AHI Administrator | MI AHI User |
|----------------------------------|------------------------------|------------------------------|
| KPI | View | View |
| KPI Measurement | View | View |
| Measurement Location Template | View | View |
| Operator Rounds Allowable Values | View | View |
| Policy | View | View |
| 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 |

| Family | MI AHI Administrator | MI AHI User |
|------------------------------|------------------------------|-------------|
| 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, <i>Unmitigated Risk</i> . |
| 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 V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

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.

Upgrade from any version V4.1.0.0 through V4.1.1.1

| 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, <i>Unmitigated Risk</i> . |
| 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. |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| Step | Task | Notes |
|------|--|---|
| 1 | Specify the alternate label that you want to use for the Unmitigated Risk column in the grid on the Asset Criticality Analysis Systems page. | Required if you do not want to use the default label, <i>Unmitigated Risk</i> . |
| 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. |

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

| 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, <i>Unmitigated Risk</i> . |
| 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. |

Upgrade from any version V3.5.1 through V3.5.1.10.0

| 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, <i>Unmitigated Risk</i> . |
| 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. |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

| 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, <i>Unmitigated Risk</i> . |
| 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. |

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

| 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, <i>Unmitigated Risk</i> . |
| 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. |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Notes |
|------|--|---|
| 1 | Specify the alternate label that you want to use for the Unmitigated Risk column in the grid on the Asset Criticality Analysis Systems page. | Required if you do not want to use the default label, <i>Unmitigated Risk</i> . |

| Step | Task | Notes |
|------|---|--|
| 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. |

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.

ACA Security Groups and Roles

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

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

| Security Group | Roles |
|----------------------|--|
| MI ACA Administrator | MI Foundation Admin |
| MI ACA Member | MI Foundation Admin MI Foundation Power MI Foundation User |
| MI ACA Owner | MI Foundation Admin MI Foundation Power |

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

| Family | 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 |

| Family | MI ACA Administrator | MI ACA Member | MI ACA Owner |
|---|------------------------------|---------------|------------------------------|
| 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 |
| 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 |

| Family | MI ACA Administrator | MI ACA Member | MI ACA Owner |
|-------------------------------|------------------------------|---------------|------------------------------|
| Mitigates Risk | View, Update, Insert, Delete | View | View, Update, Insert, Delete |
| Notification | View, Update, Insert, Delete | View | View, Update, Insert, Delete |
| Probability | View, Update, Insert, Delete | View | View |
| Protection Level | View | View | View |
| RCM FMEA Analysis | View | None | None |
| Reference Document | View, Update, Insert, Delete | View | View, Update, Insert, Delete |
| Risk | View, Update, Insert, Delete | View | View, Update, Insert, Delete |
| Risk Assessment | View, Update, Insert, Delete | View | View, Update, Insert, Delete |
| Risk Category | View, Update, Insert, Delete | View | View, Update, Insert, Delete |
| Risk Matrix | View, Update, Insert, Delete | View | View, Update, Insert, Delete |
| Risk Threshold | View, Update, Insert, Delete | View | View |
| Safety Analysis Has Equipment | View, Update, Insert, Delete | View | View, Update, Insert, Delete |
| Site Reference | View | View | View |
| System Strategy | View | None | None |

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 |

| Step | Task | Required/Optional | Notes |
|------|--|-------------------|--|
| 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. |
| 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 V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

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

Upgrade from any version V4.0.0.0 through V4.0.1.0

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

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

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

Upgrade from any version V3.5.1 through V3.5.1.10.0

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

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

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

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

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

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

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

ASI Security Groups and Roles

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

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

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

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

| Family | MI ASI Administrator | MI ASI user |
|-------------------|------------------------------|------------------------------|
| Entity Families | | |
| 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 V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V4.0.0.0 through V4.0.1.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.10.0

ASM will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

| Step | Task | Required? | Notes |
|------|--|-----------|-------|
| 1 | Move to the <i>Asset Strategy</i> family any custom rules that are defined for the following families and configured to be executed during the Asset Strategy activation process: Action, Risk, Risk Assessment, Risk Rank, Action Revision, Risk Revision, Risk Assessment Revision, and Strategy Revision. | Y | None |

| Step | Task | Required? | Notes |
|------|---|-----------|-------|
| 2 | Move to the <i>Asset Strategy Template</i> family any custom rules that are defined for the following families and configured to be executed when a new Asset Strategy Template is saved after being created from an existing Asset Strategy Template or Asset Strategy: Action, Risk, Risk Assessment, Risk Rank, and Has Risk Category. | Y | None |
| 3 | Move to the <i>Asset Strategy</i> or <i>Asset Strategy Template</i> 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 |

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

| Step | Task | Required? | Notes |
|------|---|-----------|-------|
| 1 | Move to the <i>Asset Strategy</i> 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, and Strategy Revision. | Y | None |
| 2 | Move to the <i>Asset Strategy Template</i> family any custom rules that are defined for the following families and configured to be executed when a new Asset Strategy Template is saved after being created from an existing Asset Strategy Template or Asset Strategy: Action, Risk, Risk Assessment, Risk Rank, and Has Risk Category. | Y | None |
| 3 | Move to the <i>Asset Strategy</i> or <i>Asset Strategy Template</i> 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 |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Required? | Notes |
|------|---|-----------|-------|
| 1 | Move to the <i>Asset Strategy</i> 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, and Strategy Revision. | Y | None |
| 2 | Move to the <i>Asset Strategy Template</i> family any custom rules that are defined for the following families and configured to be executed when a new Asset Strategy Template is saved after being created from an existing Asset Strategy Template or Asset Strategy: Action, Risk, Risk Assessment, Risk Rank, and Has Risk Category. | Y | None |
| 3 | Move to the <i>Asset Strategy</i> or <i>Asset Strategy Template</i> 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 |

ASM Security Groups and Roles

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

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

| Security Group | Roles |
|---|-------------------|
| MI ASM Analyst MI ASM Viewer | MI Strategy User |
| MI ASM Analyst MI ASM Reviewer MI ASM Viewer | MI Strategy Power |
| MI ASM Management Administrator MI ASM Analyst MI ASM Reviewer MI ASM Viewer | MI Strategy Admin |

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

| Family | MI ASM Analyst | MI ASM Administrator | MI ASM Reviewer | MI ASM Viewer |
|----------------------------|----------------------------------|----------------------|----------------------------------|---------------|
| 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 Optimization | 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 Asset Strategy Optimization (ASO)

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

First-Time Deployment Workflow

Deploying and configuring ASO 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 ASO on top of the basic Meridium APM system architecture.

Whether a step is required or option is indicated in the Required/Optional cell. Steps are marked as Required if you must perform the step to take advantage of ASO 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 |
|------|---|-------------------|
| 1 | Assign Security Users to ASO Security Groups via the Configuration Manager application. | Required |

Upgrading Asset Strategy Optimization (ASO) to V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V4.0.0.0 through V4.0.1.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

| 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 Asset Strategy activation process: Action, Risk, Risk Assessment, Risk Rank, Action Revision, Risk Revision, Risk Assessment Revision, and 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, and 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 |

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

| 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, and 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, and 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 |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| 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, and 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 |

Security Groups and Roles

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

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

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 <i>Has Standard Gas</i> 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 V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V4.0.0.0 through V4.0.1.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

Calibration Management will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

This module will be upgraded to V4.1.5.0 automatically when you upgrade the

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

Install the Meridium Device Service

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

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

Steps

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

Note: A calibrator does not need to be connected.

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

The **Settings** window appears.

Settings

Calibrator Device Settings

Select Device

Select Device ▼

COM Port

COM 1 ▼

Baud Rate

9600 ▼

☐ Test Connection

Device Service Settings

Service Port

2014

Cancel Done

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

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

Settings

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

[Download](#)

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

[Continue](#)

[Close](#)

4. Select **Download**.

The MeridiumDevices.exe file is downloaded.

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

The Meridium Device Service is installed.

Calibration Management Security Groups and Roles

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

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

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

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

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

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

| Family | MI Calibration Administrator | MI Calibration User |
|---------------------------------------|------------------------------|------------------------------|
| 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 |
| 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 |

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

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

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 V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V4.0.0.0 through V4.0.1.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | 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 and Roles

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

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

| Security Group | Roles |
|--|-------------------|
| MI RCM User MI RCM Viewer | MI Strategy User |
| MI RCM User MI RCM Viewer | MI Strategy Power |
| MI RCM User MI RCM Viewer MI ASI Administrator | MI Strategy Admin |

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


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

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

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

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

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

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

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

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. |

| Step | Task | Required/Optional | Notes |
|------|--|-------------------|---|
| 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. |
| 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 V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

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.

Upgrade from any version V4.1.0.0 through V4.1.1.1

| 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. |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| 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. |

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

| 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. |

Upgrade from any version V3.5.1 through V3.5.1.10.0

| 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. |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

| 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. |

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

| 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. |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| 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. |

Hazards Analysis Security Groups and Roles

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

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

| Security Group | Roles |
|---------------------|--|
| MI HA Administrator | MI Safety Admin |
| MI HA Owner | MI Safety Admin MI Safety Power |
| MI HA Facilitator | MI Safety Admin MI Safety Power MI Safety User |
| MI HA Member | MI Safety Admin MI Safety Power MI Safety User |

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

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

| Family | MI HA Administrator | MI HA Owner | MI HA Facilitator | MI HA Member |
|------------------------------|------------------------------|------------------------------|------------------------------|--------------|
| Functional Location | View | View | View | View |
| Hazards Analysis | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Hazards Analysis Cause | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Hazards Analysis Consequence | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Hazards Analysis Safeguard | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Hazards Analysis System/Node | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| HAZOP Deviation | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Human Resource | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Independent Protection Layer | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Instrumented Function | View | View | View | View |

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

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

| Family | MI HA Administrator | MI HA Owner | MI HA Facilitator | MI HA Member |
|-------------------------------|------------------------------|------------------------------|------------------------------|--------------|
| 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 |
| 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 |

| Family | MI HA Administrator | MI HA Owner | MI HA Facilitator | MI HA Member |
|--|------------------------------|------------------------------|------------------------------|--------------|
| 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 |
| 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 <i>Checklists</i> 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 <i>Equipment</i> 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 V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V4.0.0.0 through V4.0.1.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

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

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

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

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| 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 <i>Inspection</i> . | 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 and Roles

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

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


| Security Group | Roles |
|----------------|---------------------------------------|
| MI Inspection | MI Mechanical Integrity Administrator |
| | MI Mechanical Integrity Power |
| | MI Mechanical Integrity User |

The baseline family-level privileges that exist for this Security Group is summarized in the following table.

| 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 |


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

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

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

Note that:

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

 **Note:** As part of implementing Inspection Management, you will decide whether you want to link Inspection records to Equipment records, Functional Location records, or both. If you want to link Inspection records to Functional Location records, you will need to grant members of the MI Inspection Security Group at least View privileges to the Functional Location family and the Functional Location Has Equipment relationship family.

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 | <p>Deploy SQL Server Analysis Services on the SQL Server Analysis Server (Version 12 or Version 14) machine. Ensure that the SQL Server Analysis Services machine meets the system requirements.</p> <p>Deploying SQL Server Analysis Services on the SQL Server Analysis Server machine includes the following steps:</p> <ol style="list-style-type: none"> 1. Install SQL Server Analysis Services. 2. Deploy Work History Analysis Services database. <p>This is a replacement of <i>Meridium_Event_Analysis</i> database, and <i>Equipment and Functional Location Work History</i> cubes delivered as packaged solution.</p> <ol style="list-style-type: none"> 3. Create a Windows User on the Analysis Server or in your organization's Active Directory. <p>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:</p> <ul style="list-style-type: none"> • 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 <ol style="list-style-type: none"> 4. Add the user created in Step 3 to a role on all SQL Analysis Services databases you want to access in | Y | <p>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.</p> |

| Step | Task | Required? | Notes |
|------|--|-----------|--|
| | <p>Meridium Enterprise APM software.</p> <p>The role should have read and drill through permissions. Work History database already has a <i>View</i> role defined, you should add the user to this role. For more information, consult the MSDN documentation regarding Roles and Permissions for Analysis Services.</p> <p>5. Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication.</p> <p>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).</p> | | |
| 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 |

| Step | Task | Required? | Notes |
|------|---|-----------|-------|
| 6 | <p>Create Analysis Services Cube records for each cube that has been defined in SQL Server Analysis Services.</p> <p>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.</p> | 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 |

Upgrade Metrics and Scorecards to V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V4.0.0.0 through V4.0.1.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

Metrics and Scorecards will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. However, to upgrade Metric Views, ensure that the user running the upgrade utility has read permissions on the cubes associated to Metric Views and that the cubes are active. Additionally, you need to perform the following steps:

| Step | Task | Required? | Notes |
|------|---|-----------|---|
| 1 | Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: <ul style="list-style-type: none"> • 2012 • 2014 | Y | Required if you were previously using SQL Server Analysis Services 2008 R2. |
| 2 | Configure SQL Server Analysis Server for . | Y | |
| 3 | Update the existing Analysis Services Cube records so that Meridium Enterprise APM connects to cube by using the HTTP/HTTPS access. | Y | |

Upgrade from any version V3.5.1 through V3.5.1.10.0

Metrics and Scorecards will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. However, you need to perform the following additional steps:

| Step | Task | Required? | Notes |
|------|---|-----------|---|
| 1 | Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: <ul style="list-style-type: none"> • 2012 • 2014 | Y | Required if you were previously using SQL Server Analysis Services 2008 R2. |
| 2 | Configure SQL Server Analysis Server for . | Y | |
| 3 | Update the existing Analysis Services Cube records so that Meridium Enterprise APM connects to cube by using the HTTP/HTTPS access. | Y | |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

Metrics and Scorecards will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. However, to upgrade Metric Views, ensure that the user running the upgrade utility has read permissions on the cubes associated to Metric Views and the cubes are active. Additionally, you need to perform the following steps:

| Step | Task | Required? | Notes |
|------|---|-----------|---|
| 1 | Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: <ul style="list-style-type: none"> • 2012 • 2014 | Y | Required if you were previously using SQL Server Analysis Services 2008 R2. |
| 2 | Configure SQL Server Analysis Server for . | Y | |

| Step | Task | Required? | Notes |
|------|---|-----------|-------|
| 3 | Update the existing Analysis Services Cube records so that Meridium Enterprise APM connects to cube by using the HTTP/HTTPS access. | Y | |

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

Metrics and Scorecards will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. However, to upgrade Metric Views, ensure that the user running the upgrade utility has read permissions on the cubes associated to Metric Views and that the cubes are active. Additionally, you need to perform the following steps:

| Step | Task | Required? | Notes |
|------|---|-----------|---|
| 1 | Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: <ul style="list-style-type: none"> • 2012 • 2014 | Y | Required if you were previously using SQL Server Analysis Services 2008 R2. |
| 2 | Configure SQL Server Analysis Server for . | Y | |
| 3 | Update the existing Analysis Services Cube records so that Meridium Enterprise APM connects to cube by using the HTTP/HTTPS access. | Y | |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

Metrics and Scorecards will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. However, to upgrade Metric Views, ensure that the user running the upgrade utility has read permissions on the cubes associated to Metric Views and that the cubes are active. Additionally, you need to perform the following steps:

| Step | Task | Required? | Notes |
|------|---|-----------|---|
| 1 | Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions: <ul style="list-style-type: none"> • 2012 • 2014 | Y | Required if you were previously using SQL Server Analysis Services 2008 R2. |
| 2 | Configure SQL Server Analysis Server for . | Y | |
| 3 | Update the existing Analysis Services Cube records so that Meridium Enterprise APM connects to cube by using the HTTP/HTTPS access. | Y | |

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 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 Server 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 and Roles

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

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

| Security Group | Roles |
|--------------------------|--|
| MI Metrics Administrator | MI Foundation Admin MI APMNow Admin |
| MI Metrics User | MI Foundation Power MI Foundation User |
| Everyone | MI Foundation Admin MI Foundation Power MI Foundation User |

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

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

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

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

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

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.

| 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, start the Policy Execution Service. | Y | If your system architecture contains more than one Meridium Enterprise APM Server , you must complete this step for every server in the load-balanced cluster that you want to use for policy execution. You may review the log files for this service at C:\Program Files\Meridium\Logs . |
| 3 | On the Meridium Enterprise APM Server, start the Policy Trigger Service. | Y | If your system architecture contains more than one Meridium Enterprise APM Server, you must first configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution. You may review the log files for this service at C:\Program Files\Meridium\Logs . |
| 4 | On the Meridium Enterprise APM Server, reset IIS. | Y | None |
| 5 | On the Meridium Process Data Integration Server, start or restart the Process Data Integration Service. | N | Required only if you want to use OPC Tag records in your policies. |

Upgrading Policy Designer to V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

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.

Upgrade from any version V4.1.0.0 through V4.1.1.1

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 1 | On the Meridium Enterprise APM Server, start or restart the Policy Execution Service. | Y | None |
| 2 | If your system architecture contains more than one Meridium Enterprise APM Server, you must first configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution. | Y | None |
| 3 | Start or restart the Policy Trigger Service. | Y | None |
| 4 | On the Meridium Enterprise APM Server, reset IIS. | Y | None |
| 5 | On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service. | N | Required <i>only</i> if you want to use OPC Tag records in your policies. |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| Step | Task | Required? | Notes |
|------|---|-----------|-------|
| 1 | On the Meridium Enterprise APM Server, start or restart the Policy Execution Service. | Y | None |

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 2 | If your system architecture contains more than one Meridium Enterprise APM Server, you must first configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution. | Y | None |
| 3 | Start or restart the Policy Trigger Service. | Y | None |
| 4 | On the Meridium Enterprise APM Server, reset IIS. | Y | None |
| 5 | On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service. | N | Required <i>only</i> if you want to use OPC Tag records in your policies. |

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

| Step | Task | Required? | Notes |
|------|--|-----------|--|
| 1 | On the Meridium Enterprise APM Server, start or restart the Policy Execution Service. | Y | You may review the log files for this service at C:\Program Files\Meridium\Logs . |
| 2 | If your system architecture contains more than one Meridium Enterprise APM Server, you must first configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution. | Y | None |

| Step | Task | Required? | Notes |
|------|--|-----------|--|
| 3 | Start or restart the Policy Trigger Service. | Y | You may review the log files for this service at C:\Program Files\Meridium\Logs . |
| 4 | On the Meridium Enterprise APM Server, reset IIS. | Y | None |
| 5 | On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service. | N | Required <i>only</i> if you want to use OPC Tag records in your policies. |

Upgrade from any version V3.5.1 through V3.5.1.10.0

| Step | Task | Required? | Notes |
|------|--|-----------|--|
| 1 | On the Meridium Enterprise APM Server, start or restart the Policy Execution Service. | Y | You may review the log files for this service at C:\Program Files\Meridium\Logs . |
| 2 | If your system architecture contains more than one Meridium Enterprise APM Server, you must first configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution. | Y | None |
| 3 | Start or restart the Policy Trigger Service. | Y | You may review the log files for this service at C:\Program Files\Meridium\Logs . |
| 4 | On the Meridium Enterprise APM Server, reset IIS. | Y | None |

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 5 | On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service. | N | Required <i>only</i> if you want to use OPC Tag records in your policies. |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

| Step | Task | Required? | Notes |
|------|--|-----------|--|
| 1 | On the Meridium Enterprise APM Server, start or restart the Policy Execution Service. | Y | You may review the log files for this service at C:\Program Files\Meridium\Logs . |
| 2 | If your system architecture contains more than one Meridium Enterprise APM Server, you must first configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution. | Y | None |
| 3 | Start or restart the Policy Trigger Service. | Y | You may review the log files for this service at C:\Program Files\Meridium\Logs . |
| 4 | On the Meridium Enterprise APM Server, reset IIS. | Y | None |
| 5 | On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service. | N | Required <i>only</i> if you want to use OPC Tag records in your policies. |

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

| Step | Task | Required? | Notes |
|------|--|-----------|--|
| 1 | On the Meridium Enterprise APM Server, start or restart the Policy Execution Service. | Y | You may review the log files for this service at C:\Program Files\Meridium\Logs . |
| 2 | If your system architecture contains more than one Meridium Enterprise APM Server, you must first configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution. | Y | None |
| 3 | Start or restart the Policy Trigger Service. | Y | You may review the log files for this service at C:\Program Files\Meridium\Logs . |
| 4 | On the Meridium Enterprise APM Server, reset IIS. | Y | None |
| 5 | On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service. | N | Required <i>only</i> if you want to use OPC Tag records in your policies. |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Required? | Notes |
|------|---|-----------|--|
| 1 | On the Meridium Enterprise APM Server, start or restart the Policy Execution Service. | Y | You may review the log files for this service at C:\Program Files\Meridium\Logs . |

| Step | Task | Required? | Notes |
|------|--|-----------|--|
| 2 | If your system architecture contains more than one Meridium Enterprise APM Server, you must first configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution. | Y | None |
| 3 | Start or restart the Policy Trigger Service. | Y | You may review the log files for this service at C:\Program Files\Meridium\Logs . |
| 4 | On the Meridium Enterprise APM Server, reset IIS. | Y | None |
| 5 | On the Meridium Process Data Integration Server, start (or restart if it is already started) the Process Data Integration Service. | N | Required <i>only</i> if you want to use OPC Tag records in your policies. |

About the Asset Health Services

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

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

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

Services Summary

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

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

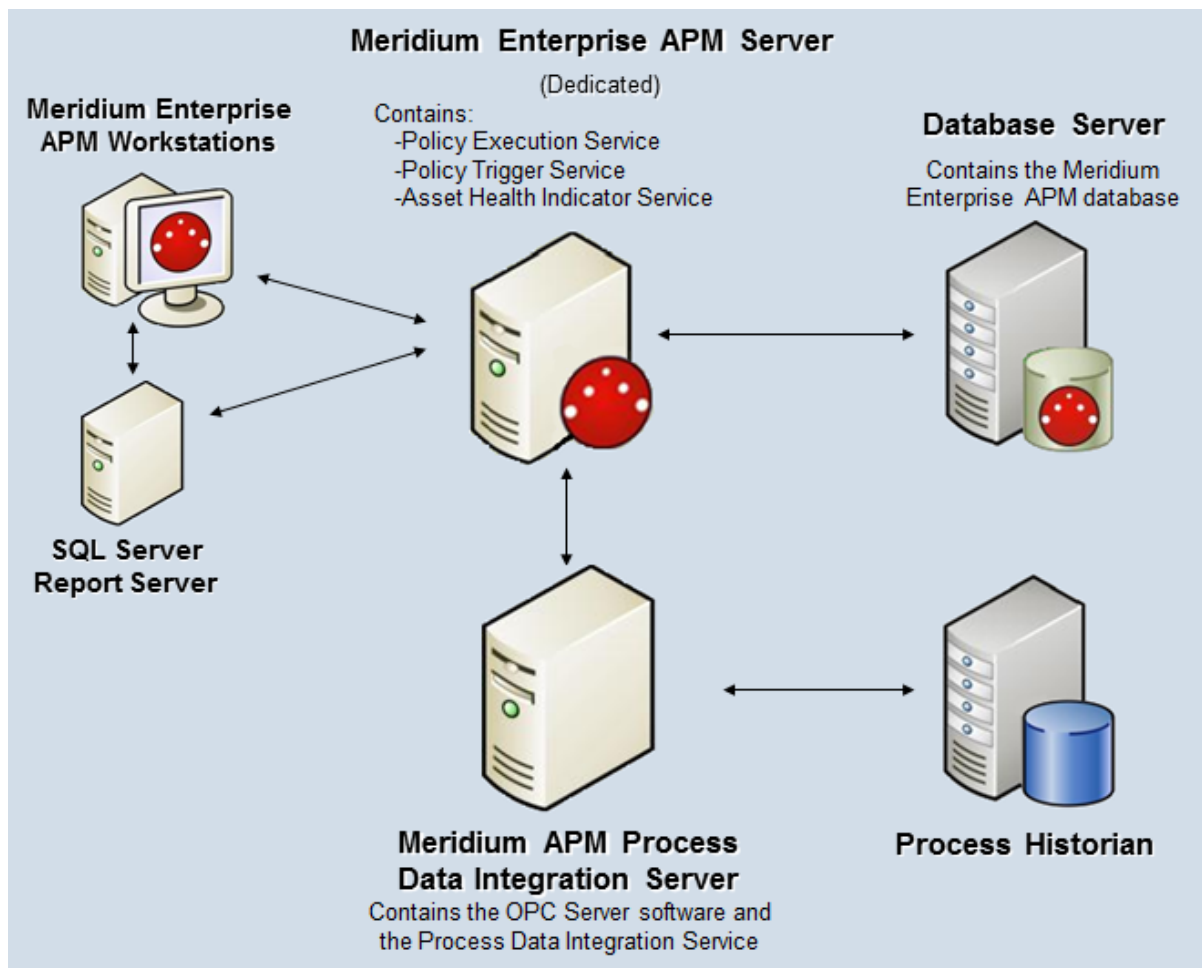
This service also facilitates the automatic creation of Health Indicator records for configured sources.

- **Policy Trigger Service:** When an input to a policy (i.e., an associated record in the Meridium Enterprise APM database or reading value in the process historian) changes or when a policy schedule is due, a message is added to the policy trigger queue. The Policy Trigger Service monitors this queue and sends these messages to an appropriate policy execution queue.
- **Policy Execution Service:** The Meridium Enterprise APM Policy Execution Service handles the execution of policies. Specifically, the Policy Execution Service monitors a corresponding policy execution queue and executes the policies that are added to it.
- **Process Data Integration (PDI) Service:** Monitors the subscribed tags (i.e., tags that are used in policies and health indicators or tags for which readings are being stored in the Meridium database) and, when data changes occur on these tags, adds messages to the appropriate queues. This service also facilitates the automatic import and synchronization of tags from a configured process historian.

Example: Standard System Architecture Configuration

The following diagram illustrates the machines in the Meridium Enterprise APM system architecture when the Policy Designer, Process Data Integration (PDI), and Asset Health Manager (AHM) modules are used together. This image depicts the standard configuration, where the OPC Server software and the Process Data Integration Service are on the *same* machine.

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




The following table summarizes the machines illustrated in this diagram and the software and services that you will install when you complete the first-time deployment steps for [Asset Health Manager](#), [Policy Designer](#), and [Process Data Integration](#).

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

About Configuring Policy Execution

Policy designers can configure a policy to be executed on a schedule or automatically when records or reading values associated with the policy are updated. This topic describes the ways that the items configured in the [first-time deployment workflow](#) facilitate each type of policy execution.

 **Note:** Only the *active instances* of *active policies* are executed.

Automatic Execution

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

Scheduled Execution

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

Configure the Policy Trigger Service

Steps

1. On the Meridium Enterprise APM Server, navigate to the folder where the Policy Trigger Service files are installed. If you installed the software in the default location, you can locate this file in the folder **C:\Program Files\Meridium\Services**.
2. Open the file **Meridium.Policies.Service.exe.config** in an application that you can use to modify XML script (e.g., Notepad).
3. Within the **<executionServers>** tags, locate the following text:

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

4. Within the **add url** attribute:
 - If you have only one Meridium Enterprise APM Server in your system architecture, accept the default value (i.e., *localhost*).
 - or-
 - If you have [more than one Meridium Enterprise APM Server in your system architecture](#), replace **localhost** with the name of the server cluster that you want to use for policy executions.
5. Save and close the file.

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

Configure Multiple Meridium Enterprise APM Servers for Policy Execution

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

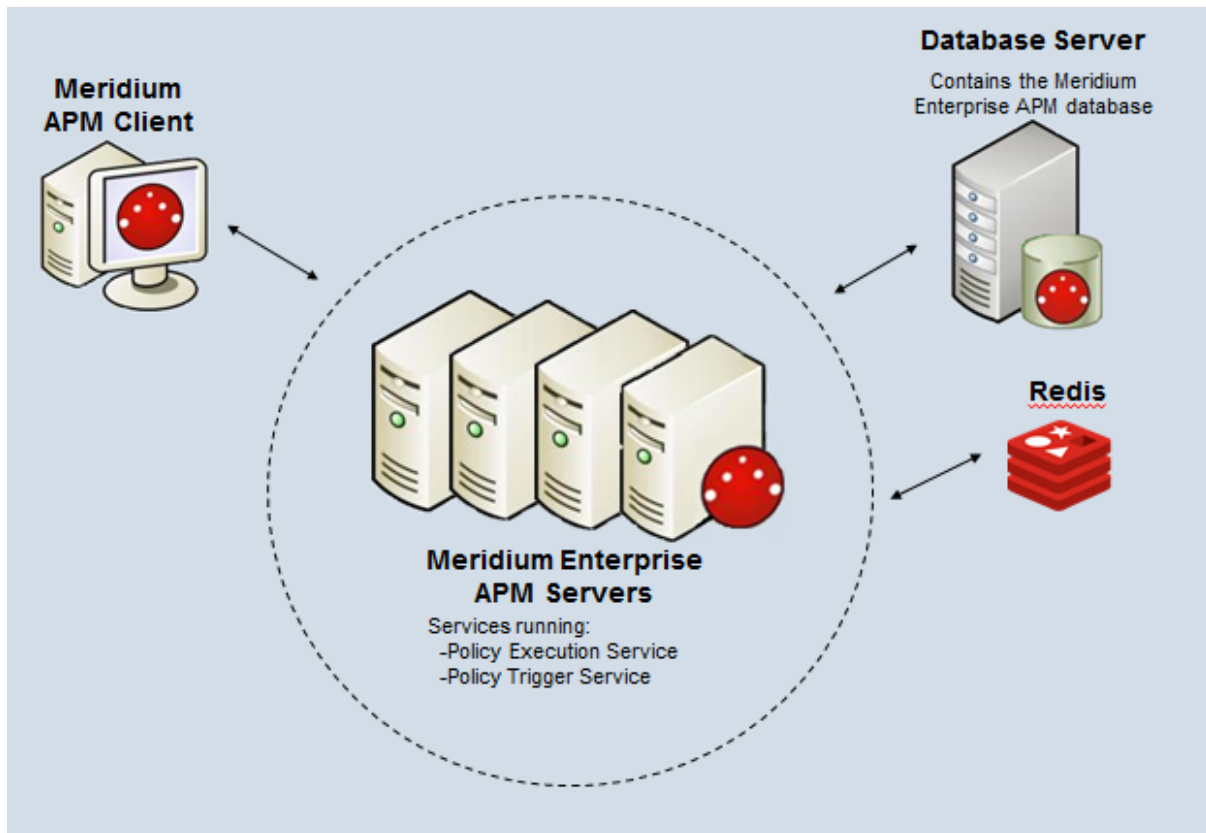
Regardless of the approach you use, you must fully configure each Meridium Enterprise APM Server according to the steps for deploying the basic Meridium Enterprise APM system architecture. In addition, each Meridium Enterprise APM Server must be configured to use the same instance of Redis.

Global Load Balancing

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

In this scenario, you must:

- [Configure the Policy Trigger service](#) on all Meridium Enterprise APM Servers to specify the name of the cluster.
- Start the Policy Execution Service on all Meridium Enterprise APM Servers.

