



GE Digital

GE Digital APM Modules and Features Deployment

V4.3.0.2.0

GE Digital APM Modules and Features Deployment

V4.3.0.2.0

© 2017 General Electric Company.

GE, the GE Monogram, and Predix are either registered trademarks or trademarks of General Electric Company. All other trademarks are the property of their respective owners.

This document may contain Confidential/Proprietary information of General Electric Company and/or its suppliers or vendors. Distribution or reproduction is prohibited without permission.

THIS DOCUMENT AND ITS CONTENTS ARE PROVIDED "AS IS," WITH NO REPRESENTATION OR WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO WARRANTIES OF DESIGN, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. ALL OTHER LIABILITY ARISING FROM RELIANCE UPON ANY INFORMATION CONTAINED HEREIN IS EXPRESSLY DISCLAIMED.

Access to and use of the software described in this document is conditioned on acceptance of the End User License Agreement and compliance with its terms.

About This Document

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

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

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


 **Note:** If you do not have access to the GE Digital APM Documentation Website, contact GE Global Support (<https://www.ge.com/digital/asset-performance-management>).

Table of Contents

| | |
|--|-----------|
| GE Digital APM Modules and Features Deployment | 1 |
| Copyright and Legal | 2 |
| About This Document | 3 |
| Table of Contents | 4 |
| Deploy Modules and Features | 12 |
| Deploy AMS Analytics | 13 |
| Deploy AMS Analytics for the First Time | 14 |
| Upgrade or Update AMS Analytics to V4.3.0.2.0 | 16 |
| Configure Oracle Specific Queries | 25 |
| Modify the AMS Analytics Overview Page for Oracle | 26 |
| About Defining the Criticality Value in AMS Asset Records | 27 |
| About Creating AMS Asset Data Source Records | 28 |
| AMS Analytics Security Groups and Roles | 29 |
| Deploy APM System Monitoring | 32 |
| Deploy APM System Monitoring for the First Time | 33 |
| Upgrade or Update APM System Monitoring to V4.3.0.2.0 | 34 |
| Configure a Windows Service for MongoDB | 35 |
| Install APM System Monitoring | 37 |
| Configure APM System Monitoring | 47 |
| Deploy Asset Criticality Analysis (ACA) | 52 |
| Deploy Asset Criticality Analysis (ACA) for the First Time | 53 |
| Upgrade or Update Asset Criticality Analysis (ACA) to V4.3.0.2.0 | 54 |
| ACA Security Groups and Roles | 57 |
| Deploy Asset Health Manager (AHM) | 60 |
| Deploy Asset Health Manager (AHM) for the First Time | 61 |
| Upgrade or Update Asset Health Manager (AHM) to V4.3.0.2.0 | 63 |
| About the Asset Health Services | 74 |
| Configure the Meridium Notification Service for AHM | 77 |

| | |
|---|-----|
| Asset Health Manager Security Groups and Roles | 78 |
| Deploy Asset Strategy Implementation (ASI) | 81 |
| Deploy Asset Strategy Implementation (ASI) for the First Time | 82 |
| Upgrade or Update Asset Strategy Implementation (ASI) to V4.3.0.2.0 | 83 |
| Asset Strategy Implementation (ASI) Security Groups and Roles | 87 |
| Install or Upgrade the ASI ABAP Add-On on the SAP System | 94 |
| Verify ASI ABAP Add-On | 98 |
| Uninstall the ASI ABAP Base Service Pack Add-On | 100 |
| Configure SAP for External Numbering | 102 |
| Configure SAP Permissions | 103 |
| About the ASI for SAP ABAP Add-on | 104 |
| Deploy Asset Strategy Management (ASM) | 105 |
| Deploy Asset Strategy Management (ASM) for the First Time | 106 |
| Upgrade or Update Asset Strategy Management (ASM) to V4.3.0.2.0 | 107 |
| Asset Strategy Management (ASM) Security Groups and Roles | 111 |
| Deploy Asset Strategy Optimization (ASO) | 120 |
| Deploy Asset Strategy Optimization (ASO) for the First Time | 121 |
| Upgrade or Update Asset Strategy Optimization (ASO) to V4.3.0.2.0 | 122 |
| Asset Strategy Optimization (ASO) Security Groups and Roles | 125 |
| Deploy Calibration Management | 126 |
| Deploy Calibration Management for the First Time | 127 |
| Upgrade or Update Calibration Management to V4.3.0.2.0 | 128 |
| Install the Meridium Device Service | 132 |
| Calibration Management Security Groups and Roles | 136 |
| Deploy Cognitive Analytics | 142 |
| Deploy Cognitive Analytics for the First Time | 143 |
| Upgrade or Update Cognitive Analytics to V4.3.0.2.0 | 144 |
| Cognitive Analytics Security Groups and Roles | 145 |
| Deploy eLog | 146 |
| Deploy eLog for the First Time | 147 |

| | |
|---|-----|
| Upgrade or Update eLog to V4.3.0.2.0 | 148 |
| eLog Security Groups and Roles | 149 |
| Deploy Failure Modes and Effects Analysis (FMEA) | 151 |
| Deploy Failure Modes and Effects Analysis (FMEA) for the First Time | 152 |
| Upgrade or Update Failure Modes and Effects Analysis (FMEA) to V4.3.0.2.0 | 153 |
| Failure Modes and Effects Analysis (FMEA) Security Groups and Roles | 155 |
| Deploy GE Analytics | 159 |
| Deploy GE Analytics for the First Time | 160 |
| Upgrade or Update GE Analytics to V4.3.0.2.0 | 162 |
| Modify the File Meridium.AMQP.service.exe.config | 165 |
| Install the GE System 1 Integration Service | 169 |
| Modify the File Meridium.GE.Service.exe.config | 171 |
| Import the GE Policies | 176 |
| GE Analytics Security Groups and Roles | 177 |
| Deploy Generation Availability Analysis (GAA) | 179 |
| Deploy Generation Availability Analysis (GAA) for the First Time | 180 |
| Upgrade or Update Generation Availability Analysis (GAA) to V4.3.0.2.0 | 183 |
| Migrate from Generation Management (GM) to Generation Availability Analysis (GAA) | 184 |
| Query Mapping | 189 |
| State Management Mapping | 190 |
| Field Mappings | 191 |
| Generation Availability Analysis (GAA) Security Groups and Roles | 210 |
| Deploy Hazards Analysis | 214 |
| Deploy Hazards Analysis for the First Time | 215 |
| Upgrade or Update Hazards Analysis to V4.3.0.2.0 | 216 |
| Hazards Analysis Security Groups and Roles | 220 |
| Deploy Inspection Management | 227 |
| Deploy Inspection Management for the First Time | 228 |
| Upgrade or Update Inspection Management to V4.3.0.2.0 | 230 |

| | |
|--|-----|
| Inspection Management Security Groups and Roles | 232 |
| Deploying Layers of Protection Analysis (LOPA) | 237 |
| Deploy LOPA for the First-Time | 238 |
| Upgrade or Update Layers of Protection Analysis (LOPA) to V4.3.0.2.0 | 240 |
| LOPA Security Groups and Roles | 241 |
| Deploy Life Cycle Cost Analysis (LCC) | 248 |
| Deploy Life Cycle Cost Analysis (LCC) for the First Time | 249 |
| Upgrade or Update Life Cycle Cost Analysis (LCC) to V4.3.0.2.0 | 250 |
| Life Cycle Cost Analysis Security Groups and Roles | 251 |
| Deploy Management of Change (MoC) | 253 |
| Deploy Management of Change (MOC) for the First Time | 254 |
| Upgrade or Update Management of Change (MoC) to V4.3.0.2.0 | 255 |
| Management of Change Security Groups and Roles | 256 |
| Deploy Metrics and Scorecards | 258 |
| Deploy Metrics and Scorecards for the First Time | 259 |
| Upgrade or Update Metrics and Scorecards to V4.3.0.2.0 | 262 |
| About Configuring a Cube for Usage Metrics Tracking | 279 |
| About Scheduling Cubes for Processing | 280 |
| Install SQL Server Analysis Services on the Server | 281 |
| Migrate SQL Server Cubes | 282 |
| Deploy the Work History Cube | 284 |
| About Modifying the Work History Cube | 285 |
| Modify the Views for Work History Cube | 287 |
| Localize the Event or Asset Criticality Values | 292 |
| Metrics and Scorecards Security Groups and Roles | 299 |
| Deploy Policy Designer | 301 |
| Deploy Policy Designer for the First Time | 302 |
| Upgrade or Update Policy Designer to V4.3.0.2.0 | 304 |
| About the Asset Health Services | 314 |
| About Configuring Policy Execution | 317 |

| | |
|--|-----|
| Configure the Policy Trigger Service | 318 |
| Configure Multiple GE Digital APM Servers for Policy Execution | 319 |
| Policy Designer Security Groups and Roles | 322 |
| Deploy Process Data Integration (PDI) | 323 |
| Deploy Process Data Integration (PDI) for the First Time | 324 |
| Upgrade or Update Process Data Integration (PDI) to V4.3.0.2.0 | 326 |
| Process Data Integration Server Roles | 334 |
| About the Asset Health Services | 335 |
| Install the Process Data Integration Service | 338 |
| Upgrade the Process Data Integration Service | 340 |
| Configure the Meridium Notification Service for PDI | 342 |
| Configure the Process Data Integration Service | 344 |
| Configure Multiple Data Sources | 348 |
| Configure Multiple Process Data Integration and OPC Servers | 349 |
| Process Data Integration Security Groups and Roles | 351 |
| Deploy Production Loss Analysis (PLA) | 353 |
| Deploy Production Loss Analysis (PLA) for the First Time | 354 |
| Upgrade or Update Production Loss Analysis (PLA) to V4.3.0.2.0 | 358 |
| Import Baseline Rules | 364 |
| Replace the Top 10 Bad Actors Query | 376 |
| Production Loss Analysis Security Groups and Roles | 380 |
| Deploy R Scripts | 384 |
| Deploy R Scripts for the First Time | 385 |
| Upgrade or Update R Scripts to V4.3.0.2.0 | 386 |
| Upgrade R Script Metadata | 388 |
| Deploy Recommendation Management | 389 |
| Deploy Recommendation Management for the First Time | 390 |
| Upgrade or Update Recommendation Management to V4.3.0.2.0 | 391 |
| Recommendation Management Security Groups and Roles | 393 |
| Deploy Reliability Analytics | 395 |

| | |
|--|-----|
| Deploy Reliability Analytics for the First Time | 396 |
| Upgrade or Update Reliability Analytics to V4.3.0.2.0 | 397 |
| Reliability Analytics Security Groups and Roles | 399 |
| Deploy Reliability Centered Maintenance (RCM) | 404 |
| Deploy Reliability Centered Maintenance (RCM) for the First Time | 405 |
| Upgrade or Update Reliability Centered Maintenance (RCM) to V4.3.0.2.0 | 406 |
| Reliability Centered Maintenance (RCM) Security Groups and Roles | 408 |
| Deploy Reports | 412 |
| Deploy Reports for the First Time | 413 |
| Upgrade or Update Reports to V4.3.0.2.0 | 414 |
| Install the APM Reports Designer | 416 |
| Set Up the APM Report Designer | 425 |
| Deploy RBI 581 | 427 |
| Deploy RBI 581 for the First Time | 428 |
| Upgrade or Update RBI 581 to V4.3.0.2.0 | 434 |
| Add the RBI-581 Tab to Criticality RBI Component Datasheets | 446 |
| RBI 581 Security Groups and Roles | 455 |
| Deploy Risk Based Inspection (RBI) | 462 |
| Deploy Risk Based Inspection (RBI) for the First Time | 463 |
| Upgrade or Update Risk Based Inspection (RBI) to V4.3.0.2.0 | 466 |
| Risk Based Inspection Security Groups and Roles | 484 |
| Deploy Root Cause Analysis (RCA) | 492 |
| Deploy Root Cause Analysis (RCA) for the First Time | 493 |
| Upgrade or Update Root Cause Analysis (RCA) to V4.3.0.2.0 | 494 |
| Root Cause Analysis Security Groups and Roles | 496 |
| Deploy Rounds | 499 |
| Deploy Rounds for the First Time | 500 |
| Upgrade or Update Rounds to V4.3.0.2.0 | 504 |
| Manage the Measurement Location Template Mappings | 515 |
| APM Sync Services Tasks | 516 |

| | |
|---|-----|
| Install APM Sync Services | 517 |
| Verify Installation of APM Sync Services | 525 |
| Install Microsoft Sync Framework | 526 |
| Modify the Web.config for An Oracle Sync Services Database Connection | 527 |
| Modify the Web.config for An SQL Sync Services Database Connection | 529 |
| Modify APM Sync Config | 531 |
| Configure Security for APM Sync Service | 533 |
| Windows Mobile Handheld Devices | 534 |
| Install the .NET Compact Framework on Windows Mobile Device | 535 |
| Install Microsoft SQL CE on Windows Mobile Device | 536 |
| Install Microsoft Sync Services for ADO.NET on Windows Mobile Device | 537 |
| Install the APM Mobile Framework on Windows Mobile Device | 538 |
| Access Device Settings Screen on Windows Mobile Device | 539 |
| Identify the Sync Server Within the APM Mobile Framework on Windows Mobile Device | 540 |
| Specify the Security Query on Windows Mobile Device | 541 |
| Modify User Time-out Value on Windows Mobile Device | 542 |
| Install Operator Rounds on Windows Mobile Device | 543 |
| Install the Barcode Add-on on Windows Mobile Device | 544 |
| Enable Barcode Scanning on Windows Mobile Device | 546 |
| Install the RFID Add-on on Windows Mobile Device | 547 |
| Enable RFID Tag Scanning on Windows Mobile Device | 549 |
| Install Translations for Operator Rounds on Windows Mobile Device | 551 |
| Uninstall APM Mobile Framework on Windows Mobile Device | 552 |
| Uninstall then RFID Add-on on Windows Mobile Device | 553 |
| Uninstall the Barcode Add-on on Windows Mobile Device | 556 |
| Uninstall Translations for Operator Rounds on Windows Mobile Device | 559 |
| Uninstall Operator Rounds on Windows Mobile Device | 562 |
| Upgrade Windows Mobile Handheld Device | 565 |
| Upgrade Steps for Lubrication | 566 |

| | |
|---|-----|
| Modify Checkpoints Linked to Multiple Assets | 574 |
| Upgrade Records with Schedules Containing End Dates | 576 |
| Rounds Security Groups and Roles | 578 |
| Deploy Rules | 586 |
| Install the GE Digital APM Rules Editor | 587 |
| Deploy SIS Management | 594 |
| Deploy SIS Management for the First Time | 595 |
| Upgrade or Update SIS Management to V4.3.0.2.0 | 598 |
| About Upgrade of LOPA and Safeguards to V4.3.0.0.0 | 602 |
| SIS Management Security Groups and Roles | 604 |
| Deploy Thickness Monitoring (TM) | 609 |
| Deploy Thickness Monitoring (TM) for the First Time | 610 |
| Upgrade or Update Thickness Monitoring (TM) to V4.3.0.2.0 | 613 |
| Use Custom TML Analysis Types | 619 |
| Install the Meridium Device Service | 621 |
| Configure the Meridium Device Service | 622 |
| Thickness Monitoring Functional Security Privileges | 623 |
| Thickness Monitoring Security Groups and Roles | 625 |

Deploy Modules and Features

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


Deploy AMS Analytics

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

Deploy AMS Analytics for the First Time

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

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

 **Note:** This GE Digital APM module is not available in the APM Now environment.

| Step | Task | Notes |
|------|--|--|
| 1 | Assign Security Users to one or more of the AMS Analytics Security Groups . | This step is required. |
| 2 | Deploy Reports . | This step is required only if you want to view reports of AMS data. |
| 3 | On the GE Digital APM Server, run the GE Digital APM Server and Add-ons installer, selecting the Meridium Integration Services check box on the Select the features you want to install screen . | This step is required. |
| 4 | Create one AMS Asset Data Source record per AMS Analytics data source whose data you want to transfer into GE Digital APM. | This step is required. |
| 5 | Test the connection to each AMS Analytics data source. | This step is required. |
| 6 | Link each AMS Asset record to the Equipment or Functional record that represents the piece of equipment or location for which the AMS Asset record exists. | This step is required. You can link AMS Tag records to Equipment or Functional Location records using one of the following: <ul style="list-style-type: none"> • Record Manager • System and Tags • Tags Data Loader |
| 7 | If you are using Asset Criticality Analysis, define the criticality field in the AMS Asset records for the equipment or location linked to each AMS Asset record. | This step is required. |

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

Upgrade or Update AMS Analytics to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

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

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

Upgrade from any version V4.0.0.0 through V4.0.1.0

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

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

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

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

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

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

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

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

Upgrade from any version V3.5.1 through V3.5.1.12.1

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

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

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

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

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

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

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

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

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

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

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

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 GE Digital 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 GE Digital 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 GE Digital 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 GE Digital APM system uses to import data from the following locations AMS Analytics data sources

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

AMS Analytics Security Groups and Roles

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

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

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

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

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

| Family | MI AMS Suite APM Administrator | MI AMS Suite APM Power User | MI AMS Suite APM User | MI AMS Asset Portal Viewer |
|------------------------|--------------------------------|------------------------------|------------------------------|----------------------------|
| Entity Families | | | | |
| AMS Asset Alert | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| AMS Asset Event | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |

| Family | MI AMS Suite APM Admin- istrator | MI AMS Suite APM Power User | MI AMS Suite APM User | MI AMS Asset Portal Viewer |
|---|--|-----------------------------------|------------------------------|----------------------------------|
| AMS Asset Recommendation | View, Update, Insert, Delete | View, Update, Insert | View, Update, Insert | View |
| Equipment | View, Update, Insert, Delete | View, Update, Insert | View | View |
| Functional Location | View, Update, Insert, Delete | View, Update, Insert | View | View |
| Tag | View, Update, Insert, Delete | View, Update | View | View |
| Tag Alert | View, Update, Insert, Delete | View, Update | View | View |
| Tag Data Source | View, Update, Insert, Delete | View | View | View |
| Tag Event | View, Update, Insert, Delete | View, Update | View | View |
| Tag Folder | View, Update, Insert, Delete | View, Update, Insert | View | View |
| Relationship Families | | | | |
| Equipment Has Equipment | View, Update, Insert, Delete | View, Update, Insert | View | View |
| Functional Location Has Equipment | View, Update, Insert, Delete | View, Update, Insert | View | View |
| Functional Location Has Functional Location | View, Update, Insert, Delete | View, Update, Insert | View | View |
| Has Consolidated Events | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Recommendations | View, Update, Insert, Delete | View, Update, Insert | View, Update, Insert | View |

| Family | MI AMS Suite APM Admin- istrator | MI AMS Suite APM Power User | MI AMS Suite APM User | MI AMS Asset Portal Viewer |
|------------------------------|--|-----------------------------------|-----------------------------|----------------------------------|
| Has Tag | View, Update, Insert, Delete | View, Update, Insert | View | View |
| Has Tag Alert | View, Update, Insert, Delete | View, Update, Insert | View | View |
| Has Tag Data Source | View, Update, Insert, Delete | View, Update, Insert | View | View |
| Has Tag Event | View, Update, Insert, Delete | View, Update, Insert | View | View |
| Tag Folder Has Tag Folder | View, Update, Insert, Delete | View, Update, Insert | View | View |

Deploy APM System Monitoring

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

Deploy APM System Monitoring for the First Time

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

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

Note: If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

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

Upgrade or Update APM System Monitoring to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

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

Configure a Windows Service for MongoDB

Before You Begin

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

Steps

1. On the machine on which you installed MongoDB Community Edition, select the Windows Start button, then navigate to and right-click **Command Prompt**, and then select **Run as administrator**.

A command prompt window appears.

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


```
mkdir c:\data\db
```

```
mkdir c:\data\log
```

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


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

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

 **Note:** In the configuration file, each tab indentation seen in the preceding text should be replaced with *two* spaces.

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

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

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

The MongoDB service is installed.

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

```
net start MongoDB
```

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

What's Next?

- Return to the [APM System Monitoring first-time deployment workflow](#).