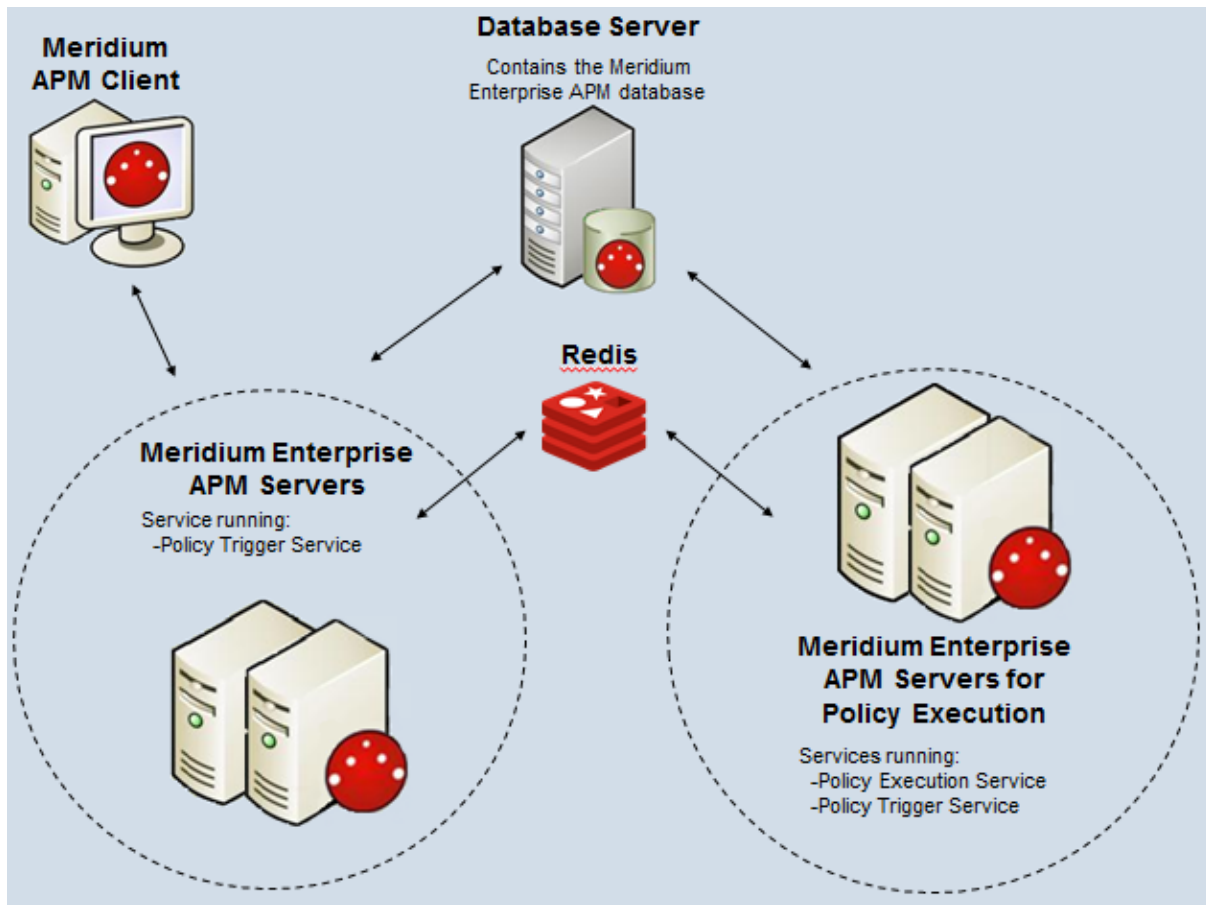


Isolated Load Balancing

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

In this scenario, you must:

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



Policy Designer Security Groups and Roles

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

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

| Security Group | Roles |
|--------------------|------------------------------------|
| MI Policy Designer | MI Health Power MI Health Admin |
| MI Policy User | MI Health User |
| MI Policy Viewer | None |

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

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


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 |

| Step | Task | Required? | Notes |
|------|---|-----------|---|
| 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. |
| 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. You may review the log files for this service at C:\Program Files\Meridium\Logs . |
| 8 | On the Meridium Enterprise APM Server, configure the Meridium Notification Service for PDI. | Y | None |
| 9 | On the Meridium Enterprise APM Server, start or restart the Meridium Notification Service. | Y | You may review the log files for this service at C:\ProgramData\Meridium . |
| 10 | Review the Process Data Integration data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. | 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 V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

| 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 |

| Step | Task | Required? | Notes |
|------|--|-----------|-------|
| 6 | In Meridium Enterprise APM, link any new OPC Tag records to related asset records. | Y | None |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| 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 |

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

| 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 | <p>When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records.</p> <p>You may review the log files for this service at C:\Program Files\Meridium\Logs.</p> |
| 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 | You may review the log files for this service at C:\ProgramData\Meridium . |
| 6 | In Meridium Enterprise APM, link any new OPC Tag records to related asset records. | Y | None |

Upgrade from any version V3.5.1 through V3.5.1.10.0

| 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 | <p>When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records.</p> <p>You may review the log files for this service at C:\Program Files\Meridium\Logs.</p> |
| 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 | You may review the log files for this service at C:\ProgramData\Meridium . |
| 6 | In Meridium Enterprise APM, link any new OPC Tag records to related asset records. | Y | None |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

| 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 | <p>When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records.</p> <p>You may review the log files for this service at C:\Program Files\Meridium\Logs.</p> |
| 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 | You may review the log files for this service at C:\ProgramData\Meridium . |
| 6 | In Meridium APM, link any new OPC Tag records to related asset records. | Y | None |

Upgrade from any version V3.5.0 through V3.5.0.0.7.2


| 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 | <p>When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records.</p> <p>You may review the log files for this service at C:\Program Files\Meridium\Logs.</p> |
| 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 | <p>You may review the log files for this service at C:\ProgramData\Meridium.</p> |
| 6 | In Meridium APM, link any new OPC Tag records to related asset records. | Y | None |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| 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 | <p>When you start the service, tags from the configured process historian are imported automatically into the Meridium Enterprise APM database as OPC Tag records.</p> <p>You may review the log files for this service at C:\Program Files\Meridium\Logs.</p> |
| 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 | You may review the log files for this service at C:\ProgramData\Meridium . |
| 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 the following field values in a Health Indicator record when reading values related to the health indicator source record (e.g., an OPC Tag or Measurement Location record) change:
 - Alert Level
 - Last Reading Date
 - Last Char Reading Value (for records that accept character values)
 - Last Numeric Reading Value (for records that accept numeric values)

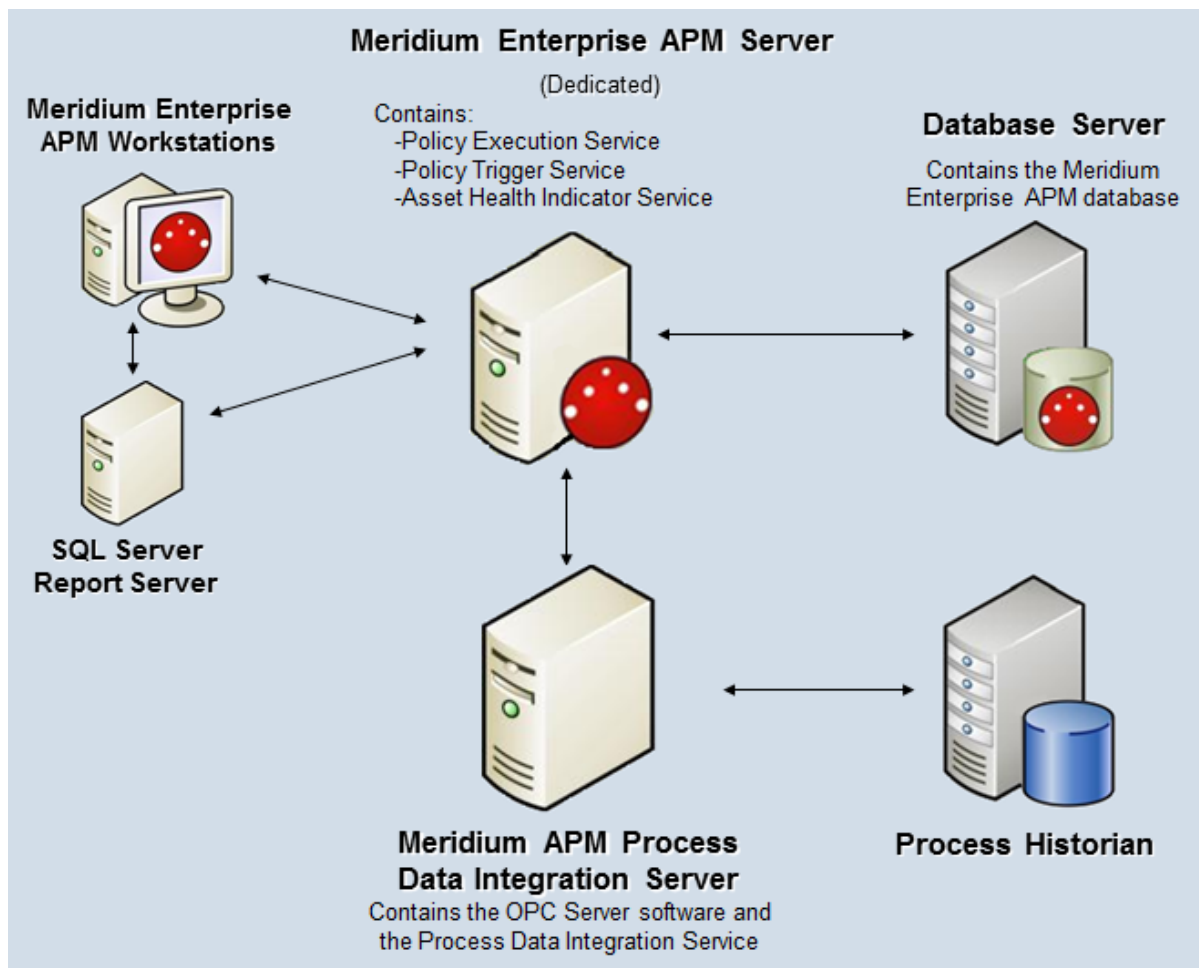
This service also facilitates the automatic creation of Health Indicator records for configured sources.

- **Policy Trigger Service:** When an input to a policy (i.e., an associated record in the Meridium Enterprise APM database or reading value in the process historian) changes or when a policy schedule is due, a message is added to the policy trigger queue. The Policy Trigger Service monitors this queue and sends these messages to an appropriate policy execution queue.
- **Policy Execution Service:** The Meridium Enterprise APM Policy Execution Service handles the execution of policies. Specifically, the Policy Execution Service monitors a corresponding policy execution queue and executes the policies that are added to it.
- **Process Data Integration (PDI) Service:** Monitors the subscribed tags (i.e., tags that are used in policies and health indicators or tags for which readings are being stored in the Meridium database) and, when data changes occur on these tags, adds messages to the appropriate queues. This service also facilitates the automatic import and synchronization of tags from a configured process historian.

Example: Standard System Architecture Configuration

The following diagram illustrates the machines in the Meridium Enterprise APM system architecture when the Policy Designer, Process Data Integration (PDI), and Asset Health Manager (AHM) modules are used together. This image depicts the standard configuration, where the OPC Server software and the Process Data Integration Service are on the *same* machine.

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



The following table summarizes the machines illustrated in this diagram and the software and services that you will install when you complete the first-time deployment steps for [Asset Health Manager](#), [Policy Designer](#), and [Process Data Integration](#).

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

Install the Process Data Integration Service

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

Steps

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

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

The **Welcome** screen appears.

3. Select **Next**.

The **License Agreement** screen appears.


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

The **Select Installation Location** screen appears.

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

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

6. Select the **Meridium Process Data Integration Service** option.

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

7. Select **Next**.

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

- If one or more prerequisites are missing on the machine, a dialog box will appear, explaining which prerequisites are missing. If this occurs, close the installer, install the missing prerequisite, and then run the installer again.
- If all the prerequisites for the selected components are installed on the machine, or you have selected components that do not require any prerequisites, the **Complete the Installation** screen appears.

8. Select **Install**.

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

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

9. Select **Finish**.

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

Upgrade the Process Data Integration Service

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

Steps

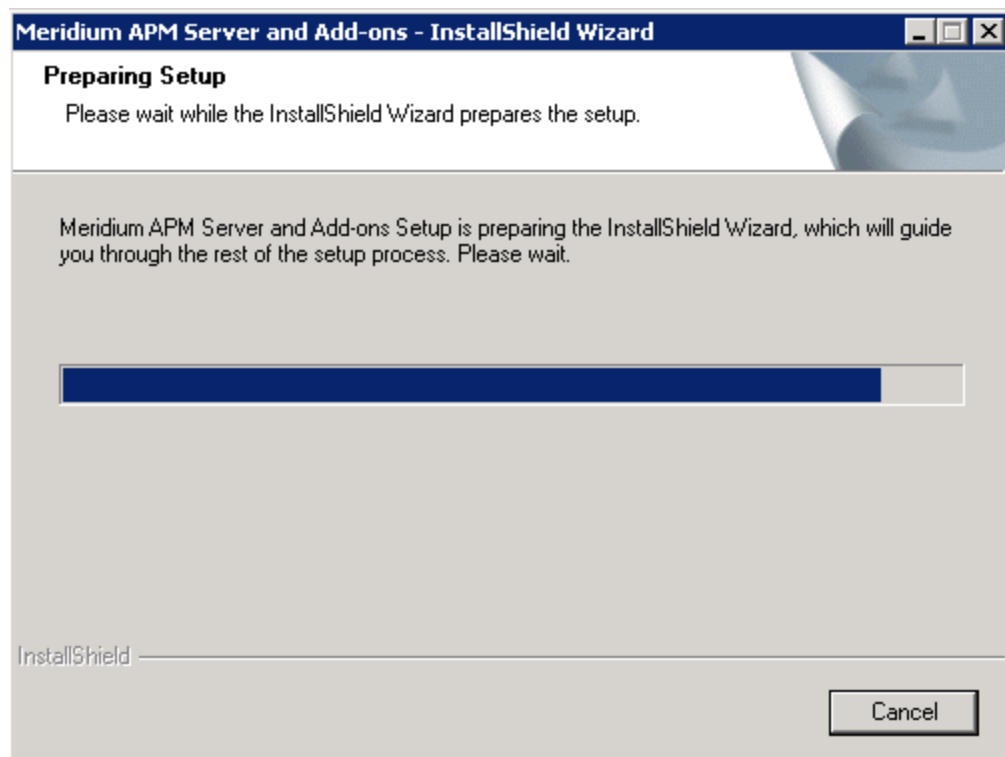
1. On the machine that will serve as the Meridium Process Data Integration Server, access the Meridium Enterprise APM distribution package, and then navigate to the folder **\\Setup\\Meridium Enterprise APM Server and Add-ons**.

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

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

3. Select **Yes**.

The **Meridium Enterprise APM Server and Add-ons** installer appears, displaying the **Preparing Setup** screen. The **Preparing Setup** screen contains a progress bar that indicates when the installer is ready to upgrade the components on your machine.



When the progress bar reaches the end, a message appears, asking if you want to upgrade your server.

4. Select **Yes**.

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

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

5. Select **Finish**.

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

Configure the Meridium Notification Service for PDI

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

Steps

1. On the Meridium Enterprise APM Server, navigate to the folder where the Meridium Notification Service files are installed. If you installed the software in the default location, you can locate these files in the folder **C:\Program Files\Meridium\Services**.
2. Open the file **Meridium.Service.Notification.exe.config** in an application that you can use to modify XML script (e.g., Notepad).
3. If you have not done so already, complete any necessary basic configuration for the Meridium Notification Service.

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

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

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

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

6. Within the **address** attribute, replace **PDISERVERNAME** with the name or IP Address of the Process Data Integration Server.
7. If you have only one Process Data Integration Server in your system architecture, save and close the file.

-or

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

- a. Copy the string within the **<notificationSettings>** tags that you uncommented in Step 4.
- b. Directly after the text that you copied (after the **/>**), paste the copied text.
- c. Within the **key** attribute, specify a unique name for the connection.

- d. Within the **endPointName** attribute, specify a unique name for the end point.
- e. Copy the string within the **<client>** tags that you uncommented in Step 5.
- f. Within the **name** attribute, enter the name for the endpoint that you specified in Step d.
- g. Modify the **address** attribute to specify the name or IP Address of the additional Process Data Integration Server.
- h. Save and close the file.

8. Start or restart the Meridium Notification Service.

Example

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

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

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

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


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

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

Configure the Process Data Integration Service

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

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

 **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 |

| Process Historian | OPCDA | OPCHDA |
|--|---------------------|---------------------|
| MatrikonOPC HDA Server for IP21* | Matrikon.OPC.IP21.1 | Matrikon.OPC.IP21.1 |
| Honeywell Uni-formance® 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. |

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

12. Save and close the file.


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

Configure Multiple Data Sources

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

Steps

1. Configure the first connection by modifying the attributes within **<meridiumConnections>** tags, as described in the instructions for [configuring the Process Data Integration Service](#).
2. Copy the text within the **<meridiumConnections>** tags (e.g., `<connection name="CONNECTION 1" applicationServer="" datasource="DATASOURCE_NAME" userId="SERVICE_USER_NAME" password="!PaSsWoRd" />`)
3. Directly after the text that you copied (after the `/>`), paste the copied text.
4. Modify the attributes as needed.

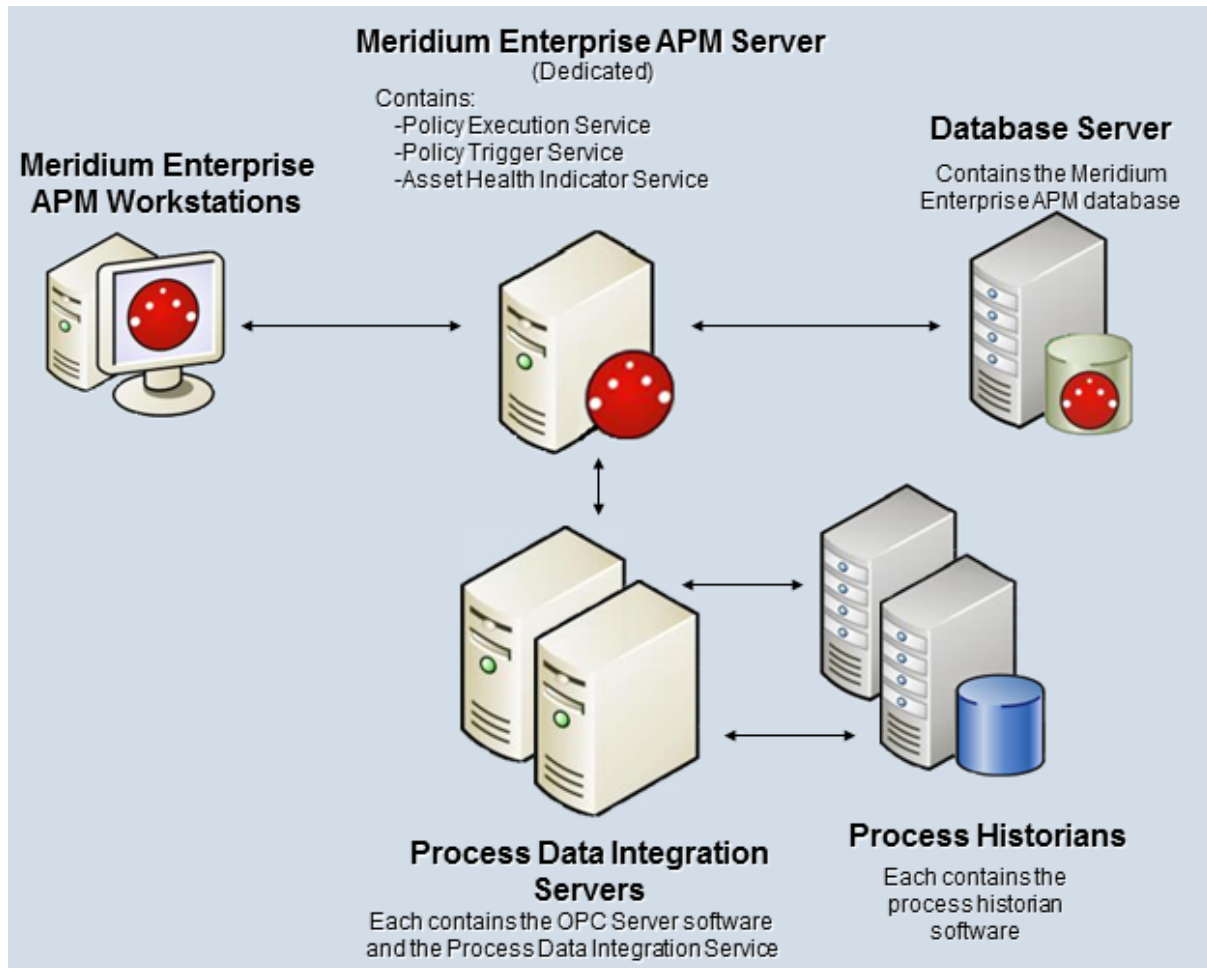
 **Note:** The connection name that you specify in each connection string must be unique.

5. Repeat these steps for each required connection.

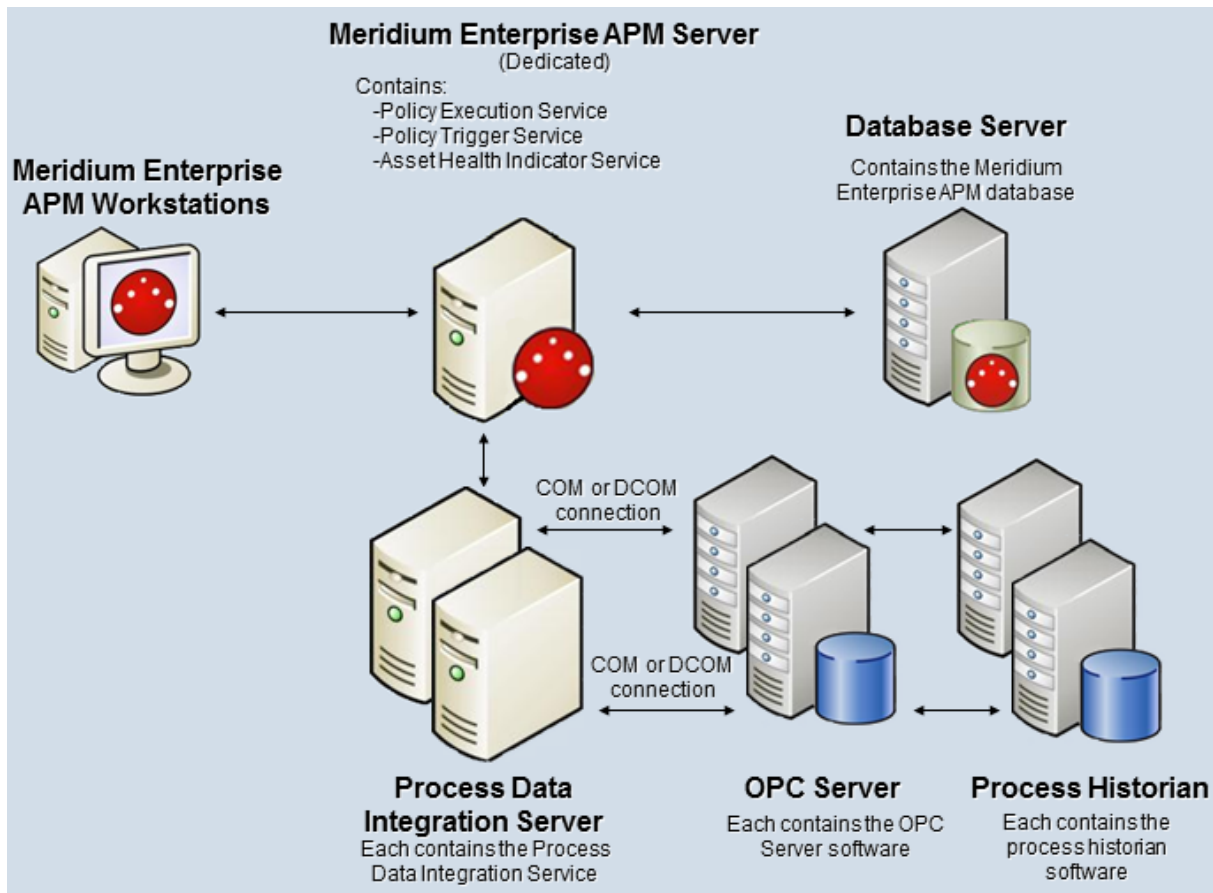
Configure Multiple Process Data Integration and OPC Servers

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

The following diagram illustrates multiple OPC Servers in the standard configuration where the OPC Server is the same machine as the Process Data Integration (PDI) Server (i.e., the OPC Server software is installed on the PDI Server).



The following diagram illustrates multiple OPC Servers in an alternative configuration where the OPC Servers are separate machines from the PDI Servers.



In either of these scenarios, when you complete the [first-time deployment steps for PDI](#), you must install and configure the Process Data Integration Service on *each* Process Data Integration Server machine.

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

- On the first Process Data Integration Server: `<connection name="EXAMPLE_CONNECTION" applicationServer="APPSERVER_NAME" data-source="DATASOURCE_NAME" userId="SERVICE_USER_NAME" password="!PaSsWoRd" xiServers="OPCSystem1" />`
- On the second Process Data Integration Server: `<connection name="EXAMPLE_CONNECTION" applicationServer="APPSERVER_NAME" data-source="DATASOURCE_NAME" userId="SERVICE_USER_NAME" password="!PaSsWoRd" xiServers="OPCSystem2" />`

Process Data Integration Security Groups and Roles

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

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

| Security Group | Roles |
|---|-----------------------------------|
| MI Process Data Integration Administrator | MI Health Admin |
| MI Process Data Integration Service | None |
| MI Process Data Integration User | MI Health User MI Health Power |

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: <ul style="list-style-type: none"> • 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 <i>Product</i> record. |

| Step | Task | Notes |
|------|------------------------------|---|
| 5 | Define production units . | <p>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.</p> <p>Each production unit is stored in a <i>Production Unit</i> record, which can be linked to an existing Functional Location record that contains more detailed information about the production unit.</p> |
| 6 | Define production profiles . | <p>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.</p> <p>Each production profile is stored in a <i>Production Profile</i> record, which is linked to the corresponding Product record and Production Unit record.</p> |

| Step | Task | Notes |
|------|---------------------------------|---|
| 7 | Define production event codes . | <p>The baseline Meridium Enterprise APM database contains <i>Production Event Code</i> 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.</p> <p>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: <i>Why are we losing production?</i> 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).</p> <p>Each event type will be stored in a separate <i>Production Event Code</i> record.</p> |
| 8 | Define impact codes . | <p>The baseline Meridium Enterprise APM database contains <i>Impact Code</i> 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.</p> |

| Step | Task | Notes |
|------|---|--|
| 9 | Define OEE codes . | The baseline Meridium Enterprise APM database contains <i>OEE Code</i> records that define a set of basic OEE codes. Therefore, this step is required only if you do not want to use the baseline OEE codes or if you want to use codes in addition to those that are provided. For non-baseline codes to be included in the OEE Metric View, however, they must be children of the baseline parent codes. |
| 10 | Define values that will be mapped to a Production Analysis . | 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: <ul style="list-style-type: none"> • 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. |
| 12 | Replace the Top 10 Bad Actors query for the PLA Overview page. | This task is optional. The Top 10 Bad Actors query is used by Meridium Enterprise APM to populate the Top 10 Bad Actors graph on the Production Loss Analysis Overview page . In some databases, when viewing this graph, you may receive an error that prevents the graph from populating correctly. If this error occurs, replace the Top 10 Bad Actors query. |

Upgrading Production Loss Analysis (PLA) to V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

| Step | Task | Notes |
|------|---|---|
| 1 | Replace the Top 10 Bad Actors query for the PLA Overview page. | This task is optional. The Top 10 Bad Actors query is used by Meridium Enterprise APM to populate the Top 10 Bad Actors graph on the Production Loss Analysis Overview page . In some databases, when viewing this graph, you may receive an error that prevents the graph from populating correctly. If this error occurs, replace the Top 10 Bad Actors query . |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| Step | Task | Notes |
|------|---|---|
| 1 | Replace the Top 10 Bad Actors query for the PLA Overview page. | This task is optional. The Top 10 Bad Actors query is used by Meridium Enterprise APM to populate the Top 10 Bad Actors graph on the Production Loss Analysis Overview page . In some databases, when viewing this graph, you may receive an error that prevents the graph from populating correctly. If this error occurs, replace the Top 10 Bad Actors query . |

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

| Step | Task | Notes |
|------|---|--|
| 1 | On the Meridium Enterprise APM Server, import the required baseline rules . | <p>⚠ IMPORTANT: This procedure must be completed <i>before</i> upgrading the Meridium Enterprise APM Server and Add Ons software on the Meridium Enterprise APM Server(s). After completing this procedure, you should return to the upgrade Meridium Enterprise APM workflow. After completing this procedure and the remainder of the upgrade Meridium Enterprise APM workflow, when you are ready to upgrade PLA, proceed to step 2 in this workflow.</p> |
| 2 | 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. |
| 3 | Set the timezones for the Production Units. | <p>If the timezones for the Production Units are set, all the Production Plan records, Plan Data records, and Production Target records will be updated based on the timezone for the respective Production Unit.</p> <p>Note: Since the date and time in PLA is now stored in UTC format, you <i>must</i> set the timezone for each Production Unit before upgrade.</p> <ul style="list-style-type: none"> • If you do not set the timezones for the Production Units, and if the Production Plan records exist in the database, the Production Plan records, Plan Data records, and Production Target records will be updated based on the timezone of the user who last modified the Production Plan record. • If you do not set the timezones for the Production Units, and if the Production Plan records do not exist in the database, the timezone for the Production Unit will be updated based on the timezone of the user who last modified the Production Unit record. |

Upgrade from any version V3.5.1 through V3.5.1.10.0

| Step | Task | Notes |
|------|---|---|
| 1 | On the Meridium Enterprise APM Server, import the required baseline rules . | ⚠ IMPORTANT: This procedure must be completed <i>before</i> upgrading the Meridium Enterprise APM Server and Add-on software on the Meridium Enterprise APM Server(s). After completing this procedure, you should return to the upgrade Meridium Enterprise APM workflow. After completing this procedure and the remainder of the upgrade Meridium Enterprise APM workflow, when you are ready to upgrade PLA, proceed to step 2 in this workflow. |
| 2 | Confirm the deployment of the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server. | 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. |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

| Step | Task | Notes |
|------|---|--|
| 1 | On the Meridium Enterprise APM Server, import the required baseline rules . | ⚠ IMPORTANT: This procedure must be completed <i>before</i> upgrading the Meridium Enterprise APM Server and Add Ons software on the Meridium Enterprise APM Server(s). After completing this procedure, you should return to the upgrade Meridium Enterprise APM workflow. After completing this procedure and the remainder of the upgrade Meridium Enterprise APM workflow, when you are ready to upgrade PLA, proceed to step 2 in this workflow. |

| Step | Task | Notes |
|------|---|---|
| 2 | 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. |

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

| Step | Task | Notes |
|------|---|--|
| 1 | On the Meridium Enterprise APM Server, import the required baseline rules . | ⚠ IMPORTANT: This procedure must be completed <i>before</i> upgrading the Meridium Enterprise APM Server and Add Ons software on the Meridium Enterprise APM Server(s). After completing this procedure, you should return to the upgrade Meridium Enterprise APM workflow. After completing this procedure and the remainder of the upgrade Meridium Enterprise APM workflow, when you are ready to upgrade PLA, proceed to step 2 in this workflow. |
| 2 | Confirm the deployment of the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server. | 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. |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Notes |
|------|---|---|
| 1 | On the Meridium Enterprise APM Server, import the required baseline rules . | ⚠ IMPORTANT: This procedure must be completed <i>before</i> upgrading the Meridium Enterprise APM Server and Add-on software on the Meridium Enterprise APM Server(s). After completing this procedure, you should return to the upgrade Meridium Enterprise APM workflow. After completing this procedure and the remainder of the upgrade Meridium Enterprise APM workflow, when you are ready to upgrade PLA, proceed to step 2 in this workflow. |
| 2 | Define OEE codes . | 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. |
| 3 | Define values that will be mapped to a Production Analysis . | By default, certain PLA values are mapped to the production data in a Production Analysis. If you want to map different or additional PLA values, you can do so by modifying the All Production Data query. |
| 4 | Confirm the deployment of the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server. | 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. |

Import Baseline Rules

Note: If you are upgrading Production Loss Analysis from a starting version that is earlier than V4.0.0.0, this procedure must be completed *before* upgrading the Meridium Enterprise APM Server and Add Ons software on the Meridium Enterprise APM Server(s). This procedure is part of the upgrade Meridium Enterprise APM and [upgrade Production Loss Analysis](#) workflows.

Before You Begin

- Acquire a copy of the baseline Meridium Enterprise APM database whose version number matches the version number of your current, pre-upgraded database. If you do not have access to the appropriate baseline database, consult a member of the Meridium, Inc. Professional Services department.

Steps

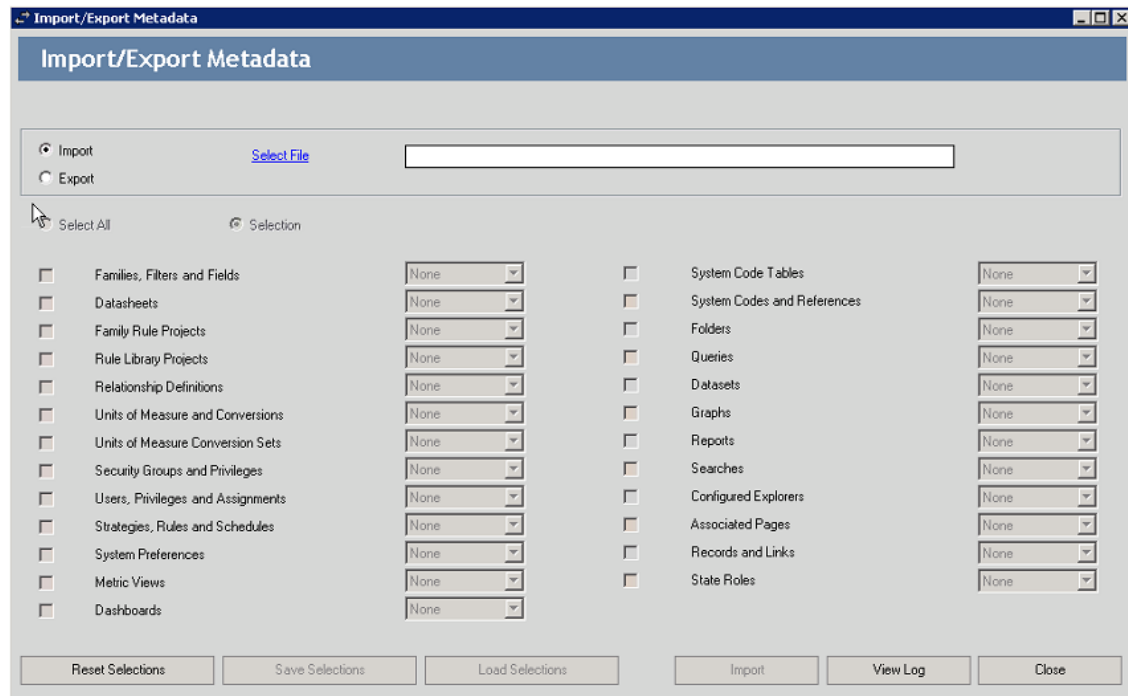
- On the Meridium Enterprise APM Server machine, via the Windows start button, access Configuration Manager.

The **Meridium APM Login** window appears.

- Enter your User ID and Password into the appropriate boxes, and then, in the **Data Source** box, select the baseline Meridium Enterprise APM database whose version number matches the version number of your current, pre-upgraded database.
- Select **Login**.
Configuration Manager opens.
- On the top navigation bar, select **Tools**, and then select **Import/Export Meridium**

Metadata.

The **Import/Export Metadata** window appears.

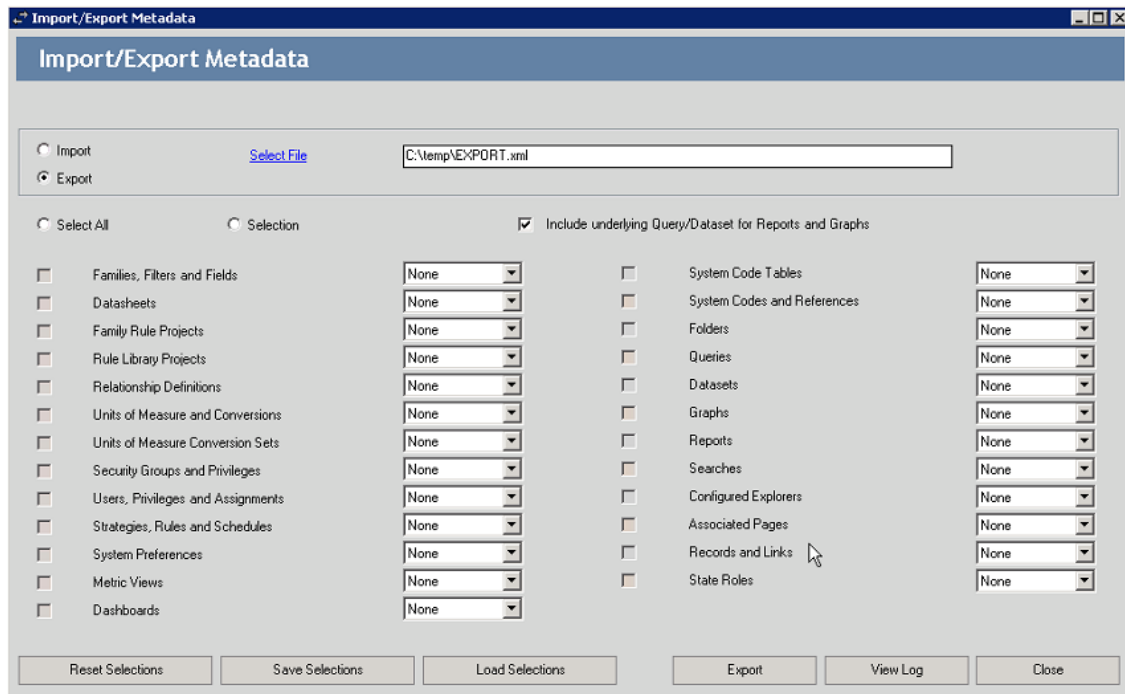


5. Select the **Export** check box, and then select **Select File**.

The **Save As** window appears.

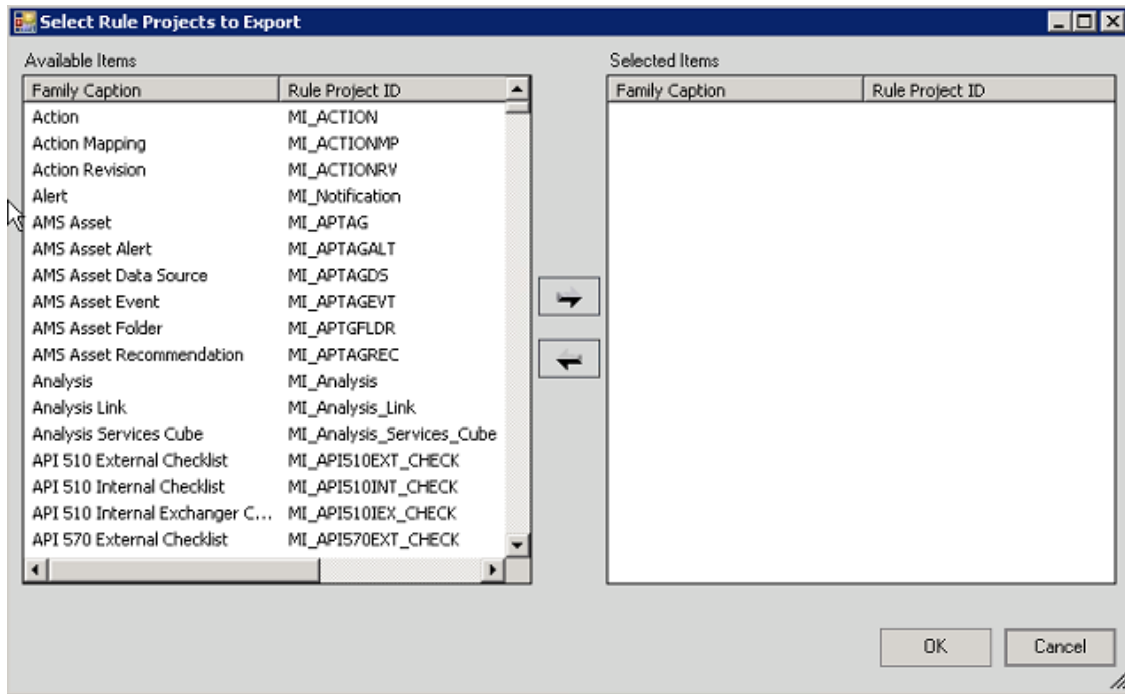
6. Navigate to the location where you want to save the exported metadata, then enter a name in the **File name:** box, and then select **Save**.


The **Save As** window closes, and the selected filepath is displayed in the **Select File** box on the **Import/Export Metadata** window.




7. Select the **Selection** check box.
8. In the drop-down list box to the right of the **Family Rule Projects** check box, select **Some**.

The **Select Rule Projects to Export** window appears.

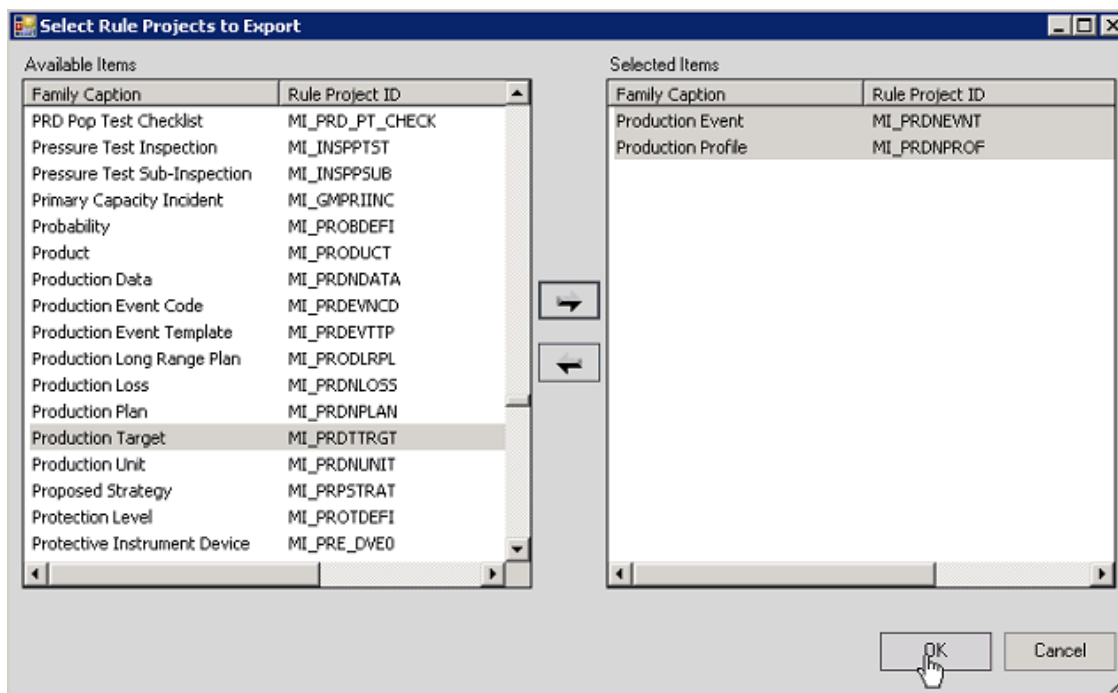


9. In the **Available Items** section, select the item whose Family Caption is Production Event, and then select .

The selected item appears in the **Selected Items** section.

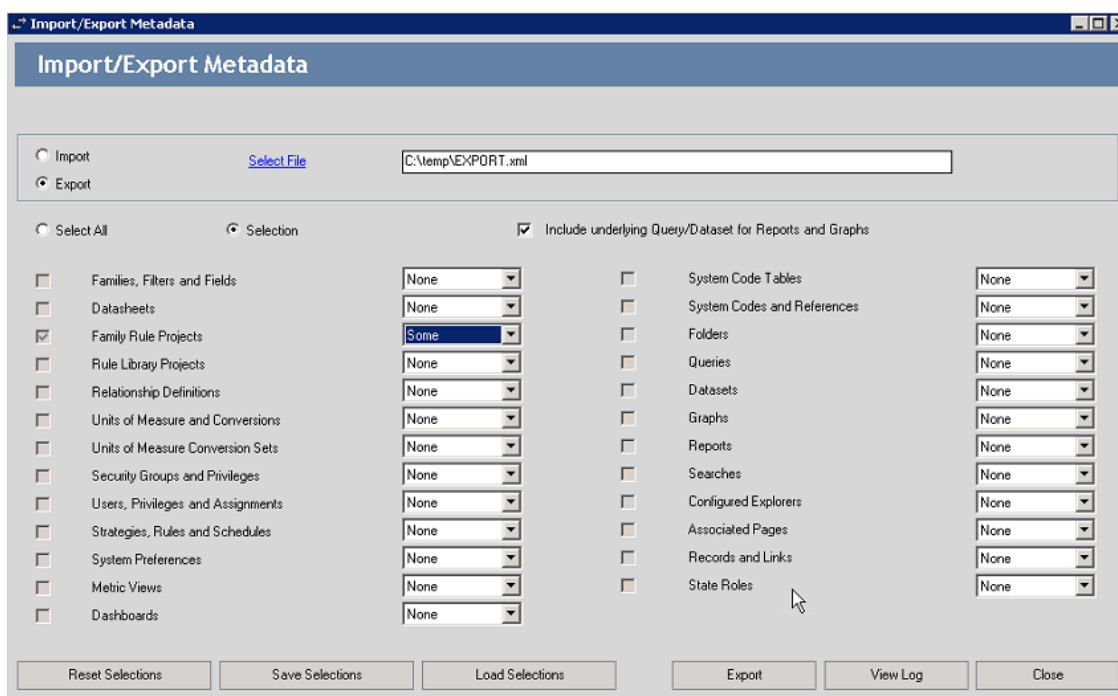
10. In the **Available Items** section, select the item whose Family Caption is Production Profile, and then select .

The selected item appears in the **Selected Items** section.



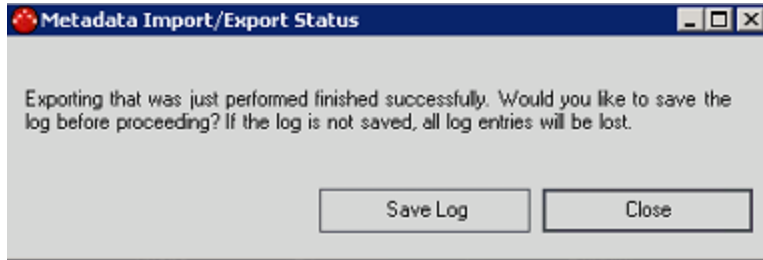
11. Select OK.

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



12. Select **Export**.

The **Metadata Import/Export Status** dialog box appears, displaying a progress bar. When the export is complete, a message appears, asking if you want to save the log.



13. Select **Save Log**.

The **Save As** window appears.

14. Navigate to the location where you want to save the export log, then enter a name in the **File name:** box, and then select **Save**.

The **Save As** window closes.

15. On the **Metadata Import/Export Status** dialog box, select **Close**.

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

16. On the **Import/Export Metadata** window, select **Close**.

The **Import/Export Metadata** window closes.

17. In Configuration Manager, on the top navigation bar, select **File**, and then select **LogOff**.

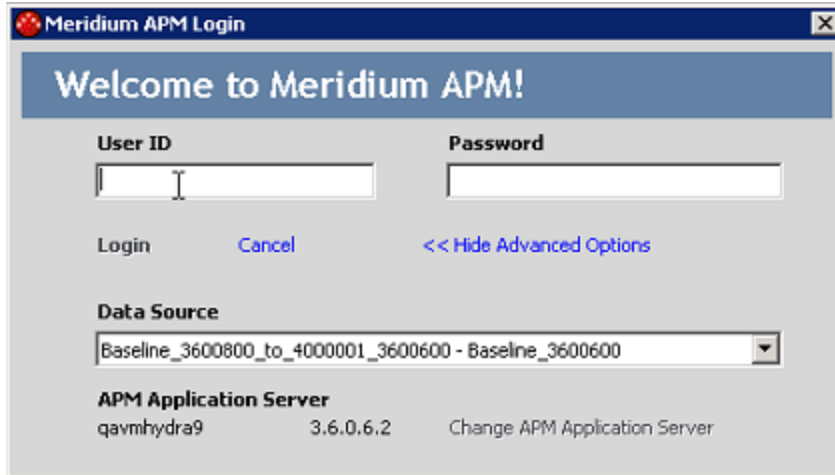
A dialog box appears, asking if you are sure that you want to log off.

18. Select **OK**.

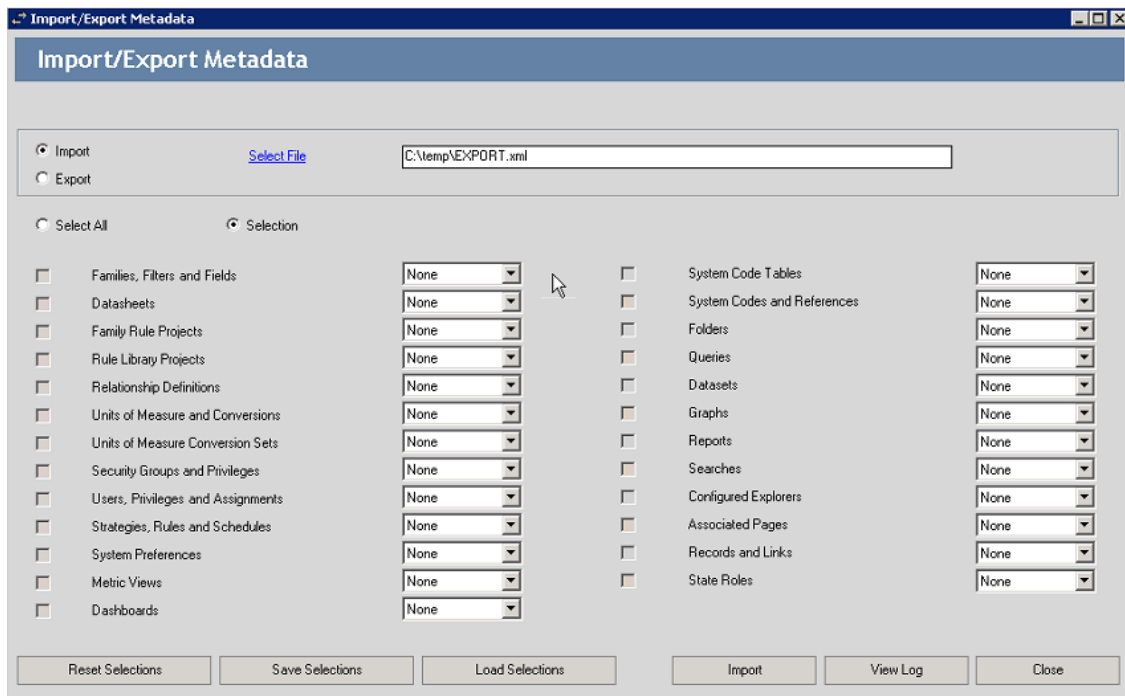
Configuration Manager closes.

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

The **Meridium APM Login** window appears.

The image shows a screenshot of the 'Meridium APM Login' window. The window has a title bar with the text 'Meridium APM Login' and a close button. Below the title bar is a blue header area with the text 'Welcome to Meridium APM!'. The main area is light gray and contains several fields and buttons. There are two input fields: 'User ID' and 'Password'. Below these fields are three buttons: 'Login', 'Cancel', and '<< Hide Advanced Options'. Below the buttons is a 'Data Source' section with a dropdown menu showing 'Baseline_3600800_to_4000001_3600600 - Baseline_3600600'. At the bottom, there is an 'APM Application Server' section with the text 'qavmhydra9 3.6.0.6.2' and a link 'Change APM Application Server'.

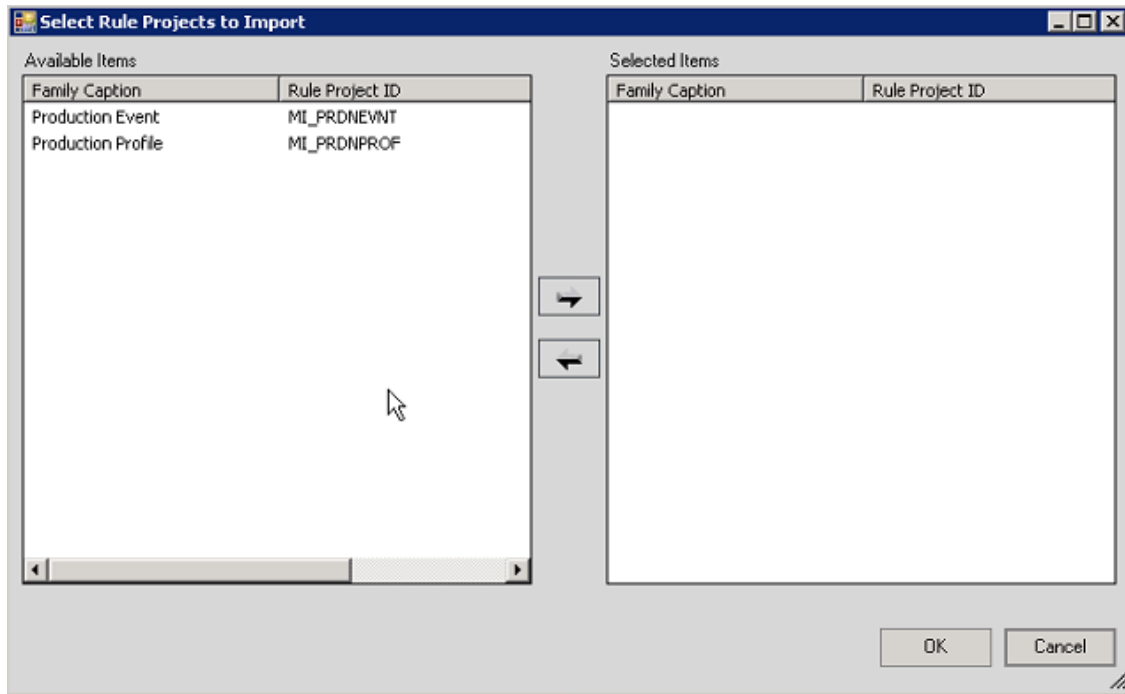
20. Enter your User ID and Password into the appropriate boxes, and then, in the **Data Source** box, select your current, pre-upgraded database.
21. Select **Login**.
Configuration Manager opens.
22. On the top navigation bar, select **Tools**, and then select **Import/Export Meridium Metadata**.
The **Import/Export Metadata** window appears.
23. Select **Select File**.
The **Open** window appears.
24. Navigate to and select the file that you saved in step 6, and then select **Open**.
The **Open** window closes, and the selected filepath is displayed in the **Select File** box on the **Import/Export Metadata** window.




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


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

The **Select Rule Projects to Import** window appears.

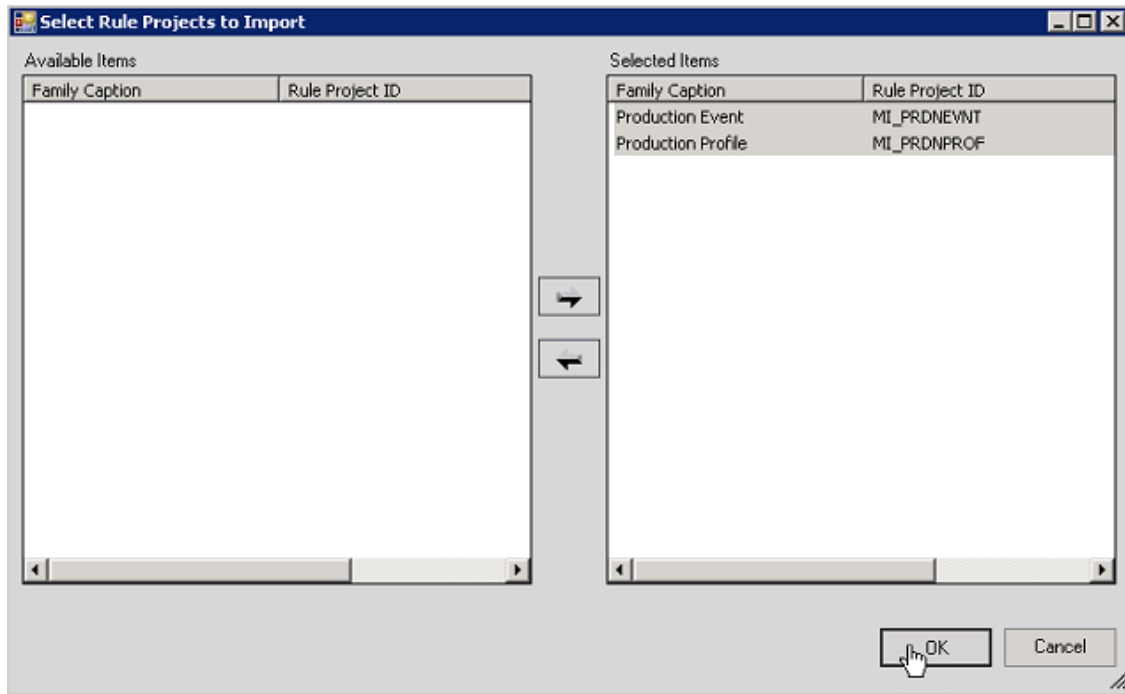


27. In the **Available Items** section, select the item whose Family Caption is Production Event, and then select .

The selected item appears in the **Selected Items** section.

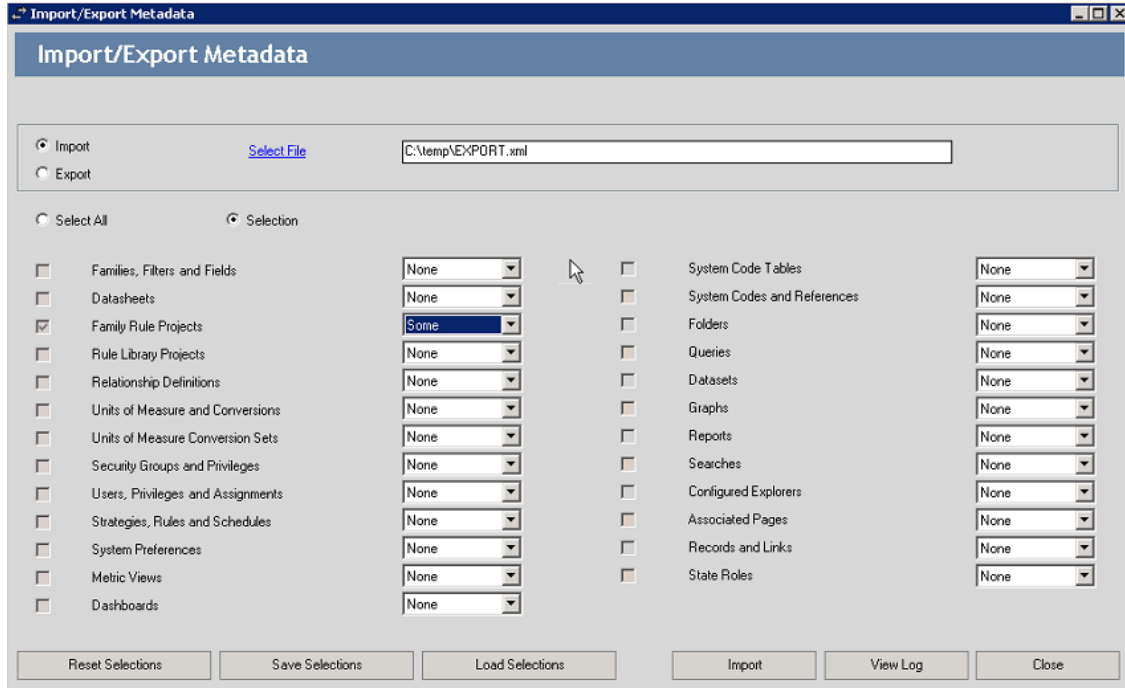
28. In the **Available Items** section, select the item whose Family Caption is Production Profile, and then select .

The selected item appears in the **Selected Items** section.



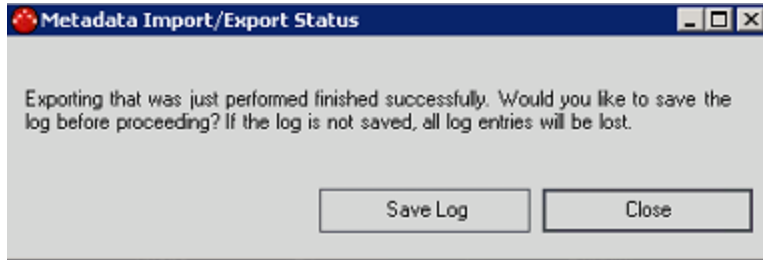
29. Select OK.

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



30. Select **Import**.

The **Metadata Import/Export Status** dialog box appears, displaying a progress bar. When the import is complete, a message appears, asking if you want to save the log.



31. Select **Save Log**.

The **Save As** window appears.

32. Navigate to the location where you want to save the import log, then enter a name in the **File name:** box, and then select **Save**.

The **Save As** window closes.

33. On the **Metadata Import/Export Status** dialog box, select **Close**.

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

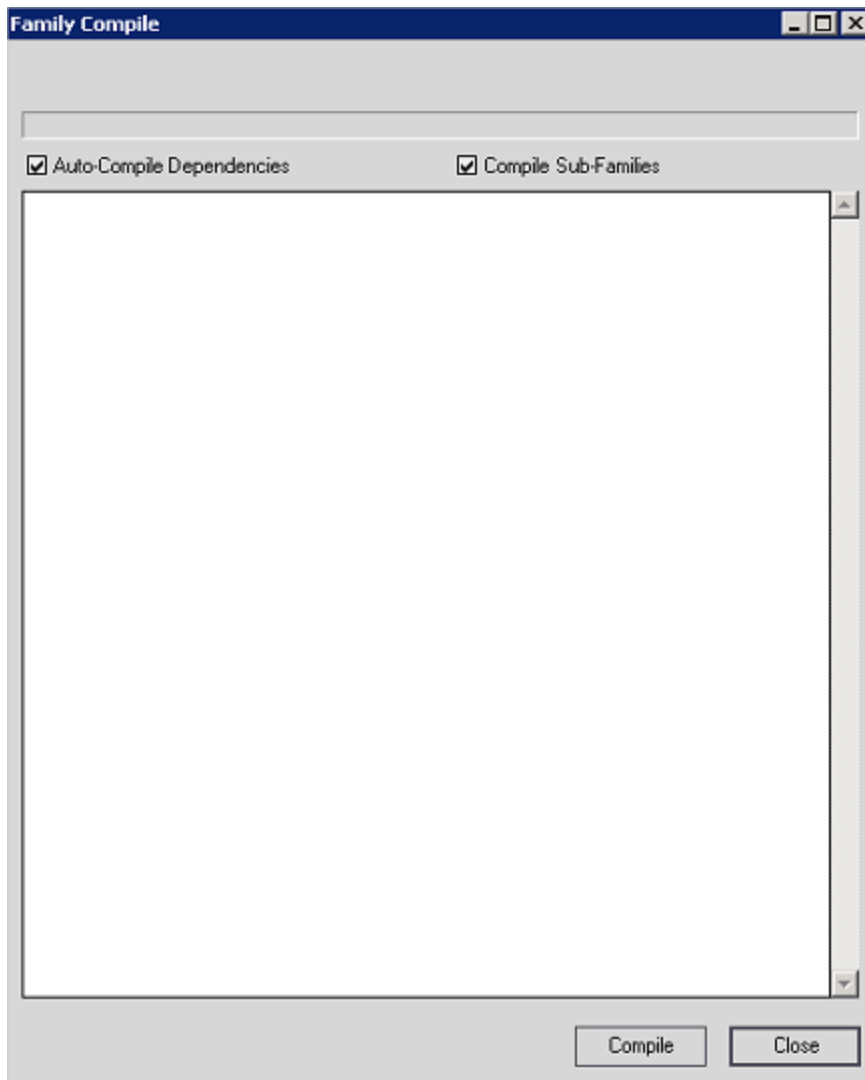
34. On the **Import/Export Metadata** window, select **Close**.

The **Import/Export Metadata** window closes.

35. In Configuration Manager, in the left pane, select the **Production Event** folder.

36. In the **Tasks** section of the workspace, select **Compile Family**.

The **Family Compile** window appears.



37. In the **Family Compile** window, select **Compile**.

In the **Family Compile** window, a progress bar appears, and successfully compiled families appear in a list as the operation progresses.

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

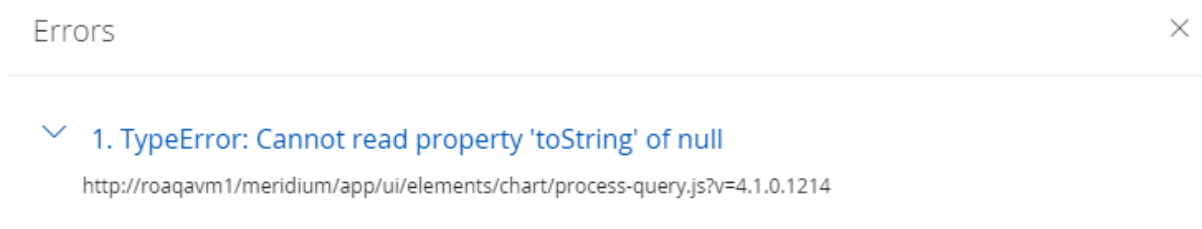
The **Family Compile** window closes.

39. In Configuration Manager, in the left pane, select the **Production Profile** folder, and then repeat steps 36 through 38.

The necessary baseline rules have been imported into your current, pre-upgraded database.

Replace the Top 10 Bad Actors Query

The **Top 10 Bad Actors** query is used by Meridium Enterprise APM to populate the **Top 10 Bad Actors** graph on the **Production Loss Analysis Overview page**. In some data-bases, when viewing this graph, you may receive the following error:

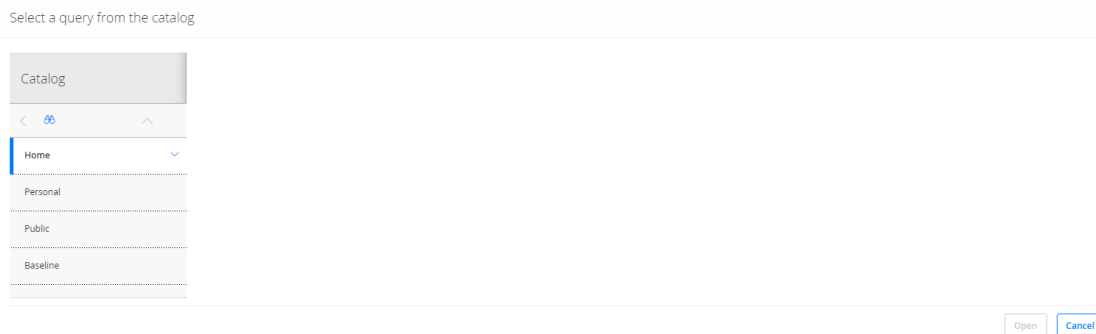


To implement the corrected query and to correct this error, complete the following steps.

Steps

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

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



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

The **Enter Parameter Values** window appears.

Enter Parameter Values

numofdays

enty_key

Home

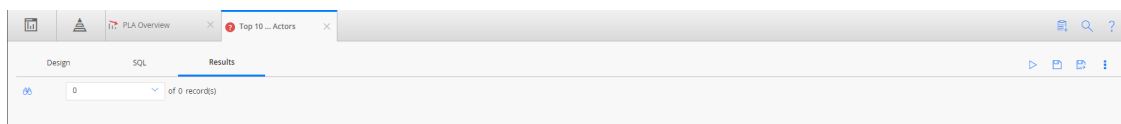
isassetcontext

Cancel
Done

4. Select OK.

Note: For the purposes of these instructions, you do not need to complete any fields in the **Enter Parameter Values** window.

The **Top 10 Actors** query page appears, displaying the **Results** tab.



5. Select the SQL tab.

The SQL query text appears in the workspace, displaying the current query.



6. In the SQL workspace, select and delete the current query text.

7. In the blank SQL workspace, copy and paste the following query text:

```
SELECT TOP 10 SUM(LossAmount) "Loss Amount" , AssetID "Asset ID" FROM
```


```
(
```

```
SELECT DISTINCT [MI_PRDNLOSS].ENTY_KEY "ENTY_KEY", [MI_PRDNLOSS].[MI_PRDNLOSS_
LOSS_AMOUNT_N] "LossAmount", [MI_EQUIP000].[MI_EQUIP000_EQUIP_TECH_NBR_C]
"AssetID" FROM [MI_EQUIP000], [MI_PRDNLOSS] JOIN_SUCC [MI_PRDNEVNT] ON {MIR_
CBPRDEVN} WHERE ([MI_PRDNEVNT].[MI_PRDNEVNT_START_DATE_D] >= MI_DateAdd('dd',
((? :s :id=numofdays) * -1), Now()) AND [MI_PRDNEVNT].[MI_PRDNEVNT_END_DATE_D]
<= MI_DateAdd('dd', 1, Now()) AND [MI_PRDNEVNT].[MI_PRDNEVNT_CAUSE_EQP_KEY_N]
IN ((? :ah :id=enty_key :child :all :current)) AND [MI_EQUIP000].ENTY_KEY =
[MI_PRDNEVNT].[MI_PRDNEVNT_CAUSE_EQP_KEY_N]) and [MI_EQUIP000].[MI_EQUIP000_
EQUIP_TECH_NBR_C] is not null
```

```
UNION
```

```
SELECT DISTINCT [MI_PRDNLOSS].ENTY_KEY "ENTY_KEY", [MI_PRDNLOSS].[MI_PRDNLOSS_
LOSS_AMOUNT_N] "LossAmount", [MI_FNCLOC00].[MI_FNCLOC00_FNC_LOC_C] "AssetID"
FROM [MI_FNCLOC00], [MI_PRDNLOSS] JOIN_SUCC [MI_PRDNEVNT] ON {MIR_CBPRDEVN}
WHERE ([MI_PRDNEVNT].[MI_PRDNEVNT_START_DATE_D] >= MI_DateAdd('dd', ((? :s :id-
d=numofdays) * -1), Now()) AND [MI_PRDNEVNT].[MI_PRDNEVNT_END_DATE_D] <= MI_
DateAdd('dd', 1, Now()) AND [MI_PRDNEVNT].[MI_PRDNEVNT_CAUSE_EQP_KEY_N] IN ((?
:ah :id=enty_key :child :all :current)) AND [MI_FNCLOC00].ENTY_KEY = [MI_
PRDNEVNT].[MI_PRDNEVNT_CAUSE_EQP_KEY_N]) and [MI_FNCLOC00].[MI_FNCLOC00_FNC_
LOC_C] is not null
```

```
) Table1 GROUP BY AssetID ORDER BY Sum(LossAmount) Desc
```

8. On the right side of the page heading, select .

The new query text is saved.