Install APM System Monitoring

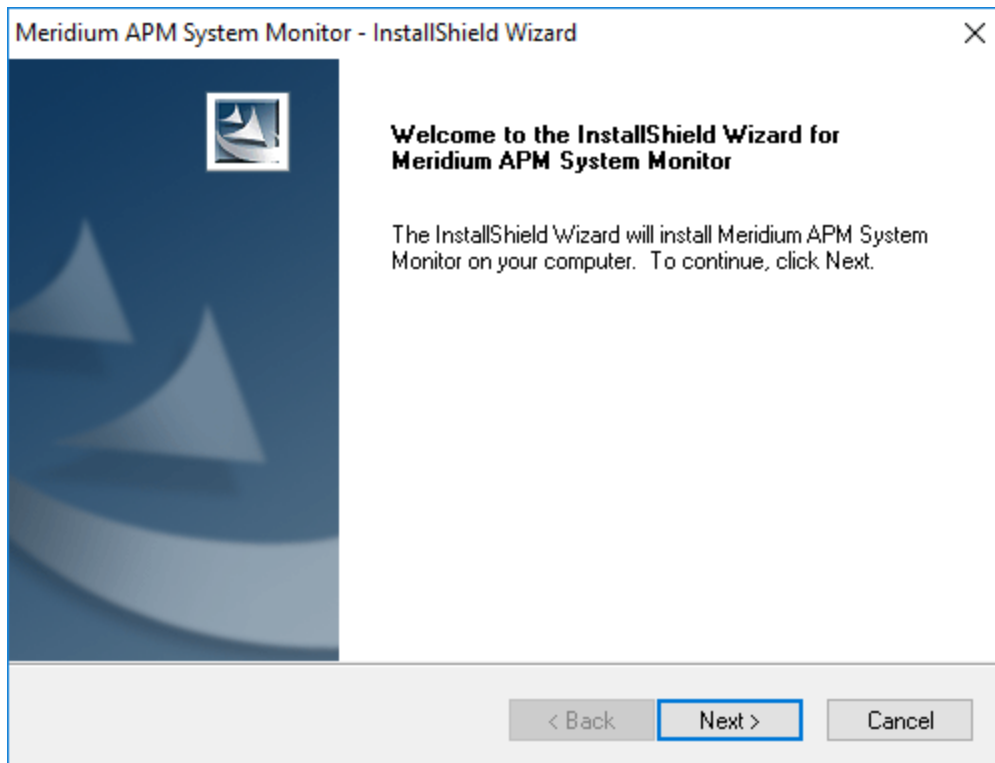
Before You Begin

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

Steps

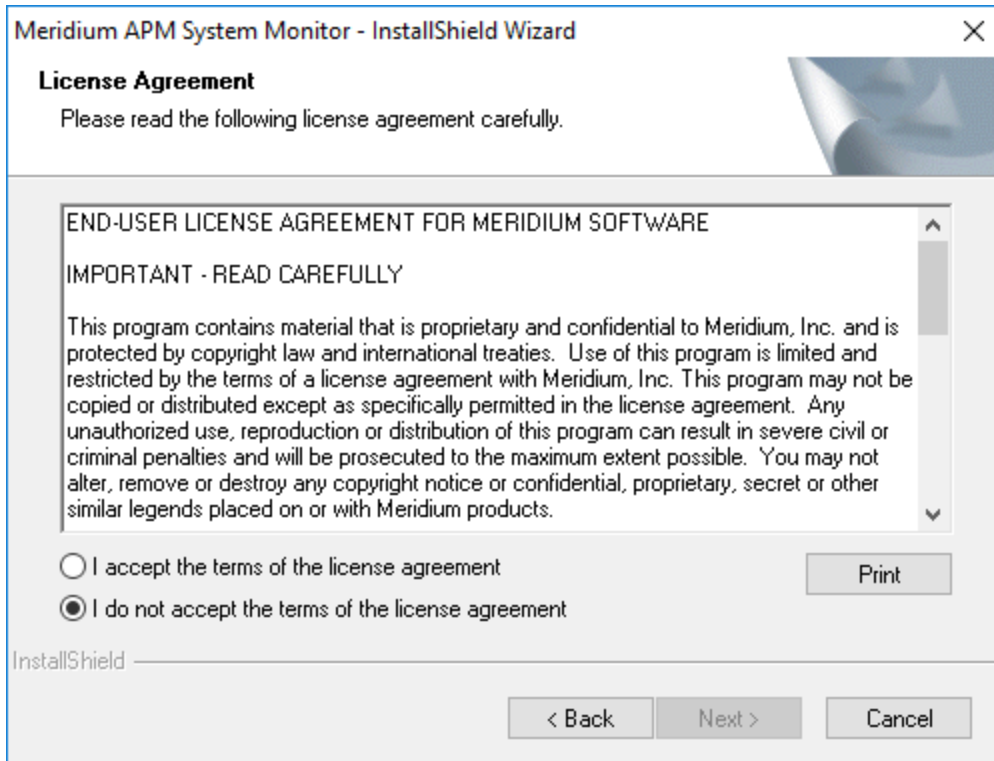
1. On the machine on which you want to install APM System Monitoring, access the GE Digital APM distribution package, and then navigate to the folder **Setup\APMSys-temMonitor**.
2. Open the file **Setup.exe**.

The Meridium APM System Monitor installer appears.



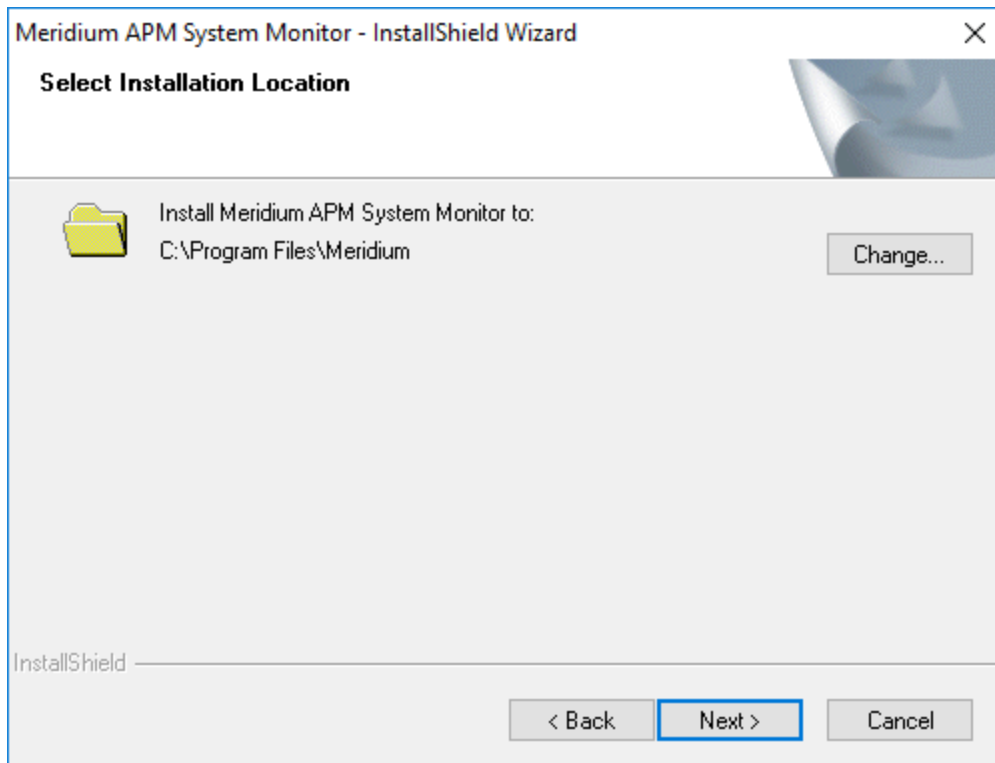
3. Select **Next**.

The **License Agreement** screen appears.



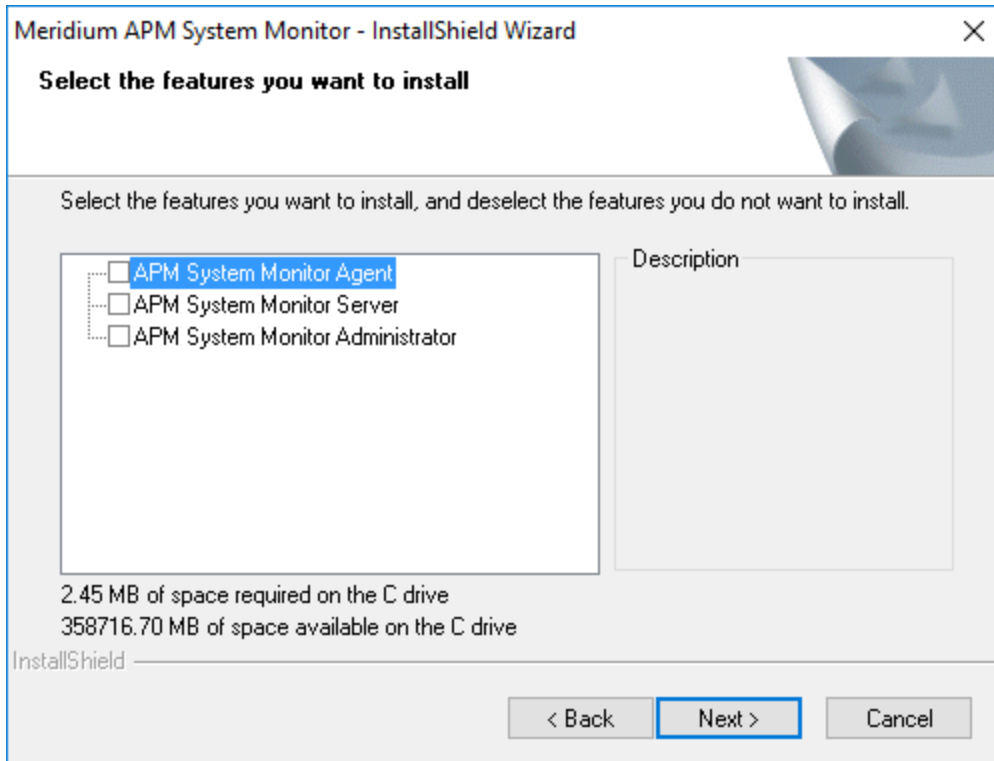
4. Read the License Agreement and, if you agree, select the **I accept the terms of the license agreement** check box. Then, select **Next**.

The **Select Installation Location** screen appears.




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


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




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

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

7. If this is the machine that will serve as the APM System Monitoring administrator, then select the **APM System Monitor Administrator** check box.

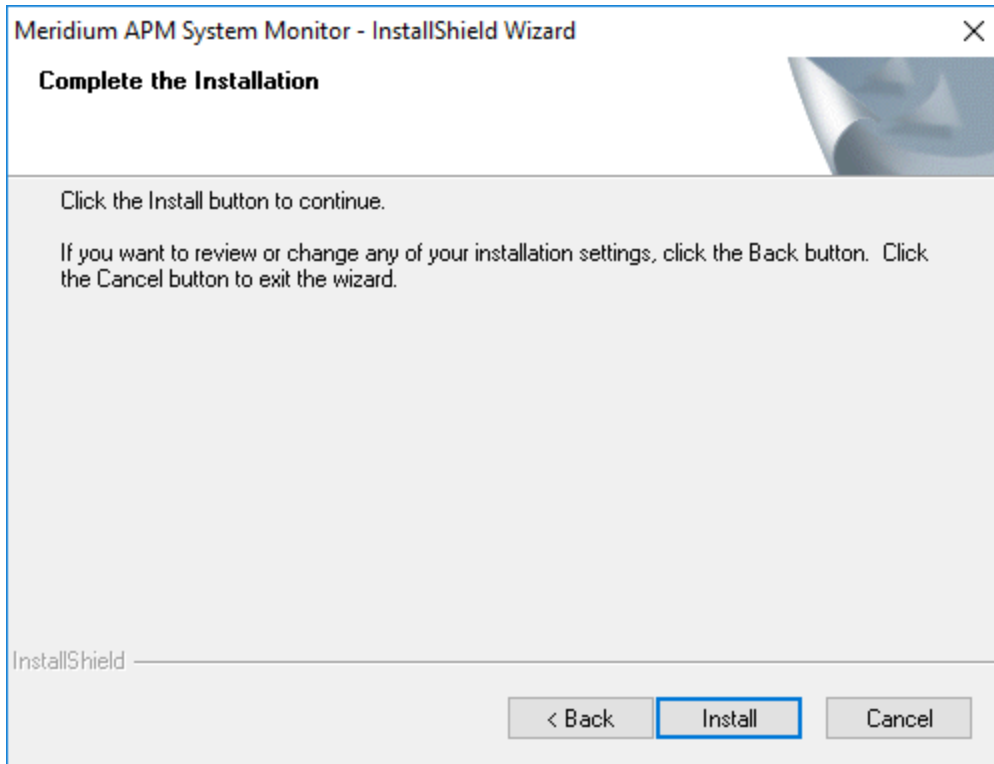
 **Note:** Only one machine will serve as the APM System Monitoring administrator.

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

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

9. Select **Next**.

The **Complete the Installation** screen appears.



10. Select **Install**.

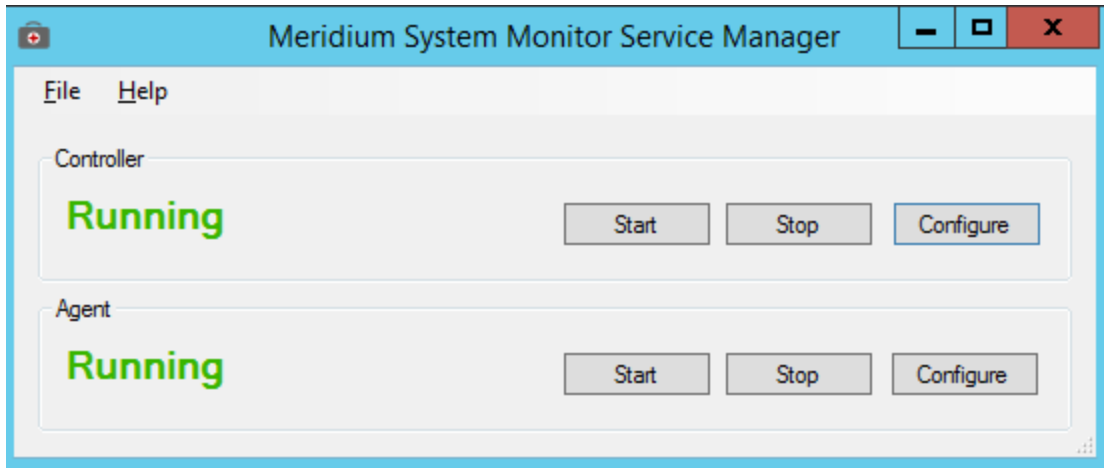
The **Setup Status** screen appears, displaying a progress bar. When the installation is complete, the **Installation is Complete** screen appears.

11. Select **Finish**.

The Meridium APM System Monitor installer closes.

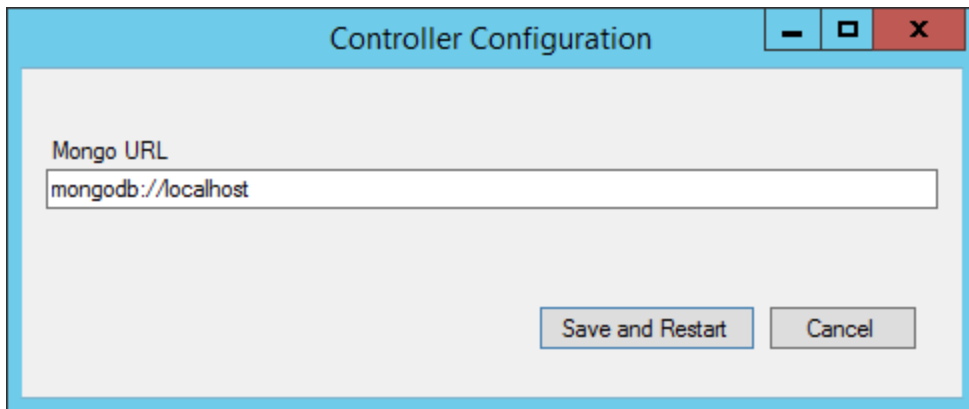
12. If the machine will serve as the APM System Monitoring controller or an APM System Monitoring agent, navigate to **C:\Program Files\Meridium\APMSystemMonitor**, and then open the file **Meridium.System.Monitor.ServiceManager.exe**. If the machine will serve only as the APM System Monitoring administrator, skip this step and proceed directly to step 16.

The **Meridium APM System Monitor Service Manager** window appears.



13. If the machine will serve as the APM System Monitoring controller, then, in the **Controller** section, select **Configure**. Otherwise, skip this step.

The **Controller Configuration** window appears.

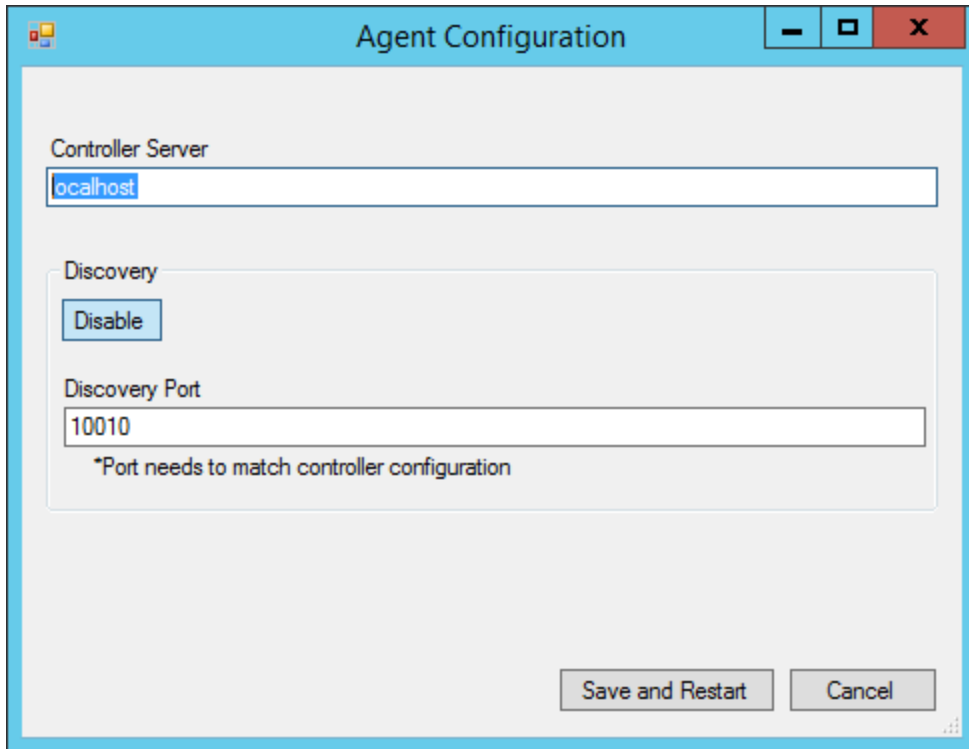


- a. In the **Mongo URL** box, enter the URL for the MongoDB database, and then select **Save and Restart**.

The machine is configured as the APM System Monitoring controller.

14. If the machine will serve as an APM System Monitoring agent, then, in the **Agent** section, select **Configure**. Otherwise, skip this step.

The **Agent Configuration** window appears.



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

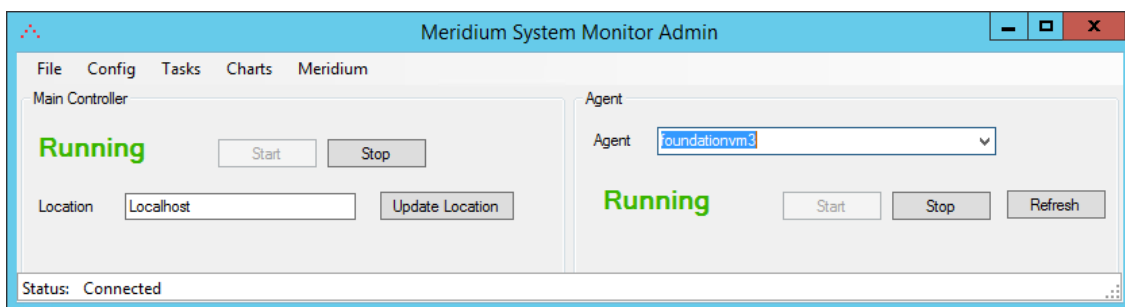
The machine is configured as an APM System Monitoring agent.

15. Close the **Meridium APM System Monitor Service Manager** window.

APM System Monitoring is installed on the machine.

16. If the machine will serve as the APM System Monitoring administrator, navigate to **C:\Program Files\Meridium\APMSystemMonitor\Admin**, and then open the file **Meridium.SystemMonitor.Admin.exe**. Otherwise, skip the remaining steps and return to the [first-time deployment workflow](#).

The **Meridium System Monitor Admin** window appears.



- a. In the **Location** box, enter the location of the APM System Monitor controller, and then select **Update Location**.

The connection status displayed in the lower-left corner of the window changes to *Connected*.


- b. Select **Config**, and then select **Settings**.

The **System Monitor Settings** window appears.