Results

- The corrected query will populate the **Top 10 Bad Actors** graph on the **Production Loss Analysis Overview** page.

Production Loss Analysis Security Groups and Roles

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

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

| Security Group | Roles |
|---|--|
| MI Production Loss Accounting Administrator | MI FE Admin |
| MI Production Loss Accounting Manager | MI FE Admin MI FE PowerUser |
| MI Production Loss Accounting Service | MI FE Admin |
| MI Production Loss Accounting User | MI FE Admin MI FE PowerUser MI FE User |

The 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 Accounting Manager | MI Production Loss Accounting Service | MI Production Loss Accounting User |
|---------------------|---|---------------------------------------|---------------------------------------|------------------------------------|
| Entity Families | | | | |
| Equipment | View, Update, Insert, Delete | View | View | View |
| Functional Location | View | View | View | View |
| Impact Code | View, Update, Insert, Delete | View | View | View |

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

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

| Family | MI Production Loss Accounting Administrator | MI Production Loss Accounting Manager | MI Production Loss Accounting Service | MI Production Loss Accounting User |
|--------------------------------------|---|---------------------------------------|---------------------------------------|------------------------------------|
| 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 |
| 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 R Scripts

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

Deploying R Scripts for the First Time

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

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed. All steps are required unless otherwise noted.

| Step | Task | Required? | Notes |
|------|---|-----------|-------|
| 1 | Ensure that your R Server is configured according to the R scripts system requirements. | Y | None |
| 2 | In Meridium Enterprise APM, specify the R Server credentials. | Y | None |

Upgrading R Scripts to V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

| Step | Task | Required? | Notes |
|------|---|-----------|-------|
| 1 | Ensure that your R Server is configured according to the R scripts system requirements. | Y | None |
| 2 | In Meridium Enterprise APM, specify the R Server credentials. | Y | None |

Upgrade from any version V4.0.0.0 through V4.0.1.0


| Step | Task | Required? | Notes |
|------|---|-----------|-------|
| 1 | Ensure that your R Server is configured according to the R scripts system requirements. | Y | None |
| 2 | In Meridium Enterprise APM, specify the R Server credentials. | Y | None |

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 1 | If you are upgrading <i>directly</i> from V3.6.0.8.0, run a script in order to upgrade R script metadata . | Y | This step is not required if you are upgrading from any V3.x version other than V3.6.0.8.0. |
| 2 | Ensure that your R Server is configured according to the R scripts system requirements. | Y | None |
| 3 | In Meridium Enterprise APM, specify the R Server credentials. | Y | None |

Upgrade R Script Metadata

If you are upgrading *directly* from V3.6.0.8.0, after upgrading your database to V4.1.5.0, you must run a script in order to upgrade existing R script metadata. This step is *not* required if you are upgrading from any V3.x version other than V3.6.0.8.0.

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

Steps

1. Copy the script corresponding to your type of database.

Oracle

```
-- select * from dbo.[MI_CTIT_RSCRIPTS]
UPDATE MI_CTIT_RSCRIPTS
SET CTIT_RSCR_DEFN_MEM = REPLACE(CTIT_RSCR_DEFN_MEM, '"DataType":"n"',
'"DataType":"N"');
UPDATE MI_CTIT_RSCRIPTS
SET CTIT_RSCR_DEFN_MEM = REPLACE(CTIT_RSCR_DEFN_MEM, '"DataType":"c"',
'"DataType":"C"');
UPDATE MI_CTIT_RSCRIPTS
SET CTIT_RSCR_DEFN_MEM = REPLACE(CTIT_RSCR_DEFN_MEM, '"DataType":"d"',
'"DataType":"D"');
UPDATE MI_CTIT_RSCRIPTS
SET CTIT_RSCR_DEFN_MEM = REPLACE(CTIT_RSCR_DEFN_MEM, '"DataType":"l"',
'"DataType":"L"');
```

SQL

```
-- select * from dbo.[MI_CTIT_RSCRIPTS]
UPDATE dbo.[MI_CTIT_RSCRIPTS]
SET CTIT_RSCR_DEFN_MEM = CAST(REPLACE(CAST(CTIT_RSCR_DEFN_MEM as NVarchar
(MAX)), '"DataType":"n"', '"DataType":"N"') AS NText)
UPDATE dbo.[MI_CTIT_RSCRIPTS]
SET CTIT_RSCR_DEFN_MEM = CAST(REPLACE(CAST(CTIT_RSCR_DEFN_MEM as NVarchar
(MAX)), '"DataType":"c"', '"DataType":"C"') AS NText)
UPDATE dbo.[MI_CTIT_RSCRIPTS]
SET CTIT_RSCR_DEFN_MEM = CAST(REPLACE(CAST(CTIT_RSCR_DEFN_MEM as NVarchar
(MAX)), '"DataType":"d"', '"DataType":"D"') AS NText)
UPDATE dbo.[MI_CTIT_RSCRIPTS]
SET CTIT_RSCR_DEFN_MEM = CAST(REPLACE(CAST(CTIT_RSCR_DEFN_MEM as NVarchar
(MAX)), '"DataType":"l"', '"DataType":"L"') AS NText)
```

2. Using SQL Server Management Studio (for SQL) or SQL Developer (for Oracle), run the script.

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 V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V4.0.0.0 through V4.0.1.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.10.0

Recommendation Management will be upgraded from V3.5.1 to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

Recommendation Management will be upgraded from V3.5.0 SP1 LP to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

Recommendation Management will be upgraded from V3.5.0 to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

This module will be upgraded to V4.1.5.0 automatically when you upgrade the

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

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.

Recommendation Management Security Groups and Roles

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

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

One baseline Security Group is provided for Recommendation Management: MI Recommendation Management User.

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

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

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 V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V4.0.0.0 through V4.0.1.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.10.0

Reliability Analytics will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

Reliability Analytics will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | 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 and Roles

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

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

| Security Group | Roles |
|------------------------------|--|
| MI Reliability Administrator | MI FE Admin |
| MI Reliability User | MI FE Admin MI FE PowerUser MI FE User |
| MI Reliability Viewer | MI FE Admin MI FE PowerUser MI FE User |

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

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

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

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

| Family | MI Reliability Administrator | MI Reliability User | MI Reliability Viewer |
|----------------------------------|------------------------------|------------------------------|-----------------------|
| System Special Action | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| System Subsystem | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| System Switch | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Weibull | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Analysis Link | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Global Events | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Mitigated TTF Distribution | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Planned Resource Usages | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Consolidated Recommendations | View | View | View |
| Has Recommendations | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Reliability | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Resource Usage | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Risk Assessments | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Root System | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Scenarios | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has System Actions | View, Update, Insert, Delete | View, Update, Insert, Delete | View |

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

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 V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V4.0.0.0 through V4.0.1.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | 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 and Roles

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

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

| Security Group | Roles |
|--|-------------------|
| MI RCM User MI RCM Viewer | MI Strategy User |
| MI RCM User MI RCM Viewer | MI Strategy Power |
| MI RCM User MI RCM Viewer MI ASI Administrator | MI Strategy Admin |

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.

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 |

| Family Caption | MI RCM User | MI RCM Viewer |
|--|------------------------------|---------------|
| 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 | View, Update, Insert, Delete | View |
| <div>  Note: The Task History relationship family is inactive in the baseline Meridium Enterprise APM database. </div> | | |
| 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 |

| Family Caption | MI RCM User | MI RCM Viewer |
|---|------------------------------|---------------|
| 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 | View, Update, Insert, Delete | View |
|  Note: The Has Task History relationship family is inactive in the baseline Meridium Enterprise APM database. | | |
| 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

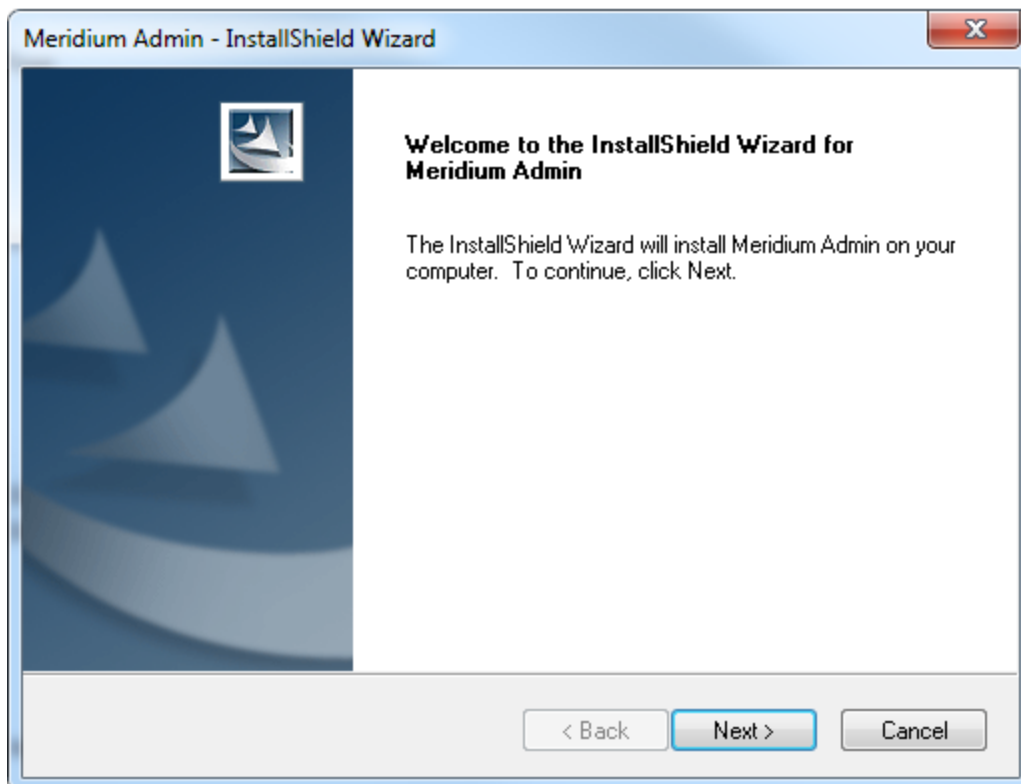
Before You Begin

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

Steps

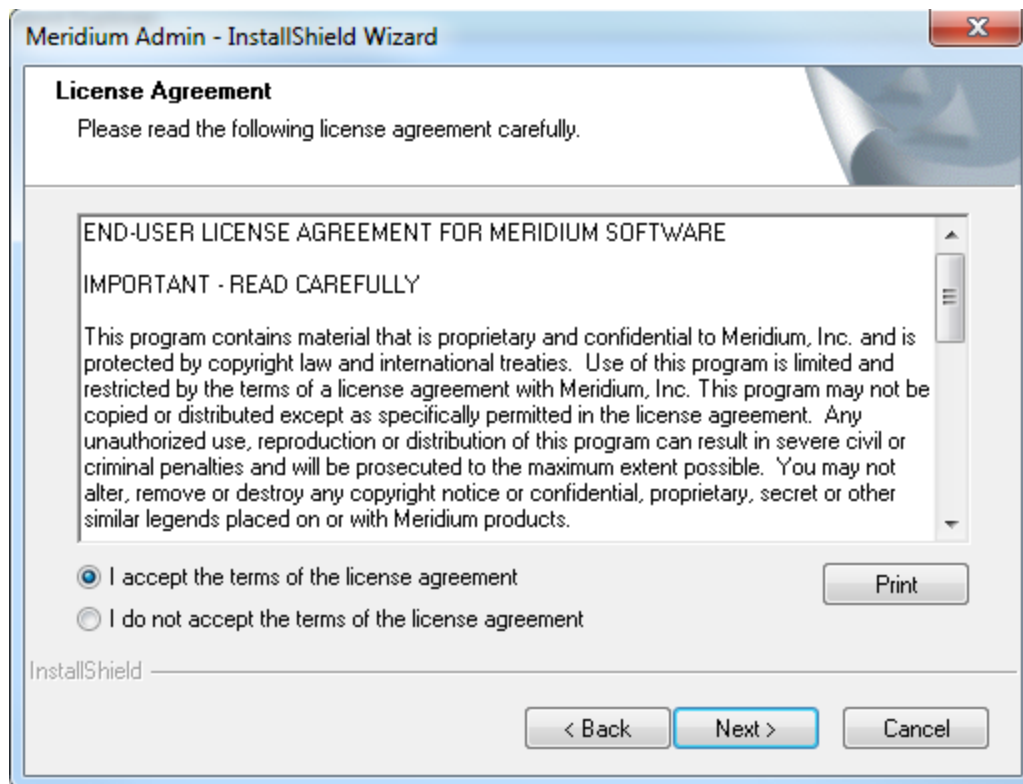
1. On the machine that will serve as the APM Reports Designer, access the Meridium APM Enterprise APM Distribution package, and navigate to the **Admin** folder.
2. Double-click the file **Setup.exe**.

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



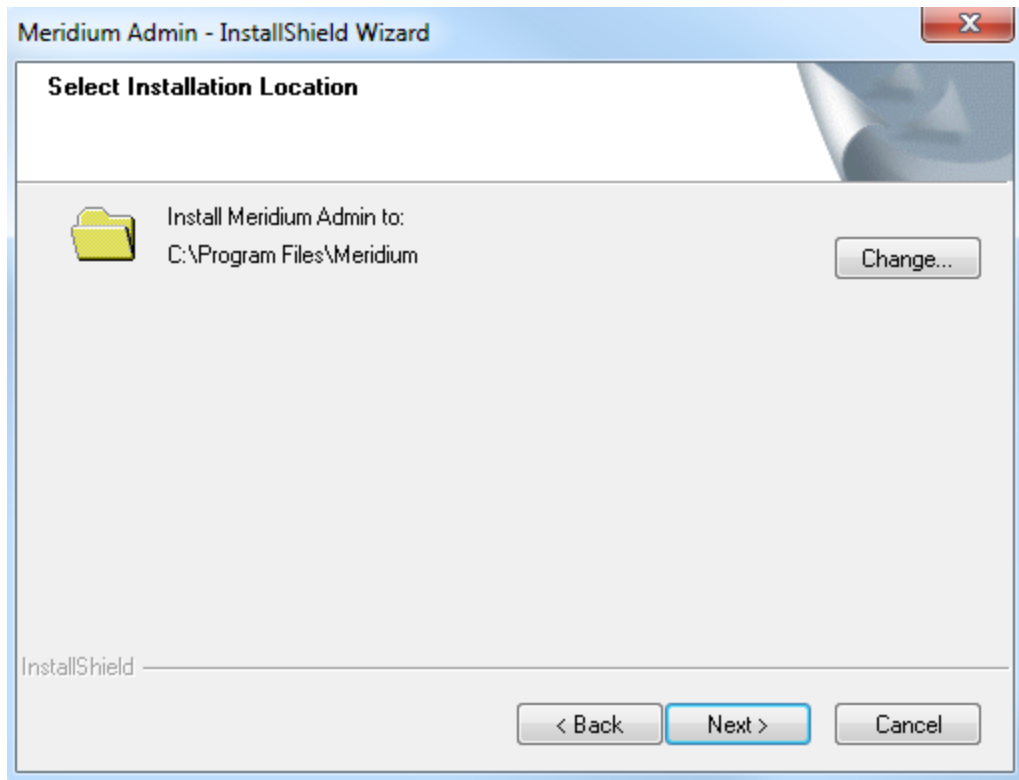
3. Select **Next**.

The **License Agreement** screen appears.



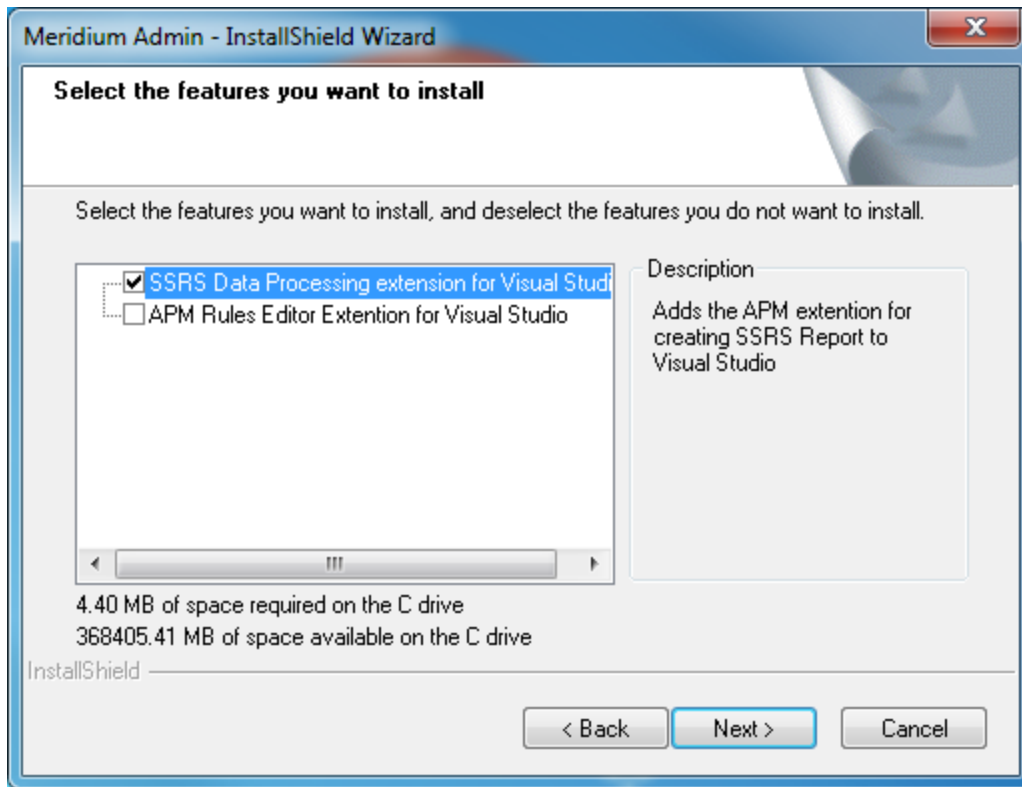
4. Read the License Agreement and, if you agree, select the **I accept the terms of the license agreement** check box. Then, select **Next**.

The **Select Installation Location** screen appears.

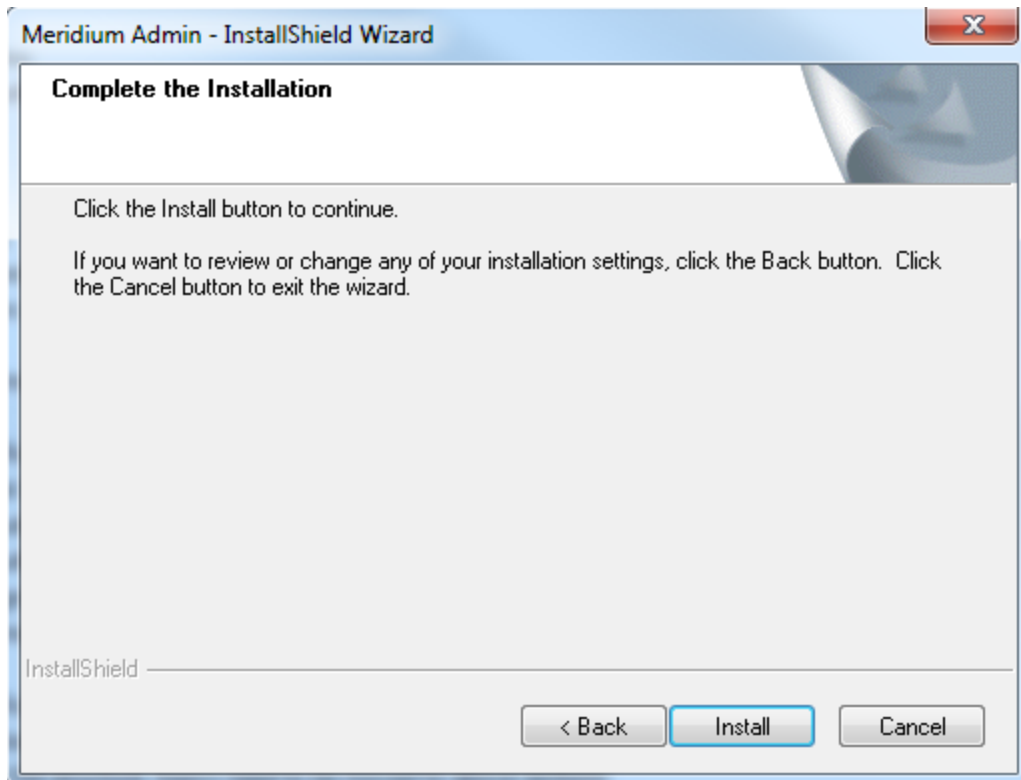


5. Select **Next** to accept the default location.

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

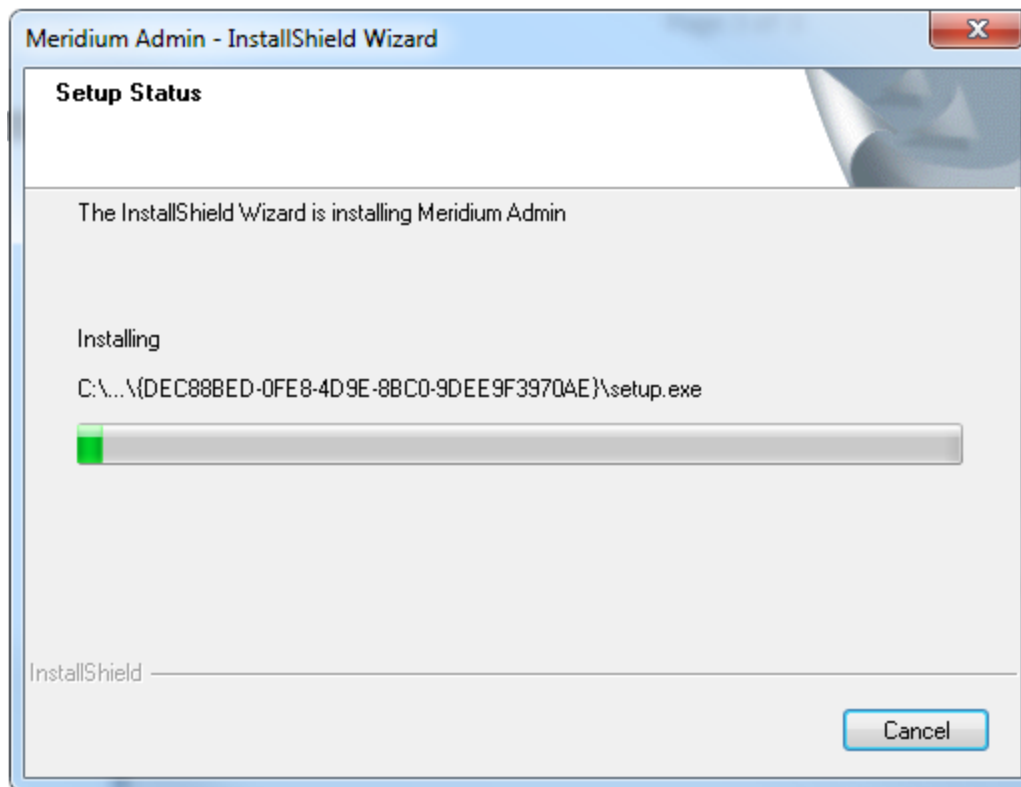


6. Select **SSRS Data Processing Extension for Visual Studio**, and then select **Next**.
The **Complete the Installation** screen appears.

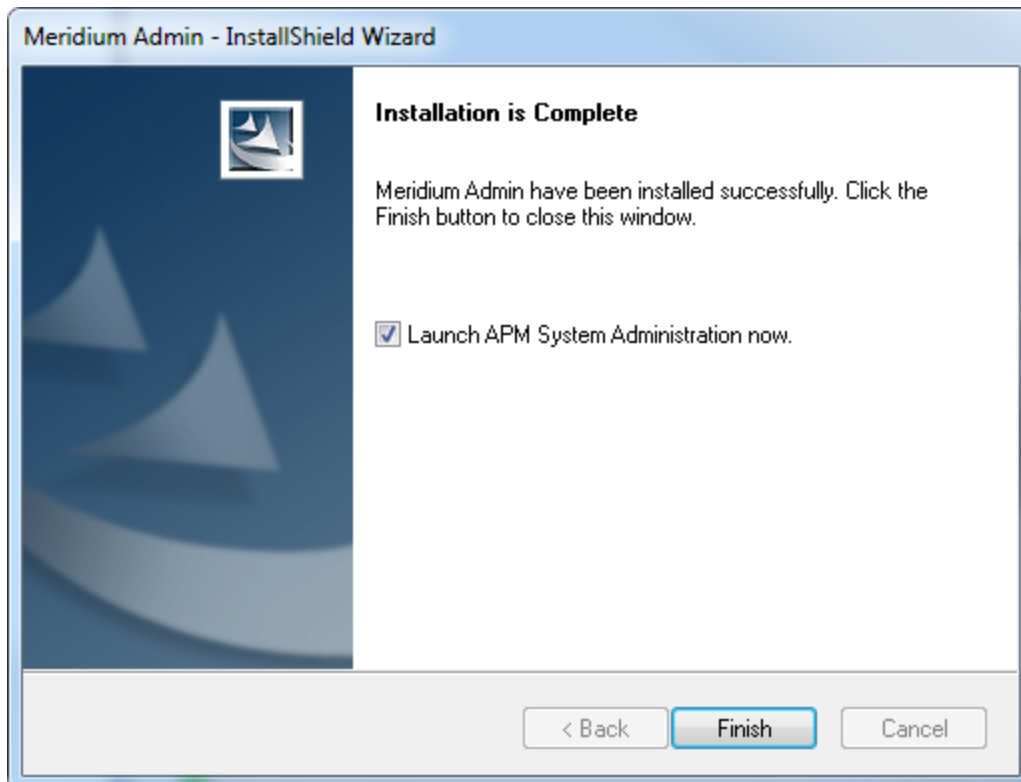



7. Select **Install**.

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.

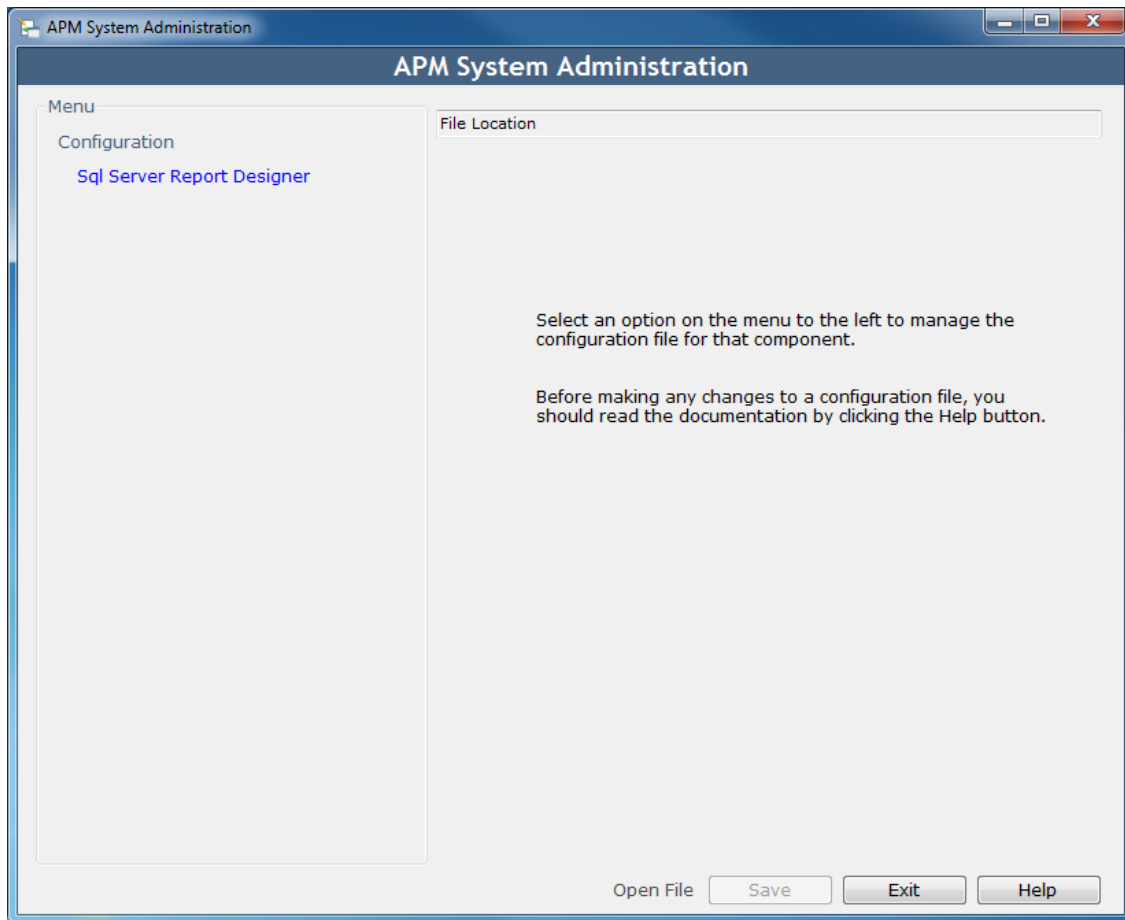


8. Clear the **Launch APM System Administration now** box, and then select **Finish**.



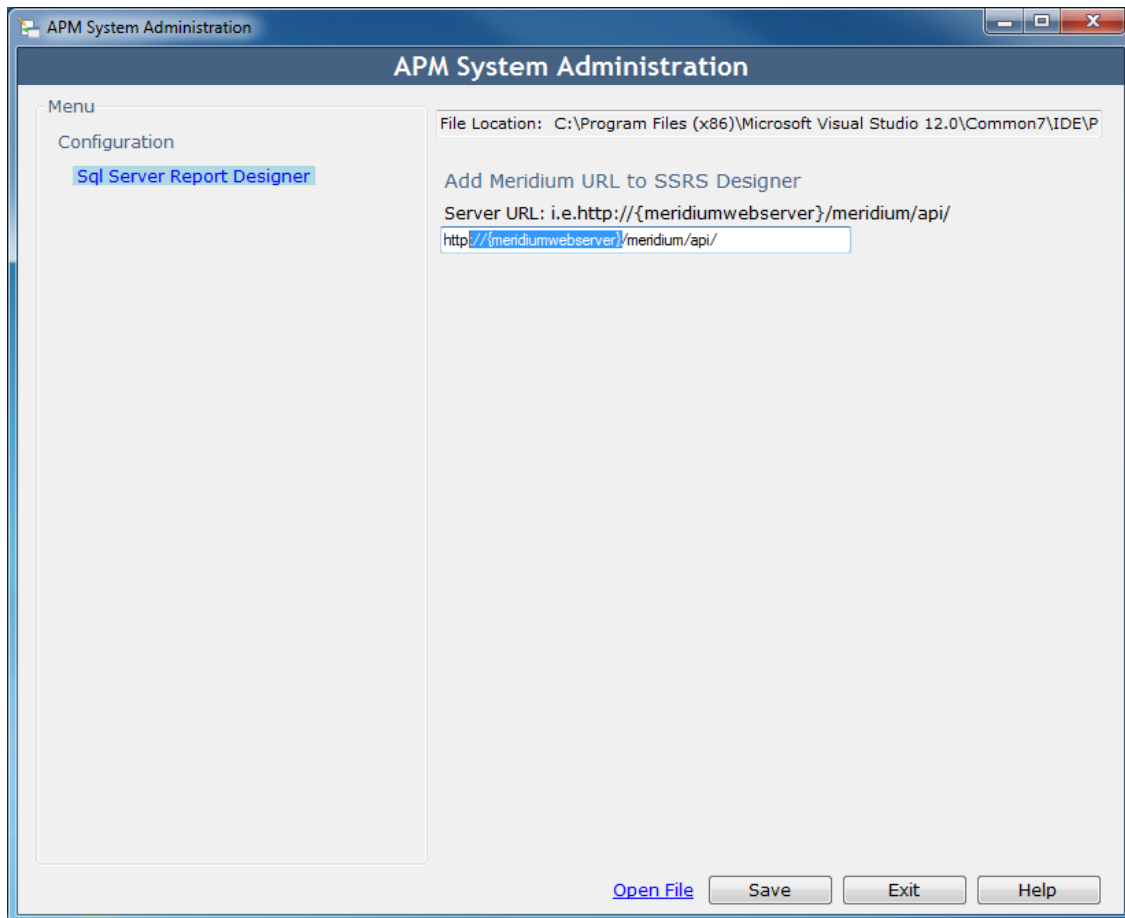
 **Note:** You may be asked to restart your system for the changes to take effect.

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.