The screenshot shows the 'System Monitor Settings' dialog box. The title bar is blue and contains the text 'System Monitor Settings' along with standard window control buttons (minimize, maximize, close). The main area is light gray and contains the following fields and controls:

- Controller Location:** Text box containing 'Localhost'.
- API Key:** Empty text box.
- Meridium URL Host:** Text box containing 'https://apmsmdev.azure-api.net/api/'.
- Customer Key:** Empty text box.
- User Name:** Empty text box.
- Database URL:** Text box containing 'mongodb://localhost'.
- Allow Discovery?:** Check box with a checkmark.
- Announcement Port:** Spinner box showing '10010'.
- Proxy Port:** Spinner box showing '11014'.
- Can Send Output To Meridium:** Check box with a checkmark.
- Buttons:** 'Update' and 'Cancel' buttons at the bottom.

- c. In the **Controller Location** box, enter the location of the APM System Monitor controller.
- d. Enter values in the **API Key**, **Customer Key**, and **User Name** boxes. You should have received these values from GE Global Support.
- e. If you did not install MongoDB in the default location, modify the value in the **Database URL** box as needed.
- f. If you want to disallow discovery, clear the **Allow Discovery** check box.

 **Note:** Disallowing discovery is not recommended, but may be necessary, depending on your firewall settings. A firewall may prevent automatic discovery by APM System Monitoring.

- g. If needed, modify the values in the **Announcement Port** and **Proxy Port** boxes.
- h. Select **Update**.

The **System Monitor Settings** window closes.

- i. On the **Meridium System Monitor Admin** window, select **Config**, and then select **General**.

The **General Config** window appears.


The screenshot shows the 'General Config' window with the following settings:

- Log Level To Store:** Trace, Debug, Info, Warn, and Error (checked).
- Log Level To Output:** Trace, Debug, Info, Warn, and Error (checked).
- Days In Storage:** 7
- Days In Outputs:** 7
- Can Send Log Files Daily:** Checked
- Send Log Files At:** 7:00:00 AM
- Email Server:** (empty)
- From Address:** (empty)
- To:** (empty)

- j. In the **Log Level To Store** and **Log Level to Output** sections, select the check box for each log level that you want to monitor.

Tip: GE Digital recommends that you select only the **Error** check boxes. If additional check boxes are selected, the log files produced may be very large.

- k. In the **Days In Storage** box, select the number of days logs should be stored in the system before deletion.
- l. In the **Days In Outputs** box, select the number of days worth of information that should be used to populate GE Digital APM dashboards.
- m. Enter values in the **Email Server**, **From Address**, and **To** boxes, and then select **Update**.

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

The **General Config** window closes.

- n. On the **Meridium System Monitor Admin** window, select **Config**, and then select **Agents**.

The **Agents** window appears.

What's Next?

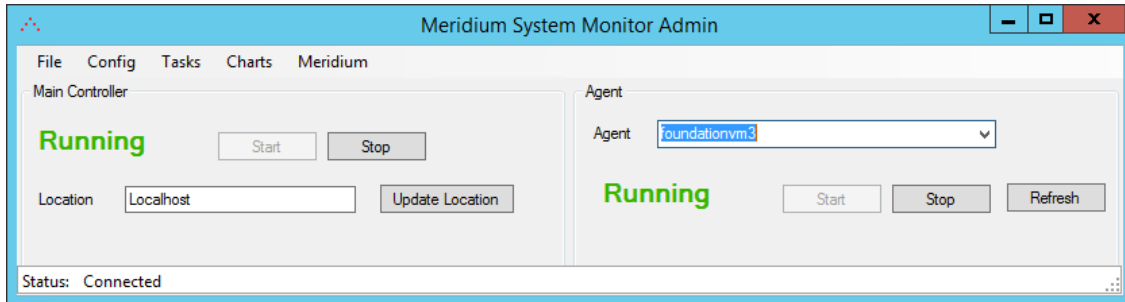
- Return to the APM System Monitoring [first-time deployment](#) or [upgrade](#) workflow.

Configure APM System Monitoring

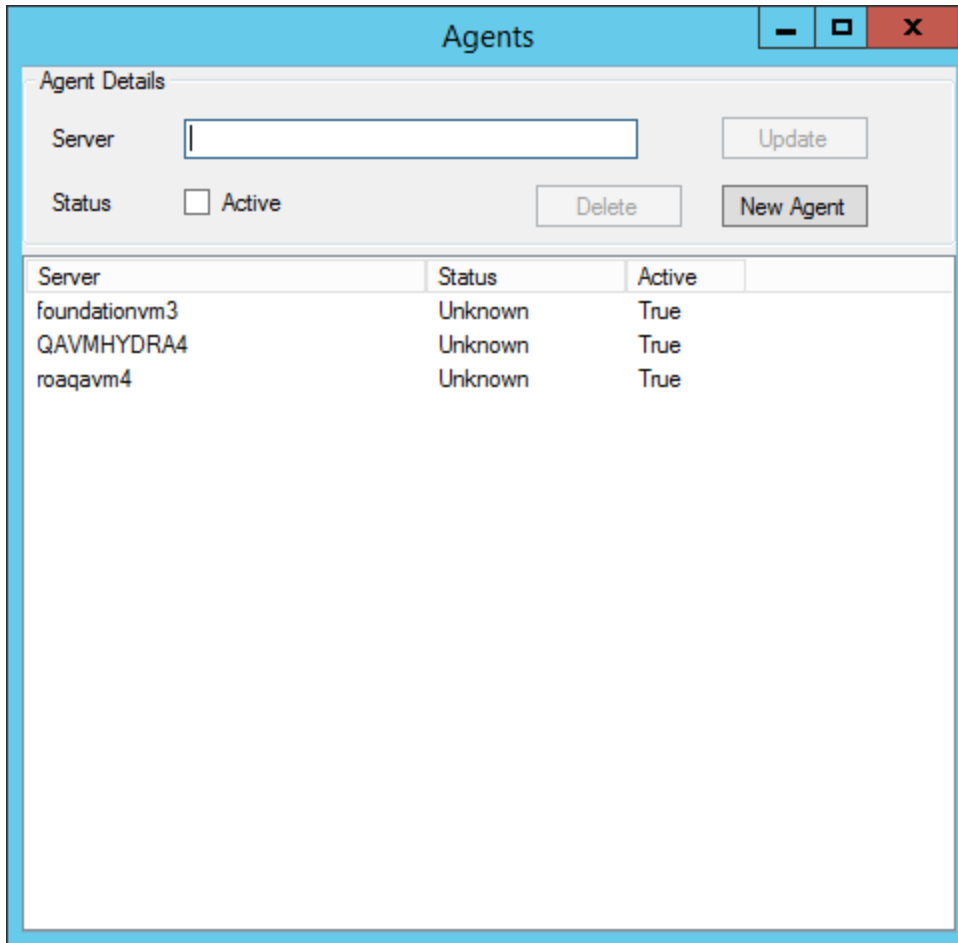
Steps

1. On the machine serving as the APM System Monitoring administrator, navigate to **C:\Program Files\Meridium\APMSystemMonitor\Admin**, and then open the file **Meridium.SystemMonitor.Admin.exe**.


The **Meridium System Monitor Admin** window appears.



2. On the **Meridium System Monitor Admin** window, select **Config**, and then select **Agents**.
The **Agents** window appears.



3. As needed, modify the configuration of the agents, and then close the **Agents** window.

 **Note:** If you have allowed discovery (i.e., the **Allow Discovery?** check box on the **System Monitor Settings** window is selected), the **Delete** and **New Agent** buttons on the **Agents** window are disabled.

4. On the **Meridium System Monitor Admin** window, select **Config**, and then select **Alerts**.
The **Alerts** window appears.

The image shows a window titled "Alerts" with a light blue header. Below the header is a section labeled "Alert Details" containing several fields:

- Name: IIS Reset Alert
- Alert Type: lisReset
- Process Type: None
- Event Type: None
- Status: Active
- Threshold: 1
- Minutes Above: 1

On the right side of the "Alert Details" section are three buttons: "New", "Update", and "Delete".

Below the "Alert Details" section is a table with the following data:

| Name | Type | Process | Event | Active | Threshold | Minutes... |
|-----------------|----------|---------|-------|--------|-----------|------------|
| IIS Reset Alert | lisReset | None | None | True | 1 | 1 |

5. As needed, modify the configuration of the alerts, and then close the **Alerts** window.
6. On the **Meridium System Monitor Admin** window, select **Config**, and then select **APM**.
The **Configure APM Output** window appears.

The image shows a 'Configure APM Output' dialog box. It has a title bar with standard window controls. The main area contains the following fields and controls:

- Allow APM Output:** A checkbox that is currently unchecked.
- Database Type:** A dropdown menu with 'Oracle' selected.
- Database Name:** An empty text input field.
- SQL Instance:** An empty text input field.
- User ID:** An empty text input field.
- Password:** An empty text input field.
- Ora Port:** A spin box with the value '0' and up/down arrow buttons.
- Ora Host:** An empty text input field.
- Ora Service:** An empty text input field.

At the bottom of the dialog are two buttons: 'Update' and 'Cancel'.

7. If you want to access APM System Monitoring information within GE Digital APM, enter values in the available fields, and then close the window.

Note: If you do not configure the settings on this window, you can still access APM System Monitoring information via the **Charts** menu on the **Meridium System Monitor Admin** window. If you configure these settings, you will also be able to access APM System Monitoring information via the **APM System Monitoring** page in GE Digital APM.

8. To create a new task, on the **Meridium System Monitor Admin** window, select **Tasks**, and then select the type of task that you want to create or modify.

The **Tasks** window appears, displaying the information related to the selected task. The following image displays an example of the window for tasks of the type *ServerCpuUsage*.

The screenshot shows the 'Tasks' configuration window. The 'Alert Details' section includes the following fields:

- Task Type: ServerCpuUsage
- Day of Week: Wednesday
- Start Time (UTC): 4:00:00 AM
- End Time (UTC): 3:59:59 AM
- Frequency (Seconds): 30
- Event Type: None
- Process Type: None
- Database Type: Oracle
- Database Name: (empty)
- Connection String: (empty)

Buttons for 'New', 'Update', and 'Delete' are visible. A 'Ports' section is also present with a value of 0 and buttons for 'Update', 'Delete', and 'New'.

Below the form is a table with the following data:

| Task Type | Process Type | Start Time | End Time | Freq | Day Of Week | Is Active | Event Type |
|---------------|--------------|------------|----------|------|-------------|-------------------------------------|------------|
| ServerCpuU... | None | 4:00 AM | 3:59 AM | 30 | Wednesday | <input checked="" type="checkbox"/> | None |
| ServerCpuU... | None | 4:00 AM | 3:59 AM | 30 | Friday | <input checked="" type="checkbox"/> | None |

- As needed, create new tasks and modify existing tasks, and then close the **Tasks** window. The configuration of APM System Monitoring has been updated.

What's Next?

- Return to the APM System Monitoring [first-time deployment](#) or [upgrade](#) workflow.


Deploy Asset Criticality Analysis (ACA)

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

Deploy Asset Criticality Analysis (ACA) for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

| Step | Task | Notes |
|------|---|--|
| 1 | Assign Security Users to one or more of the ACA Security Groups and Roles . | This step is required. |
| 2 | Review the ACA data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed. | This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families. |
| 3 | Lock the Risk Matrix. | This step is required only if you do not want risk values to be specified manually via the Risk Matrix. |

Upgrade or Update Asset Criticality Analysis (ACA) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

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

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

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

Upgrade from any version V4.0.0.0 through V4.0.1.0

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

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

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

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

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

Upgrade from any version V3.5.1 through V3.5.1.12.1

| Step | Task | Notes |
|------|-----------------------|---|
| 1 | Lock the Risk Matrix. | This step is required only if you do not want risk values to be specified manually via the Risk Matrix. |

| Step | Task | Notes |
|------|---|--|
| 2 | Create Criticality Mapping records and link them to corresponding Risk Threshold records. | This step is required only if you want to update your SAP system to reflect the criticality value that is determined in ACA. |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

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

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

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

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

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

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 APM Viewer |
| 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 |
|---------------------------------------|------------------------------|---------------|------------------------------|
| Entity | | | |
| Asset Criticality Analysis | View, Update, Insert, Delete | View | View, Update, Insert, Delete |
| Asset Criticality Analysis Has System | View, Update, Insert, Delete | View | View, Update, Insert, Delete |
| Asset Criticality Analysis System | View, Update, Insert, Delete | View | View, Update, Insert, Delete |
| Consequence | View, Update, Insert, Delete | View | View |
| Consequence Modifier | View, Update, Insert, Delete | View | View |

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

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


Deploy Asset Health Manager (AHM)

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

Deploy Asset Health Manager (AHM) for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

| Step | Task | Notes |
|------|--|---|
| 1 | Assign Security Users to one or more of the Asset Health Manager Security Groups and Roles . | This step is required. |
| 2 | On the GE Digital APM Server, configure the Meridium Notification Service for AHM. | This step is required. |
| 3 | On the GE Digital APM Server, start or restart the Meridium Notification Service. | This step is required. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 4 | On the GE Digital APM Server, start the Meridium AHI Service (Asset Health Indicator Service). | This step is required. When you start the service, Health Indicator records are created or updated automatically based on health indicator and reading source records. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 5 | Review the AHM data model to determine which relationship definitions you will need to modify to include your custom asset families. | This step is required only if you store asset information in families other than the baseline Equipment and Functional Location families. |

| Step | Task | 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. | <p>This step is required.</p> <p>If you are using custom asset families and relationships (see Step 5), make sure that the equivalent records and links exist in the database.</p> |
| 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. | <p>This step is required.</p> <p>Baseline Health Indicator Mapping records exist for the following health indicator source families:</p> <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. | <p>This step is required.</p> |
| 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. | <p>This step is optional.</p> |
| 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. | <p>This step is optional.</p> <p>Refer to the Asset Health Manager end user help for more information about events.</p> |

Upgrade or Update Asset Health Manager (AHM) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

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

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

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

Upgrade from any version V4.1.0.0 through V4.1.7.4.0


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

Upgrade from any version V4.0.0.0 through V4.0.1.0

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


Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

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

| Step | Task | Notes |
|------|--|--|
| 2 | On the GE Digital APM Server, start or restart the Meridium Notification Service. | <p>This step is required.</p> <p>You may review the log files for this service at C:\ProgramData\Meridium\Logs.</p> |
| 3 | Start or restart the Meridium AHI Service (Asset Health Indicator Service). | <p>This step is required.</p> <p>You may review the log files for this service at C:\ProgramData\Meridium\Logs.</p> |
| 4 | Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each. | <p>This step is required.</p> <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 data-bbox="802 890 1398 1192" style="border: 1px solid yellow; padding: 5px;"> <p> Note: Alternatively, prior to upgrading to V4.3.0.2.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records. Removing the exclusions after upgrading will cause the GE Digital APM system to generate health indicators automatically.</p> </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. | <p>This step is required.</p> |
| 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. | <p>This step is required.</p> |

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


Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

| Step | Task | Notes |
|------|--|--|
| 1 | On the GE Digital APM Server, configure the Meridium Notification Service for AHM. | This step is required. |
| 2 | On the GE Digital APM Server, start or restart the Meridium Notification Service. | This step is required. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 3 | Start or restart the Meridium AHI Service (Asset Health Indicator Service). | This step is required. You may review the log files for this service at C:\ProgramData\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. | <p>This step is required.</p> <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 style="border: 1px solid yellow; padding: 5px;"> <p> Note: Alternatively, prior to upgrading to V4.3.0.2.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records. Removing the exclusions after upgrading will cause the GE Digital APM system to generate health indicators automatically.</p> </div> |


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

Upgrade from any version V3.5.1 through V3.5.1.12.1

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

| Step | Task | Notes |
|------|--|--|
| 4 | Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each. | <p>This step is required.</p> <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 style="border: 1px solid yellow; padding: 5px;"> <p> Note: Alternatively, prior to upgrading to V4.3.0.2.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records. Removing the exclusions after upgrading will cause the GE Digital APM system to generate health indicators automatically.</p> </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. | This step is required. |
| 6 | If you are using custom Health Indicator Mapping records, specify values in the Type Field and Type Value fields to ensure that the mappings are used for the appropriate reading type. | This step is required. |
| 7 | On the Process Data Integration Server, start (or restart if it is already started) the Meridium Process Data Integration Service. | This step is required only if you are using OPC Tag records as health indicators sources. |


Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

| Step | Task | Notes |
|------|--|---|
| 1 | On the GE Digital APM Server, configure the Meridium Notification Service for AHM. | This step is required. |
| 2 | On the GE Digital APM Server, start or restart the Meridium Notification Service. | This step is required. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 3 | Start or restart the Meridium AHI Service (Asset Health Indicator Service). | This step is required. You may review the log files for this service at C:\ProgramData\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. | <p>This step is required.</p> <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 data-bbox="982 1192 1396 1612" style="border: 1px solid black; padding: 5px;"> <p> Note: Alternatively, prior to upgrading to V4.3.0.2.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records. Removing the exclusions after upgrading will cause the GE Digital APM system to generate health indicators automatically.</p> </div> |


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

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

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

| Step | Task | Notes |
|------|--|--|
| 4 | Review the potential health indicator source records in your database and specify whether or not health indicators should be automatically created for each. | <p>This step is required.</p> <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 style="border: 1px solid yellow; padding: 5px;"> <p> Note: Alternatively, prior to upgrading to V4.3.0.2.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records. Removing the exclusions after upgrading will cause the GE Digital APM system to generate health indicators automatically.</p> </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. | This step is required. |
| 6 | If you are using custom Health Indicator Mapping records, specify values in the Type Field and Type Value fields to ensure that the mappings are used for the appropriate reading type. | This step is required. |
| 7 | On the Process Data Integration Server, start (or restart if it is already started) the Meridium Process Data Integration Service. | This step is required only if you are using OPC Tag records as health indicators sources. |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Notes |
|------|--|---|
| 1 | On the GE Digital APM Server, configure the Meridium Notification Service for AHM. | This step is required. |
| 2 | On the GE Digital APM Server, start or restart the Meridium Notification Service. | This step is required. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 3 | Start or restart the Meridium AHI Service (Asset Health Indicator Service). | This step is required. You may review the log files for this service at C:\ProgramData\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. | <p>This step is required.</p> <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 data-bbox="802 1037 1398 1335" style="border: 1px solid yellow; padding: 5px;"> <p> Note: Alternatively, prior to upgrading to V4.3.0.2.0, you can use the Health Indicator Builder in V3 to create Health Indicator records for the necessary source records. Removing the exclusions after upgrading will cause the GE Digital APM system to generate health indicators automatically.</p> </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. | This step is required. |

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

About the Asset Health Services

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

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

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

Services Summary

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

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

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

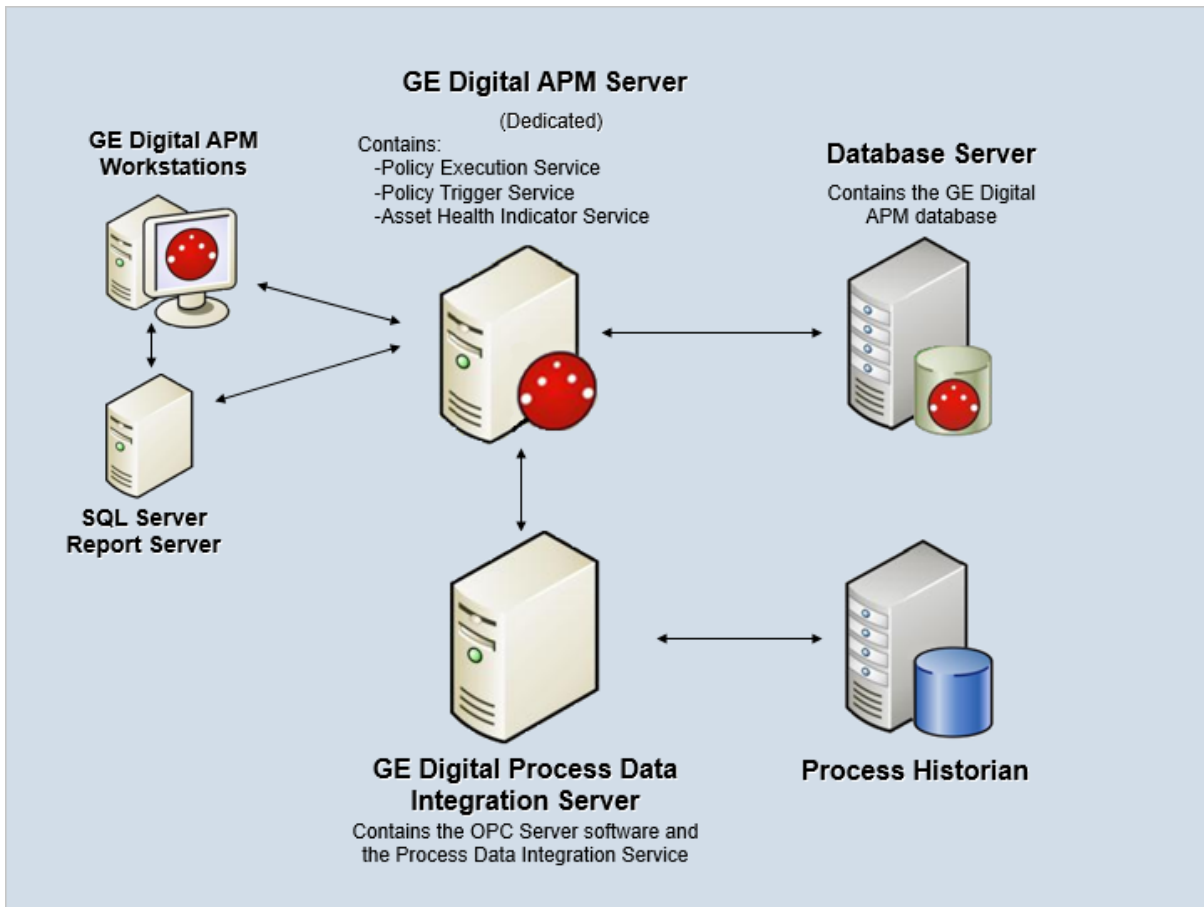
- **Policy Trigger Service:** When an input to a policy (i.e., an associated record in the GE Digital APM database or reading value in the process historian) changes or when a policy schedule is due, a message is added to the policy trigger queue. The Policy Trigger Service monitors this queue and sends these messages to an appropriate policy execution queue.
- **Policy Execution Service:** The Meridium 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 GE Digital APM database) and, when data changes occur on these tags, adds messages to the appropriate queues. This service also facilitates the automatic import and synchronization of tags from a configured process historian.

Example: Standard System Architecture Configuration

The following diagram illustrates the machines in the GE Digital 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 GE Digital APM Servers, [multiple OPC Servers](#), or [multiple GE Digital 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](#), [Process Data Integration](#), and [Policy Designer](#).

| Machine | Software Installed | Asset Health Service Installed Automatically with Service Software |
|-----------------------|--------------------------------|--|
| GE Digital APM Server | GE Digital APM Server software | Asset Health Indicator Service |
| | | Policy Trigger Service |
| | | Policy Execution Service |

| Machine | Software Installed | Asset Health Service Installed Automatically with Service Software |
|--|---|--|
| Process Data Integration Server, which also acts as the OPC Server | Process Data Integration Service software | Process Data Integration Service |
| | OPC Server software | N/A |
| Process Historian | Process historian software | N/A |

Configure the Meridium Notification Service for AHM

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 GE Digital APM Servers.

Steps

1. On the GE Digital 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 Strategy Admin MI Strategy Power |
| MI AHI User | MI Health Power MI Health User MI Strategy Admin MI Strategy Power MI Strategy User |
| MI AHI Viewer | None |

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

| Family | MI AHI Administrator | MI AHI User | MI AHI Viewer |
|--------------------------|------------------------------|----------------------|---------------|
| Entity Families | | | |
| Checkpoint Task | View, Update, Insert | View, Update, Insert | View |
| Event Mapping | View, Update, Insert, Delete | View | View |
| Health Indicator | View, Update, Insert, Delete | View, Update | View |
| Health Indicator Mapping | View, Update, Insert, Delete | View | View |

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

| Family | MI AHI Administrator | MI AHI User | MI AHI Viewer |
|------------------------------|------------------------------|------------------------------|---------------|
| Has OPC Tag | View | View | View |
| Has Readings | View | View | View |
| Has Recommendations | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Timestamped Value | View, Update, Insert, Delete | View | View |
| Health Indicator Has Mapping | View, Update, Insert, Delete | View | View |
| Health Indicator Has Source | View, Update, Insert, Delete | View | View |


Deploy Asset Strategy Implementation (ASI)

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

Deploy Asset Strategy Implementation (ASI) for the First Time

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

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

 **Note:** This GE Digital APM module is not available in the APM Now environment.

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

Upgrade or Update Asset Strategy Implementation (ASI) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

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

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

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

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

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

| Step | Task | Notes |
|------|---|--|
| 2 | Remove rule projects that inherit MeasurementLocation_AM or MeasurementLocation_EM rule projects. | <p>This step is required only if you have customized the baseline rule projects MeasurementLocation_AM and MeasurementLocation_EM.</p> <p>The baseline rules for the MeasurementLocation_AM and MeasurementLocation_EM rule projects have been removed. Therefore, the customized rule projects that inherit these rule projects do not run.</p> |

Upgrade from any version V4.0.0.0 through V4.0.1.0

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

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

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

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

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

Upgrade from any version V3.5.1 through V3.5.1.12.1

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

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

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

| Step | Task | Notes |
|------|---|--|
| 2 | Remove rule projects that inherit MeasurementLocation_AM or MeasurementLocation_EM rule projects. | <p>This step is required only if you have customized the baseline rule projects MeasurementLocation_AM and MeasurementLocation_EM.</p> <p>The baseline rules for the MeasurementLocation_AM and MeasurementLocation_EM rule projects have been removed. Therefore, the customized rule projects that inherit these rule projects do not run.</p> |

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

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

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

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

Asset Strategy Implementation (ASI) Security Groups and Roles

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

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

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

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

| Family | MI ASI Administrator | MI ASI User | MI ASI Viewer |
|-----------------|------------------------------|--------------|---------------|
| Entity Families | | | |
| Action | None | View, Update | View |
| Action Mapping | View, Update, Insert, Delete | View | View |
| Active Strategy | None | View | View |
| Asset Strategy | None | View | View |

| Family | MI ASI Admin- istrator | MI ASI User | MI ASI Viewer |
|---------------------------------|---------------------------------|---------------------------------|------------------|
| Calibration Task | None | View, Update, Insert, Delete | View |
| Consequence | None | View | View |
| Cycle | None | View, Update, Insert, Delete | View |
| Equipment | View, Update, Insert, Delete | View, Update, Insert | View |
| Execution Mapping | View, Update, Insert, Delete | View | View |
| Functional Location | View, Update, Insert, Delete | View, Update, Insert | View |
| Health Indicator | None | View | View |
| Health Indicator Mapping | None | View | View |
| Hierarchy Item Child Definition | None | View | View |
| Hierarchy Item Definition | None | View | View |
| Implementation Authorization | View, Update, Insert, Delete | View | View |
| Implementation Package | None | View, Update, Insert, Delete | View |
| Inspection Task | None | View, Update, Insert, Delete | View |
| KPI | None | View | View |
| KPI Measurement | None | View | View |
| Maintenance Item | None | View, Update, Insert, Delete | View |
| Maintenance Package | None | View, Update, Insert, Delete | View |
| Maintenance Plan | None | View, Update, Insert, Delete | View |
| Material | None | View, Update, Insert, Delete | View |

| Family | MI ASI Administrator | MI ASI User | MI ASI Viewer |
|----------------------------------|------------------------------|------------------------------|---------------|
| Measurement Location | None | View, Update, Insert, Delete | View |
| Measurement Location Group | None | View, Update, Insert, Delete | View |
| Measurement Location Template | View, Update, Insert, Delete | View, Update, Insert | View |
| Notification | None | View, Update, Insert, Delete | View |
| Object List Item | None | View, Update, Insert, Delete | View |
| Operation | None | View, Update, Insert, Delete | View |
| Operator Rounds Allowable Values | None | View | View |
| Probability | None | View | View |
| Proposed Strategy | None | View | View |
| Protection Level | None | View | View |
| PRT | None | View, Update, Insert, Delete | View |
| PRT Template | View, Update, Insert, Delete | View | View |
| RCM FMEA Asset | None | View | View |
| RCM FMEA Recommendation | None | View | View |
| Risk | None | View | View |
| Risk Assessment | None | View | View |
| Risk Category | None | View | View |
| Risk Matrix | None | View | View |
| Risk Rank | None | View | View |
| Risk Threshold | None | View | View |


| Family | MI ASI Administrator | MI ASI User | MI ASI Viewer |
|---|------------------------------|------------------------------|---------------|
| SAP System | View, Update, Insert, Delete | View | View |
| Site Reference | View | View | View |
| System Strategy | None | View | View |
| Task List | None | View, Update, Insert, Delete | View |
| Task Types | None | View | View |
| Thickness Monitoring Task | None | View, Update, Insert, Delete | View |
| Unit Strategy | None | View | View |
| Work Management Item Child Definition | View, Update, Insert, Delete | View | View |
| Work Management Item Definition | View, Update, Insert, Delete | View | View |
| Work Management Item Definition Configuration | View, Update, Insert, Delete | View | View |
| Relationship Families | | | |
| Authorized to Implement | View, Update, Insert, Delete | View | View |
| Documents Action | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Actions | None | View | View |
| Has Action Mapping | View, Update, Insert, Delete | View | View |
| Has Action Revisions | None | View | View |
| Has Active Strategy | None | View | View |
| Has Asset Strategy | None | View | View |
| Has Associated Recommendation | None | View | View |
| Has Checkpoint | None | View, Insert | View |

| Family | MI ASI Administrator | MI ASI User | MI ASI Viewer |
|--------------------------------|------------------------------|------------------------------|---------------|
| Has Child Hierarchy Item | None | View | View |
| Has Child Work Management Item | View, Update, Insert, Delete | View | View |
| Has Cycles | None | View, Update, Insert, Delete | View |
| Has Driving Recommendation | None | View | View |
| Has Execution Mapping | View, Update, Insert, Delete | View | View |
| Has Health Indicators | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has KPI Measurement | None | View | View |
| Has Maintenance Item | None | View, Update, Insert, Delete | View |
| Has Maintenance Package | None | View, Update, Insert, Delete | View |
| Has Material | None | View, Update, Insert, Delete | View |
| Has Measurement Location Group | None | View, Update, Insert, Delete | View |
| Has Mitigation Revisions | None | View | View |
| Has Object List Item | None | View, Update, Insert, Delete | View |
| Has Operation | None | View, Update, Insert, Delete | View |
| Has Proposed Strategy | None | View | View |
| Has PRT | None | View, Update, Insert, Delete | View |
| Has Reference Values | None | View | View |
| Has Risk | None | View | View |
| Has Risk Category | None | View | View |

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

| Family | MI ASI Admin- istrator | MI ASI User | MI ASI Viewer |
|--------------------|---------------------------------|---------------------------------|------------------|
| Was Applied to PRT | View, Update, Insert, Delete | View, Update, Insert, Delete | View |

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

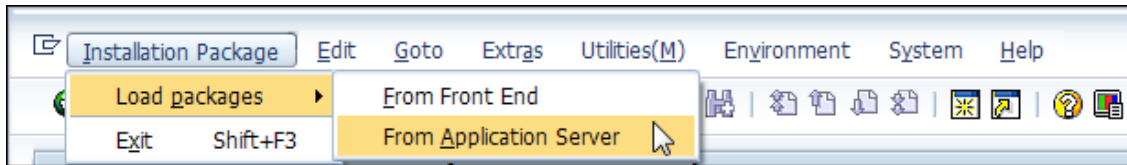
 **Note:** To complete the following instructions successfully, you must use SAP client 000.

Before You Begin

Determine the release and level of your current ABAP installation by completing the [steps to verify the ABAP installation](#).

Steps

1. On a machine from which you can access the SAP Server, access your ASI ABAP installation package.
2. If your currently installed ABAP release is *420_600* and level is *0000*, and you are *not* installing the ASI ABAP Add-on in an S/4 Hana SAP system, proceed to step 19. Otherwise, proceed to the next step.
3. Navigate to the folder **\\SAP ASI ABAP Add-On\Service Pack Files\ECC6** or **\\SAP ASI ABAP Add-On\Service Pack Files\S/4 Hana**, and then select one of the following folders:
 - **Exchange Upgrade:** To upgrade the ASI ABAP Add-on when upgrading to a new SAP version.
 - **Installation:** To install the ASI ABAP Add-on for the first time.
 - **Upgrade:** To upgrade the ASI ABAP Add-on.
4. Copy the .pat file(s).
5. On the SAP Server, paste the copied file(s) into the folder *usr\sap\trans\eps\in*.
6. Log in to the SAP system as a user with:
 - SCTSIMPSSL and S_CTS_ADMIN authorizations.
 - or-
 - SAP_ALL authorization
7. Run the following transaction: *SAINT*
The **Add-On Installation Tool** screen appears.
8. On the **Installation Package** menu, then select **Load Packages**, and then select **From Application Server**.




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

9. Select **Yes**.

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

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

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

10. Select the .pat file(s) that you copied previously.
11. Select .

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

12. Select **Start**.

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

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


The **Support Package selection** tab appears.

14. Select **Continue**.
15. Select **Continue** again.

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

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

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

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

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

18. Select **Finish**.

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

19. In the installation package, navigate to the folder `\\SAP ASI ABAP Add-On\Support Package\ECC6`.

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

-or-

If your ABAP release was any other version, navigate to the folder `\\V4.0.0`.

21. Copy the .pat file(s).

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

23. Log in to the SAP system.

24. Run the following transaction: *SPAM*.

The **Support Package Manager** screen appears.

25. On the **Support Package** menu, select **Load Packages**, and then select **From Application Server**.

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

26. Select **Yes**.


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

27. Select **Back**.

28. Select **Display/define**.

The **Component Selection** dialog box appears.

29. Select **MIAPMINT**.

30. When prompted, confirm that the patch will be imported into the queue, and then select 

.

31. On the **Support Package** menu, select .

32. On the **SPAM: Import: Queue** dialog box, select .

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

33. Select **Continue**.

Another message appears, indicating that the import process was successful.

34. Select .

35. On the **Support Package** menu, select .

The installation is complete.

What's Next?

- [Configure SAP for External Numbering](#)

Verify ASI ABAP Add-On

Steps

1. In SAP, on the **System** menu, select **Status**.

The **System: Status** window appears.

The screenshot shows the 'SAP data' window with two main sections: 'Repository data' and 'SAP System data'. The 'Repository data' section includes fields for Transaction (SE37), Program (screen) (SAPLSFUNCTIO...), Screen number (3000), Program (GUI) (SAPLSFUNCTIO...), and GUI status (WB_WITH_TOOL...). The 'SAP System data' section includes Component version (SAP ECC 6.0), Installation number (0020243634), License expiration (31.12.9999), and Unicode System (Yes). A magnifying glass icon is visible next to the Component version field.

2. In the **SAP System data** section, select .

The **Support Package Level for Installed Software Components** window appears.

| Software Compon... | Release | Level | Highest Support ... | Short Description of Software Compon |
|--------------------|---------|-------|---------------------|--------------------------------------|
| SLL_PI | 900_604 | 0001 | SAPK-90A01INSL... | GTS Plug-In |
| WFMCORE | 200 | 0016 | SAPK-20016INWF... | WFMCORE 200 Upgrade: Meta-Comm |
| GRCFND_A | 300 | 0001 | SAPK-30001INGR... | GRC Foundation ABAP |
| GRCPCRTA | 300_700 | 0007 | SAPK-30307INGR... | GRCPC 300 RTA for 700 |
| EHSM | 100 | 0001 | SAPK-10001INEH... | SAP EHS Management Extension 1.0 |
| AIN | 400 | 0002 | SAPK-40002INAIN | AIN 400 : Add-On Supplement |
| MIAPMINT | 400_600 | 0000 | - | Meridium APM Integration Interfaces |
| MRSS | 700 | 0005 | SAPK-70005INMR... | Multi Resource Service Scheduling |

At the bottom of the table, there are navigation arrows and a search input field. Below the table, there are three icons: a green checkmark, a red X, and a document icon.

3. If you have deployed the SAP Adapter's ABAP Add-On package, scroll down until you see the Software Component *MIAPM*. If you see the following values in the following columns, the Add-On was applied successfully:

- **Release:**

- ECC6: *420_600* or *400_600*, depending on the version of SAP that you have installed.
- S/4 Hana: *400_750*
- **Level:**
 - ECC6: *0032*
 - S/4 Hana: *0000*

What's Next?

- [Return to the workflow](#) Return to the workflow for the next step in the deployment process.

Uninstall the ASI ABAP Base Service Pack Add-On

Note: The uninstall feature is available only in SAP versions S/4 Hana 1511 and later. To complete these steps, you *must* use SAP client 000.

Before You Begin

- [Verify the release and level of your ASI ABAP installation.](#)

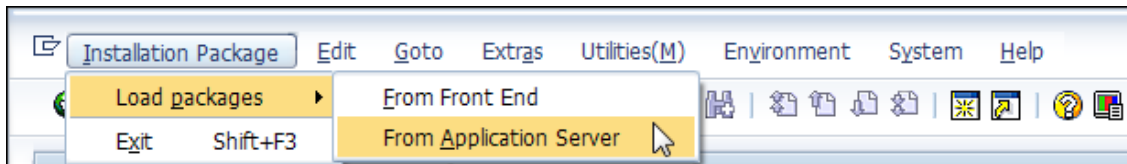
Steps

1. On a machine with access to the SAP Server, insert the SAP Interfaces installation DVD.
2. Navigate to the folder \\SAP ASI ABAP Add-On\Service Pack Files\S4Hana\Uninstall, and then copy the .pat file(s).
3. On the SAP server, navigate to the folder \\usr\sap\trans\EPS\in, and then paste the copied files.
4. Log in to the SAP server as a user with either *SCTSIMPSGL* and *S_CTS_ADMIN* authorizations or *SAP_ALL* authorization.

5. Enter *SAINT*.

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

6. Select **Installation Package**, then select **Load packages**, and then select **From Application Server**.



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

7. Select **Yes**.

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

SAINT: Uploading Packages from the File System

| OCS File Name | Package | Result | RC | Message Text |
|---------------|----------------------|--------|------|-----------------------|
| D070020243634 | SAPK-400COINMIAPMINT | | 0000 | Uploaded successfully |

8. Select the .pat file(s) that you copied previously.

The **Message Text** column displays the message *Uploaded successfully*.

9. Select .

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

10. Select the **Uninstallable components** tab.

MIAPM appears in the list of add-on packages that can be uninstalled.

11. Select **MIAPM**, and then select **Continue**.

The **Start options** dialog box appears.

12. Select **Default options**.

13. Select .

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

14. Select **Finish**.

Results

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

Configure SAP for External Numbering

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

Steps

1. Define the following External Number Ranges according to SAP documentation:

| Object Type | From Number | To Number |
|-------------------------------|------------------|------------------|
| Maintenance Plan | M00000000001 | M99999999999 |
| Maintenance Item | M000000000000001 | M999999999999999 |
| General Maintenance Task List | M0000001 | M9999999 |

⚠ IMPORTANT: For details on configuring SAP for External Numbering, see the documentation for your SAP system.

What's Next?

- [Configure SAP Permissions](#)

Configure SAP Permissions

If you will be sending data to SAP using ASI Implementation Packages, you must configure SAP Permissions.

Steps

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

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

About the ASI for SAP ABAP Add-on

GE Digital APM ASI for SAP extends the basic functionality of Asset Strategy Implementation (ASI) by offering integration with SAP. Deploying ASI for SAP requires two steps:

- Activating the ASI for SAP license in the GE Digital APM database. This documentation assumes that you activated the license when you completed the steps for creating or upgrading your GE Digital APM database.
- [Deploying the ASI for SAP ABAP add-on](#), which is a package that must be deployed on your SAP system to allow for integration between your GE Digital APM system and your SAP system.

The files necessary to deploy ASI for SAP are provided on the ASI for SAP ABAP Add-on DVD, which is not included in the standard GE Digital APM distribution but can be obtained from GE Digital upon request.

The ASI for SAP ABAP Add-on DVD contains installation files, upgrade files, and exchange files. In this documentation, we provide details on using the installation and upgrade files. You will need to use the exchange files if you upgrade an SAP system on which the ASI for SAP ABAP Add-on package has been installed. In that case, the SAP upgrade procedure will prompt you to access the exchange files for ASI for SAP. You can find the files in the Exchange Upgrade Files folder on the ASI for SAP ABAP Add-on DVD. Within the Exchange Upgrade Files folder, you will see subfolders representing the version of SAP to which you are upgrading. When prompted for an ASI for SAP exchange file, use the files in these subfolders. This documentation does not provide specific instructions for using these files during an SAP upgrade.

For information about what is included in the ASI ABAP Add-on, see the file `SAP_ASI_<version>_ObjectList.pdf`, which is located on the ASI for SAP ABAP Add-on installation DVD in the root folder.