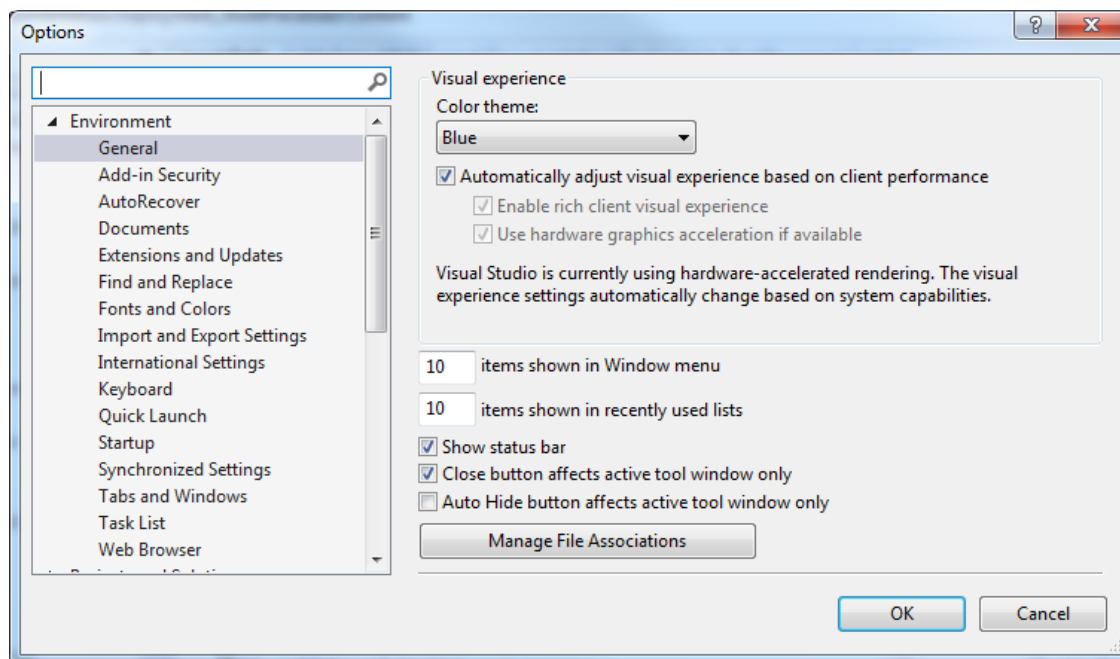
Before You Begin

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

Steps

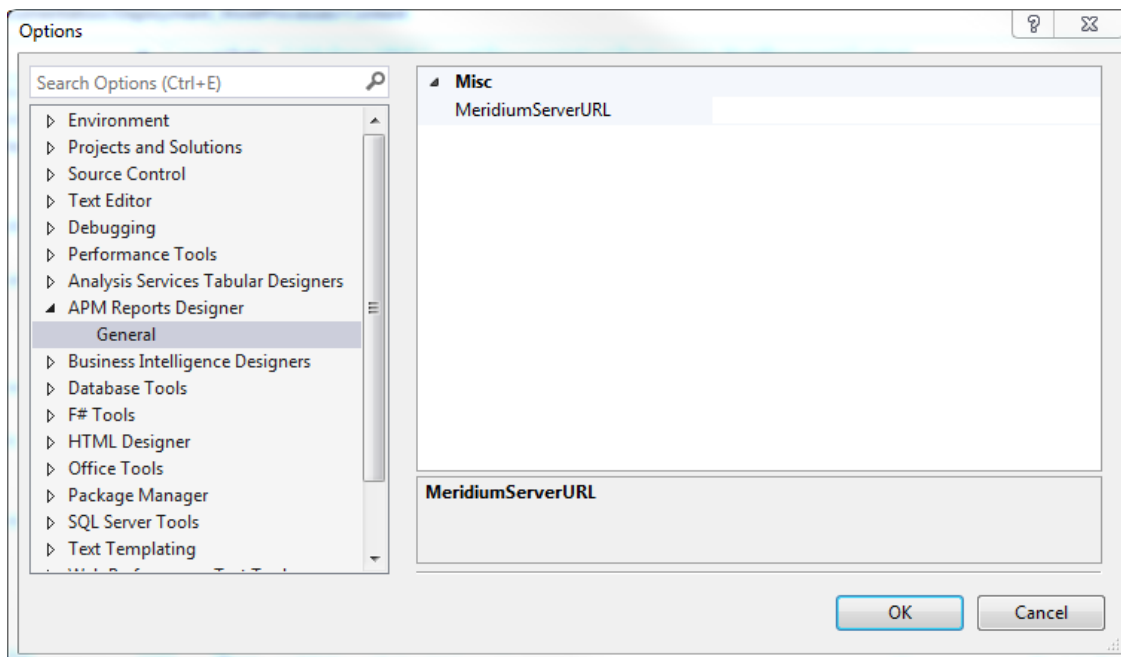
1. On the Meridium Enterprise APM Server, open Microsoft Visual Studio.
2. On the **Tools** menu, select **Options**.

The **Options** window appears.



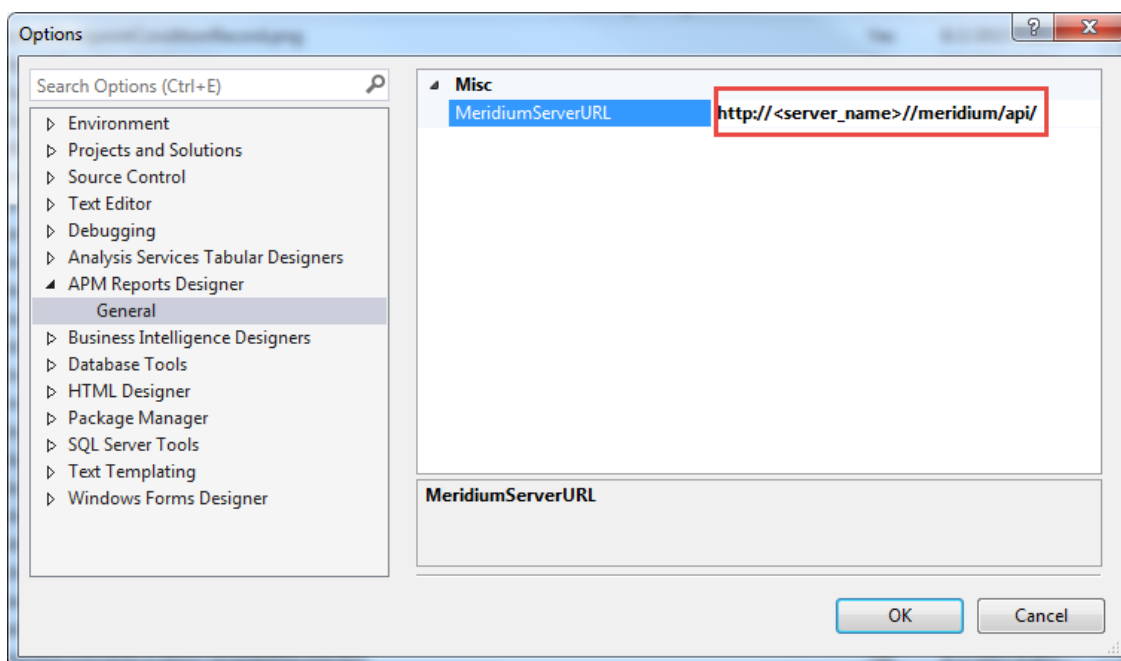
3. On the **Options** window, in the left section, select **APM Report Designer**, and then select **General**.

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 RBI 581

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

Deploying RBI 581 for the First Time

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

These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed. All steps are required unless otherwise noted.

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 1 | RBI 581 is dependent on R Scripts and the third-party software that is required to implement R Scripts. Review and complete the steps required for deploying R Scripts. | Y | The third-party software should be installed and connection preferences configured before proceeding. |
| 2 | Assign Security Users to one or more of the RBI Security Groups . | Y | Users will need permissions to the RBI 581 families in order to use the RBI 581 functionality. RBI 581 families are assigned to the baseline RBI Security Groups. |
| 3 | Add the following types of RBI 581 users to at least one TM Security Group : <ul style="list-style-type: none"> Users who are responsible for completing the steps necessary to use TM Analysis values to calculate RBI 581 corrosion rates. Users who should be able to navigate to TM via RBI 581. | N | Required <i>only</i> if you are using the integration between the RBI 581 and TM modules. |
| 4 | 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. |

| 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 | |

Upgrading RBI 581 to V4.1.5.0


The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.


The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.


Upgrade from any version V4.1.0.0 through V4.1.1.1

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.


Upgrade from any version V4.0.0.0 through V4.0.1.0

 **Note:** While RBI 581 was introduced in Meridium Enterprise APM V4.1.0.0, if you are an existing customer with V4.0.0.0, the following tasks should be completed.

| Step | Task | Required? | Notes |
|------|---|-----------|--|
| 1 | <p>RBI 581 is dependent on R Scripts and the third-party software that is required to implement R Scripts. Review and complete the steps required for deploying R Scripts.</p> <div>  IMPORTANT: After deploying R Scripts, reset IIS. </div> | Y | The third-party software must be installed, and connection setting should be configured. |

| Step | Task | Required? | Notes |
|------|---|-----------|---|
| 2 | <p>On your Meridium Enterprise APM Application Server, using Configuration Manager, import the following:</p> <ul style="list-style-type: none"> MI_DATA_GRP.zip <p>This file should be located on your application server at C:\Meridium\DbUpg\MI_DB_MASTER_4010500\4010500\IEU_ManualImports. You may need to extract the 4010500 archive from the MI_DB_MASTER_4010500 archive.</p> | Y | <p>Updated Data Mapping Group and InsulationType records are required by RBI 581.</p> <div>  Note: This step will <i>not</i> create data mappings for RBI 581. It will only create the Data Mapping Group records required by RBI 581 in order to prevent any errors from occurring. To implement data mapping, proceed to the next task and review the notes. </div> <p>The content for the following families has been updated in V4.1.5.0:</p> <ul style="list-style-type: none"> MI_TASK_TYPE.xml MI_REPFLUIDS.xml MI_ |


| Step | Task | Required? | Notes |
|------|--|-----------|---|
| | | | EQUIPTYP.xml <ul style="list-style-type: none"> • MI_INSP_STRAT.xml • MI_INSUTYPE.xml • MI_POLICY.xml • MI_PTDEMECH.xml |
| 3 | <p>⚠ IMPORTANT: If you complete the following step, <i>all existing changes</i> to data mapping in the RBI 581 and Risk Based Inspection modules will be reverted to baseline. <i>All customization for data mappings will be lost.</i> Do <i>not</i> perform this step unless your organization will be satisfied with the baseline data mappings, or you are prepared to customize the records again following the execution of the script.</p> <p>Via your database manager application, execute the SQL script available in the following KBA: https://meridium.custhelp.com/app/answers/detail/a_id/3028</p> | N | <p>While not required, if you do not complete this step, data mappings will <i>not</i> be created between families in RBI 581. You will either need to create the data mappings manually, or enter data into each new record.</p> |

| Step | Task | Required? | Notes |
|------|---|-----------|--|
| 4 | <p>On your Meridium Enterprise APM Application Server, using Configuration Manager, import the following</p> <ul style="list-style-type: none"> • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml <p>These files should be located on your application server at C:\Meridium\DbUpg\MI_DB_MASTER_4010500\4010500\IEU\Other\RecordsLinks. You may need to extract the 4010500 archive from the MI_DB_MASTER_4010500 archive.</p> | Y | <p>Updated RBI Strategy Mapping Composite Entities are required for RBI 581.</p> <div>  Note: Manually importing this content <i>will</i> overwrite your existing Strategy Mapping Composite Entities. </div> |
| 5 | <p>Add the 581 tab to the datasheet of one or more of the following Criticality RBI Component families:</p> <ul style="list-style-type: none"> • Cylindrical Shell • Exchanger Bundle • Exchanger Header • Exchanger Tube • Piping • Tank Bottom | N | <p>This step is required <i>only</i> if you have customized the datasheet for one or more Criticality RBI Components.</p> <p>For example, if you only customized the datasheet for the Criticality RBI Component - Piping and Criticality RBI Component - Tank Bottom families, you would only need to add the 581 tab to these two datasheets.</p> |

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

| Step | Task | Required? | Notes |
|------|--|-----------|--|
| 1 | <p><u>Add the 581 tab to the datasheet of one or more of the following Criticality RBI Component families:</u></p> <ul style="list-style-type: none"> • Cylindrical Shell • Exchanger Bundle • Exchanger Header • Exchanger Tube • Piping • Tank Bottom | N | <p>This step is required <i>only</i> if you have customized the datasheet for one or more Criticality RBI Components.</p> <p>For example, if you only customized the datasheet for the Criticality RBI Component - Piping and Criticality RBI Component - Tank Bottom families, you would only need to add the 581 tab to these two datasheets.</p> |

Modify the Review Analyses for Asset Query

 **Note:** The **Review Analyses by Asset** query is used by Meridium Enterprise APM to populate the **Change Analysis States** window when *both* the *Risk Based Inspection* and *RBI 581* modules are activated. When only Risk Based Inspection is active, the **Review Analyses by Asset 580** query is used. When only RBI 581 is active, the **Review Analyses by Asset 581** query is used.

If you have customized the **Review Analyses by Asset** query, and want to retain the changes, perform the following steps:

1. In the Catalog, navigate to Public\Meridium\Modules\Risk Based Inspection\Queries, and then select the **Review Analyses by Asset** link.

The **Query** page appears, displaying the **Results** workspace. The **Enter Parameter Values** window appears.

2. Select **Cancel**.

3. In the workspace heading, select the **SQL** tab.

The **SQL** workspace appears, displaying the SQL code.

4. Copy the SQL code.

5. On the top navigation bar, close the tab corresponding to the **Review Analyses by Asset** query, and then select the **Catalog** tab.

The Catalog reappears.

6. In the same Catalog folder, select the **Review Analyses by Asset 580** link.

The **Query** page appears, displaying the **Results** workspace. The **Enter Parameter Values** window appears.

7. Select **Cancel**.

8. In the workspace heading, select the **SQL** tab.

The **SQL** workspace appears, displaying the SQL code.

9. Select all the existing code, and then delete it.


10. Paste the code copied from the **Review Analyses by Asset** query.

11. In the upper right corner, select .

The **Review Analyses by Asset 580** query is saved.

12. On the top navigation bar, close the tab that corresponds to the **Review Analyses By Asset 580** query, and then select the **Catalog** tab.

The Catalog reappears.


13. In the Catalog, select the check box corresponding to the **Review Analyses By Asset** query, and then, in the upper right corner, select .

The **Confirm Delete** window appears.

14. Select **OK**.

The **Review Analyses by Asset** query is deleted.

15. In the catalog, navigate to Baseline\Meridium\Modules\Risk Based Inspection\Queries.

16. Select the check box corresponding to the **Review Analyses by Asset** query, and then, in the upper right corner, select .


The **Catalog Folder Browser** window appears.

17. In the hierarchy, navigate to Public\Meridium\Modules\Risk Based Inspection\Queries, and then select **Done**.

The query is copied to the folder, and the **Success** dialog box appears.

18. Select **OK**.

The **Change Analysis States** window will now function as expected.

 **Note:** If both the Risk Based Inspection and RBI 581 modules are active, your customizations, while preserved in the **Review Analyses by Asset 580** query, will need to be manually integrated into the new **Review Analyses by Asset** query located at Public\Meridium\Modules\Risk Based Inspection\Queries in the Catalog, if you want those customizations to appear.

Add the 581 Tab to Criticality RBI Component Datasheets

If you have customized the datasheet for one or more of the Criticality RBI Components, after activating the RBI 581 license you will need to perform the following procedure to add the 581 tab to those customized datasheets. The following table indicates the fields that should appear on each Criticality RBI Component datasheet.


| Caption | Field ID | Criticality RBI Component - Cylindrical Shell | Criticality RBI Component - Exchanger Bundle | Criticality RBI Component - Exchanger Header | Criticality RBI Component - Exchanger Tube | Criticality RBI Component - Piping | Criticality RBI Component - Tank Bottom |
|------------------------|-----------------------------------|---|--|--|--|------------------------------------|---|
| Coefficient Y Material | MI_CCRBIC-OM_COEFFICIENT_Y_MTRL_C | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Percent Liquid Volume | MI_RBICO-MPO_PER_LIQ_VOL_N | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Cladding Present | MI_CCRBIC-OM_CLADDING_PRESENT_L | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Caption | Field ID | Crit- icality RBI Com- pon- ent - Cylind- rical Shell | Crit- icality RBI Com- pon- ent - Excha- nger Bundl- e | Criticality RBI Com- ponent - Exchanger- Header | Crit- icality RBI Com- pon- ent - Excha- nger Tube | Crit- icality RBI Com- pon- ent - Piping | Crit- icality RBI Com- pon- ent - Tank B- ottom |
|-------------------|----------------------------------|---|---|---|--|--|---|
| Detection System | MI_CCRBIC-OM_DETECTION_SYSTEM_C | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mitigation System | MI_CCRBIC-OM_MITIGATION_SYSTEM_C | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Fluid Velocity | MI_CCRBIC-OM_FLUID_VELOCITY_N | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Isolation System | MI_CCRBIC-OM_ISOLA_SYSTEM_CHR | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Geometry Type | MI_CCRBIC-OM_GEOMETRY_TYPE_C | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Caption | Field ID | Crit- icality RBI Com- pon- ent - Cylind- rical Shell | Crit- icality RBI Com- pon- ent - Excha- nger Bundl- e | Criticality RBI Com- pon- ent - Exchanger- Header | Crit- icality RBI Com- pon- ent - Excha- nger Tube | Crit- icality RBI Com- pon- ent - Piping | Crit- icality RBI Com- pon- ent - Tank B- ottom |
|------------------------------------|---|---|---|--|--|--|---|
| GFF Com- ponent Type | MI_ CCRBIC- OM_ GFF_ COMP- O_ TYPE_ CHR | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Minimum Structural Thickness | MI_ CCRBIC- OM_ MNM- M_ STRCTR- L_THS_ N | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Furnished Cladding Thk | MI_ CCRBIC- OM_ FRNSH- D_ CLDD- G_THK_ N | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Liner Present | MI_ CCRBIC- OM_ LINER_ PRESE_ CHR | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Caption | Field ID | Crit- icality RBI Com- pon- ent - Cylind- rical Shell | Crit- icality RBI Com- pon- ent - Excha- nger Bundl- e | Criticality RBI Com- ponent - Exchanger- Header | Crit- icality RBI Com- pon- ent - Excha- nger Tube | Crit- icality RBI Com- pon- ent - Piping | Crit- icality RBI Com- pon- ent - Tank B- ottom |
|--|--|---|---|---|--|--|---|
| Liner Type | MI_ CCRBIC- OM_ LINER_ TP_C | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Has Release Prevention - Barrier? | MI_ CCRBIC- TB_ HAS_ RELEA_ PREVE_ F | × | × | × | × | × | ✓ |
| CM Corrosion - Rate | MI_ CCRBIC- OM_ CM_ COR_ RT_C | ✓ | ✓ | ✓ | × | ✓ | ✓ |
| Corrosion Allow | MI_ RBICO- MPO_ CORR- O_ ALLO- W_N | ✓ | ✓ | ✓ | × | ✓ | ✓ |

Steps

 **Note:** This procedure should be repeated for each Criticality RBI Component data-sheet that has been previously customized.

1. Access the **Family Management** page.
2. In the left pane, locate the Criticality RBI Component whose datasheet you want to

modify.

In the **Family Management** workspace, the corresponding Criticality RBI Component family appears.

3. At the top of the workspace, select the **Datasheets** tab, and then select the **Manage Datasheets** link.

The **Datasheet Builder** page appears, displaying the datasheet for the selected Criticality RBI Component family.

4. In the upper right corner, select .

A **new section** tab appears, displaying a blank section.

5. In the new tab, delete *new section* and enter *581*.

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

In the upper right corner,  is enabled.

7. Select .


In the **581** section, a blank table is created.

8. In the right column, in the top cell, enter *Value(s)*.

9. In the left pane, locate a field that corresponds to [the table at the beginning of this topic](#), and drag that field into the empty cell in the **Value(s)** column. For example, drag the Coefficient Y Material field from the left pane into the empty cell in the **Value(s)** column.

In the cell, an input box that corresponds to the selected field appears.

10. In the left column, enter the caption that corresponds to the field. For example, if you added the Coefficient Y Material field to the **Value(s)** column, then enter *Coef-ficient Y Material* into the corresponding cell in the left column.

11. At the top of the workspace, select .

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

12. Repeat steps 9 to 11 for each of the fields specified in [the table at the beginning of this topic](#).

13. In the upper right corner, select **Save**.

The datasheet for the Criticality RBI Component you selected in step 2 is saved, and the **581** tab will now appear on that Criticality RBI Component datasheet.

RBI 581 Security Groups and Roles

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

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 : <ul style="list-style-type: none"> • 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 <i>Recommendation Creation Enabled</i> 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 <i>Enable Recommendations to be Generated at Created State</i> 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 <i>Created</i> state. |
| 7 | Modify the <i>Allow Override of Calculated Unmitigated Risk Values</i> setting in the RBI Global Preferences workspace. | N | This setting is disabled by default. This task is necessary only if you want to enable this setting because you use a custom calculator. |
| 8 | Modify the <i>Consider Half-Life when Determining Inspection Task Interval</i> 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. |

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 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. |
| 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 V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.


Upgrade from any version V4.0.0.0 through V4.0.1.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

| 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. |
| 2 | Copy your customized SQL code from the Review Analyses by Asset query to the Review Analyses by Asset 580 query, and then replace the Review Analyses by Asset query with its baseline version. | N | This step is required <i>only</i> if you have previously customized the query that is used to populate the list of analyses on the RBI - Review Analyses page. |


| Step | Task | Required? | Notes |
|------|---|-----------|--|
| 3 | <p>Using Search, locate and modify the Data Mapping Query record named RBI-CNAFC MI_CCRBICTB-MI_CRCOEVAL by Component.</p> <ul style="list-style-type: none"> In the related Data Mapping Column-Field Pair record where the Source Query Field is set to Toxic Mixture, ensure the Target Field(s) field is set to <i>Toxic Mixture</i>. In the related Data Mapping Column-Field Pair record where the Source Query Field is set to Toxic Model, ensure the Target Field(s) field is set to <i>Toxic Fluid</i>. | N | <p>This step is required <i>only</i> if you have previously customized data mappings in RBI, and only if you did not complete this step as part of a previous upgrade.</p> <p>If you already completed this step when completing the upgrade workflow for RBI 581, you do not need to repeat it.</p> |

| Step | Task | Required? | Notes |
|------|--|-----------|--|
| 4 | <p>On your Meridium Enterprise APM Application Server, using Configuration Manager, import the following</p> <ul style="list-style-type: none"> 09_MI_RRSKMAP.xml 10_MI_RRSKMDT.xml <p>These files should be located on your application server at C:\Meridium\DbUpg\MI_DB_MASTER_4010500\4010500\IEU\Other\RecordsLinks. You may need to extract the 4010500 archive from the MI_DB_MASTER_4010500 archive.</p> | N | <p>Updated RBI Pipeline Strategy Mapping Composite Entities are required for RBI 580.</p> <p>This step is required <i>only</i> if you have previously customized data mappings in Pipeline, and only if you did not complete this step as part of a previous upgrade.</p> <div>  Note: Manually importing this content <i>will</i> overwrite your existing Strategy Mapping Composite Entities. </div> |

Upgrade from any version V3.5.1 through V3.5.1.10.0

| Step | Task | Required? | Notes |
|------|---|-----------|---|
| 1 | <p>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.</p> | N | <p>Required if you use Policy records to generate RBI Recommendation records.</p> |

| Step | Task | Required? | Notes |
|------|--|-----------|--|
| 2 | <p>Import the Inspection Strategy records that Meridium, Inc. modified in order to fix issues in existing Inspection Strategy records. To do so:</p> <ol style="list-style-type: none"> 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 <i>MI_INSP_STRAT.xml</i> from this location. <p>The file is imported, and the associated Inspection Strategy records are created, replacing the previous ones.</p> | Y | |
| 3 | <p>Copy your customized SQL code from the Review Analyses by Asset query to the Review Analyses by Asset 580 query, and then replace the Review Analyses by Asset query with its baseline version.</p> | N | <p>This step is required <i>only</i> if you have previously customized the query that is used to populate the list of analyses on the RBI - Review Analyses page.</p> |


| Step | Task | Required? | Notes |
|------|--|-----------|--|
| 4 | <p>On your Meridium Enterprise APM Application Server, using Configuration Manager, import the following</p> <ul style="list-style-type: none"> • 09_MI_RRSKMAP.xml • 10_MI_RRSKMDT.xml <p>These files should be located on your application server at C:\Meridium\DbUpg\MI_DB_MASTER_4010500\4010500\IEU\Other\Record-Links. You may need to extract the 4010500 archive from the MI_DB_MASTER_4010500 archive.</p> | N | <p>Updated RBI Pipeline Strategy Mapping Composite Entities are required for RBI 580.</p> <p>This step is required <i>only</i> if you have previously customized data mappings in Pipeline, and only if you did not complete this step as part of a previous upgrade.</p> <div>  Note: Manually importing this content <i>will</i> overwrite your existing Strategy Mapping Composite Entities. </div> |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

| Step | Task | Required? | Notes |
|------|---|-----------|---|
| 1 | <p>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.</p> | N | <p>Required if you use Policy records to generate RBI Recommendation records.</p> |

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 2 | <p>Import the Inspection Strategy records that Meridium, Inc. modified in order to fix issues in existing Inspection Strategy records. To do so:</p> <ol style="list-style-type: none"> 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 <i>MI_INSP_STRAT.xml</i> from this location. <p>The file is imported, and the associated Inspection Strategy records are created, replacing the previous ones.</p> | Y | |
| 3 | <p>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.</p> | N | Required if you want to use Inspection Grouping functionality. |
| 4 | <p>In Functional Location records that represent units in your facility, select the Is a Unit? check box.</p> | Y | This step will ensure that queries used by RBI modules function correctly when returning results. |


| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 5 | Using the <i>Belongs to a Unit</i> relationship, link Equipment records to Functional Location records representing units to which that equipment belongs (i.e., the field <i>Is a Unit?</i> contains the value <i>True</i>). | Y | |
| 6 | Modify the <i>Enable Recommendations to be Generated at Created State</i> 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 <i>Created</i> state. |
| 7 | Copy your customized SQL code from the Review Analyses by Asset query to the Review Analyses by Asset 580 query, and then replace the Review Analyses by Asset query with its baseline version. | N | This step is required <i>only</i> if you have previously customized the query that is used to populate the list of analyses on the RBI - Review Analyses page. |

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 8 | <p>On your Meridium Enterprise APM Application Server, using Configuration Manager, import the following</p> <ul style="list-style-type: none"> 09_MI_RRSKMAP.xml 10_MI_RRSKMDT.xml <p>These files should be located on your application server at C:\Meridium\DbUpg\MI_DB_MASTER_4010500\4010500\IEU\Other\RecordsLinks. You may need to extract the 4010500 archive from the MI_DB_MASTER_4010500 archive.</p> | N | <p>Updated RBI Pipeline Strategy Mapping Composite Entities are required for RBI 580.</p> <p>This step is required <i>only</i> if you have previously customized data mappings in Pipeline, and only if you did not complete this step as part of a previous upgrade.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> Note: Manually importing this content <i>will</i> overwrite your existing Strategy Mapping Composite Entities.</p> </div> |

Upgrade from any version V3.5.0 through V3.5.0.0.7.2


| Step | Task | Required? | Notes |
|------|---|-----------|---|
| 1 | <p>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.</p> | N | <p>Required if you use Policy records to generate RBI Recommendation records.</p> |

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 2 | <p>Import the Inspection Strategy records that Meridium, Inc. modified in order to fix issues in existing Inspection Strategy records. To do so:</p> <ol style="list-style-type: none"> 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 <i>MI_INSP_STRAT.xml</i> from this location. <p>The file is imported, and the associated Inspection Strategy records are created, replacing the previous ones.</p> | Y | |
| 3 | <p>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.</p> | N | Required if you want to use Inspection Grouping functionality. |
| 4 | <p>In Functional Location records that represent units in your facility, select the Is a Unit? check box.</p> | Y | This step will ensure that queries used by RBI modules function correctly when returning results. |
| 5 | <p>Using the <i>Belongs to a Unit</i> relationship, link Equipment records to Functional Location records representing units to which that equipment belongs (i.e., the field <i>Is a Unit?</i> contains the value <i>True</i>).</p> | Y | |


| Step | Task | Required? | Notes |
|------|--|-----------|--|
| 6 | Modify the <i>Enable Recommendations to be Generated at Created State</i> 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 <i>Created</i> state. |
| 7 | <p>On your Meridium Enterprise APM Application Server, using Configuration Manager, import the following</p> <ul style="list-style-type: none"> • 09_MI_RRSKMAP.xml • 10_MI_RRSKMDT.xml <p>These files should be located on your application server at C:\Meridium\DbUpg\MI_DB_MASTER_4010500\4010500\IEU\Other\Record-Links. You may need to extract the 4010500 archive from the MI_DB_MASTER_4010500 archive.</p> | N | <p>Updated RBI Pipeline Strategy Mapping Composite Entities are required for RBI 580.</p> <p>This step is required <i>only</i> if you have previously customized data mappings in Pipeline, and only if you did not complete this step as part of a previous upgrade.</p> <div>  Note: Manually importing this content <i>will</i> overwrite your existing Strategy Mapping Composite Entities. </div> |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| 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 | <p>Import the Inspection Strategy records that Meridium, Inc. modified in order to fix issues in existing Inspection Strategy records. To do so:</p> <ol style="list-style-type: none"> 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_I EU\50_Other\2_RecordsLinks. 2. Import the file <i>MI_INSP_STRAT.xml</i> from this location. <p>The file is imported, and the associated Inspection Strategy records are created, replacing the previous ones.</p> | 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 <i>Belongs to a Unit</i> relationship, link Equipment records to Functional Location records representing units to which that equipment belongs (i.e., the field <i>Is a Unit?</i> contains the value <i>True</i>). | Y | |
| 6 | Modify the <i>Enable Recommendations to be Generated at Created State</i> 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 <i>Created</i> state. |
| 7 | <p>On your Meridium Enterprise APM Application Server, using Configuration Manager, import the following</p> <ul style="list-style-type: none"> • 09_MI_RRSKMAP.xml • 10_MI_RRSKMDT.xml <p>These files should be located on your application server at C:\Meridium\DbUpg\MI_DB_MASTER_4010500\4010500\IEU\Other\RecordsLinks. You may need to extract the 4010500 archive from the MI_DB_MASTER_4010500 archive.</p> | N | <p>Updated RBI Pipeline Strategy Mapping Composite Entities are required for RBI 580.</p> <p>This step is required <i>only</i> if you have previously customized data mappings in Pipeline, and only if you did not complete this step as part of a previous upgrade.</p> <div>  Note: Manually importing this content <i>will</i> overwrite your existing Strategy Mapping Composite Entities. </div> |

Modify the Review Analyses for Asset Query

 **Note:** The **Review Analyses by Asset** query is used by Meridium Enterprise APM to populate the **Change Analysis States** window when *both* the *Risk Based Inspection* and *RBI 581* modules are activated. When only Risk Based Inspection is active, the **Review Analyses by Asset 580** query is used. When only RBI 581 is active, the **Review Analyses by Asset 581** query is used.

If you have customized the **Review Analyses by Asset** query, and want to retain the changes, perform the following steps:

1. In the Catalog, navigate to Public\Meridium\Modules\Risk Based Inspection\Queries, and then select the **Review Analyses by Asset** link.

The **Query** page appears, displaying the **Results** workspace. The **Enter Parameter Values** window appears.

2. Select **Cancel**.

3. In the workspace heading, select the **SQL** tab.

The **SQL** workspace appears, displaying the SQL code.

4. Copy the SQL code.

5. On the top navigation bar, close the tab corresponding to the **Review Analyses by Asset** query, and then select the **Catalog** tab.

The Catalog reappears.

6. In the same Catalog folder, select the **Review Analyses by Asset 580** link.

The **Query** page appears, displaying the **Results** workspace. The **Enter Parameter Values** window appears.

7. Select **Cancel**.

8. In the workspace heading, select the **SQL** tab.

The **SQL** workspace appears, displaying the SQL code.

9. Select all the existing code, and then delete it.


10. Paste the code copied from the **Review Analyses by Asset** query.

11. In the upper right corner, select .

The **Review Analyses by Asset 580** query is saved.

12. On the top navigation bar, close the tab that corresponds to the **Review Analyses By Asset 580** query, and then select the **Catalog** tab.

The Catalog reappears.


13. In the Catalog, select the check box corresponding to the **Review Analyses By Asset** query, and then, in the upper right corner, select .

The **Confirm Delete** window appears.

14. Select **OK**.

The **Review Analyses by Asset** query is deleted.

15. In the catalog, navigate to Baseline\Meridium\Modules\Risk Based Inspection\Queries.

16. Select the check box corresponding to the **Review Analyses by Asset** query, and then, in the upper right corner, select .


The **Catalog Folder Browser** window appears.

17. In the hierarchy, navigate to Public\Meridium\Modules\Risk Based Inspection\Queries, and then select **Done**.

The query is copied to the folder, and the **Success** dialog box appears.

18. Select **OK**.

The **Change Analysis States** window will now function as expected.

 **Note:** If both the Risk Based Inspection and RBI 581 modules are active, your customizations, while preserved in the **Review Analyses by Asset 580** query, will need to be manually integrated into the new **Review Analyses by Asset** query located at Public\Meridium\Modules\Risk Based Inspection\Queries in the Catalog, if you want those customizations to appear.

Risk Based Inspection Security Groups and Roles

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

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

| Security Group | Roles |
|----------------------|--|
| MI RBI Administrator | MI Mechanical Integrity Administrator |
| MI RBI Analyst | MI Mechanical Integrity Administrator MI Mechanical Integrity Power |

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 |


| Family | MI RBI Administrator | MI RBI Analyst |
|---|------------------------------|------------------------------|
| 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 |
| 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 |

| Family | MI RBI Administrator | MI RBI Analyst |
|------------------------------------|------------------------------|------------------------------|
| Meridium Reference Tables | View, Update, Insert, Delete | View |
| Policy | View | View |
| Potential Degradation Mechanisms | View, Update, Insert, Delete | View |
| RBI Criticality Analysis | View, Update, Insert, Delete | View, Update, Insert, Delete |
| RBI 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 |

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

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

| Family | MI RBI Administrator | MI RBI Analyst |
|-------------------------|------------------------------|------------------------------|
| 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 V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V4.0.0.0 through V4.0.1.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

This module will be upgraded to V4.1.5.0 automatically when you upgrade the

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

Root Cause Analysis Security Groups and Roles

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

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

| Security Group | Roles |
|-------------------------|--|
| MI PROACT Administrator | MI FE Admin |
| MI PROACT Team Member | MI FE Admin MI FE PowerUser MI FE User |
| MI PROACT Viewer | MI FE Admin MI FE PowerUser MI FE User |

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

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

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

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

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

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.