Deploy Asset Strategy Management (ASM)

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

Deploy Asset Strategy Management (ASM) for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

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

Upgrade or Update Asset Strategy Management (ASM) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

| Step | Task | Notes |
|------|---|--|
| 1 | Prior to upgrading your database, review any Action records that are linked to HI Sources and link the HI Sources to Health Indicator records if necessary. | <p>This step is optional.</p> <p>As of V4.3.0.2.0, actions are implemented by health indicators rather than by HI Sources. When you upgrade to V4.3.0.2.0, if an action was previously implemented as an HI Source, if that HI Source has a related health indicator, the action will be linked to that health indicator during the upgrade. Similarly, if the action has multiple health indicators, one of them will be selected to implement the action. However, if the HI Source does <i>not</i> have a related health indicator, the action will no longer be implemented after the upgrade. Therefore, you should complete this step if you want to ensure your actions in these scenarios have an implementation after the upgrade (i.e., be linked to a Health Indicator record).</p> <p>This change does not impact Measurement Locations.</p> |

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

| Step | Task | Notes |
|------|---|--|
| 1 | Prior to upgrading your database, review any Action records that are linked to HI Sources and link the HI Sources to Health Indicator records if necessary. | <p>This step is optional.</p> <p>As of VV4.3.0.2.0, actions are implemented by health indicators rather than by HI Sources. When you upgrade to VV4.3.0.2.0, if an action was previously implemented as an HI Source, if that HI Source has a related health indicator, the action will be linked to that health indicator during the upgrade. Similarly, if the action has multiple health indicators, one of them will be selected to implement the action. However, if the HI Source does <i>not</i> have a related health indicator, the action will no longer be implemented after the upgrade. Therefore, you should complete this step if you want to ensure your actions in these scenarios have an implementation after the upgrade (i.e., be linked to a Health Indicator record).</p> <p>This change does not impact Measurement Locations.</p> |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| Step | Task | Notes |
|------|---|--|
| 1 | Prior to upgrading your database, review any Action records that are linked to HI Sources and link the HI Sources to Health Indicator records if necessary. | <p>This step is optional.</p> <p>As of VV4.3.0.2.0, actions are implemented by health indicators rather than by HI Sources. When you upgrade to VV4.3.0.2.0, if an action was previously implemented as an HI Source, if that HI Source has a related health indicator, the action will be linked to that health indicator during the upgrade. Similarly, if the action has multiple health indicators, one of them will be selected to implement the action. However, if the HI Source does <i>not</i> have a related health indicator, the action will no longer be implemented after the upgrade. Therefore, you should complete this step if you want to ensure your actions in these scenarios have an implementation after the upgrade (i.e., be linked to a Health Indicator record).</p> <p>This change does not impact Measurement Locations.</p> |

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in

the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.1

ASM will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

| Step | Task | 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. | This step is required. |
| 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. | This step is required. |
| 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. | This step is required. |

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

| Step | Task | Notes |
|------|---|------------------------|
| 1 | Move to the <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. | This step is required. |
| 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. | This step is required. |
| 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. | This step is required. |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Notes |
|------|---|------------------------|
| 1 | Move to the <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. | This step is required. |
| 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. | This step is required. |
| 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. | This step is required. |

Asset Strategy Management (ASM) Security Groups and Roles

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

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

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

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

| Family | MI ASM Analyst | MI ASM Administrator | MI ASM Reviewer | MI ASM Viewer |
|-----------------|------------------------------|----------------------|------------------------------|---------------|
| Entity Families | | | | |
| Action | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Action Mapping | View | None | None | None |

| Family | MI ASM Analyst | MI ASM Administrator | MI ASM Reviewer | MI ASM Viewer |
|-----------------------------------|------------------------------|------------------------------|------------------------------|----------------------|
| Active Strategy | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Analysis Link | View | View | View | View |
| Asset Criticality Analysis | View | View | View | View |
| Asset Criticality Analysis System | View | View | View | View |
| Asset Strategy | View, Update, Insert, Delete | View | View, Update | View |
| Calibration Task | View | None | View | None |
| Checkpoint Task | View, Update, Insert | View, Update, Insert | View, Update, Insert | View, Update, Insert |
| Consequence | View | View, Update, Insert, Delete | View | View |
| Distribution | View, Update, Insert, Delete | View | View | View |
| Execution Mapping | View | None | None | None |
| Growth Model | View | View | View | View |
| Health Indicator | View, Update, Insert, Delete | None | View, Update | View, Update |
| Health Indicator Mapping | View | View, Update, Insert, Delete | View | View |
| Hierarchy Item Child Definition | View | View, Update, Insert, Delete | View | View |
| Hierarchy Item Definition | View | View, Update, Insert, Delete | View | View |
| Implementation Package | View, Insert | None | None | None |
| Inspection Task | View | None | View | View |
| KPI | View | View | View | View |
| KPI Measurement | View | View | View | View |

| Family | MI ASM Analyst | MI ASM Administrator | MI ASM Reviewer | MI ASM Viewer |
|----------------------------------|------------------------------|------------------------------|------------------------------|---------------|
| Measurement Location | View | View | View | View |
| Measurement Location Group | View, Update, Insert | None | None | None |
| Measurement Location Template | View | View | View | View |
| Operator Rounds Allowable Values | View | View | View | View |
| Probability | View | View, Update, Insert, Delete | View | View |
| Proposed Strategy | View, Update, Insert, Delete | View | View, Update | View |
| Protection Level | View | View | View | View |
| RBI Degradation Mechanisms | View, Update | None | None | None |
| RBI Recommendation | View, Update | None | None | None |
| RCM FMEA Asset | View, Update, Insert, Delete | View | View | View |
| Reading | View | View | View | View |
| Reliability Distribution | View | View | View | View |
| Reliability Growth | View | View | View | View |
| Risk Assessment | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Risk Category | View | View, Update, Insert, Delete | View | View |
| Risk Matrix | View | View, Update, Insert, Delete | View | View |
| Risk Rank | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Risk Threshold | View | Insert, View, Update, Delete | View | View |
| Site Reference | View | View | View | View |

| Family | MI ASM Analyst | MI ASM Administrator | MI ASM Reviewer | MI ASM Viewer |
|----------------------------|------------------------------|------------------------------|-----------------|---------------|
| System Action | View, Update, Insert, Delete | View | View | View |
| System Action Mapping | View | View, Update, Insert, Delete | View | View |
| System Action Optimization | View, Update, Insert, Delete | View | View | View |
| System Action Result | View, Update, Insert, Delete | View | View | View |
| System Analysis | View, Update, Insert, Delete | View | View | View |
| System Element | View, Update, Insert, Delete | View | View | View |
| System Element Result | View, Update, Insert, Delete | View | View | View |
| System Global Event | View, Update, Insert, Delete | View | View | View |
| System Resource | View, Update, Insert, Delete | View | View | View |
| System Resource Result | View, Update, Insert, Delete | View | View | View |
| System Resource Usage | View, Update, Insert, Delete | View | View | View |
| System Risk Assessment | View, Update, Insert, Delete | View | View | View |
| System Scenario | View, Update, Insert, Delete | View | View | View |
| System Sensor | View, Update, Insert, Delete | View | View | View |
| System Strategy | View, Update, Insert, Delete | View | View, Update | View |
| Unit Strategy | View, Update, Insert, Delete | View | View, Update | View |

| Family | MI ASM Analyst | MI ASM Administrator | MI ASM Reviewer | MI ASM Viewer |
|---|------------------------------|------------------------------|------------------------------|---------------|
| Work Management Item Child Definition | View | None | None | None |
| Work Management Item Definition | View | None | None | None |
| Work Management Item Definition Configuration | View | None | None | None |
| Relationship Families | | | | |
| Asset Criticality Analysis Has System | View | View | View | View |
| Has Action Driver | View, Update, Insert, Delete | None | None | None |
| Has Action Mapping | View | None | None | None |
| Has Action Revisions | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Actions | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Active Strategy | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Asset Strategy | View, Update, Insert, Delete | View | View | View |
| Has Associated Recommendation | View, Update, Insert, Delete | View | View | View |
| Has Associated Strategy | View, Update, Insert, Delete | View | View | View |
| Has Checkpoint | View | None | None | None |
| Has Child Hierarchy Item | View | View, Update, Insert, Delete | View | View |
| Has Child Work Management Item | View | None | None | None |
| Has Driving Recommendation | View, Update, Insert, Delete | View | View, Delete | View |

| Family | MI ASM Analyst | MI ASM Administrator | MI ASM Reviewer | MI ASM Viewer |
|--------------------------------|------------------------------|------------------------------|------------------------------|---------------|
| Has Execution Mapping | View | None | None | None |
| Has Functional Location | View | None | View | None |
| Has Global Events | View, Update, Insert, Delete | View | View | View |
| Has Health Indicators | View, Update, Insert, Delete | View | View | View |
| Has Measurement Location Group | View, Update, Insert, Delete | None | None | None |
| Has Mitigated TTF Distribution | View, Update, Insert, Delete | View | View | View |
| Has Mitigation Revisions | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Planned Resource Usages | View, Update, Insert, Delete | View | View | View |
| Has Proposed Strategy | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Readings | View | View | View | View |
| Has Recommendations | View, Update, Insert, Delete | None | None | N/A |
| Has Reference Values | View | View, Update, Insert, Delete | View | View |
| Has Resource Usages | View, Update, Insert, Delete | View | View | View |
| Has Risk | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Risk Assessments | View, Update, Insert, Delete | View | View | View |
| Has Risk Category | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Risk Matrix | View | None | None | None |

| Family | MI ASM Analyst | MI ASM Administrator | MI ASM Reviewer | MI ASM Viewer |
|-------------------------------|------------------------------|----------------------|------------------------------|---------------|
| Has Risk Revisions | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Root System | View, Update, Insert, Delete | View | View | View |
| Has Scenarios | View, Update, Insert, Delete | View | View | View |
| Has Strategy | View, Update, Insert, Delete | View | View | View |
| Has Strategy Revision | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has System Actions | View, Update, Insert, Delete | View | View | View |
| Has System Elements | View, Update, Insert, Delete | View | View | View |
| Has System Optimization | View, Update, Insert, Delete | View | View | View |
| Has System Resources | View, Update, Insert, Delete | View | View | View |
| Has System Results | View, Update, Insert, Delete | View | View | View |
| Has System Risks | View, Update, Insert, Delete | View | View | View |
| Has System Strategy | View, Update, Insert, Delete | View | View | View |
| Has TTF Distribution | View, Update, Insert, Delete | View | View | View |
| Has TTR Distribution | View, Update, Insert, Delete | View | View | View |
| Has Unplanned Resource Usages | View, Update, Insert, Delete | View | View | View |
| Has Work Management Item | View, Update, Insert | None | None | None |

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

Associating a Strategy with a Specific Site

Some companies that use the GE Digital 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 GE Digital 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.


Deploy Asset Strategy Optimization (ASO)

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

Deploy Asset Strategy Optimization (ASO) for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

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

Upgrade or Update Asset Strategy Optimization (ASO) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital 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 V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

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

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

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

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

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

Asset Strategy Optimization (ASO) Security Groups and Roles

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

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

Deploy Calibration Management

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

Deploy Calibration Management for the First Time

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

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

Note: If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

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

Upgrade or Update Calibration Management to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

| Step | Task | Notes |
|------|--|--|
| 1 | Uninstall the previous version of the GE Digital APM Device Service on all of the machines that will connect to devices that will be used with Calibration Management. | Install the GE Digital APM Device Service on all of the machines that will connect to devices that will be used to send and receive data with Calibration Management. |
| 2 | Install the GE Digital APM Device Service on all of the machines that will connect to devices that will be used with Calibration Management. | This step is required only if you will use any device to send and receive data in Calibration Management. If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 2850 . |
| 3 | On the machine on which the GE Digital APM Server is running, select the Windows Start button, then navigate to and right-click Command Prompt , and then select Run as administrator . A command prompt window appears. | This step is required. |

| Step | Task | Notes |
|------|--|------------------------|
| 4 | Through command prompt, navigate to the installation folder (e.g., C:\Program Files\Meridium\Upgrade). | This step is required. |
| 5 | <p>On the command prompt window, enter the following:</p> <pre>Meridium.DbUtility.CalibDeviceMappingsUpgradeUtility.exe <datasourceID> <username> <password></pre> <p>Where,</p> <ul style="list-style-type: none"> • <datasourceID> is the identification of your data source. • <username> is the GE Digital APM username. • <password> is the GE Digital APM password. | This step is required. |

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

| Step | Task | Notes |
|------|--|--|
| 1 | Uninstall the previous version of the GE Digital APM Device Service on all of the machines that will connect to devices that will be used with Calibration Management. | Install the GE Digital APM Device Service on all of the machines that will connect to devices that will be used to send and receive data with Calibration Management. |
| 2 | Install the GE Digital APM Device Service on all of the machines that will connect to devices that will be used with Calibration Management. | This step is required only if you will use any device to send and receive data in Calibration Management. If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 2850 . |

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

| Step | Task | Notes |
|------|--|---|
| 1 | Uninstall the previous version of the GE Digital APM Device Service on all of the machines that will connect to devices that will be used with Calibration Management. | Install the GE Digital APM Device Service on all of the machines that will connect to devices that will be used to send and receive data with Calibration Management. |

| Step | Task | Notes |
|------|--|--|
| 2 | Install the GE Digital APM Device Service on all of the machines that will connect to devices that will be used with Calibration Management. | This step is required only if you will use any device to send and receive data in Calibration Management. If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 2850 . |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| Step | Task | Notes |
|------|--|--|
| 1 | Uninstall the previous version of the GE Digital APM Device Service on all of the machines that will connect to devices that will be used with Calibration Management. | Install the GE Digital APM Device Service on all of the machines that will connect to devices that will be used to send and receive data with Calibration Management. |
| 2 | Install the GE Digital APM Device Service on all of the machines that will connect to devices that will be used with Calibration Management. | This step is required only if you will use any device to send and receive data in Calibration Management. If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 2850 . |

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital 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 V4.3.0.2.0 automatically when you upgrade the components in

the basic GE Digital APM system architecture. No additional steps are required.


Install the Meridium Device Service

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

The Meridium Device Service can be installed as part of the workflow when you try to [send data to 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. Select the **Calibration Tools** tab.

The **Calibration Tools** section appears, displaying a list of test equipment and standard gas cylinders.

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

The **Calibrator Settings** window appears.

Calibrator Settings ×

Calibrator Device Settings

Select Device

Done

4. In the **Select Device** box, select the required device.
5. If you selected the CMX Calibration Management software, enter values in the following fields:

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

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

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

⚠ IMPORTANT: GE Digital APM supports port numbers in the range of COM1 through COM4. If the communication port number of the calibrator does not fall within this range, you must change the value in the Device Manager, or connect the calibrator to a different port.

- If you want to test the connection of the Fluke documenting process calibrator, select the **Perform Connection Test** check box.

📄 Note: The **Baud Rate** box contains the value *9600*. You cannot change this value.

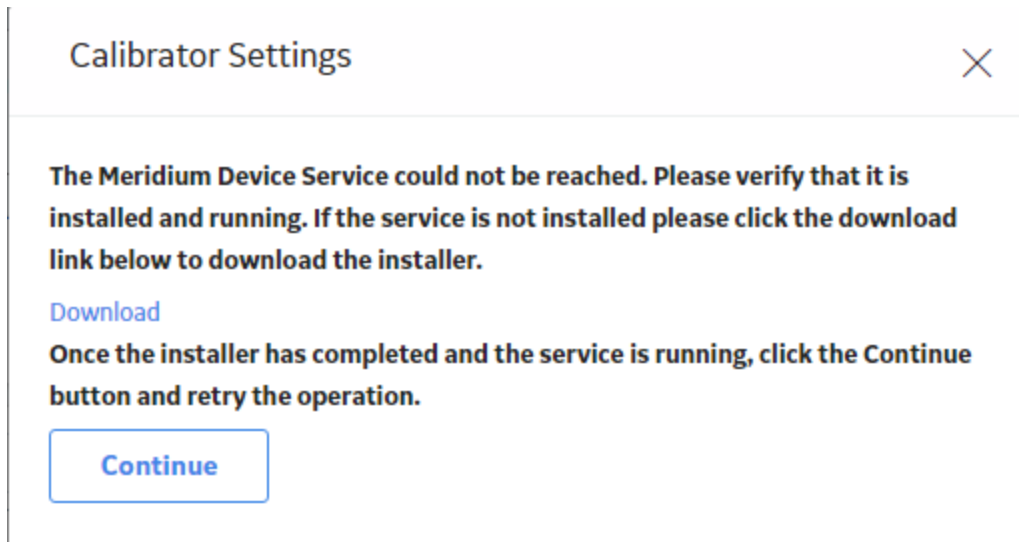
- In the **Device Service Settings Service Port** box, enter the value of the service port number that you have configured. The default value in the **Device Service Settings Service Port** box is *2014*.

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

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

6. Select **Done**.

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



7. Select **Download**.

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

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

The Meridium Device Service is installed.

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 |
| MI Calibration Viewer | MI APM Viewer MI Safety Admin MI Safety Power MI Safety User MI Strategy Admin MI Strategy Power MI Strategy 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 | MI Calibration Viewer |
|-----------------|------------------------------|---------------------|-----------------------|
| Entity Families | | | |

| Family | MI Calibration Administrator | MI Calibration User | MI Calibration Viewer |
|--|------------------------------|------------------------------|-----------------------|
| Alert | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Asset Safety Preferences | View, Update, Insert, Delete | View | View |
| Calibration (Event) | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Calibration, Analog | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Calibration, Analyzer Multi-Component | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Calibration, Analyzer Single Component | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Calibration, CMX | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Calibration, Discrete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Calibration, Functional Test | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Calibration, Weight Scale | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Calibration Device Driver | View, Update, Insert, Delete | View | View |
| Calibration Device Mapping | View, Update, Insert, Delete | View | View |
| Calibration Mapping Family | View, Update, Insert, Delete | View | View |
| Calibration Mapping Field | View, Update, Insert, Delete | View | View |
| Calibration Profile | View, Update, Insert, Delete | View | View |
| Calibration Profile Template Defaults | View, Update, Insert, Delete | View | View |

| Family | MI Calibration Administrator | MI Calibration User | MI Calibration Viewer |
|---|------------------------------|------------------------------|-----------------------|
| Calibration Recommendation | View, Update, Insert, Delete | View, Update, Insert | View |
| Calibration Result | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Calibration Results, Analog | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Calibration Results, Analyzer | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Calibration Result, Discrete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Calibration Results, Functional Test | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Calibration Setup Defaults | View, Update, Insert, Delete | View | View |
| Calibration Strategy | View, Update, Insert, Delete | View | View |
| Calibration Task | View, Update, Insert, Delete | View | View |
| Calibration Task Revision | View, Update, Insert, Delete | View | View |
| Calibration Template | View, Update, Insert, Delete | View | View |
| Calibration Template, Analog | View, Update, Insert, Delete | View | View |
| Calibration Template, Discrete | View, Update, Insert, Delete | View | View |
| Calibration Template, Weight Scale | View, Update, Insert, Delete | View | View |
| Calibration Template, Single Component Analyzer | View, Update, Insert, Delete | View | View |
| Calibration Template, Multi-Component Analyzer | View, Update, Insert, Delete | View | View |

| Family | MI Calibration Administrator | MI Calibration User | MI Calibration Viewer |
|---------------------------------------|------------------------------|------------------------------|-----------------------|
| Calibration Template, Functional Test | View, Update, Insert, Delete | View | View |
| Calibration Template, CMX | View, Update, Insert, Delete | View | View |
| Calibration Template Defaults | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Calibration Template Detail | View, Update, Insert, Delete | View | View |
| Calibration Template Detail, Analyzer | View, Update, Insert, Delete | View | View |
| Calibrator | View, Update, Insert, Delete | View | View |
| Equipment | View | View | View |
| Functional Location | View | View | View |
| Reference Document | View, Update, Insert, Delete | View | View |
| SAP System | View | View | View |
| Standard Gas | View, Update, Insert, Delete | View | View |
| Standard Gas Components | View, Update, Insert, Delete | View | View |
| Standard Gas Cylinder | View, Update, Insert, Delete | View | View |
| Task | View, Update, Insert, Delete | View | View |
| Task Types | View, Update, Insert, Delete | View | View |
| Test Equipment | View, Update, Insert, Delete | View | View |
| Test Equipment History | View, Update, Insert, Delete | View | View |

| Family | MI Calibration Administrator | MI Calibration User | MI Calibration Viewer |
|--|------------------------------|------------------------------|-----------------------|
| Work History | View | View | View |
| Work History Detail | View | View | View |
| Relationship Families | | | |
| Calibration Device Driver Has Mapping | View, Update, Insert, Delete | View | View |
| Calibrator has Device Driver | View, Update, Insert, Delete | View | View |
| Calibration Mapping Has Family | View, Update, Insert, Delete | View | View |
| Calibration Mapping Has Field | View, Update, Insert, Delete | View | View |
| Calibration Mapping Has Strategy | View, Update, Insert, Delete | View | View |
| Equipment Has Equipment | View | View | View |
| Functional Location Has Equipment | View | View | View |
| Functional Location Has Functional Location(s) | View | View | View |
| Has Associated Recommendation | View, Update, Insert, Delete | View | View |
| Has Calibration | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Calibration Profiles | View, Update, Insert, Delete | View | View |
| Has Calibration Results | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Consolidated Recommendations | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Driving Recommendations | View, Update, Insert, Delete | View | View |

| Family | MI Calibration Administrator | MI Calibration User | MI Calibration Viewer |
|--------------------------------|------------------------------|------------------------------|-----------------------|
| Has Event Detail | 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 |
| Has Standard Gas | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Standard Gas Components | View, Update, Insert, Delete | View | View |
| Has Standard Gas Details | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Superseded Recommendations | View, Update, Insert, Delete | View | View |
| Has Task Revision | View, Update, Insert, Delete | View | View |
| Has Tasks | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Templates | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Template Detail | View, Update, Insert, Delete | View | View |
| Has Test Equipment | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Work History | View | View | View |
| Test Equipment Has Equipment | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Test Equipment Has History | View, Update, Insert, Delete | View, Update, Insert, Delete | View |

Deploy Cognitive Analytics

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

Deploy Cognitive Analytics for the First Time

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

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

Note: If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

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

Upgrade or Update Cognitive Analytics to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Cognitive Analytics Security Groups and Roles

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

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

| Security Group | Roles |
|----------------------------|----------------------------|
| MI Cognitive User | MI Analytics Power |
| MI Cognitive Administrator | MI Analytics Administrator |

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

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


Deploy eLog


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 eLog 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 GE Digital APM system architecture.

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

| Step | Task | Notes |
|------|---|---|
| 1 | If needed, create Log Entry subfamilies to store the information that you want to log. | This step is required only if the baseline Log Entry family does not contain all the information that you want to document. |
| 2 | <p>Review the eLog data model to determine which relationship definitions you will need to add to include your custom Log Entry subfamilies, or to store your classified data in custom subfamilies.</p> <p>Via Configuration Manager, modify any relationship definitions as needed. When you create a Log Entry subfamily, all fields from the Log Entry family will be inherited automatically. You can then create additional family fields as necessary.</p> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p> IMPORTANT: Fields inherited from the Log Entry family should not be modified.</p> </div> | This step is required only if you store information in families other than the baseline Log Entry family. |
| 3 | Assign Security Users to one or more of the eLog Security Groups or Roles . | This step is required. |
| 4 | Create Shift records to assign Shifts to your log entries. | This step is required. |

Upgrade or Update eLog to V4.3.0.2.0


The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

eLog Security Groups and Roles

 **Note:** To create a Primary Event in eLog, you must be a member of the [MI GAA Analyst Security Group](#).

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

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

| Security Group | Roles |
|-----------------------|---|
| MI eLog Viewer | MI APM Viewer MI Foundation Admin MI Foundation Power MI Foundation User |
| MI eLog Contributor | MI Foundation Admin MI Foundation Power MI Foundation User |
| MI eLog Administrator | MI Foundation Admin |

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

| Family | eLog Viewer | eLog Contributor | eLog Administrator |
|------------------------------------|-------------|------------------------------|------------------------------|
| Entity Families | | | |
| Log Entry and all its sub-families | View | View, Create, Update, Delete | View, Create, Update, Delete |
| Shift | View | View, Create, Update, Delete | View, Create, Update, Delete |
| Reference Document | View | View, Create, Update, Delete | View, Create, Update, Delete |

| Family | eLog Viewer | eLog Contributor | eLog Administrator |
|--------------------------------|-------------|------------------------------|------------------------------|
| General Recommendation | View | View, Create, Update, Delete | View, Create, Update, Delete |
| Relationship Families | | | |
| Action Is Assigned To | View | View, Create, Update, Delete | View, Create, Update, Delete |
| Asset Is Risk Increased | View | View, Create, Update, Delete | View, Create, Update, Delete |
| Asset Is Safety Bypassed | View | View, Create, Update, Delete | View, Create, Update, Delete |
| Asset Has Log Entries | View | View, Create, Update, Delete | View, Create, Update, Delete |
| Asset Has Shifts | View | View, Create, Update, Delete | View, Create, Update, Delete |
| Has Recommendations | View | View, Create, Update, Delete | View, Create, Update, Delete |
| Has Reference Documents | View | View, Create, Update, Delete | View, Create, Update, Delete |
| Has Shift Transition Arriving | View | View, Create, Update, Delete | View, Create, Update, Delete |
| Has Shift Transition Departing | View | View, Create, Update, Delete | View, Create, Update, Delete |
| Log Entry Has Human Resources | View | View, Create, Update, Delete | View, Create, Update, Delete |
| Log Has Events | View | View, Create, Update, Delete | View, Create, Update, Delete |
| Shift Has Log Entries | View | View, Create, Update, Delete | View, Create, Update, Delete |


Deploy Failure Modes and Effects Analysis (FMEA)

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

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

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

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

Upgrade or Update Failure Modes and Effects Analysis (FMEA) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

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

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital 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 V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

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

Failure Modes and Effects Analysis (FMEA) Security Groups and Roles

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


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


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

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


| Family 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 |

| Family Caption | MI RCM User | MI RCM Viewer |
|-------------------------|------------------------------|---------------|
| 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 |

| Family Caption | MI RCM User | MI RCM Viewer |
|---|------------------------------|---------------|
| Risk Rank | View, Update, Insert, Delete | View |
| Risk Threshold | View | View |
| Site Reference | View | View |
| Task History | View, Update, Insert, Delete | View |
| <div style="border: 1px solid yellow; padding: 5px;">  Note: The Task History relationship family is inactive in the baseline GE Digital 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 |
| 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 |

| Family Caption | MI RCM User | MI RCM Viewer |
|---|------------------------------|---------------|
| 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 |
| <div style="border: 1px solid yellow; padding: 5px;">  Note: The Has Task History relationship family is inactive in the baseline GE Digital APM database. </div> | | |
| Has Tasks | View, Update, Insert, Delete | View |
| Has Templates | View, Update, Insert, Delete | View |
| Is Based on RCM FMEA Failure Effect | View | View |
| Is RCM FMEA Asset | View, Update, Insert, Delete | View |

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

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

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


Deploy GE Analytics

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

Deploy GE Analytics for the First Time

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

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

 **Note:** This GE Digital APM module is not available in the APM Now environment.

| Step | Task | Notes |
|------|--|--|
| 1 | Assign Security Users to one or more of the GE Analytics Security Groups and Roles . | This step is required. |
| 2 | Modify the file Meridium.AMQP.Service.exe.config to configure the RabbitMQ connection. | This step is required. |
| 3 | Restart the AMQP Service. | This step is required. |
| 4 | Install GE System 1 Integration Service . | This step is required. |
| 5 | Create and configure the GE Connection record to connect to the GE Message Broker Server. | This step is required. |
| 6 | Modify the file Meridium.GE.Service.exe.config to configure the GE Service. | This step is required. |
| 7 | Configure the GE Service to restart automatically. | This step is required. |
| 8 | Start the GE Service. | This step is required. Once the GE Service is started, the GE Enterprise hierarchy will import automatically into the GE Digital APM database. |
| 9 | Configure GE Enterprise and Filter records . | This step is required. These records are created automatically by the GE Service. |
| 10 | Stop and then start the GE Service. | This step is required. |

| Step | Task | Notes |
|------|---|--|
| 11 | Link tags to assets (i.e., equipment and functional locations). | This step is required. You must repeat this step for any GE Tags records that are imported from your GE system. New tags are imported automatically. |
| 12 | Import the GE Analytics policies. | This step is required only if you want to use GE policies. |

Upgrade or Update GE Analytics to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

| Step | Task | Notes |
|------|--|------------------------|
| 1 | Ensure that your version of Enterprise Impact is supported according to the GE Analytics system requirements . | This step is required. |
| 2 | Modify the file Meridium.GE.Service.exe.config . | This step is required. |
| 3 | On the Enterprise Impact Message Server, restart Meridium.GE.Service. | This step is required. |
| 4 | Modify the file Meridium.AMQP.Service.exe.config . | This step is required. |
| 5 | On the GE Digital APM Server, restart Meridium.AMQP.Service. | This step is required. |

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

| Step | Task | Notes |
|------|--|------------------------|
| 1 | Ensure that your version of Enterprise Impact is supported according to the GE Analytics system requirements . | This step is required. |
| 2 | Modify the file Meridium.GE.Service.exe.config . | This step is required. |
| 3 | On the GE Fleet Message Server, restart Meridium.GE.Service. | This step is required. |
| 4 | Modify the file Meridium.AMQP.Service.exe.config . | This step is required. |
| 5 | On the GE Digital APM Server, restart Meridium.AMQP.Service. | This step is required. |

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

The GE Analytics module was introduced in Meridium V4.2.0.0. To utilize GE Analytics in V4.3.0.2.0, follow the [GE Analytics First-Time Deployment Workflow](#).

Upgrade from any version V4.0.0.0 through V4.0.1.0

The GE Analytics module was introduced in Meridium V4.2.0.0. To utilize GE Analytics in V4.3.0.2.0, follow the [GE Analytics First-Time Deployment Workflow](#).

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

| Step | Task | Notes |
|------|---|---|
| 1 | Ensure that your version of Enterprise Impact is supported by the GE Analytics module . | This step is required. |
| 2 | Modify the file Meridium.GE.Service.exe.config . | This step is required. |
| 3 | Modify the file Meridium.AMQP.Service.exe.config . | This step is required. |
| 4 | Run the following update query: UPDATE [MI_GETAG] SET [MI_GETAG].[MI_TAG_SYSTEM_ID_C] = [MI_GEENT].[MI_GEENT_ID_C]. | This step is required only if you want to use the Asset and Tag Data Loader to create relationships between GE tags and assets. |

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

| Step | Task | Notes |
|------|---|---|
| 1 | Ensure that your version of Enterprise Impact is supported by the GE Analytics module . | This step is required. |
| 2 | Modify the file Meridium.GE.Service.exe.config . | This step is required. |
| 3 | Modify the file Meridium.AMQP.Service.exe.config . | This step is required. |
| 4 | Run the following update query: UPDATE [MI_GETAG] SET [MI_GETAG].[MI_TAG_SYSTEM_ID_C] = [MI_GEENT].[MI_GEENT_ID_C]. | This step is required only if you want to use the Asset and Tag Data Loader to create relationships between GE tags and assets. |

Upgrade from any version V3.5.1 through V3.5.1.12.1

GE System 1 Integration was introduced in Meridium APM V3.6.0.6.0. To utilize GE Analytics in V4.3.0.2.0, follow the [GE Analytics First-Time Deployment Workflow](#).

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

GE System 1 Integration was introduced in Meridium APM V3.6.0.6.0. To utilize GE Analytics in V4.3.0.2.0, follow the [GE Analytics First-Time Deployment Workflow](#).

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

GE System 1 Integration was introduced in Meridium APM V3.6.0.6.0. To utilize GE Analytics in V4.3.0.2.0, follow the [GE Analytics First-Time Deployment Workflow](#).


Upgrade from any version V3.4.5 through V3.4.5.0.1.4

GE System 1 Integration was introduced in Meridium APM V3.6.0.6.0. To utilize GE Analytics in V4.3.0.2.0, follow the [GE Analytics First-Time Deployment Workflow](#).

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

Steps

1. On your GE Digital APM Server, navigate to the folder where the **Meridium.AMQP.service.exe.config** is installed. If you installed the software in the default location, you can locate this file in the following location: **C:\Program Files\Meridium\Services**.
2. Open the file **Meridium.AMQP.service.exe.config** in an application that you can use to modify XML script (e.g., Notepad).
3. Within the <apmMqConnections> tags, uncomment the example connection tag by deleting <!--EXAMPLE: and the corresponding --> from the beginning and end of the string.
4. Within the <apmMqConnections> tags, configure the attributes, by replacing the values within the quotation marks with the values detailed in the following chart.

 **Note:** The heartbeat attributes should not be edited.

| Attribute | Replace text... | ... with the following values: | Notes |
|------------|-----------------------|---|--|
| server key | KEY | A unique connection key. | If there are multiple server entries containing the same key in the configuration file, the last defined server entry is used and all others with the same key are removed when the service starts. |
| host | ENTER_BROKER_HOSTNAME | The host name of the GE Fleet Message Broker. | If there are multiple server entries containing the same host name in the configuration file, the last defined server entry is used and the other host names with the same key will be logged as errors in the service log file. |

| Attribute | Replace text... | ... with the following values: | Notes |
|-----------|--------------------|---|---|
| port | 5672 | <p>The appropriate port for your configuration.</p> <ul style="list-style-type: none"> The default SSL port is 5671. The default HTTP port is 5672, and is the port preconfigured in the config file. | None |
| user | ENTER_MQ_USER_NAME | The user name for the RabbitMQ Message Broker. | This field is not required if using SSL to connect to the message broker. |
| password | ENTER_MQ_PASSWORD | The password for the RabbitMQ Message Broker. | <p>This field is not required if using SSL to connect to the message broker.</p> <div style="border: 1px solid black; padding: 5px; background-color: #ffffcc;"> <p>Note: Do not delete the ! in front of the password. This symbol is not part of the password itself. Instead, this symbol will cause the password to be encrypted automatically when the service is restarted.</p> </div> |

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

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

| Attribute | Replace text... | ... with the following values: | Notes |
|-------------------|-------------------|--|--|
| sslCertPassPhrase | SSL_CERT_PASSWORD | SSL certificate password. | <div style="border: 1px solid yellow; padding: 5px;"> <p>Note: Do not delete the ! in front of the password. This symbol is not part of the password itself. Instead, this symbol will cause the password to be encrypted automatically when the service is restarted.</p> </div> |
| sslCertPath | PATH_TO_CERT | File path to the directory where the SSL certificate is stored. | The SSL certificate is not supplied by GE Digital It should be obtained from a third-party certificate authority. |
| tlsVersions | 1.2 | <p>The desired encryption algorithm.</p> <ul style="list-style-type: none"> The default value is 1.2. Alternatively, to support multiple algorithms, you can enter multiple values, and then separate the values with a semicolon. | Only tls1.1 and tls1.2 versions are supported. |

6. Save and close the file.

Results

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


What's Next?

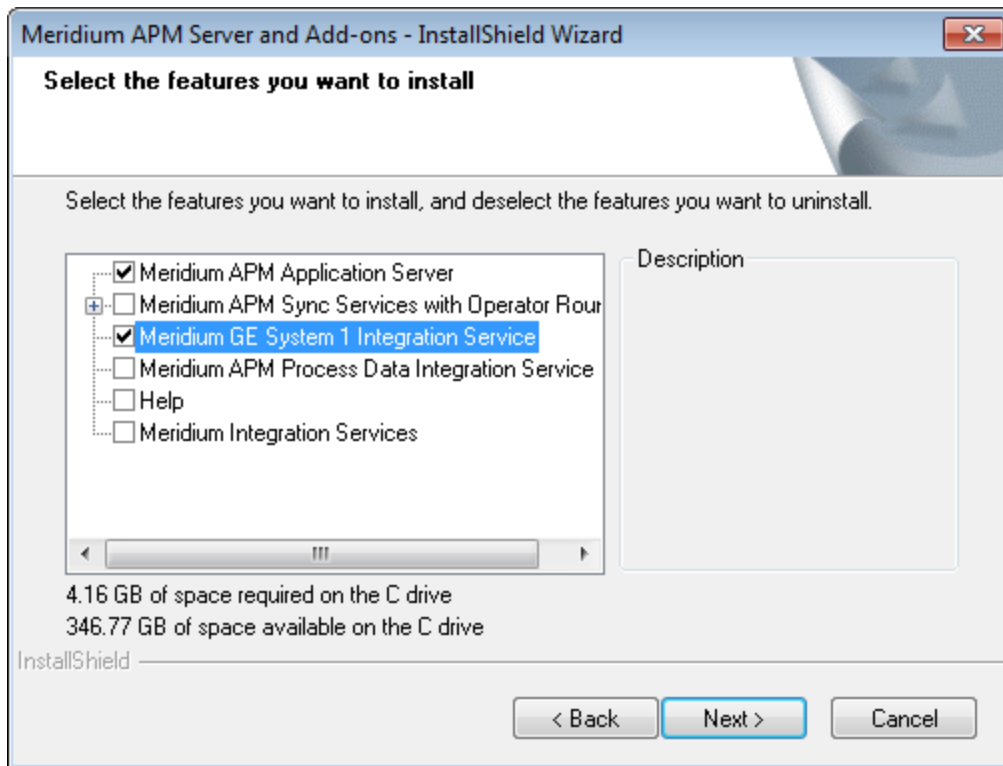
- Return to the [GE First-Time Deployment Workflow](#).

Install the GE System 1 Integration Service

Steps

1. On GE Fleet Message Server, access the GE Digital 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 GE System 1 Integration Service** option.

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



7. Select **Next**.

The **Complete the Installation** screen appears.

8. Select **Install**.

The **Installation is Complete** screen appears.

9. Select **Finish**.

The GE System 1 Integration Service is installed.


What's Next?

- [Modify the File Meridium.GE.Service.exe.config.](#)


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

Steps

1. On the machine on which you are configuring the Meridium GE Service, navigate to the folder where the Meridium GE Service is installed. If you installed the software in the default location, you can locate this file in the following location: **<root:>\Program Files\Meridium\Services**.
2. Open the file **Meridium.GE.Service.exe.config** in an application that you can use to modify XML script (e.g., Notepad).
3. In the file, within the **<configuration>** tags, locate the following text:
`<apmMqConnections>`
4. Within the **<apmMqConnections>** tags, uncomment the example connection tag by deleting **<!--EXAMPLE:** and the corresponding **-->** from the beginning and end of the string.
5. Within the **<apmMqConnections>** tags, configure the attributes, by replacing the values within the quotation marks with the values detailed in the following chart.


 **Note:** The heartbeat attributes should not be edited.

| Attribute | Replace text... | ... with the following values: | Notes |
|------------|-----------------|--------------------------------|---|
| server key | KEY | A unique connection key. | If there are multiple server entries containing the same key in the configuration file, the last defined server entry is used and all others with the same key are removed when the service starts. |

| Attribute | Replace text... | ... with the following values: | Notes |
|-----------|-----------------------|--|---|
| host | ENTER_BROKER_HOSTNAME | The host name of the GE Fleet Message Broker. | If there are multiple server entries containing the same host name in the configuration file, the last defined server entry is used and the other host names with the same key will be logged as errors in the service log file. |
| port | 5672 | The appropriate port for your configuration. <ul style="list-style-type: none"> The default SSL port is 5671. The default HTTP port is 5672, and is the port preconfigured in the config file. | None |
| user | ENTER_MQ_USER_NAME | The user name for the RabbitMQ Message Broker. | This field is not required if using SSL to connect to the message broker. |
| password | ENTER_MQ_PASSWORD | The password for the RabbitMQ Message Broker. | This field is not required if using SSL to connect to the message broker. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> Note: Do not delete the ! in front of the password. This symbol is not part of the password itself. Instead, this symbol will cause the password to be encrypted automatically when the service is restarted.</p> </div> |

6. If you are using SSL configuration, configure the attributes, by replacing the values within


the quotation marks with the values detailed in the following chart.

| Attribute | Replace text... | ... with the following values: | Notes |
|-------------------|-------------------|--|--|
| sslEnabled | FALSE | TRUE | None |
| sslServerName | SSL_SERVER_NAME | The Common Name (CN) where the SSL certificate stored. | Typically, this is the host name of the server to which this client will connect. |
| sslCertPassPhrase | SSL_CERT_PASSWORD | SSL certificate password. |  Note: Do not delete the ! in front of the password. This symbol is not part of the password itself. Instead, this symbol will cause the password to be encrypted automatically when the service is restarted. |
| sslCertPath | PATH_TO_CERT | File path to the directory where the SSL certificate is stored. | The SSL certificate is not supplied by GE Digital It should be obtained from a third-party certificate authority. |
| tlsVersions | 1.2 | <p>The desired encryption algorithm.</p> <ul style="list-style-type: none"> The default value is 1.2. Alternatively, to support multiple algorithms, you can enter multiple values, and then separate the values with a semicolon. | Only tls1.1 and tls1.2 versions are supported. |

7. Within the <meridiumconnections> tags, uncomment the example connection tag by

deleting <!--EXAMPLE: and the corresponding --> from the beginning and end of the string.

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

| Attribute | Replace text... | ... with the following values: | Notes |
|-------------------|------------------|---|--|
| name | NAME | A name to identify the connection to the database. | This value is used only by the configuration file. |
| apmMqKey | KEY | The key of the apmMqConnection to use for this connection. | The key must match at least one of the defined keys in the apmMqConnection section. |
| applicationServer | ENTER_APP_SERVER | The name of the GE Digital APM server. | None |
| datasource | DATA_SOURCE | The name of the GE Digital APM data source to which you want to connect. | The data source value is case sensitive and should be typed exactly as it is defined for the GE Digital APM Server in the Data Sources section of Operations Manager. |
| userId | ENTER_USER | The User ID of the Security User whose credentials should be used to log in to the specified GE Digital APM database. | None |
| password | ENTER_PASS | The password for the specified user. |  Note: Do not delete the ! in front of the password. This symbol is not part of the password itself. Instead, this symbol will cause the password to be encrypted automatically when the service is restarted. |

9. Save and close the file.

Results

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

What's Next?