Meridium APM Sync Server


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

| Step | Task | Required/Optional | Notes |
|------|--|-------------------|-------|
| 1 | Configure the Meridium APM Sync Server. Configuring the Meridium APM Sync Server includes completing the following steps: <ul style="list-style-type: none"> • Install Meridium APM Sync Services. • Install the Microsoft Sync Framework. • Modify the file web.config depending on Oracle database provider or SQL database provider. • Modify the file MeridiumSync.config. | Optional | None |
| 2 | Configure security for the MeridiumSyncService Service . | Optional | None |

Module level Configuration Tasks

| 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 | <p>Assign the desired Security Users to the following Security Groups:</p> <ul style="list-style-type: none"> • MI Operator Rounds Administrator • MI Operator Rounds Mobile User <div>  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. </div> | 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 |
|------|--|-------------------|---|
| 6 | <p>If you have created a new asset family, create a relationship definition as follows:</p> <ul style="list-style-type: none"> Relationship family: Has Checkpoint Predecessor: The asset family Successor: The Measurement Location family or Lubrication Requirement family Cardinality: One to Many | Optional | Required if you created an asset family that you want to link to a Measurement Location or a Lubrication Requirement using the <i>Has Checkpoint</i> relationship family. |
| 7 | <p>Create a relationship definition as follows:</p> <ul style="list-style-type: none"> Relationship family: Has OPR Recommendation Predecessor: Lubrication Requirement or Measurement Location family Successor: Operator Rounds Recommendation Cardinality: One to Many | Optional | Required, in mobile devices, if you want to create OPR Recommendations with photographs. |
| 8 | 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. |
| 9 | 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. |
| 10 | Set up the Scheduled Compliance task . | Required | The scheduled compliance task starts as soon as the Rounds module is deployed, and is set to run continuously as long as Rounds in use. |

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

Windows Mobile Hand Held Device

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

| Step | Task | Required/Optional | Notes |
|------|---|-------------------|---|
| 1 | Ensure that all the Windows Mobile handheld devices that you want to use with Operator Rounds meet the software requirements. | Required | None |
| 2 | Install the .NET Compact Framework. | Required | None |
| 3 | Install Microsoft SQL CE. Install Microsoft SQL CE. | Required | None |
| 4 | Install Microsoft Sync Services for ADO.NET. | Required | None |
| 5 | Install the Meridium APM Mobile Framework. | Required | None |
| 6 | Access Device Settings Screen. | Required | None |
| 7 | Identify the Sync Server within the Meridium Enterprise APM Mobile Framework. | Required | None |
| 8 | Specify the security query to be used with the Meridium APM Mobile Framework. | Required | None |
| 9 | Modify the user time-out value. | Optional | None |
| 10 | Install Operator Rounds. | Required | None |
| 11 | Configure barcode scanning. Configuring barcode scanning includes the followings steps: <ul style="list-style-type: none"> Install the Barcode add-on. Enable barcode scanning. | Optional | Required if you will use an Barcode scanner with Operator Rounds. |

| Step | Task | Required/Optional | Notes |
|------|---|-------------------|--|
| 12 | Configure RFID tag scanning. Configuring RFID scanning includes the following steps: <ul style="list-style-type: none">• Install the RFID add-on.• Enable RFID tag scanning. | Optional | Required if you will use an RFID scanner with Operator Rounds. |
| 13 | Install translations for Operator Rounds. | Optional | None |


Upgrading Rounds to V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

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

 **Note:** The following step is only applicable to the upgrades from v3.x to v4, and is not required if you are upgrading from an earlier v4 release.

In Meridium Enterprise APM V4.1.5.0, a Checkpoint can be linked to *one* asset. During upgrade from versions v3.x to V4.1.5.0, the related asset entity key is added to a field on the Checkpoint family. Hence, if you have Checkpoints that are linked to more than one asset, then you must remove the linkage to the additional assets prior to the upgrade.

To do so, perform the following steps:

1. Using an appropriate database management tool, run the following query in the database configured with the current version of Meridium Enterprise APM that you will configure to work with Meridium Enterprise APM V4.1.5.0.

For example, run the following query:

For Measurement Location in the database:

```
SELECT
```

```
MI_MEAS_LOC.ENTY_KEY as "ML_KEY",
```

```
MI_ENTITIES.ENTY_ID as "ML ID",
```

```
MIV_MIR_HS_MEASLOC.PRED_ENTY_KEY as "Asset Key"
```

```
FROM MI_MEAS_LOC
```



```
JOIN MIV_MIR_HS_MEASLOC ON MI_MEAS_LOC.ENTY_KEY = MIV_MIR_HS_MEASLOC.SUCC_
ENTY_KEY
```

```
JOIN MI_ENTITIES on MIV_MIR_HS_MEASLOC.SUCC_ENTY_KEY = MI_ENTITIES.ENTY_KEY
```

```
AND SUCC_ENTY_KEY IN
```

```
(
```

```
SELECT
```

```
SUCC_ENTY_KEY
```

```
FROM MIV_MIR_HS_MEASLOC
```

```
GROUP BY SUCC_ENTY_KEY
```

```
HAVING COUNT( * ) > 1
```

```
)
```

```
ORDER BY 1,2;
```

```
GO
```

For Lubrication Requirement in the database:

```
SELECT
```

```
MI_LUBR_REQ.ENTY_KEY as "LR_KEY",
```

```
MI_ENTITIES.ENTY_ID as "LR ID",
```

```
MIV_MIR_HS_MEASLOC.PRED_ENTY_KEY as "Asset Key"
```

```
FROM MI_LUBR_REQ
```

```
JOIN MIV_MIR_HS_MEASLOC ON MI_LUBR_REQ.ENTY_KEY = MIV_MIR_HS_MEASLOC.SUCC_
ENTY_KEY
```

```
JOIN MI_ENTITIES on MIV_MIR_HS_MEASLOC.SUCC_ENTY_KEY = MI_ENTITIES.ENTY_KEY
```

```
AND SUCC_ENTY_KEY IN
```

```
(
```

```
SELECT
```

```
SUCC_ENTY_KEY
```

```
FROM MIV_MIR_HS_MEASLOC
```

```
GROUP BY SUCC_ENTY_KEY
```

```
HAVING COUNT( * ) > 1
```

```
)
```

```
ORDER BY 1,2;
```

```
GO
```

A list of Checkpoints that are linked to multiple assets appears, providing the Checkpoint key, Checkpoint ID, and the Asset Key of the assets linked to the Checkpoint.

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

The left pane displays the records that are related to the Checkpoint.

3. Unlink the additional assets from the Checkpoint 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).

Upgrade from any version V4.1.0.0 through V4.1.1.1

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 1 | Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework , on the mobile device that you will use for data collection. | 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. |
| 3 | Confirm the assignment of Users for the existing route subscriptions and make additional assignments if needed. | Yes | Required |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 1 | Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework , on the mobile device that you will use for data collection. | 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. |
| 3 | Confirm the assignment of Users for the existing route subscriptions and make additional assignments if needed. | Yes | Required |

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

| Step | Task | Required? | Notes |
|------|--|-----------|--|
| 1 | Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework , on the mobile device that you will use for data collection. | 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. |
| 3 | Confirm the assignment of Users for the existing route subscriptions and make additional assignments if needed. | Yes | Routes that were subscribed to by a user in Meridium Mobile APM will be assigned to the user automatically through the DB upgrade process. |

Upgrade from any version V3.5.1 through V3.5.1.10.0

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 1 | Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework , on the mobile device that you will use for data collection. | 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. |
| 3 | Assign mobile device users to Routes. | No | Required if you will use a mobile device for data collection. |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 1 | Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework , on the mobile device that you will use for data collection. | 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. |
| 3 | Assign mobile device users to Routes. | No | Required if you will use a mobile device for data collection. |

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 1 | Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework , on the mobile device that you will use for data collection. | 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. |

| Step | Task | Required? | Notes |
|------|---------------------------------------|-----------|---|
| 3 | Assign mobile device users to Routes. | No | Required if you will use a mobile device for data collection. |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 1 | Install the Meridium Enterprise APM mobile application, or the Meridium APM Mobile Framework , on the mobile device that you will use for data collection. | 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. |
| 3 | Assign mobile device users to Routes. | No | Required if you will use a mobile device for data collection. |

Manage the Measurement Location Template Mappings

The Measurement Location Template family and the Measurement Location family are provided as part of the baseline Rounds data model. If you create a Measurement Location Template in the Meridium Enterprise APM application, you can then create a Measurement Location based on that template. If you do so, all values in Measurement Location Template fields that also exist on the Measurement Location will be mapped automatically to the new Measurement Location.

You might find that the Measurement Location Template and Measurement Location datasheets do not contain all the fields that you need. If so, you can add fields to the Measurement Location Template family so that the values from the new fields will be mapped to Measurement Locations based on that template. To do so, you will need to:

1. Create a new Measurement Location Template field.
2. Add the new Measurement Location Template field to the Measurement Location Template datasheet.
3. Create a new Measurement Location field. We recommend that the field caption of this field be the same as the field caption you defined for the Measurement Location Template field. This will ensure that the text in the field IDs that identify the fields are the same. If they are not the same, the values will not be mapped from the Measurement Location Template to the Measurement Location.
4. Add the new Measurement Location field to the Measurement Location datasheet.

Meridium APM Sync Services Tasks

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

Install Meridium APM Sync Services

Before You Begin

- You must be logged in as the administrator for the system.
- IIS must be reset before installation.
- [Install Microsoft Sync Framework](#).

Steps

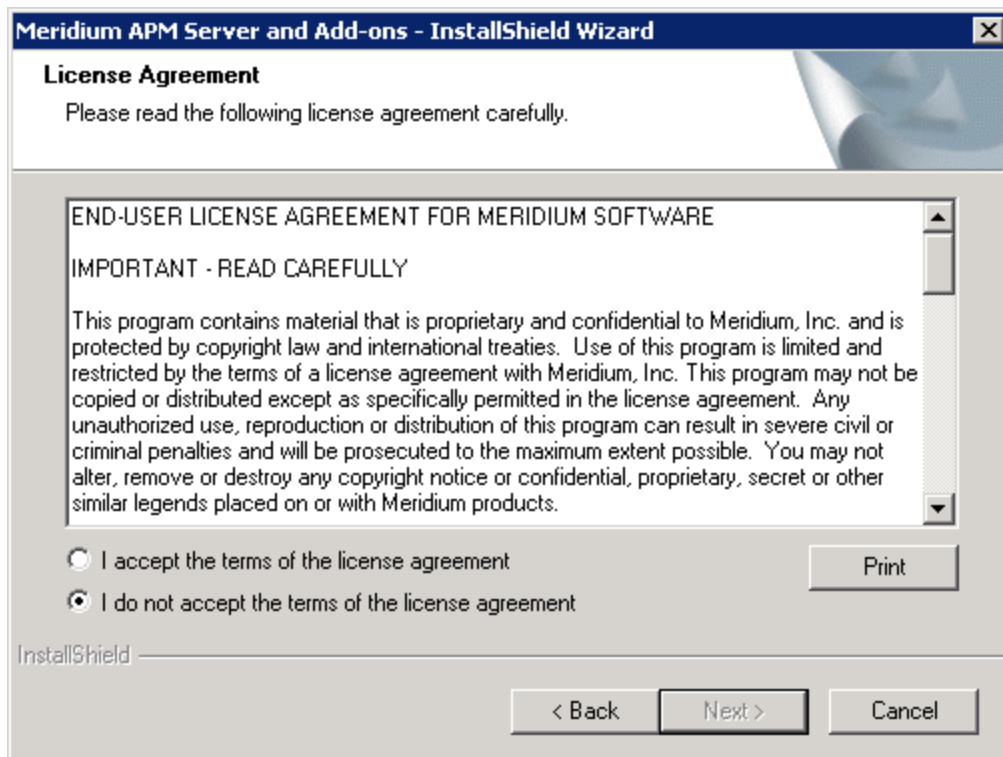
1. On the Meridium APM Sync Server machine, access the Meridium Enterprise APM distribution package, and then navigate to the **Meridium APM Server and Add-ons** folder.
2. Open the file **Setup.exe**.

The **Meridium APM Server and Add-ons** installer screen appears.



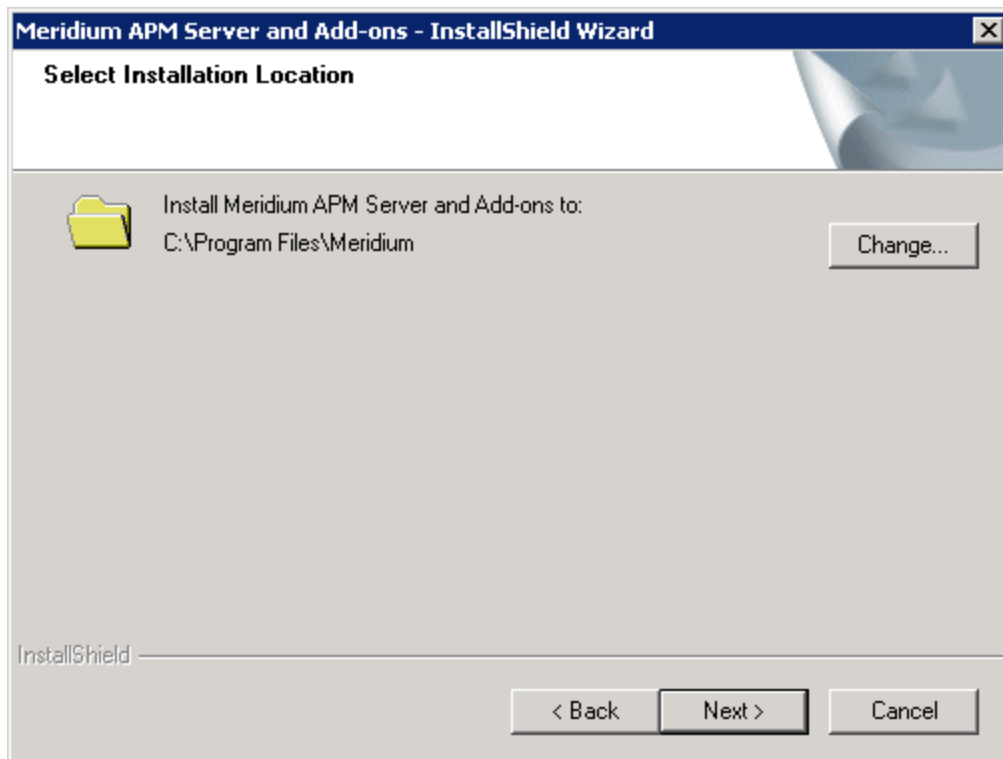
3. Select **Next**.

The **License Agreement** screen appears.



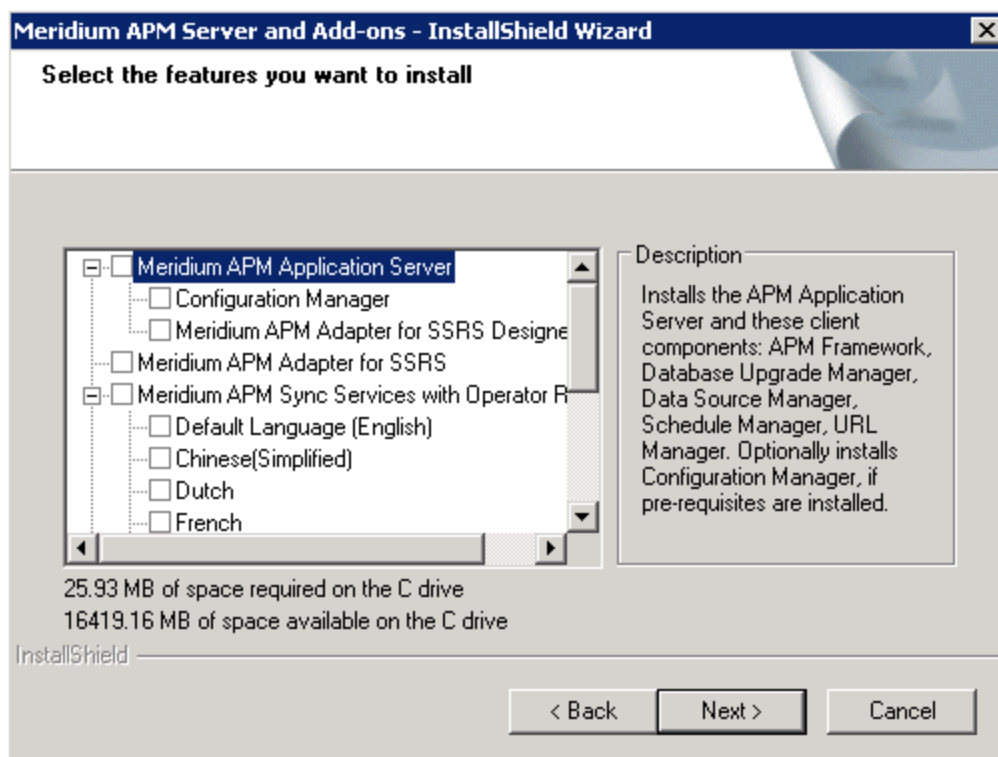
4. Read the License Agreement and, if you agree, select the **I accept the terms of the license agreement** option. Then, select **Next** button.

The **Select Installation Location** screen appears.



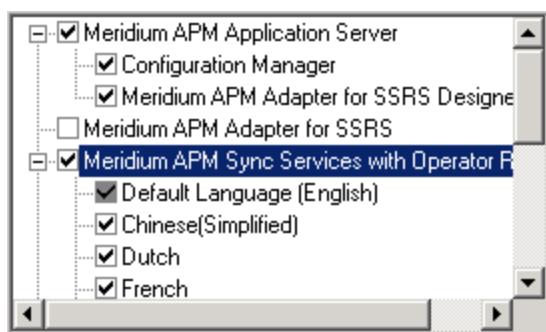
5. Select **Next** to accept the default location.

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



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

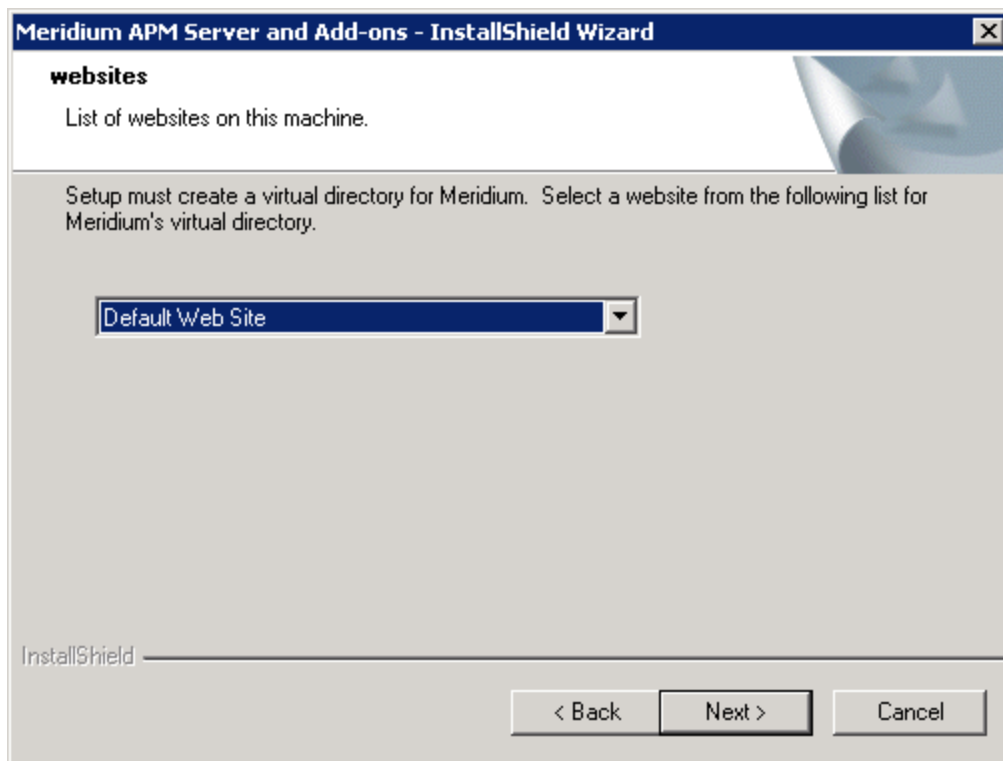
6. Select the **Meridium APM Application Server** and **Meridium APM Sync Services with Operator Rounds** check boxes. All the subnodes that appear below these nodes become selected automatically.




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

7. Select **Next**.

The **websites** screen appears.

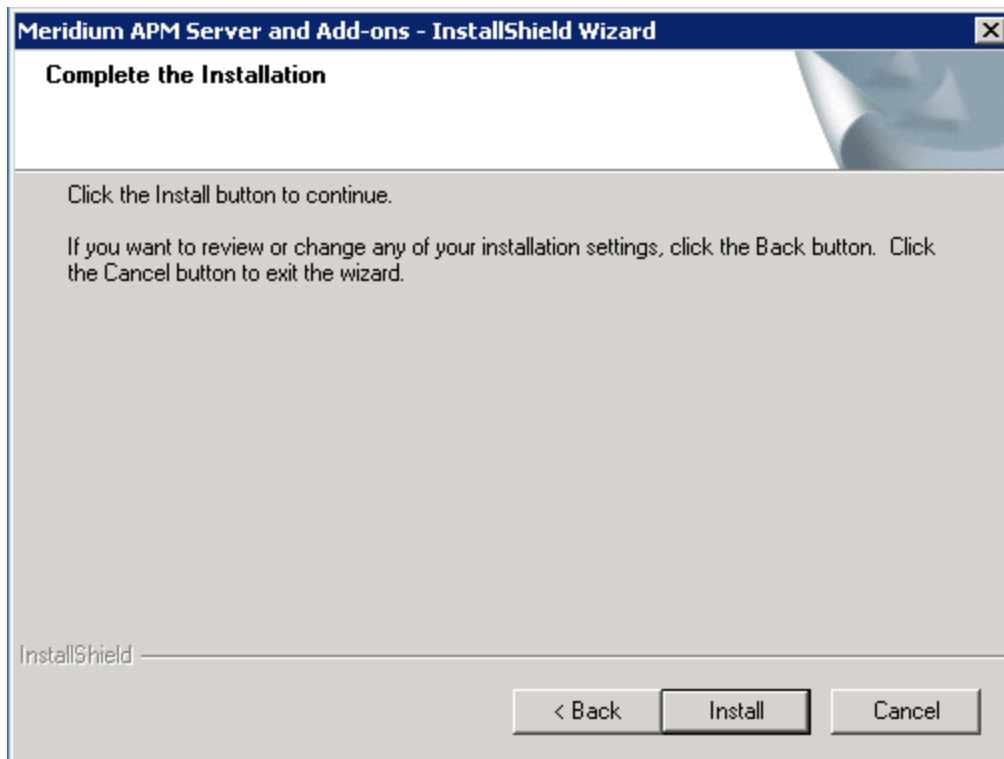


8. Select the website where you want to create a virtual directory for Meridium APM Sync Services.

 **Note:** You can accept the default selection.

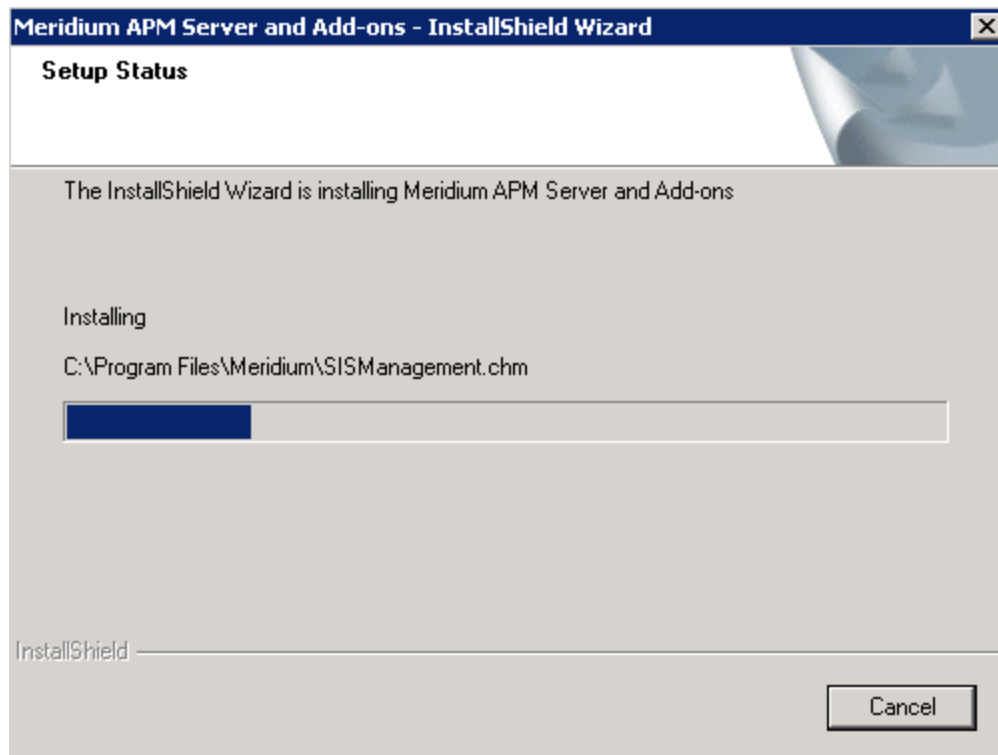
9. Select **Next**.

The **Complete the Installation** screen appears.

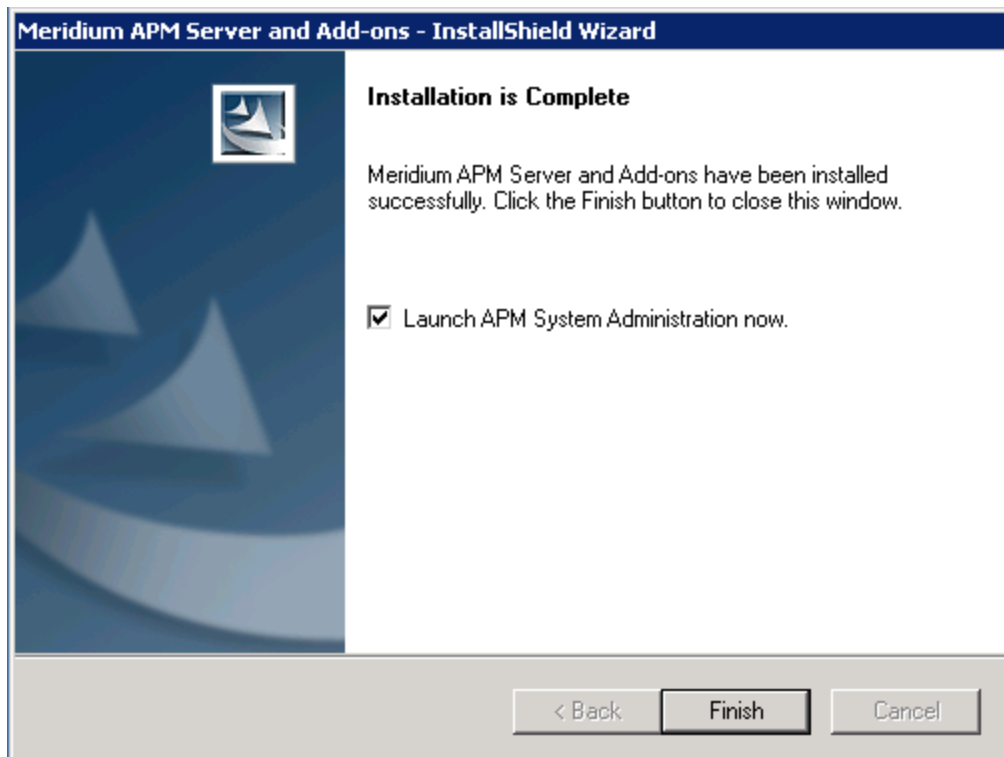


10. Select **Install**.

The **Setup Status** screen appears.




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



11. Select **Finish**.

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

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

Verify Installation of Meridium APM Sync Services

Steps

1. On the Meridium APM Sync Server machine, open Internet Explorer.
2. Navigate to the URL `http://<Sync_Server_Name>.meridium.com/MeridiumSyncService/MeridiumSyncService.svc`,
where `<Sync_Server_Name>` is the name or IP address of the server, on which Meridium APM Sync Services is installed.

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

SyncService Service

You have created a service.

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

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

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

C#

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


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

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

Visual Basic

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

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

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

Install Microsoft Sync Framework

Before You Begin

- You must be logged in as the administrator for the system.
- IIS must be reset before installation.
- [Install .NET Framework 3.5 SP1](#).


Steps

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

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

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

3. Select **Next**.

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


3. Select **Finish**.

Microsoft Sync Framework is now installed.

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

These instructions assume that:

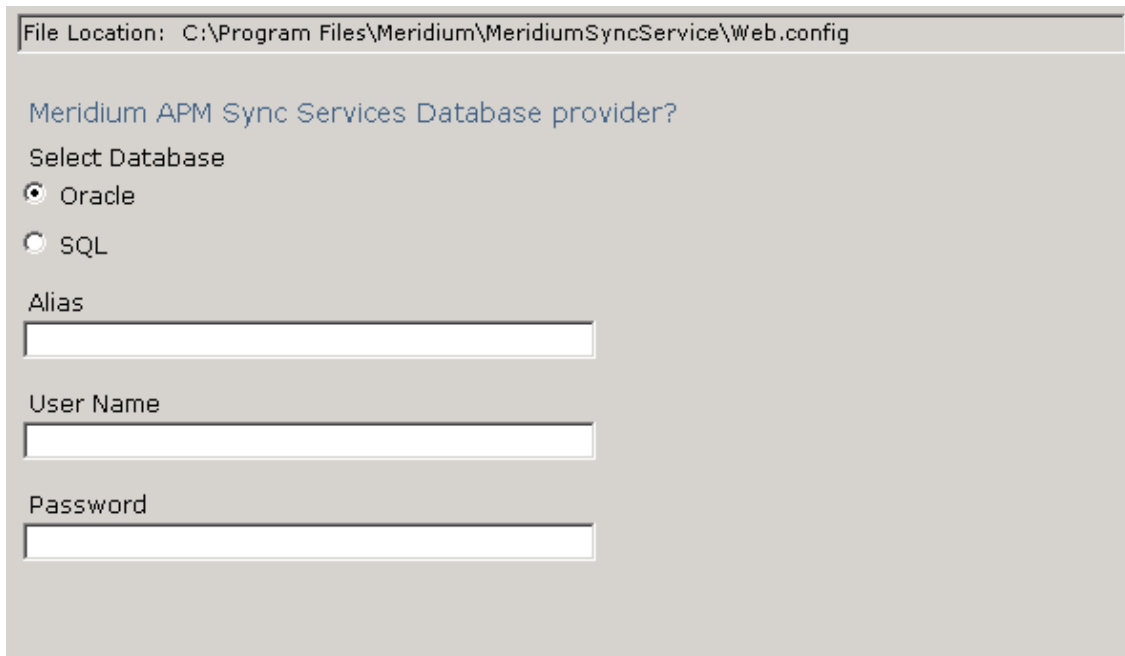
- The Oracle database that will contain the database tables for the Meridium APM Sync Services already exists.
- You have accessed the APM System Administration tool on the Meridium APM Sync Server machine.

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

Steps

1. Access the Meridium Enterprise APM System Administration Tool.
2. In the **Configuration** section, select **Sync Services Database** link.

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



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

Meridium APM Sync Services Database provider?

Select Database

☒ Oracle

☐ SQL

Alias

User Name

Password

3. In the **Select Database** section, accept the default selection, **Oracle**.
4. In the **Alias** box, enter the database alias. This value is case-sensitive.


5. In the **User Name** box, enter the user name that you want to use to connect to the database.
6. In the **Password** box, enter the password associated with the user name you entered in the **User Name** box. This setting is case-sensitive.
7. At the bottom of the APM System Administration window, select **Save**.

Your changes are saved to the web.config file.

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

These instructions assume that:

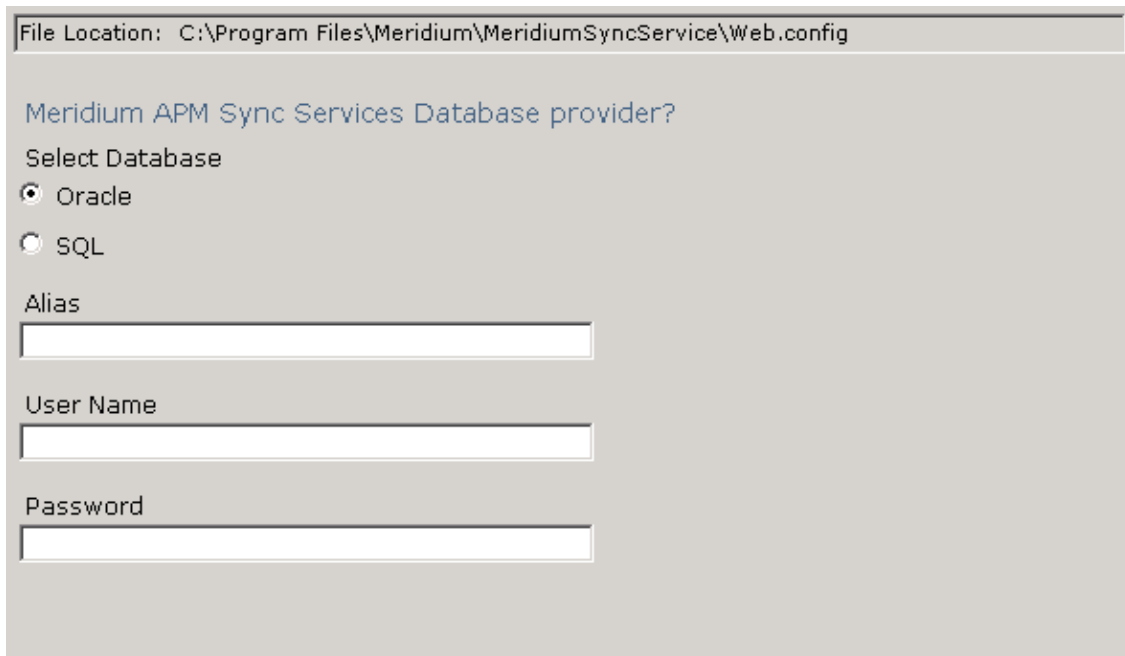
- The SQL database that will contain the database tables for the Meridium APM Sync Services already exists.
- You have accessed the APM System Administration tool on the Meridium APM Sync Server machine.