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

Import the GE Policies

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

Steps

1. Using the Import and Export tool , import the following XML files, one at a time:
 - **GE Event Response.xml**
 - **PLA_Policy.xml**

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

The following policies are now available in GE Digital APM.

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

GE Analytics Security Groups and Roles

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

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

| Security Group | Roles |
|---------------------|-----------------------------------|
| MI GE Administrator | MI Health Admin |
| MI GE User | MI Health User MI Health Power |
| MI GE Viewer | None |

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

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

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

| Family | MI GE Administrator | MI GE User | MI GE Viewer |
|-------------------------|------------------------------|------------------------------|--------------|
| Has Consolidated Events | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has GE Enterprise | View, Update, Insert, Delete | View | View |
| Has GE Filter | View, Update, Insert, Delete | View | View |
| Has Tag | View, Update, Insert, Delete | View | View |
| Has Tag Event | View, Update, Insert, Delete | View | View |


Deploy Generation Availability Analysis (GAA)

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

Deploy Generation Availability Analysis (GAA) for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

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

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

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

Upgrade or Update Generation Availability Analysis (GAA) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.




Upgrade from any version V4.2.0.0 through V4.2.0.9.1




This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.



Migrate from Generation Management (GM) to Generation Availability Analysis (GAA)

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

| Step | Task | Notes |
|------|--|------------------------|
| 1 | <p>Using the file Meridium.DbUtility.GAAUpgradeUtility.exe stored in the installation folder (e.g., C:\Program Files\Meridium\Upgrade), set the following information:</p> <ul style="list-style-type: none">• User ID in the <code>userId</code> field.• Password in the <code>password</code> field.• Database name in the <code>datasourceId</code> field.• Regulatory organization (NERC, CEA) in the <code>fuelReportingOrganization</code> field. | This step is required. |

| Step | Task | Notes |
|------|---|---|
| 2 | <p>In the Generation Company family:</p> <ul style="list-style-type: none"> In the Enterprise 1 Code (MI_GMCOMPNY_ERP_01_CD_C) field, enter the Asset ID. <div data-bbox="412 449 894 541" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p> Note: The Asset ID is the Entity ID of the functional location.</p> </div> <ul style="list-style-type: none"> In the Enterprise 1 Description (MI_GMCOMPNY_ERP_01_DESC_C) field, for the Primary Regulatory Organization, enter the value <i>NERC</i> or <i>CEA</i>. <div data-bbox="412 716 894 873" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p> Note: If the Primary Regulatory Organization information has not been set, an exception error will occur.</p> </div> <ul style="list-style-type: none"> In the Enterprise 3 Code (MI_GMCOMPNY_ERP_03_CD_C) field, enter the Country ID. <div data-bbox="412 1014 894 1140" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p> Note: In GE Digital APM V4.3.0.0.0, the Country field is required.</p> </div> | <p>This step is required.</p> <p>The GAA Company will receive the site key from the associated functional location.</p> |

| Step | Task | Notes |
|------|---|---|
| 3 | <p>In the Generation Plant family:</p> <ul style="list-style-type: none"> In the Enterprise 1 Code (MI_GM_PLANT_ERP_01_CD_C) field, enter the Asset ID. <div data-bbox="412 449 894 541" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p> Note: The Asset ID is the Entity ID of the functional location.</p> </div> <ul style="list-style-type: none"> In the Enterprise 1 Description (MI_GM_PLANT_ERP_01_DESC_C) field, for the Primary Regulatory Organization, enter the value <i>NERC</i> or <i>CEA</i>. <div data-bbox="412 716 894 873" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p> Note: If the Primary Regulatory Organization information has not been set, an exception error will occur.</p> </div> <ul style="list-style-type: none"> In the Enterprise 4 Code (MI_GM_PLANT_ERP_04_CD_C) field, enter the time zone for the Plant. <div data-bbox="412 1014 894 1136" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p> Note: If the time zone information is invalid, an exception error will occur.</p> </div> | <p>This step is required.</p> <p>The GAA Plant will receive the site key from the associated functional location.</p> |

| Step | Task | Notes | | | | | | | | | | |
|----------------------------------|--|---|----------------------------------|--------------------------------|------------------------|----------------------------------|----------------------|--------------------------------|---------------------------|-------------------------------------|-------------------------|-----------------------------------|
| 4 | <p>In the Generation Unit family:</p> <ul style="list-style-type: none"> In the Enterprise 1 Code (MI_GM_UNIT0_ERP_01_CD_C) field, enter the Asset ID. <div data-bbox="412 810 896 903" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p> Note: The Asset ID is the Entity ID of the functional location.</p> </div> <ul style="list-style-type: none"> In the Enterprise 1 Description (MI_GM_UNIT0_ERP_01_DESC_C) field, for the Primary Regulatory Organization, enter the value <i>NERC</i> or <i>CEA</i>. <div data-bbox="412 1075 896 1234" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p> Note: If the Primary Regulatory Organization information has not been set, an exception error will occur.</p> </div> | <p>This step is required.</p> <p>The GAA Unit will receive the site key from the associated functional location.</p> <p>The Primary Event and the Contributing Event will receive the site key from the GAA Unit.</p> <p>The values in the Generation Unit records will be mapped to the corresponding fields in Unit Capacity records as shown in the following table:</p> <table border="1" data-bbox="922 768 1398 1402"> <thead> <tr> <th data-bbox="922 768 1138 898">Fields in Generation Unit record</th> <th data-bbox="1138 768 1398 898">Fields in Unit Capacity record</th> </tr> </thead> <tbody> <tr> <td data-bbox="922 898 1138 1026">Gross Maximum Capacity</td> <td data-bbox="1138 898 1398 1026">Nameplate Gross Maximum Capacity</td> </tr> <tr> <td data-bbox="922 1026 1138 1155">Net Maximum Capacity</td> <td data-bbox="1138 1026 1398 1155">Nameplate Net Maximum Capacity</td> </tr> <tr> <td data-bbox="922 1155 1138 1283">Gross Dependable Capacity</td> <td data-bbox="1138 1155 1398 1283">Nameplate Gross Dependable Capacity</td> </tr> <tr> <td data-bbox="922 1283 1138 1402">Net Dependable Capacity</td> <td data-bbox="1138 1283 1398 1402">Nameplate Net Dependable Capacity</td> </tr> </tbody> </table> <p>By default, the Unit Capacity record will be created for all the units with the value in Start Date field set to 01/01/1900 and the value in End Date field set to null.</p> | Fields in Generation Unit record | Fields in Unit Capacity record | Gross Maximum Capacity | Nameplate Gross Maximum Capacity | Net Maximum Capacity | Nameplate Net Maximum Capacity | Gross Dependable Capacity | Nameplate Gross Dependable Capacity | Net Dependable Capacity | Nameplate Net Dependable Capacity |
| Fields in Generation Unit record | Fields in Unit Capacity record | | | | | | | | | | | |
| Gross Maximum Capacity | Nameplate Gross Maximum Capacity | | | | | | | | | | | |
| Net Maximum Capacity | Nameplate Net Maximum Capacity | | | | | | | | | | | |
| Gross Dependable Capacity | Nameplate Gross Dependable Capacity | | | | | | | | | | | |
| Net Dependable Capacity | Nameplate Net Dependable Capacity | | | | | | | | | | | |

| Step | Task | Notes |
|------|--|---|
| 5 | <div data-bbox="331 663 894 789" style="border: 1px solid red; padding: 5px; margin-bottom: 10px;"> <p>⚠ IMPORTANT: R server must be configured and running before you run the GAAUpgradeUtility.exe.</p> </div> <p>Run the file GAAUpgradeUtility.exe.</p> | <p>This step is required.</p> <p>During the upgrade:</p> <ul style="list-style-type: none"> • The states in the Incident Reporting Status field for Primary Events and the states in the Reporting Status field for Performance records <u>will be updated to the new State Management.</u> • <u>The queries in V3.6.0.0.0 will be replaced by the queries in V4.3.0.0.0.</u> • The Is Default field will be set to <i>True</i> for all records in the <u>GAA Configuration family.</u> • <u>The upgrade will map the existing fields in the Events and Performance data to the fields in the new families.</u> • The Event Details for all the Units will be generated. <p>After you complete this step, a log file is generated containing detailed information about the upgrade process.</p> |