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

Steps

1. Access the Meridium Enterprise APM System Administration Tool.
2. In the **Configuration** section, select **Sync Services Database**.

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



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

Meridium APM Sync Services Database provider?

Select Database

☒ Oracle

☐ SQL

Alias

User Name

Password

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

The SQL settings appear and replace the Oracle settings.

The screenshot shows a configuration window titled "Meridium APM Sync Services Database provider?". At the top, a text box displays the "File Location: C:\Program Files\Meridium\MeridiumSyncService\Web.config". Below the title, there is a section labeled "Select Database" with two radio button options: "Oracle" and "SQL". The "SQL" option is selected. Below this, there are four text input fields labeled "DB Server", "DB Name", "User Name", and "Password", each with a corresponding empty text box for user input.

4. In the **DB Server** box, enter the name of the Database Server that contains the database.
5. In the **DB Name** box, enter the database name.
6. In the **User Name** box, enter the user name that you want to use to connect to the database.
7. In the **Password** box, enter the password associated with the user name you entered in the **User Name** box. This setting is case-sensitive.
8. At the bottom of the **APM System Administration** window, select **Save**.

Modify Meridium Sync Config

When you perform a sync operation in the Meridium APM Mobile Framework, the device connects to the Meridium APM Sync Server, which in turn connects to the specified Meridium APM Application Server and logs in to the data source defined in the file MeridiumSync.config. Security User credentials are required for logging in to the data source.

Before you can perform a sync operation, you will need to define the following settings on the Meridium APM Sync Server:

- The Meridium Enterprise APM Server
- The Meridium Enterprise APM data source
- The Meridium APM Sync Services Security User credentials that will be used to connect the Meridium APM Sync Server to the Meridium Enterprise APM database

The user you specify must have the family-level privileges required to access all data that needs to be downloaded to the Windows Mobile Device for a given application. The MI Operator Rounds Administrator and MI Operator Rounds Mobile User Security Groups, which are provided with the baseline Operator Rounds product, have these privileges. Therefore, you can create your own Security User and assign it to either one of these Security Groups for this purpose.

To specify these settings, you will need to modify the MeridiumSync.Config file via the APM System Administration tool on the Meridium APM Sync Server machine.

The following instructions provide details on defining the Meridium Enterprise APM Server, data source, and Sync Services Security User credentials in the MeridiumSync.config file. These instructions assume that you have:

- Created the Security User whose credentials you will enter in the configuration file and granted them the appropriate permissions to Operator Rounds families.
- Accessed the APM System Administration tool on the Meridium APM Sync Services server machine.

Steps

1. Access the Meridium Enterprise APM System Administration Tool.
2. In the **Configuration** section, select **Meridium Sync Config** link.

The contents of the MeridiumSync.Config file appear in the Meridium Sync Config Changes section.

File Location: C:\Program Files\Meridium\MeridiumSyncService\Bin\MeridiumSync.Config

Meridium Sync Config Changes

Server:


Data Source:

User Name:

Password:

By default, the **Server** box contains the name of the machine on which you are currently working.

3. In the **Server** box, enter the name of the Meridium Enterprise APM Server machine that you want to use with Sync Services.
4. In the **Data Source** box, enter the name of the Meridium Enterprise APM data source to which you want to log in. This data source must be configured on the Application Server machine defined in the **Server** box.

 **Note:** This value is case-sensitive. You must define the data source name using the same case that is used in Data Source Manager.

5. In the **User Name** box, enter the User ID of the Meridium APM Security User that you want to use for logging in to the data source identified in the **Data Source** box.
6. In the **Password** box, enter the password associated with the Meridium Enterprise APM Security User identified in the **User Name** box. This password will be encrypted in the file.
7. At the bottom of the **APM System Administration** window, select **Save**.

Your changes are saved to the MeridiumSync.config file.

Configure Security for Meridium Sync Service

When you install Meridium APM Sync Services, the service MeridiumSyncService is created under the Default Web Site in IIS on the Meridium APM Sync Server machine. The Windows user account that is configured at the Default Web Site level to be used for anonymous access is granted permission to the following folder:

<root>\MeridiumSyncService

Where <root> is the drive and root folder where the Meridium APM Sync Services was installed (e.g., **C:\Program Files\Meridium**).

If you configure a different Windows user account to be used for anonymous access at the MeridiumSyncService level, you must grant that user the following permissions to the folder **<root>\MeridiumSyncService**:

- Modify
- Read & Execute
- List Folder Contents
- Read
- Write

If these permissions are not granted, when any user attempts to perform a sync operation in the Meridium APM Mobile Framework, an error message will be displayed, and synchronization will fail. For details on granting these permissions, see the Microsoft documentation.

Windows Mobile Handheld Devices

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

Install the .NET Compact Framework on Windows Mobile Device

Before You Begin

- You must be logged in as the administrator on the Windows Mobile device.
- [Install Microsoft Sync Framework.](#)
- [Install Meridium APM Sync Services](#)

Steps

1. On the Windows Mobile handheld device, open Internet Explorer, and navigate to the URL **http://<machine>/MeridiumSyncService**, where **<machine>** is the name or IP address of the server on which Meridium APM Sync Services is installed.

You are redirected automatically to one of the following URLs, and then a download screen appears:

- For Windows Mobile devices: **http://<machine>/MeridiumSyncService/winmodownload.aspx.**
2. If the device is running Windows Mobile 2003, select **PPC2003\NETCFv35.PPC.ARMV4.CAB.**

or

If the device is running Windows Mobile 5.0 or later, select **WCE500\NETCFv35.WM.ARMV4i.CAB.**

A message appears, asking if you really want to download the file.

3. Select **Yes.**

The file is downloaded, and the .NET Compact Framework is installed. When the installation is complete, a message will appear indicating that the installation is successful and instructing you to restart the device.

Install Microsoft SQL CE on Windows Mobile Device

Steps

1. On the Windows Mobile handheld device, open Internet Explorer, and then navigate to the URL **http://<machine>/MeridiumSyncService**, where **<machine>** is the name or IP address of the server on which Meridium APM Sync Services is installed.

You are redirected automatically to one of the following URLs, and then a download screen appears:

- For Windows Mobile devices: **http://<machine>/MeridiumSyncService/winmodownload.aspx**.
2. If the device is running Windows Mobile 2003, select **PPC2003\SQLCE.PPC.ARM4.CAB**.

or

If the device is running Windows Mobile 5.0 or later, select **WCE500\SQLCE.WCE5.ARMV4i.CAB**.

A message appears, asking if you really want to download the file.

3. Select **Yes**.

The file is downloaded, and the Microsoft SQL CE is installed. When the installation is complete, a message will appear, indicating that the installation is successful.

Install Microsoft Sync Services for ADO.NET on Windows Mobile Device

Steps

1. On the Windows Mobile handheld device, open Internet Explorer, and then navigate to the URL **http://<machine>/MeridiumSyncService**, where **<machine>** is the name or IP address of the server on which Meridium APM Sync Services is installed.

You are redirected automatically to one of the following URLs, and then a download screen appears:

- For Windows Mobile devices: **http://<machine>/MeridiumSyncService/winmodownload.aspx**.

2. If the device is running Windows Mobile 2003, select **PPC2003\SYNCSERVICES.WCE.CAB**.

or

If the device is running Windows Mobile 5.0 or later, select **WCE500\SQLCE.WCE5.ARMV4i.CAB**.

A message appears, asking if you really want to download the file.

3. Select **Yes**.

The file is downloaded, and the **Microsoft Sync Services for ADO.NET** is installed. When the installation is complete, a message will appear, indicating that the installation is successful.

Install the Meridium APM Mobile Framework on Windows Mobile Device

Steps

1. On the Windows Mobile handheld device, open Internet Explorer, and then navigate to the URL **http://<machine>/MeridiumSyncService**, where **<machine>** is the name or IP address of the server on which Meridium Enterprise APM Sync Services is installed.

You are redirected automatically to one of the following URLs, and then a download screen appears:

- For Windows Mobile devices: **http://<machine>/MeridiumSyncService/winmodownload.aspx**.

2. Select **MF.X.APM.360.ARM4.CAB**.

A message appears, asking if you really want to download the file.

3. Select **Yes**.

The file is downloaded, and the Meridium APM Mobile Framework is installed. When the installation is complete, a message will appear, indicating that the installation is successful.

The **Meridium APM Mobile Framework** screen appears, indicating that no users are available on the Windows Mobile device yet.

Access Device Settings Screen on Windows Mobile Device

Steps

1. On the Windows Start menu, select **Programs**.

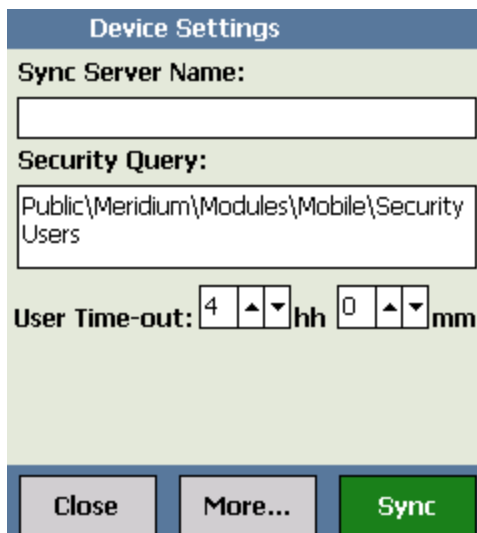
The **Programs** screen appears.

2. Select **APM Mobile Framework**.

The **Meridium APM Mobile Framework** screen appears.

3. Select **Settings**.

The **Device Settings** screen appears.



Device Settings

Sync Server Name:

Security Query:

Public\Meridium\Modules\Mobile\Security Users

User Time-out: 4 hh 0 mm

Close **More...** **Sync**

Identify the Sync Server Within the APM Mobile Framework on Windows Mobile Device

Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** screen appears.

2. Select **APM Mobile Framework**.


The **Meridium APM Mobile Framework** screen appears.



3. Select **Settings**.

The **Device Settings** screen appears.

4. In the **Sync Server Name** box, type the name or IP address of the server on which Meridium APM Sync Services is installed.

 **Note:** At this point, you can also specify the security query.

5. Select **Sync**.

The **Synchronizer** screen appears, displaying the progress of the synchronization process. When the synchronization process is complete, a message will appear, indicating whether or not the process was successful.

6. When the process is complete, select **Close**.

Specify the Security Query on Windows Mobile Device

1. On the Windows Start menu, select **Programs**.

The **Programs** screen appears.

2. Select **APM Mobile Framework**.

The **Meridium APM Mobile Framework** screen appears.

3. Select **Settings**.

The **Device Settings** screen appears, displaying the **Sync Server Name** and **Security Query** boxes. The **Security Query** box is used to store the path to the query that determines who can log into Operator Rounds on the device. Note that the default security query is Security Users, which is stored in the Meridium APM Catalog folder **\\Public\Meridium\Modules\Mobile**.

4. In the **Security Query** box, enter the path to the query that you want to use to determine who can log into Operator Rounds on the device.

If the query is stored in the Meridium APM Catalog folder **\\Public\Meridium\Modules\Operator Rounds\Queries\Download Queries**, type the name of the query. If the query is stored in a subfolder of the Meridium APM Catalog folder **\\Public\Meridium\Modules\Operator Rounds\Queries\Download Queries**, type the path to the query, starting with the first subfolder name.

For example, if the Chicago Users query is stored in the Meridium APM Catalog folder **\\Public\Meridium\Modules\Operator Rounds\Queries\Download Queries**, enter Chicago Users.

Likewise, if the Chicago Users query is stored in the Meridium APM Catalog folder **\\Public\Meridium\Modules\Operator Rounds\Queries\Download Queries\Users\Chicago**, enter Users\Chicago\Chicago Users.

5. Select **Sync**.

The **Synchronizer** screen appears, displaying the progress of the synchronization process.

Modify User Time-out Value on Windows Mobile Device

By default, if the Windows Mobile Device is left idle for four hours or longer and is not in the process of downloading data, the current Security User will be logged out of the Meridium APM Mobile Framework automatically, and the log in screen will be displayed. You can change the default user time-out value via the **Device Settings** screen to decrease or increase the amount of time a user should remain logged in to the Meridium APM Mobile Framework if the device is left idle and is not in the process of downloading data.

Steps

1. Access the **Device Settings** screen.
2. Use the **User Time-out** boxes to select or type the value that represents the amount of time a user should remain logged in to the Meridium APM Mobile Framework, if the device is left idle and is not in the process of downloading data.
3. Select **Close**.

The **login** screen is highlighted, and your changes to the time-out value are applied.

Install Operator Rounds on Windows Mobile Device

Before You Begin

- You must be logged in as the administrator for the system.
- [Install Meridium APM Mobile Framework](#).

Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** screen appears.

2. Select **APM Mobile Framework**.

The **Meridium APM Mobile Framework** screen appears.

3. Select **Applications**.


The **Add/Remove Applications** screen appears.

4. In the list of available applications, select the **Install** button that appears to the right of **Operator Rounds**.

A message appears, asking if you want to install Operator Rounds.

5. Select **Yes**.

The installation process begins. The **Meridium APM Mobile Framework** closes, and the **Operator Rounds** application is installed.

 **Note:** After the installation is complete, the Meridium APM Mobile Framework will reopen automatically and return you to the **Meridium APM Mobile Framework** screen.

Install the Barcode Add-on on Windows Mobile Device

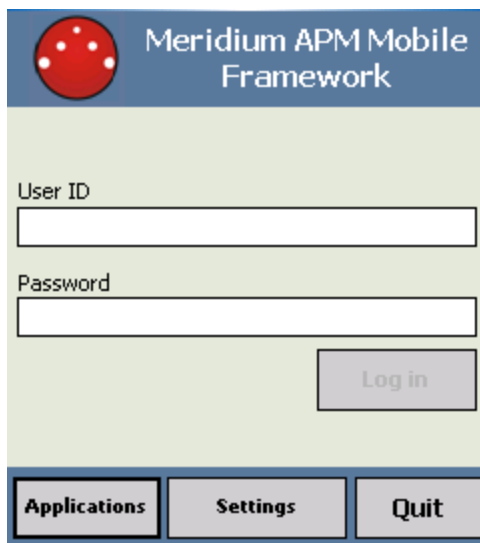
Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** window appears.

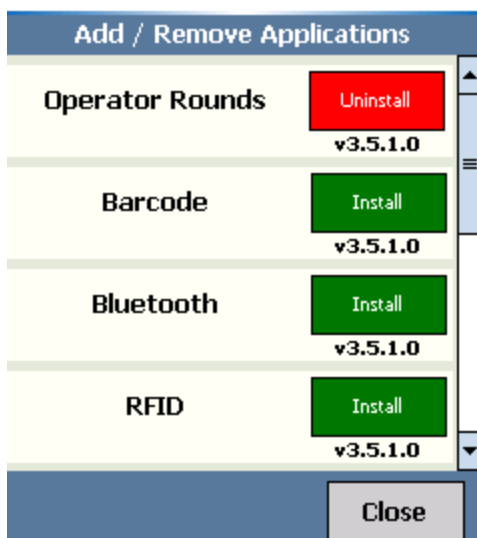
2. Select **APM Mobile Framework**.

The **Meridium APM Mobile Framework** window appears.



3. Select **Applications**.

The **Add/Remove Applications** window appears.




4. In the list of available applications, select the **Install** button that appears to the right of **Barcode**.

A message appears, asking if you want to install the Barcode add-on.

5. Select **Yes**.

The installation process begins. The Meridium APM Mobile Framework closes, and the Barcode add-on is installed.

 **Note:** After the installation is complete, the Meridium APM Mobile Framework will reopen automatically, and the Meridium APM Mobile Framework screen appears and you can enable Barcode scanning.

Enable Barcode Scanning on Windows Mobile Device

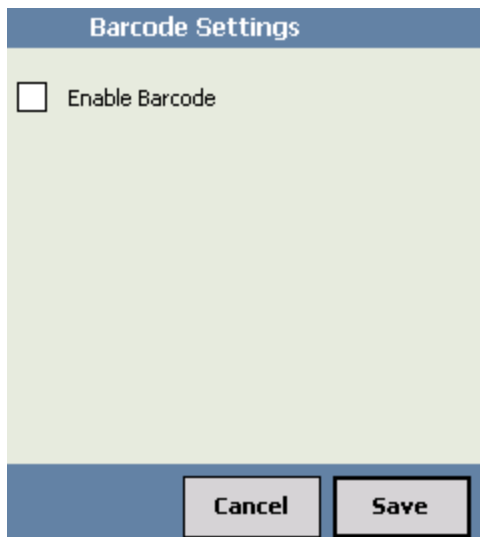
Before You Begin

- [Install the Barcode add-on.](#)

Steps

1. On the Windows Mobile device, [access the Device Settings screen.](#)
2. Select **More**.
3. Select **Barcode**.

The **Barcode Settings** screen appears.



4. Select the **Enable Barcode** check box.
 5. Select **Save**.
- Barcode scanning is enabled, and the Device Settings screen is highlighted.
6. Select **Close**.

You are returned to the **login** page.

Install the RFID Add-on on Windows Mobile Device

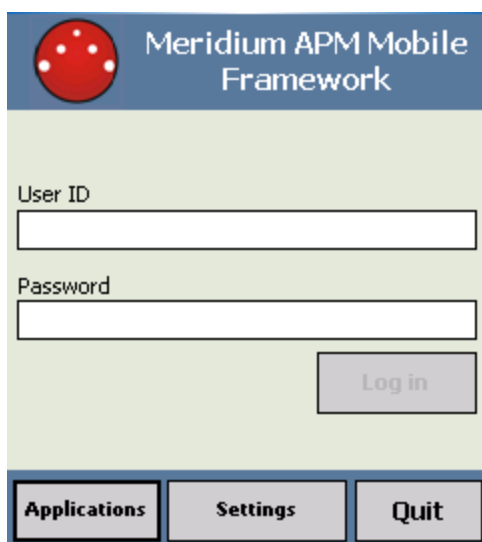
Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** screen appears.

2. Select **APM Mobile Framework**.

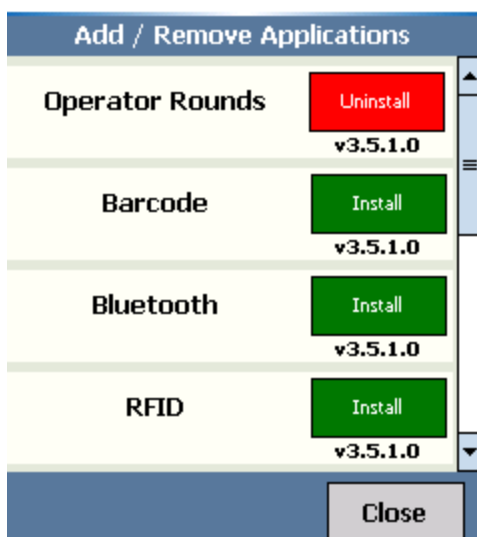
The **Meridium APM Mobile Framework** screen appears.



The screenshot shows the Meridium APM Mobile Framework application interface. At the top is a blue header with a red circular logo containing four white dots and the text "Meridium APM Mobile Framework". Below the header is a light green background with two input fields: "User ID" and "Password". To the right of the "Password" field is a grey "Log in" button. At the bottom, there is a blue bar with three buttons: "Applications", "Settings", and "Quit".

3. Select **Applications**.

The **Add/Remove Applications** screen appears.



The screenshot shows the "Add / Remove Applications" screen. It has a blue header with the text "Add / Remove Applications". Below the header is a list of applications with their respective status buttons and versions. The applications are: "Operator Rounds" with a red "Uninstall" button and version "v3.5.1.0"; "Barcode" with a green "Install" button and version "v3.5.1.0"; "Bluetooth" with a green "Install" button and version "v3.5.1.0"; and "RFID" with a green "Install" button and version "v3.5.1.0". At the bottom right is a grey "Close" button.


| Application | Action | Version |
|-----------------|-----------|----------|
| Operator Rounds | Uninstall | v3.5.1.0 |
| Barcode | Install | v3.5.1.0 |
| Bluetooth | Install | v3.5.1.0 |
| RFID | Install | v3.5.1.0 |

4. In the list of applications, select the **Install** button that appears to the right of **RFID**.

A message appears, asking if you want to install the RFID add-on.

5. Select **Yes**.

The installation process begins. During this process, the **Meridium APM Mobile Framework** closes, and the RFID add-on is installed.

 **Note:** After the installation process is complete, the **Meridium APM Mobile Framework** reopens automatically, and the Meridium APM Mobile Framework screen appears.

Enable RFID Tag Scanning on Windows Mobile Device

Before You Begin

- [Install the RFID add-on.](#)

Steps

1. [Access the Device Settings screen.](#)



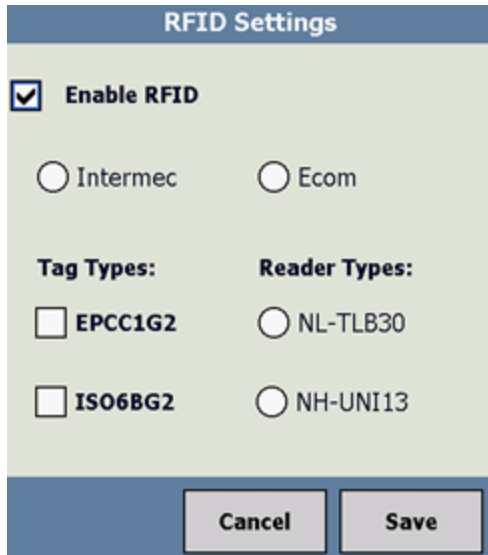
2. Select **More**.

A menu appears, displaying additional buttons that are conditionally enabled according to the add-ons that you have installed.



3. Select **RFID**.

The **RFID Settings** screen appears.




The image shows a dialog box titled "RFID Settings". At the top, there is a checked checkbox labeled "Enable RFID". Below this, there are two radio button options: "Intermec" and "Ecom". Under the "Intermec" section, there are two checkboxes: "EPCC1G2" and "ISO6BG2". Under the "Ecom" section, there are two radio button options: "NL-TLB30" and "NH-UNI13". At the bottom of the dialog box, there are two buttons: "Cancel" and "Save".

4. Select the **Enable RFID** check box.
5. Select the type of **RFID reader** (i.e., Intermec or Ecom) that you will use.
6. If you selected Intermec, select the check box that corresponds with the classification of RFID tags that you will use:
 - **EPCC1G2**: Select this check box if your RFID tags are classified as Electronic Product Code Class 1 Generation 2 tags.
 - **ISO6BG2**: Select this check box if your RFID tags are classified as International Standards Organization 18000-6B Generation 2 tags.
7. If you select Ecom, select the check box that corresponds with the classification of RFID types that you will use:
 - **NL-TLB30**: Select this check box if your RFID reader types are classified as Low Frequency.
 - **NH-UNI13**: Select this check box if your RFID reader types are classified as High Frequency.
8. Select **Save**.
 RFID scanning is enabled, and you are returned to the **Device Settings** screen.
9. Select **Close**.

Install Translations for Operator Rounds on Windows Mobile Device

Before You Begin

- You must be logged in as the administrator for the system.
- [Install Meridium APM Mobile Framework](#).

 **Note:** To deploy translations for Operator Rounds, in addition to completing the following steps, you will also need to ensure that the regional setting on the device is set to the corresponding language.

Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** screen appears.

2. Select **APM Mobile Framework**.

The **Meridium APM Mobile Framework** screen appears.

3. Select **Applications**.


The Add/Remove Applications screen appears.

4. In the list of available applications, select the **Install** button that appears to the right of the application that you want to install.

A message appears, asking if you are sure that you want to install translations for the selected language.

5. Select **Yes**.

The installation process begins. **Meridium APM Mobile Framework** closes, and the translations are installed.

 **Note:** After the installation is complete, the Meridium APM Mobile Framework will reopen automatically and return you to the Meridium APM Mobile Framework screen.

Uninstall Meridium APM Mobile Framework on Windows Mobile Device

Steps

1. On the Windows Mobile handheld device, access the **Remove Programs** feature supplied via the operating system.
2. In the list of installed programs, select **MFX APM Mobile Framework**, and then select **Remove**.

A message appears, asking if you really want to remove the program.

3. Select **Yes**.

The Meridium APM Mobile Framework is removed from the Windows Mobile handheld device.

Uninstall then RFID Add-on on Windows Mobile Device

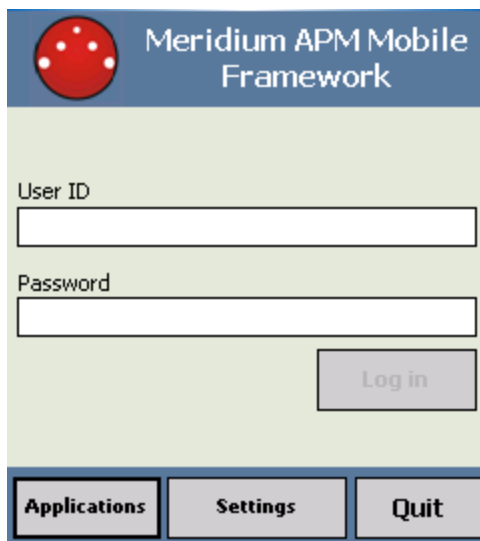
Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** screen appears.

2. Select **APM Mobile Framework**.

The **Meridium APM Mobile Framework** screen appears.



3. Select **Applications**.

The **Add/Remove Applications** screen appears. This following image shows an example of the **Add/Remove Applications** screen.



4. In the list of available applications, to the right of **RFID** , select **Uninstall**.

The **Uninstall** screen appears, prompting you to enter your username and password.

The screenshot shows a window titled "Uninstall". It contains the text "Enter login information to remove the Operator Rounds installation." Below this text are two input fields: "User ID" and "Password". An "Uninstall" button is located below the "Password" field, and it is currently disabled (grayed out). A "Cancel" button is located at the bottom right of the window.

5. In the **User ID** box, enter your username.

The **Uninstall** button is enabled.

6. In the **Password** box, enter your password.

Note: If the credentials that you enter are not associated with a Security User who is a Super User or member of the MI Operator Rounds Administrator Secur-

ity Group, a message will appear, indicating that you do not have the privileges required to uninstall the application.

7. Select **Uninstall**.

The uninstallation process begins. The Meridium APM Mobile Framework closes, and the **RFID** add-on is uninstalled.

Uninstall the Barcode Add-on on Windows Mobile Device

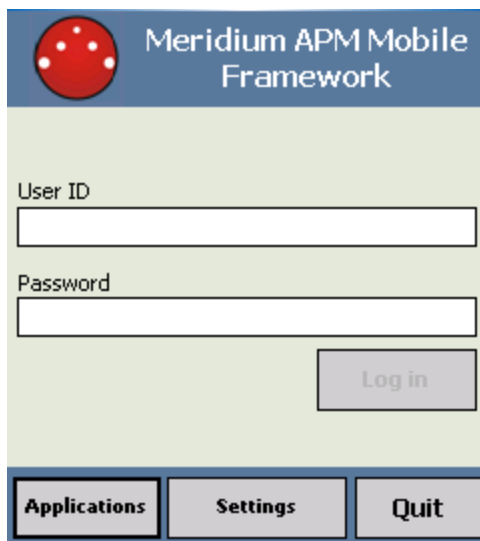
Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** screen appears.

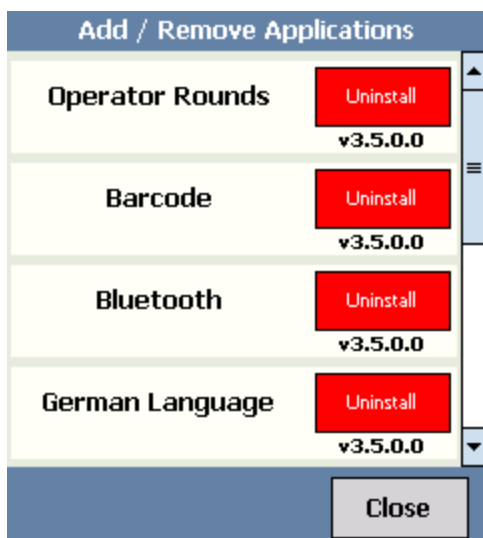
2. Select **APM Mobile Framework**.

The **Meridium APM Mobile Framework** screen appears.



3. Select **Applications**.

The **Add/Remove Applications** screen appears. This following image shows an example of the **Add/Remove Applications** screen.



4. In the list of available applications, to the right of **Barcode**, select **Uninstall**.

The **Uninstall** screen appears, prompting you to enter your username and password.

The screenshot shows a window titled "Uninstall". It contains the text "Enter login information to remove the Operator Rounds installation." Below this text are two input fields: "User ID" and "Password". To the right of the "Password" field is a disabled "Uninstall" button. At the bottom right of the window is a "Cancel" button.

5. In the **User ID** box, enter your username.
The **Uninstall** button is enabled.
6. In the **Password** box, enter your password.

Note: If the credentials that you enter are not associated with a Security User who is a Super User or member of the MI Operator Rounds Administrator Secur-

ity Group, a message will appear, indicating that you do not have the privileges required to uninstall the application.

7. Select **Uninstall**.

The uninstallation process begins. The Meridium APM Mobile Framework closes, and the Barcode add-on is uninstalled.

Uninstall Translations for Operator Rounds on Windows Mobile Device

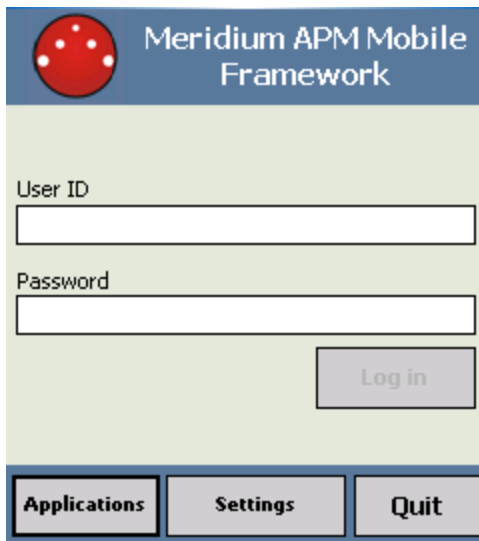
Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** screen appears.

2. Select **APM Mobile Framework**.

The **Meridium APM Mobile Framework** screen appears.



3. Select **Applications**.

The **Add/Remove Applications** screen appears. This following image shows an example of the **Add/Remove Applications** screen.



4. In the list of available applications, to the right of the language whose translation you want to uninstall, select **Uninstall**.

The **Uninstall** screen appears, prompting you to enter your username and password.

The screenshot shows a window titled "Uninstall". It contains the text "Enter login information to remove the Operator Rounds installation." Below this text are two input fields: "User ID" and "Password". To the right of the "Password" field is a grey "Uninstall" button. At the bottom right of the window is a grey "Cancel" button.

5. In the **User ID** box, enter your username.
The **Uninstall** button is enabled.
6. In the **Password** box, enter your password.

Note: If the credentials that you enter are not associated with a Security User who is a Super User or member of the MI Operator Rounds Administrator

Security Group, a message will appear, indicating that you do not have the privileges required to uninstall the application.

7. Select **Uninstall**.

The uninstallation process begins. The Meridium APM Mobile Framework closes, and the translations add-on for a language is uninstalled.

Uninstall Operator Rounds on Windows Mobile Device

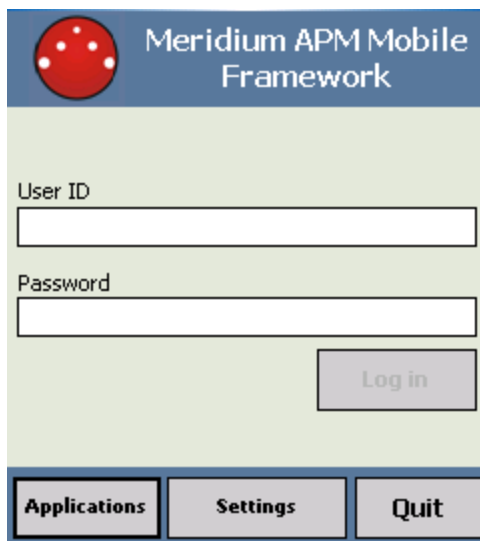
Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** screen appears.

2. Select **APM Mobile Framework**.

The **Meridium APM Mobile Framework** screen appears.



3. Select **Applications**.

The **Add/Remove Applications** screen appears. This following image shows an example of the **Add/Remove Applications** screen.




4. In the list of available applications, to the right of the **Operator Rounds**, select **Uninstall**.

The **Uninstall** screen appears, prompting you to enter your username and password.

A screenshot of a dialog box titled "Uninstall". The text inside says "Enter login information to remove the Operator Rounds installation." Below this text are two input fields: "User ID" and "Password". The "User ID" field is highlighted with a yellow background. Below the input fields is a grey button labeled "Uninstall". At the bottom right of the dialog box is a grey button labeled "Cancel".

5. In the **User ID** box, enter your username.
The **Uninstall** button is enabled.
6. In the **Password** box, enter your password.

 **Note:** If the credentials that you enter are not associated with a Security User who is a Super User or member of the MI Operator Rounds Administrator

Security Group, a message will appear, indicating that you do not have the privileges required to uninstall the application.

7. Select **Uninstall**.


The uninstallation process begins. The Meridium APM Mobile Framework closes, and the **Operator Rounds** is uninstalled.

Upgrade Windows Mobile Handheld Device

After you upgrade the Meridium APM Sync Server, you will need to upgrade each Windows Mobile Device that connects to that server. This can be done by initiating a synchronization operation from within the Meridium APM Mobile Framework or from within Operator Rounds on each device that needs to be upgraded. After any updated data has been transferred to the server, a message will appear in the synchronization log, indicating that the server has been updated and that an update of the handheld components needs to be performed. The update will begin automatically.

During the update process, depending upon the device's operating system, messages may appear indicating that the Meridium APM components are already installed and that they need to be reinstalled. If you see these messages, you must select the **Yes** button. One message will appear for each component that is installed (i.e., Meridium APM Mobile Framework, Operator Rounds, and the Barcode and/or RFID add-ons). On other device operating systems, however, these messages do not appear, and the Meridium APM Mobile Framework closes automatically to allow the upgrade process to be completed.

When the upgrade process is complete, all applications that were previously installed will be reinstalled and updated automatically to the version to which you upgraded. In addition, any settings that were previously configured will be retained (e.g., the name of the security query). You will be redirected to the Operator Rounds login screen, where you can log in and begin using the Operator Rounds application.

 **Note:** You are not required to update Windows Mobile Devices all at once or within a specific timeframe after upgrading the Meridium APM Sync Server. If desired, you can simply allow the update to occur automatically the next time users synchronize with the server.

Security Groups and Privileges In Rounds

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

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

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

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 | MI Operator Rounds Administrator | MI Operator Rounds Mobile User | MAPM Security Group |
|-----------------|----------------------------------|--------------------------------|---------------------|
| Entity Families | | | |

| Family | 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 |
| 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, Update, Insert, Delete | View, Update, Insert, Delete |
| 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, Update, Insert, Delete | View, Update, Insert, Delete |
| Route | View, Update, Insert, Delete | View, Update | View, Update |

| Family | MI Operator Rounds Administrator | MI Operator Rounds Mobile User | MAPM Security Group |
|------------------------------|----------------------------------|--------------------------------|------------------------------|
| 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 |
| 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, Update, Insert, Delete | View, Update, Insert, Delete |
| Has Route | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete |

| Family | MI Operator Rounds Administrator | MI Operator Rounds Mobile User | MAPM Security Group |
|------------------------------|----------------------------------|--------------------------------|------------------------------|
| 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 |

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

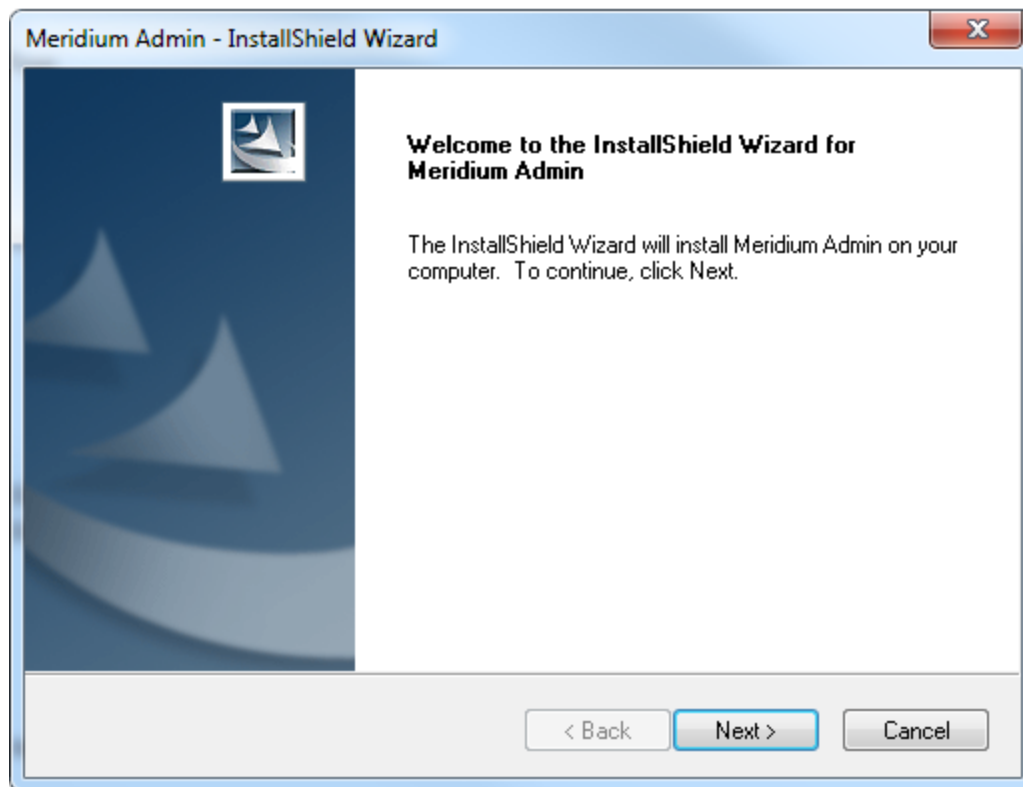
Before You Begin

- Microsoft Visual Studio 2013 Professional or Microsoft Visual Studio 2015 Professional must be installed on every workstation where you want to work with Meridium, Inc. rules in the Meridium Enterprise APM system.
- If you are using Microsoft Visual Studio 2013 Professional, then, after Microsoft Visual Studio 2013 Professional is installed, on the same machine, access the Meridium Enterprise APM third-party software distribution package, then navigate to the folder **\\Microsoft VS2015 Shell**, then run the installer **vs_isoshell.exe**, and then run the installer **vs_intshelladditional.exe**. These installers must be run in the order prescribed. This operation is required only if you are using Microsoft Visual Studio 2013 Professional.
- MSXML must also be installed on these workstations.
- You must be logged in as the administrator for the system.

Steps

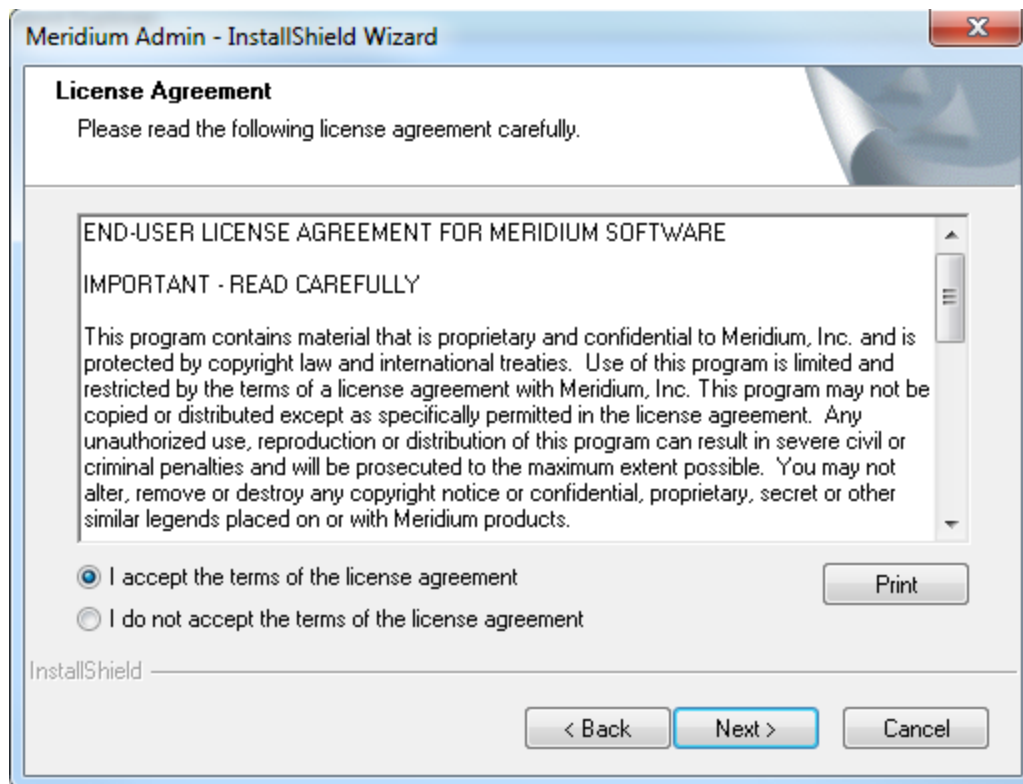
1. On the machine that will serve as the Meridium rules editor, access the Meridium Enterprise APM distribution package, and then navigate to the folder **\\General Release\\Meridium APM Setup\\Setup\\Admin**.
2. Open the file **Setup.exe**.

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



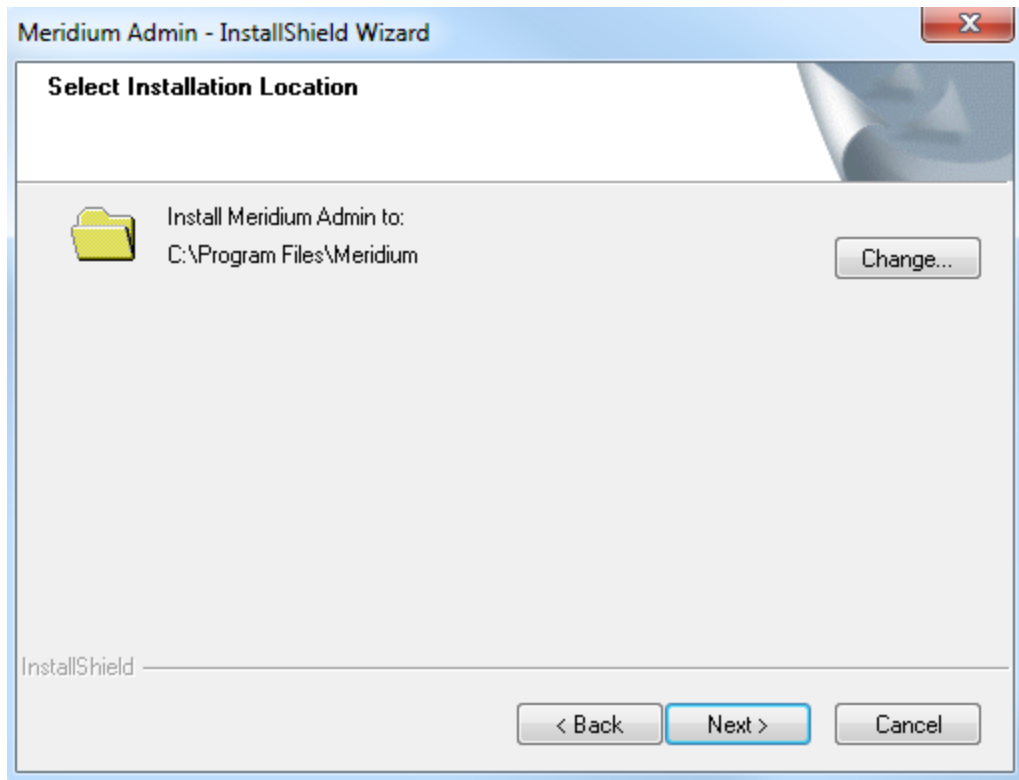
3. Select **Next**.

The **License Agreement** screen appears.



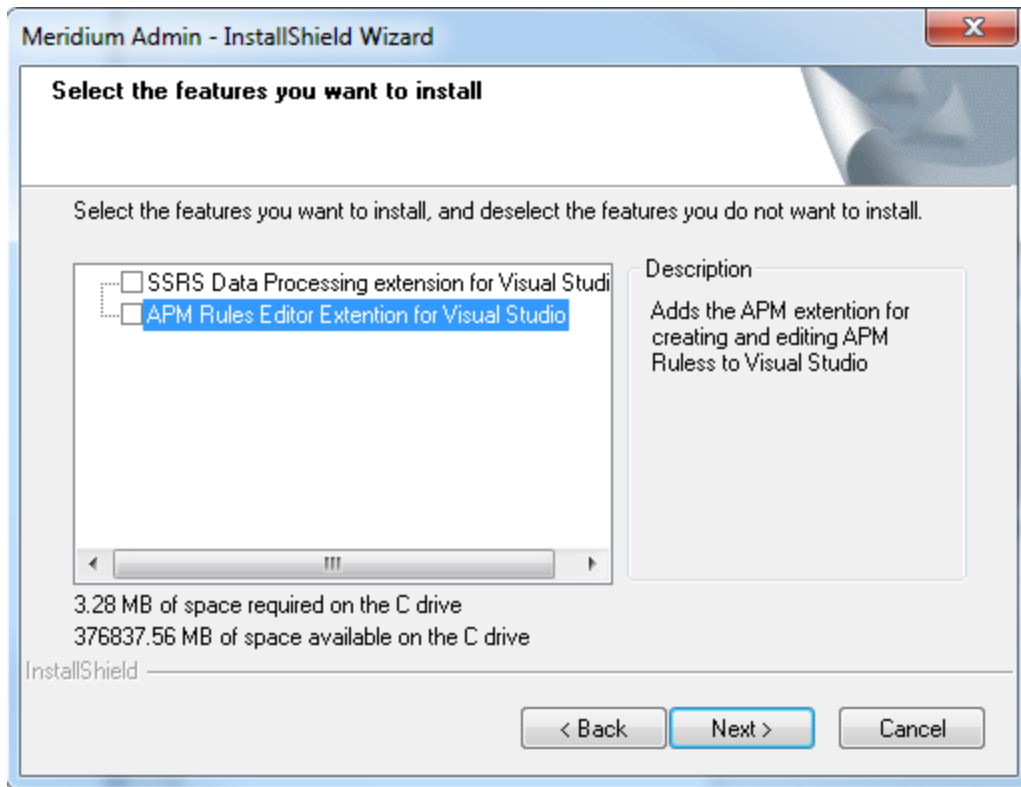
4. Read the License Agreement and, if you agree, select the **I accept the terms of the license agreement** option. Then, select **Next** button.

The **Select Installation Location** screen appears.



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

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

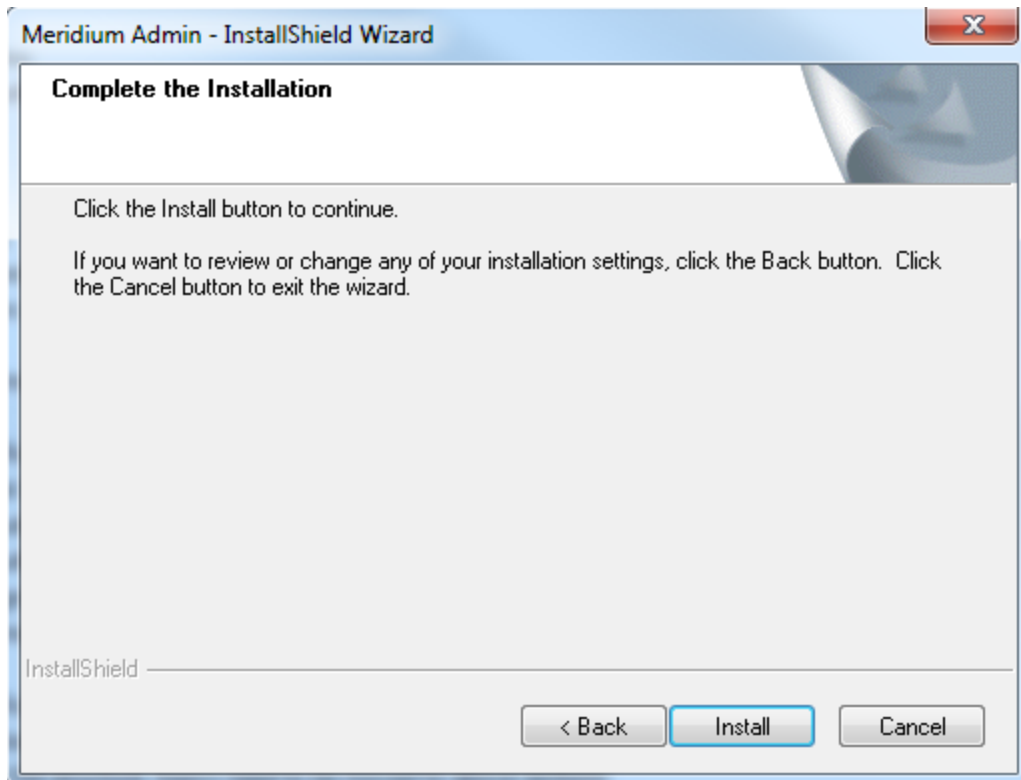


6. Select the **APM Rules Editor Extension for Visual Studio** option.

Meridium Enterprise APM performs a check to make sure that your machine contains the required prerequisites for the features that you want to install. If one or more prerequisites are missing or there is not enough space on the machine, a dialog box will appear, explaining which prerequisites are missing or asking to free up space. If this occurs, close the installer, install the missing prerequisite or free up some space, and then run the installer again.

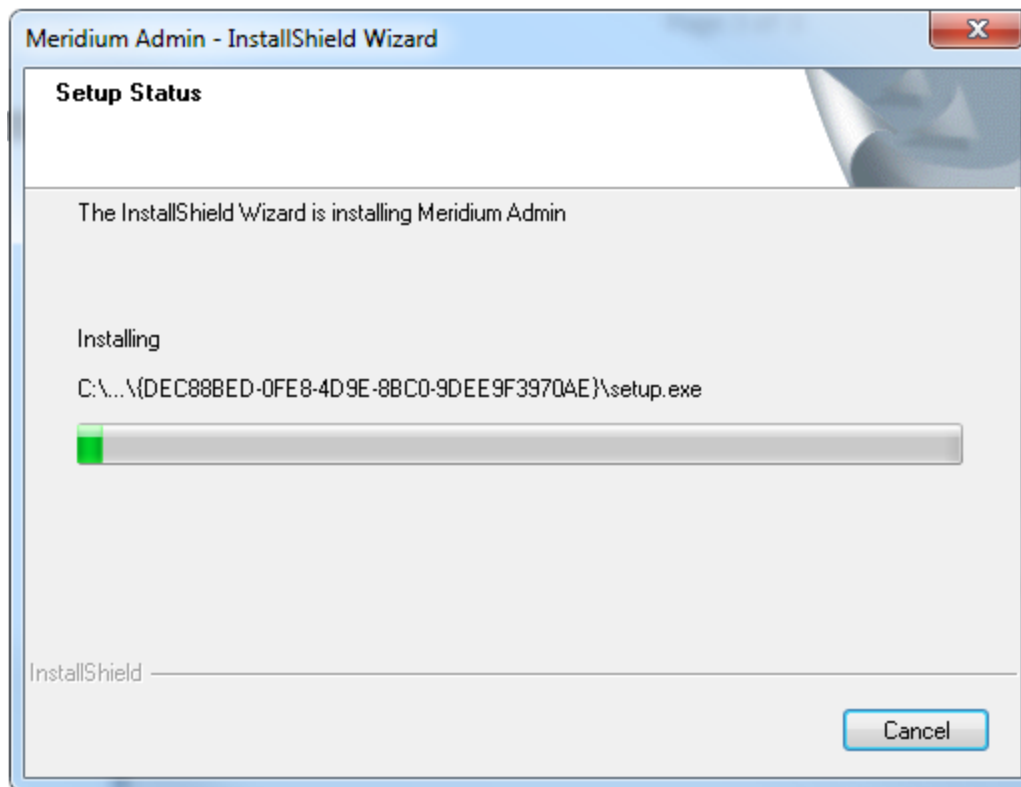
7. Select **Next**.

The **Complete the Installation** screen appears.

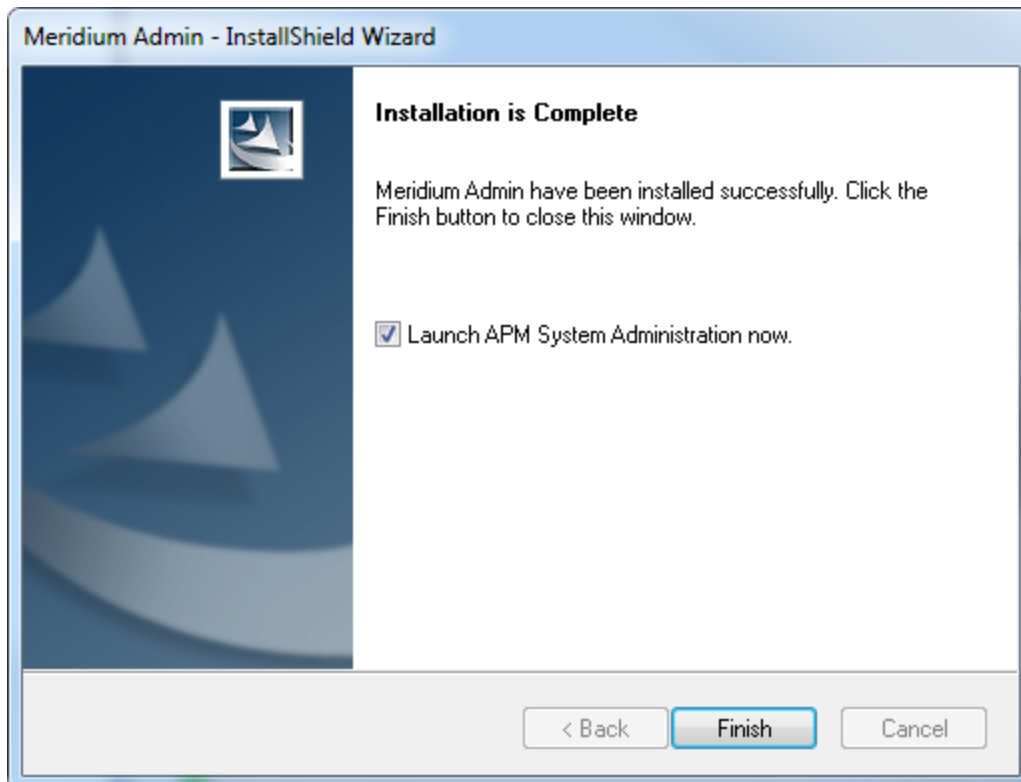


8. Select **Install**.

The **Setup Status** screen appears, which displays a progress bar that shows the progress of the installation process. After the progress bar reaches the end, a message appears, indicating that Meridium Admin is installed successfully. Optionally, you can select to launch the APM System Administration tool when the installer window closes.



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



Results

- The Meridium Rules Editor is installed.

What's Next?

- [Access the Meridium Rules Editor.](#)

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 access 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 data-sheet. |
| 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. |

Upgrading SIS Management to V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

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.

Upgrade from any version V4.1.0.0 through V4.1.1.1

| 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. |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| 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. |

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

| 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. |

Upgrade from any version V3.5.1 through V3.5.1.10.0

| 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. |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

| 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. |

| 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. |

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

| 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. |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| 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. |

SIS Management Security Groups and Roles

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

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

| Security Group | Roles |
|----------------------|--|
| MI SIS Administrator | MI Safety Admin |
| MI SIS Engineer | MI Safety Admin MI Safety Power MI Safety User |
| MI SIS User | MI Safety Admin MI Safety Power MI Safety User |

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

| Family | MI SIS Administrator | MI SIS Engineer | MI SIS User |
|-----------------------------------|------------------------------|------------------------------|-------------|
| Entity Families | | | |
| Asset_Criticality_Analysis | View | None | None |
| Asset_Criticality_Analysis_System | View | None | None |
| Consequence | View, Update, Insert, Delete | View | View |
| Consequence_Modifier | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Equipment | View | View | View |

| Family | MI SIS Administrator | MI SIS Engineer | MI SIS User |
|--|---------------------------------|---------------------------------|---------------------------------|
| External_Assessment | View, Update, Insert, Delete | View, Update, Insert, Delete | None |
| Functional_Location | View | View | View |
| Functional_Systems | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Functional_Test_Detail | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Human_Resource | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Independent_Layer_of_Pro- tection | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Instrumented_Function | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| IPL_Type | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| LOPA | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Notification | View, Update, Insert, Delete | View, Update, Insert, Delete | None |
| PHA_Internal_Assessment | View, Update, Insert, Delete | View, Update, Insert, Delete | None |
| Probability | View, Update, Insert, Delete | View | View |
| Protection_Level | View, Update, Insert, Delete | View, Insert | View |
| Protective_Instrument_Loop | View, Update, Insert, Delete | View, Insert | View |
| Protective_Instrument_ Loop_Element | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Proven_In_Use_Justification | View, Update, Insert, Delete | View, Update, Insert, Delete | View |

| Family | MI SIS Administrator | MI SIS Engineer | MI SIS User |
|--------------------------------------|---------------------------------|---------------------------------|---------------------------------|
| RBI_Components | View, Update, Insert, Delete | View, Update, Insert, Delete | None |
| Reference_Document | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Risk | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Risk_Assessment | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Risk_Assessment_Recom- mendation | 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_Assess- ment | View, Update, Insert, Delete | View, Update, Insert, Delete | None |
| Risk_Threshold | View, Update, Insert, Delete | View | View |
| Safety_Instrumented_Sys- tem | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Safety_Integrity_Level | View, Update, Insert, Delete | View | View |
| SIF_Common_Cause_Failure | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| SIL_Analysis | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| SIL_Threshold | View, Update, Insert, Delete | View | View |
| SIS_Proof_Test | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete |
| SIS_Proof_Test_Template | View, Update, Insert, Delete | View, Update, Insert, Delete | View |

| Family | MI SIS Administrator | MI SIS Engineer | MI SIS User |
|---|------------------------------|------------------------------|-------------|
| SIS_Proof_Test_Template_Detail | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| SIS_Trip_Report | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| SIS_Trip_Report_Detail | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Site_Reference | View | View | View |
| Task | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Time_Based_Inspection_Interval | View | View | View |
| Time_Based_Inspection_Setting | View | View | View |
| Relationship_Families | | | |
| Analysis_Has_Human_Resource | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Asset_Criticality_Analysis_Has_System | View | None | View |
| Equipment_Has_Equipment | View | View | View |
| Functional_Location_Has_Equipment | View | View | View |
| Functional_Location_Has_Functional_Location | View | View | View |
| Has_Consequence_Modifier | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Equipment | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Functional_Location | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Functional_Location_Detail | View, Update, Insert, Delete | View, Update, Insert, Delete | View |

| Family | MI SIS Administrator | MI SIS Engineer | MI SIS User |
|---|---------------------------------|---------------------------------|---------------------------------|
| Has_Functional_Test | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Has_Functional_Test_Detail | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Has_Hazard_Event | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_HAZOP_Reference | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Has_IF | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Independent_Pro- tection_Layer | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Instrumented_Func- tion_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_Revi- sion | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_LOPA | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_LOPA_Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_PIL_Device | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_PIL_Device_Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_PIL_Group | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_PIL_Group_Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_PIL_Subsystem | View, Update, Insert, Delete | View, Update, Insert, Delete | View |

| Family | MI SIS Administrator | MI SIS Engineer | MI SIS User |
|---------------------------------|------------------------------|------------------------------|--------------|
| Has_PIL_Subsystem_Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Proven_In_Use_Justification | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_RBI_Components | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Recommendations | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Reference_Documents | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Insert |
| Has_Reference_Values | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Risk | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Risk_Category | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Risk_Matrix | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_SIF_Common_Cause_Failures | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_SIL_Assessment | View, Update, Insert, Delete | View, Update, Insert, Delete | None |
| Has_SIS_Analysis_Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_SIS_Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_SIS_Trip_Report_Detail | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Site_Reference | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Task_History | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Insert |

| Family | MI SIS Administrator | MI SIS Engineer | MI SIS User |
|------------------------------------|---------------------------------|---------------------------------|-------------|
| Has_Tasks | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Task_Revision | View | View | View |
| Has_Template_Detail | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Templates | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Time_Based_Inspection_Interval | View | View | View |
| Migrates_Risk | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Was_Promoted_to_ASM | View, Update, Insert, Delete | View, Update, Insert, Delete | View |

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 | <p>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.</p> <p>The following relationships <i>must</i> be defined regardless of whether you follow TM Best Practice:</p> <ul style="list-style-type: none"> For the <i>Equipment</i> 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 <i>blank</i>. For the <i>TML Group</i> 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 <i>blank</i>. |
| 4 | Configure global settings. | N | <p>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.</p> |

| Step | Task | Required? | Notes |
|------|---|-----------|---|
| 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. |
| 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 V4.1.5.0

The following tables outline the steps that you must complete to upgrade this module to V4.1.5.0. These instructions assume that you have completed the steps for upgrading the basic Meridium Enterprise APM system architecture.

The steps that you must complete may vary depending on the version from which you are upgrading. Follow the workflow provided in the appropriate section.

Upgrade from any version V4.1.0.0 through V4.1.1.1

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V4.0.0.0 through V4.0.1.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.10.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.7.0

This module will be upgraded to V4.1.5.0 automatically when you upgrade the components in the basic Meridium Enterprise APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.2

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 1 | <p>Manually update TM Analyses for which you used custom corrosion rates. To do so:</p> <ol style="list-style-type: none"> 1. Locate the records that you will need to update by running the following query: <pre>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)</pre> 2. Use the Bulk Analyze tool to update TM Analyses associated with the Equipment and TML Group records returned by this query. | N | <p>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.</p> |

| Step | Task | Required? | Notes |
|------|---|-----------|-------|
| | <p>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 the records requiring update:</p> <ul style="list-style-type: none">• 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. <p>Then, run the Bulk Analyze tool using your custom records.</p> | | |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Required? | Notes |
|------|---|-----------|---|
| 1 | <p>Update certain TM Analyses to correct TML Corrosion Analyses for which you performed measurement variance evaluation prior to V4.1.5.0. To do so:</p> <ol style="list-style-type: none"> 1. Locate the records that you will need to update by creating a query that returns TML Corrosion Analyses whose: <ul style="list-style-type: none"> • 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 | <p>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.</p> |

| Step | Task | Required? | Notes |
|------|--|-----------|---|
| 2 | <p>Manually update TM Analyses for which you used custom corrosion rates. To do so:</p> <ol style="list-style-type: none"> 1. Locate the records that you will need to update by running the following query: <pre>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)</pre> 2. Use the Bulk Analyze tool to update TM Analyses associated with the Equipment and TML Group records returned by this query. | N | <p>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) <i>inches per day</i> instead of <i>IN/YR (TM)</i> (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.</p> |

| Step | Task | Required? | Notes |
|------|---|-----------|-------|
| | <p>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 the records requiring update:</p> <ul style="list-style-type: none">• 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. <p>Then, run the Bulk Analyze tool using your custom records.</p> | | |

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 CIP (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 CIP (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 CIP (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 datalogger will be connected.

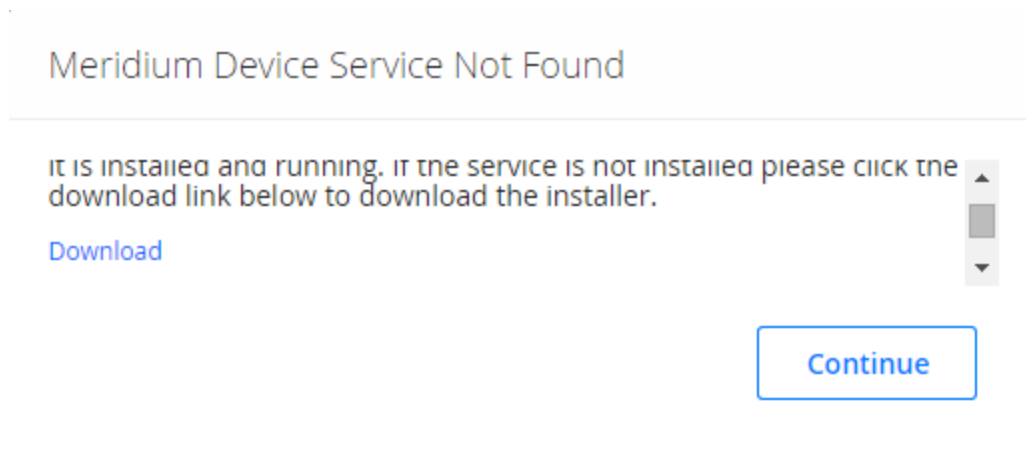
The Meridium Device Service can be installed in the normal workflow when using data-loggers with Thickness Monitoring.

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 Calculator | No | Yes | No |
| Archive Corrosion Rates | 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? |
|---|--|--|---|
| Reset the Maximum Historical Corrosion Rate | Yes | No | No |
| Exclude TMLs | No | Yes | No |
| Renew TMLs | No | Yes | No |
| Reset User Preferences | Yes | No | No |
| Set Color Coding Preferences | Yes | No | No |

Thickness Monitoring Security Groups and Roles

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

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

| Security Group | Roles |
|---------------------------------------|--|
| MI Thickness Monitoring Administrator | MI Mechanical Integrity Administrator |
| MI Thickness Monitoring Inspector | MI Mechanical Integrity Administrator MI Mechanical Integrity Power MI Mechanical Integrity User |
| MI Thickness Monitoring User | MI Mechanical Integrity Administrator MI Mechanical Integrity Power MI Mechanical Integrity User |

The 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 |

| Family | MI Thickness Monitoring Administrator | MI Thickness Monitoring Inspector | MI Thickness Monitoring User |
|--|---------------------------------------|-----------------------------------|------------------------------|
| 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 |
| 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 Sub-component Analysis Settings | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete |

| Family | MI Thickness Monitoring Administrator | MI Thickness Monitoring Inspector | MI Thickness Monitoring User |
|---|---------------------------------------|-----------------------------------|------------------------------|
| Has Archived Sub-component Corrosion Analyses | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Has Corrosion Analyses | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Has Corrosion Analysis Settings | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Has Datapoints | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Has Measurements | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Has Roles | View, Update, Insert, Delete | View | View |
| Has Task Execution | View, Insert | View, Insert | View |
| Has Task Revision | View, Insert | View, Insert | View |
| Has Tasks | View, Insert | View, Insert | View, Insert |
| Has TML Group | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Is a User | View | View | View |
| User Assignment | View | View | View |