Query Mapping

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

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

State Management Mapping

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

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

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

Field Mappings

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

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

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

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

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|---|--|
| Primary Fuel BTUs Total (MI_GMCAPHST_PRI_FUEL_BTUS_N) | Fuel BTUs - Total (MI_PERF_FUEL_BTUS_TOTA_N) |
| Primary Fuel Code (MI_GMCAPHST_PRI_FUEL_CODE_C) | Fuel Code (MI_PERF_FUEL_FUEL_CODE_C) |
| Primary Grindability Index (MI_GMCAPHST_PRI_GRIND_INDEX_N) | Grindability Index (MI_PERF_FUEL_GRIN_INDE_NBR) |
| Primary Percent Alkalines (MI_GMCAPHST_PRI_PERCE_ALKAL_N) | Percent Alkalines (MI_PERF_FUEL_PERC_ALKA_N) |
| Primary Percent Ash (MI_GMCAPHST_PRI_PERCE_ASH_N) | Percent Ash (MI_PERF_FUEL_PERC_ASH_N) |
| Primary Percent Moisture (MI_GMCAPHST_PRI_PERCE_MOIST_N) | Percent Moisture (MI_PERF_FUEL_PERC_MOIS_N) |
| Primary Percent Sulfur (MI_GMCAPHST_PRI_PERCE_SULFU_N) | Percent Sulfur (MI_PERF_FUEL_PERC_SULF_N) |
| Primary Quantity Burned (MI_GMCAPHST_PRI_QUANT_BURNE_N) | Quantity Burned (MI_PERF_FUEL_QUAN_BURN_N) |
| Primary Quantity Burned Unit of Measure (MI_GMCAPHST_PRIM_BURN_UOM_C) | Quantity Burned Unit of Measure (MI_PERF_FUEL_QTY_BRN_UNITMES_C) |
| Secondary Ash Softening Temp (MI_GMCAPHST_SEC_ASH_SOFTE_TE_N) | Ash Softening Temperature (MI_PERF_FUEL_ASH_SOFT_TEMP_N) |
| Secondary Average Heat Content (MI_GMCAPHST_SEC_AVG_HEAT_N) | Average Heat Content (MI_PERF_FUEL_AVER_HEAT_CONT_N) |
| Secondary Fuel Code (MI_GMCAPHST_SEC_FUEL_CODE_C) | Fuel Code (MI_PERF_FUEL_FUEL_CODE_C) |
| Secondary Grindability Index (MI_GMCAPHST_SEC_GRIND_INDEX_N) | Grindability Index (MI_PERF_FUEL_GRIN_INDE_NBR) |
| Secondary Percent Alkalines (MI_GMCAPHST_SEC_PERCE_ALKAL_N) | Percent Alkalines (MI_PERF_FUEL_PERC_ALKA_N) |
| Secondary Percent Ash (MI_GMCAPHST_SEC_PERCE_ASH_N) | Percent Ash (MI_PERF_FUEL_PERC_ASH_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|--|---|
| Secondary Percent Moisture (MI_GMCAPHST_SEC_PERCE_MOIST_N) | Percent Moisture (MI_PERF_FUEL_PERC_MOIS_N) |
| Secondary Percent Sulfur (MI_GMCAPHST_SEC_PERCE_SULFU_N) | Percent Sulfur (MI_PERF_FUEL_PERC_SULF_N) |
| Secondary Quantity Burned (MI_GMCAPHST_SEC_QUANT_BURNE_N) | Quantity Burned (MI_PERF_FUEL_QUAN_BURN_N) |
| Secondary Quantity Burned Unit of Measure (MI_GMCAPHST_SECND_BURN_UOM_C) | Quantity Burned Unit of Measure (MI_PERF_FUEL_QTY_BRN_UNITMES_C) |
| Sum of Fuel BTUs (MI_GMCAPHST_SUM_OF_FUEL_BTUS_N) | Sum of Fuel BTUs (MI_PERF_FUEL_SUM_OF_BTUS_N) |
| Capacity History (Net) | GAA Performance Indexes |
| Capacity Factor (N) (MI_GMCAPHST_N_CAPAC_FAC_N) | Capacity Factor (MI_PERF_INDX_CAPA_FACT_N) |
| D1 Eqv Upl Derate Hrs (N) (MI_GMCAPHST_D1_HRS_N) | D1 Equivalent Unplanned Derate Hours (MI_PERF_INDX_D1_EQ_UPL_DR_HR_N) |
| D1 Eqv Upl Derate MWh (N) (MI_GMCAPHST_D1_EQV_UPL_DRT_N) | D1 Equivalent Unplanned Derate MWh (MI_PERF_INDX_D1_EQ_UPL_DR_MW_N) |
| D2 Eqv Upl Derate Hrs (N) (MI_GMCAPHST_D2_HRS_N) | D2 Equivalent Unplanned Derate Hours (MI_PERF_INDX_D2_EQ_UPL_DR_HR_N) |
| D2 Eqv Upl Derate MWh (N) (MI_GMCAPHST_D2_EQV_UPL_DRT_N) | D2 Equivalent Unplanned Derate MWh (MI_PERF_INDX_D2_EQ_UPL_DR_MW_N) |
| D3 Eqv Upl Derate Hrs (N) (MI_GMCAPHST_D3_HRS_N) | D3 Equivalent Unplanned Derate Hours (MI_PERF_INDX_D3_EQ_UPL_DR_HR_N) |
| D3 Eqv Upl Derate MWh (N) (MI_GMCAPHST_D3_EQV_UPL_DRT_C) | D3 Equivalent Unplanned Derate MWh (MI_PERF_INDX_D3_EQ_UPL_DR_MW_N) |
| D4 Eqv Maint Derate Hrs (N) (MI_GMCAPHST_MNT_DRT_HRS_D4_N) | D4 Equivalent Maintenance Derating Hours (MI_PERF_INDX_D4_EQ_MN_DR_HRS_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|---|--|
| D4 Eqv Maint Derate MWh (N) (MI_GMCAPHST_D4_EQV_MNT_DRT_N) | D4 Equivalent Maintenance Derate MWH (MI_PERF_INDX_D4_EQ_MN_DR_MW_N) |
| Eqv Avail Factor (N) (MI_GMCAPHST_EQV_AVAIL_FAC_NE_N) | Equivalent Availability Factor (MI_PERF_INDX_EQ_AVAI_FACT_N) |
| Eqv Derate Ext (N) (MI_GMCAPHST_EQV_DRT_EXT_N_N) | Equivalent Derate Extension (MI_PERF_INDX_EQ_DR_EXT_N) |
| Eqv Forced Derate Hrs (N) (MI_GMCAPHST_FORCE_DRT_HRS_D1_N) | Equivalent Forced Derated Hours (MI_PERF_INDX_EQ_FORC_DR_HRS_N) |
| Eqv Forced Outage Factor (N) (MI_GMCAPHST_EQV_FRC_OU_FAC_N_N) | Equivalent Forced Outage Factor (MI_PERF_INDX_EQ_FORC_OUT_FAC_N) |
| Eqv Forced Outage Rate (N) (MI_GMCAPHST_EQV_FRC_OUT_RA_N_N) | Equivalent Forced Outage Rate (MI_PERF_INDX_EQ_FOR_OUT_RATE_N) |
| Eqv Forced Outage Rate Dmd (N) (MI_GMCAPHST_EQV_FRC_ORT_DE_N_N) | Equivalent Forced Outage Rate Demand (MI_PERF_INDX_EQ_FOR_OT_RTDEM_N) |
| Eqv Maint Derate Hrs (N) (MI_GMCAPHST_EMDH_N_N) | Equivalent Maintenance Derated Hours (MI_PERF_INDX_EQ_MN_DR_HRS_N) |
| Eqv Maint Derate Hrs RS (N) (MI_GMCAPHST_EMDHRS_HRS_N_N) | Equivalent Maintenance Derated Hours During Reserve Shutdown (MI_PERF_INDX_EQ_MN_DR_HR_RS_N) |
| Eqv Maint Outage Factor (N) (MI_GMCAPHST_EQV_MN_OU_FAC_N_N) | Equivalent Maintenance Outage Factor (MI_PERF_INDX_EQ_MN_OUT_FAC_N) |
| Eqv Maintenance Outage Rate (N) (MI_GMCAPHST_EQV_MN_OU_RA_N_N) | Equivalent Maintenance Outage Rate (MI_PERF_INDX_EQ_MN_OUT_RAT_N) |
| Eqv Planned Derate Hrs (N) (MI_GMCAPHST_PL_DRT_HRS_PD_N) | Equivalent Planned Derated Hours (MI_PERF_INDX_EQ_PLN_DR_HRS_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|--|--|
| Eqv Planned Derate Hrs RS (N) (MI_GMCAPHST_EPDHRS_HRS_N_N) | Equivalent Planned Derated Hours During Reserve Shutdown (MI_PERF_INDX_EQ_PL_DR_HR_RS_N) |
| Eqv Planned Derate MWh (N) (MI_GMCAPHST_PD_EQV_PL_DRT_M_N) | Equivalent Planned Derate MWH (MI_PERF_INDX_EQ_PLN_DR_MWH_N) |
| Eqv Planned Outage Factor (N) (MI_GMCAPHST_EQV_PL_OU_FAC_N_N) | Equivalent Planned Outage Factor (MI_PERF_INDX_EQ_PLN_OUT_FAC_N) |
| Eqv Planned Outage Rate (N) (MI_GMCAPHST_EQV_PLAN_OU_RA_N_N) | Equivalent Planned Outage Rate (MI_PERF_INDX_EQ_PLN_OUT_RATE_N) |
| Eqv Sched Derate Hrs (N) (MI_GMCAPHST_ESDH_N_N) | Equivalent Scheduled Derated Hours (MI_PERF_INDX_EQ_SCH_DR_HRS_N) |
| Eqv Sched Outage Factor (N) (MI_GMCAPHST_EQV_SCH_OU_FAC_N_N) | Equivalent Scheduled Outage Factor (MI_PERF_INDX_EQ_SCH_OUT_FAC_N) |
| Eqv Sched Outage Factor (N) (MI_GMCAPHST_EQV_SEA_DRT_HO_N_N) | Equivalent Seasonal Derated Hours (MI_PERF_INDX_EQ_SEAS_DR_HRS_N) |
| Eqv Seasonal Derate MWh (N) (MI_GMCAPHST_EQV_SEA_DRT_MW_N_N) | Equivalent Seasonal Derate MWH (MI_PERF_INDX_EQ_SEAS_DR_MWH_N) |
| Eqv Unavail Factor (N) (MI_GMCAPHST_EQV_UNAV_FAC_NE_N) | Equivalent Unavailability Factor (MI_PERF_INDX_EQ_UNAV_FAC_N) |
| Eqv Unplanned Outage Rate (N) (MI_GMCAPHST_EQV_UNPL_OU_RA_N_N) | Equivalent Unplanned Outage Rate (MI_PERF_INDX_EQ_UNPL_OUT_RAT_N) |
| Eqv Upl Derate Hrs (N) (MI_GMCAPHST_EUDH_N) | Equivalent Unplanned Derated Hours (MI_PERF_INDX_EQ_UNPL_DR_HRS_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|---|---|
| Eqv Upl Derate Hrs RS (N) (MI_GMCAPHST_EUDHRS_HRS_N_N) | Equivalent Unplanned Derated Hours During Reserve Shutdown (MI_PERF_INDX_EQ_UNPL_DR_HR_S_N) |
| Eqv Upl Frcd Derate Hrs RS (N) (MI_GMCAPHST_EUFDH_HRS_N_N) | Equivalent Unplanned Forced Derate Hours (MI_PERF_INDX_EQ_UPLFRC_DR_HR_N) |
| Eqv Upl Frcd Derate MWh RS (N) (MI_GMCAPHST_EUFDH_MWH_N_N) | Equivalent Unplanned Forced Derate MWH (MI_PERF_INDX_EQ_UPLFRC_DR_MW_N) |
| Eqv Uplanned Outage Factor (N) (MI_GMCAPHST_EQV_UPL_OU_FAC_N_N) | Equivalent Unplanned Outage Factor (MI_PERF_INDX_EQ_UNPL_OUT_FAC_N) |
| Ext Maint Derate Eqv Hrs (N) (MI_GMCAPHST_EXT_MNT_DRTEQVHR_N) | Extension of Maintenance Derating Equivalent Hours (MI_PERF_INDX_EXT_MN_DR_EQ_HR_N) |
| Ext Maint Derate Eqv MWh (N) (MI_GMCAPHST_EXT_OF_MNT_D_MW_N) | Extended Maintenance Derate Equivalent MWH (MI_PERF_INDX_EXT_MN_DR_EQ_MW_N) |
| Ext Pln Derate Eqv Hrs (N) (MI_GMCAPHST_EXT_PL_DRT_EQV_H_N) | Extension of Planned Derating Equivalent Hours (MI_PERF_INDX_EXT_PL_DR_EQ_HR_N) |
| Ext Pln Derate Eqv MWh (N) (MI_GMCAPHST_EXT_PL_DRT_EQU_N) | Extended Planned Derate Equivalent MWH (MI_PERF_INDX_EXT_PL_DR_EQ_MW_N) |
| Forced Outage MWh (N) (MI_GMCAPHST_FORCE_OUT_MWH_N) | Forced Outage MWH (MI_PERF_INDX_FORC_OUT_MWH_N) |
| Maint Outage MWh (N) (MI_GMCAPHST_MNT_OUT_MWH_N) | Maintenance Outage MWH (MI_PERF_INDX_MAIN_OUT_MWH_N) |
| Maint Outage Sched Ext MWh (N) (MI_GMCAPHST_MNT_OUT_SCHD_EXT_N) | Maintenance Outage Scheduled Extension MWH (MI_PERF_INDX_MN_OT_SCHEXT_MW_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|---|---|
| Maint and Ext Outage MWh (N) (MI_GMCAPHST_MNT_EXT_OUTMWH_N) | Maintenance and Extension Outage MWH (MI_PERF_INDX_MN_ND_EXT_OT_MW_N) |
| NonCurtailing Event MWh (N) (MI_GMCAPHST_NC_NONCU_EVT_MWH_N) | Non Curtailing Event MWH (MI_PERF_INDX_NON_CURT_EVT_MW_N) |
| Output Factor (N) (MI_GMCAPHST_N_OUTPU_FAC_N) | Output Factor (N) (MI_GAA_PERF_OUTPUT_FACT_NET_N) |
| Planned Outage MWh (N) (MI_GMCAPHST_PL_OUT_MWH_N) | Planned Outage MWH (MI_PERF_INDX_PLN_OUT_MW_N) |
| Planned and Ext Outage MWh (N) (MI_GMCAPHST_PL_EXT_OUTMWH_N) | Planned and Extension Outage MWH (MI_PERF_INDX_PLN_EXT_OT_MW_N) |
| Pln Outage Sched Ext MWh (N) (MI_GMCAPHST_PLN_OUT_SCHD_EXT_N) | Planned Outage Scheduled Extension MWH (MI_PERF_INDX_PL_OT_SC_EXT_MW_N) |
| Reserve Shutdown MWh (N) (MI_GMCAPHST_RESER_SHUTD_MWH_N) | Reserve Shutdown MWH (MI_PERF_INDX_RSRV_SHUT_MW_N) |
| Seasonal Derate Factor (N) (MI_GMCAPHST_SEA_DRT_FAC_NE_N) | Seasonal Derating Factor (MI_PERF_INDX_SEAS_DR_FAC_N) |
| Startup Failure MWh (N) (MI_GMCAPHST_SF_STRT_FAIL_MWH_N) | Startup Failure MWH (MI_PERF_INDX_STAR_FAIL_MW_N) |
| Total Eqv Derate Hrs (N) (MI_GMCAPHST_TOTAL_DRT_HRS_N) | Total Equivalent Derate Hours (MI_PERF_INDX_TOTA_EQ_DR_HR_N) |
| Total Eqv Derate MWh (N) (MI_GMCAPHST_TOTAL_EQV_DRT_MW_N) | Total Equivalent Derate MWH (MI_PERF_INDX_TOTA_EQ_DR_MW_N) |
| U1 Unplanned Outage MWh (N) (MI_GMCAPHST_U1_UPL_OUT_MWH_N) | U1 Unplanned Outage MWH (MI_PERF_INDX_U1_UNPL_OUT_MW_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|--|---|
| U2 Unplanned Outage MWh (N) (MI_GMCAPHST_U2_UPL_OUT_MWH_N) | U2 Unplanned Outage MWH (MI_PERF_INDX_U2_UNPL_OUT_MW_N) |
| U3 Unplanned Outage MWh (N) (MI_GMCAPHST_U3_UPL_OUT_MWH_N) | U3 Unplanned Outage MWH (MI_PERF_INDX_U3_UNPL_OUT_MW_N) |
| Unit Derating Factor (N) (MI_GMCAPHST_UNIT_DRT_FAC_NE_N) | Unit Derating Factor (MI_PERF_INDX_UNIT_DR_FAC_N) |
| Weightage Type | Weightage Type (MI_PERF_INDX_WEIG_TYPE_C) |
| Performance Summary Key | Performance Summary Key (MI_PERF_INDX_PERF_SUMM_KEY_N) |
| Capacity History (Gross) | GAA Performance Indexes |
| Capacity Factor (G) (MI_GMCAPHST_G_CAPAC_FAC_N) | Capacity Factor (MI_PERF_INDX_CAPA_FACT_N) |
| D1 Eqv Upl Derate Hrs (G) (MI_GMCAPHST_D1_EQV_UPL_G_DRT_N) | D1 Equivalent Unplanned Derate Hours (MI_PERF_INDX_D1_EQ_UPL_DR_HR_N) |
| D1 Eqv Upl Derate MWh (G) (MI_GMCAPHST_D1_EQV_UPL_DRTG_N) | D1 Equivalent Unplanned Derate MWH (MI_PERF_INDX_D1_EQ_UPL_DR_MW_N) |
| D2 Eqv Upl Derate Hrs (G) (MI_GMCAPHST_D2_EQV_UPL_G_DRT_N) | D2 Equivalent Unplanned Derate Hours (MI_PERF_INDX_D2_EQ_UPL_DR_HR_N) |
| D2 Eqv Upl Derate MWh (G) (MI_GMCAPHST_D2_EQV_UPL_DRTG_N) | D2 Equivalent Unplanned Derate MWH (MI_PERF_INDX_D2_EQ_UPL_DR_MW_N) |
| D3 Eqv Upl Derate Hrs (G) (MI_GMCAPHST_D3_EQV_UPL_G_DRT_N) | D3 Equivalent Unplanned Derate Hours (MI_PERF_INDX_D3_EQ_UPL_DR_HR_N) |
| D3 Eqv Upl Derate MWh (G) (MI_GMCAPHST_D3_EQV_UPL_DRTG_N) | D3 Equivalent Unplanned Derate MWH (MI_PERF_INDX_D3_EQ_UPL_DR_MW_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|---|---|
| D4 Eqv Maint Derate Hrs (G) (MI_GMCAPHST_D4_EQV_MNT_G_DRT_N) | D4 Equivalent Maintenance Derating Hours (MI_PERF_INDX_D4_EQ_MN_DR_HRS_N) |
| D4 Eqv Maint Derate MWh (G) (MI_GMCAPHST_D4_EQV_MNT_DRTG_N) | D4 Equivalent Maintenance Derate MWH (MI_PERF_INDX_D4_EQ_MN_DR_MW_N) |
| Eqv Avail Factor (G) (MI_GMCAPHST_EQV_AVAIL_FAC_N) | Equivalent Availability Factor (MI_PERF_INDX_EQ_AVAI_FACT_N) |
| Eqv Derate Ext (G) (MI_GMCAPHST_EQV_DRT_EXT_G_N) | Equivalent Derate Extension (MI_PERF_INDX_EQ_DR_EXT_N) |
| Eqv Forced Derate Hrs (G) (MI_GMCAPHST_FRC_DRT_HRS_D1_G_N) | Equivalent Forced Derated Hours (MI_PERF_INDX_EQ_FORC_DR_HRS_N) |
| Eqv Forced Outage Factor (G) (MI_GMCAPHST_EQV_FRC_OU_FAC_G_N) | Equivalent Forced Outage Factor (MI_PERF_INDX_EQ_FORC_OUT_FAC_N) |
| Eqv Forced Outage Rate (G) (MI_GMCAPHST_EQV_FORCE_OUT_N) | Equivalent Forced Outage Rate (MI_PERF_INDX_EQ_FOR_OUT_RATE_N) |
| Eqv Forced Outage Rate Dmd (G) (MI_GMCAPHST_EQV_FRC_ORT_DE_G_N) | Equivalent Forced Outage Rate Demand (MI_PERF_INDX_EQ_FOR_OT_RTDEM_N) |
| Eqv Maint Derate Hrs (G) (MI_GMCAPHST_EMDH_G_N) | Equivalent Maintenance Derated Hours (MI_PERF_INDX_EQ_MN_DR_HRS_N) |
| Eqv Maint Outage Factor (G) (MI_GMCAPHST_EQV_MN_OU_FAC_G_N) | Equivalent Maintenance Outage Factor (MI_PERF_INDX_EQ_MN_OUT_FAC_N) |
| Eqv Maintenance Outage Rate (G) (MI_GMCAPHST_EQV_MN_OU_RA_G_N) | Equivalent Maintenance Outage Rate (MI_PERF_INDX_EQ_MN_OUT_RAT_N) |
| Eqv Planned Derate Hrs (G) (MI_GMCAPHST_PD_EQV_PL_G_DRT_N) | Equivalent Planned Derated Hours (MI_PERF_INDX_EQ_PLN_DR_HRS_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|--|--|
| Eqv Planned Derate Hrs RS (G) (MI_GMCAPHST_EPDHRS_HRS_G_N) | Equivalent Planned Derated Hours During Reserve Shutdown (MI_PERF_INDX_EQ_PL_DR_HR_RS_N) |
| Eqv Planned Derate MWh (G) (MI_GMCAPHST_PD_EQV_PL_DRT_MG_N) | Equivalent Planned Derate MWH (MI_PERF_INDX_EQ_PLN_DR_MWH_N) |
| Eqv Planned Outage Factor (G) (MI_GMCAPHST_EQV_PL_OU_FAC_G_N) | Equivalent Planned Outage Factor (MI_PERF_INDX_EQ_PLN_OUT_FAC_N) |
| Eqv Planned Outage Rate (G) (MI_GMCAPHST_EQV_PLAN_OU_RA_G_N) | Equivalent Planned Outage Rate (MI_PERF_INDX_EQ_PLN_OUT_RATE_N) |
| Eqv Sched Derate Hrs (G) (MI_GMCAPHST_ESDH_G_N) | Equivalent Scheduled Derated Hours (MI_PERF_INDX_EQ_SCH_DR_HRS_N) |
| Eqv Sched Outage Factor (G) (MI_GMCAPHST_EQV_SCH_OU_FAC_G_N) | Equivalent Scheduled Outage Factor (MI_PERF_INDX_EQ_SCH_OUT_FAC_N) |
| Eqv Sched Outage Factor (G) (MI_GMCAPHST_EQV_SCH_OU_FAC_G_N) | Equivalent Seasonal Derated Hours (MI_PERF_INDX_EQ_SEAS_DR_HRS_N) |
| Eqv Seasonal Derate MWh (G) (MI_GMCAPHST_EQV_SESO_DRT_MW_N) | Equivalent Seasonal Derate MWH (MI_PERF_INDX_EQ_SEAS_DR_MWH_N) |
| Eqv Unavail Factor (G) (MI_GMCAPHST_EQV_UNAVA_FAC_N) | Equivalent Unavailability Factor (MI_PERF_INDX_EQ_UNAV_FAC_N) |
| Eqv Unplanned Outage Rate (G) (MI_GMCAPHST_EQV_UNPL_OU_RA_G_N) | Equivalent Unplanned Outage Rate (MI_PERF_INDX_EQ_UNPL_OUT_RAT_N) |
| Eqv Upl Derate Hrs (G) (MI_GMCAPHST_EUDH_G_N) | Equivalent Unplanned Derated Hours (MI_PERF_INDX_EQ_UNPL_DR_HRS_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|---|---|
| Eqv Upl Derate Hrs RS (G) (MI_GMCAPHST_EUDHRS_HRS_G_N) | Equivalent Unplanned Derated Hours During Reserve Shutdown (MI_PERF_INDX_EQ_UNPL_DR_HR_S_N) |
| Eqv Upl Frcd Derate Hrs RS (G) (MI_GMCAPHST_EUFDH_HRS_N) | Equivalent Unplanned Forced Derate Hours (MI_PERF_INDX_EQ_UPLFRC_DR_HR_N) |
| Eqv Upl Frcd Derate MWh RS (G) (MI_GMCAPHST_EUFDH_MWH_N) | Equivalent Unplanned Forced Derate MWH (MI_PERF_INDX_EQ_UPLFRC_DR_MW_N) |
| Eqv Uplanned Outage Factor (G) (MI_GMCAPHST_EQV_UPL_OU_FAC_G_N) | Equivalent Unplanned Outage Factor (MI_PERF_INDX_EQ_UNPL_OUT_FAC_N) |
| Ext Maint Derate Eqv Hrs (G) (MI_GMCAPHST_EXT_MNT_DRT_GEQV_N) | Extension of Maintenance Derating Equivalent Hours (MI_PERF_INDX_EXT_MN_DR_EQ_HR_N) |
| Ext Maint Derate Eqv MWh (G) (MI_GMCAPHST_EXT_OF_MNT_D_MWG_N) | Extended Maintenance Derate Equivalent MWH (MI_PERF_INDX_EXT_MN_DR_EQ_MW_N) |
| Ext Pln Derate Eqv Hrs (G) (MI_GMCAPHST_EXT_PL_DRT_G_N) | Extension of Planned Derating Equivalent Hours (MI_PERF_INDX_EXT_PL_DR_EQ_HR_N) |
| Ext Pln Derate Eqv MWh (G) (MI_GMCAPHST_EXT_PL_DRT_EQUG_N) | Extended Planned Derate Equivalent MWH (MI_PERF_INDX_EXT_PL_DR_EQ_MW_N) |
| Forced Outage MWh (G) (MI_GMCAPHST_FORCE_OUT_MWHG_N) | Forced Outage MWH (MI_PERF_INDX_FORC_OUT_MWH_N) |
| Maint Outage MWh (G) (MI_GMCAPHST_MNT_OUT_MWHG_N) | Maintenance Outage MWH (MI_PERF_INDX_MAIN_OUT_MWH_N) |
| Maint Outage Sched Ext MWh (G) (MI_GMCAPHST_MNT_OUT_SCH_EXTG_N) | Maintenance Outage Scheduled Extension MWH (MI_PERF_INDX_MN_OT_SCHEXT_MW_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|---|---|
| Maint and Ext Outage MWh (G) (MI_GMCAPHST_MNT_EXT_OUTMWHG_N) | Maintenance and Extension Outage MWH (MI_PERF_INDX_MN_ND_EXT_OT_MW_N) |
| NonCurtailing Event MWh (G) (MI_GMCAPHST_NC_NC_EVT_MWHG_N) | Non Curtailing Event MWH (MI_PERF_INDX_NON_CURT_EVT_MW_N) |
| Output Factor (G) (MI_GMCAPHST_G_OUTPU_FAC_N) | Output Factor (G) (MI_GAA_PERF_OUTPUT_FACT_GROS_N) |
| Planned Outage MWh (G) (MI_GMCAPHST_PL_OUT_MWHG_N) | Planned Outage MWH (MI_PERF_INDX_PLN_OUT_MW_N) |
| Planned and Ext Outage MWh (G) (MI_GMCAPHST_PL_EXT_OUTMWHG_N) | Planned and Extension Outage MWH (MI_PERF_INDX_PLN_EXT_OT_MW_N) |
| Pln Outage Sched Ext MWh (G) (MI_GMCAPHST_PLN_OUT_SCH_EXTG_N) | Planned Outage Scheduled Extension MWH (MI_PERF_INDX_PL_OT_SC_EXT_MW_N) |
| Reserve Shutdown MWh (G) (MI_GMCAPHST_RESER_SHUTD_MWHG_N) | Reserve Shutdown MWH (MI_PERF_INDX_RSRV_SHUT_MW_N) |
| Seasonal Derate Factor (G) (MI_GMCAPHST_SEA_DRT_FAC_N) | Seasonal Derating Factor (MI_PERF_INDX_SEAS_DR_FAC_N) |
| Startup Failure MWh (G) (MI_GMCAPHST_SF_STR_FAIL_MWHG_N) | Startup Failure MWH (MI_PERF_INDX_STAR_FAIL_MW_N) |
| Total Eqv Derate Hrs (G) (MI_GMCAPHST_TOTAL_DRT_HRS_G_N) | Total Equivalent Derate Hours (MI_PERF_INDX_TOTA_EQ_DR_HR_N) |
| Total Eqv Derate MWh (G) (MI_GMCAPHST_TOT_EQV_DRT_MWG_N) | Total Equivalent Derate MWH (MI_PERF_INDX_TOTA_EQ_DR_MW_N) |
| U1 Unplanned Outage MWh (G) (MI_GMCAPHST_U1_UPL_OUT_MWHG_N) | U1 Unplanned Outage MWH (MI_PERF_INDX_U1_UNPL_OUT_MW_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|--|---|
| U2 Unplanned Outage MWh (G) (MI_GMCAPHST_U2_UPL_OUT_MWHG_N) | U2 Unplanned Outage MWH (MI_PERF_INDX_U2_UNPL_OUT_MW_N) |
| U3 Unplanned Outage MWh (G) (MI_GMCAPHST_U3_UPL_OUT_MWHG_N) | U3 Unplanned Outage MWH (MI_PERF_INDX_U3_UNPL_OUT_MW_N) |
| Unit Derating Factor (G) (MI_GMCAPHST_UNIT_DRT_FAC_N) | Unit Derating Factor (MI_PERF_INDX_UNIT_DR_FAC_N) |
| Capacity History | GAA Performance Summary |
| Actual Unit Starts (MI_GMCAPHST_ACTUA_UNIT_STRT_N) | Actual Unit Starts (MI_GAA_PERF_ACT_UNIT_STAR_N) |
| Attempted Unit Starts (MI_GMCAPHST_ATTEM_UNIT_STRT_N) | Attempted Unit Starts (MI_GAA_PERF_ATT_UNIT_STAR_N) |
| Availability Factor (MI_GMCAPHST_AVAIL_FAC_N) | Availability Factor (MI_GAA_PERF_AVAI_FACT_N) |
| Available Hrs (MI_GMCAPHST_AVAIL_HRS_N) | Available Hours (MI_GAA_PERF_AVAI_HRS_N) |
| Average Run Time (MI_GMCAPHST_AVER_RUN_TIME_N) | Average Run Time (MI_GAA_PERF_AVG_RUN_TIME_N) |
| Demonstrated Max Capacity (N) (MI_GMCAPHST_DEMON_N_MAXIM_CP_N) | Demonstrated Max Capacity (MI_GAA_PERF_DEMO_MAX_CAPA_N) |
| Ext Sched Outages Hrs (MI_GMCAPHST_EXT_OF_SCHED_OUT_N) | Extension of Scheduled Outage Hours (MI_GAA_PERF_EXT_SCH_OUT_HRS_N) |
| Forced Outage Factor (MI_GMCAPHST_FORCE_OUT_FAC_N) | Forced Outage Factor (MI_GAA_PERF_FORC_OUT_FACT_N) |
| Forced Outage Hrs (MI_GMCAPHST_FORCE_OUT_HRS_N) | Forced Outage Hours (MI_GAA_PERF_FORC_OUT_HRS_N) |
| Forced Outage Rate (MI_GMCAPHST_FORCE_OUT_RATE_N_N) | Forced Outage Rate (MI_GAA_PERF_FORC_OUT_RATE_N) |
| Forced Outage Rate Demand (MI_GMCAPHST_FRC_OUT_RT_DM_N_N) | Forced Outage Rate Demand (MI_GAA_PERF_FORC_OUT_RAT_DEM_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|---|---|
| GADS Unit Code (MI_GMCAPHST_UNIT_CODE_N) | Primary Unit Code (MI_GAA_PERF_PRIM_UNIT_CODE_N) |
| GADS Utility Code (MI_GMCAPHST_UTIL_CODE_N) | Primary Utility Code (MI_GAA_PERF_PRIM_UTIL_CODE_N) |
| Gross Actual Capacity (G) (MI_GMCAPHST_G_ACTUA_CAPAC_N) | Gross Actual Capacity (G) (MI_GAA_PERF_GROSS_ACTU_CAPA_N) |
| Gross Actual Generation (G) (MI_GMCAPHST_G_ACTUA_GENER_N) | Gross Actual Generation (G) (MI_GAA_PERF_GROSS_ACTU_GENE_N) |
| Gross Dependable Capacity (G) (MI_GMCAPHST_G_DEPEN_CAPAC_N) | Gross Dependable Capacity (G) (MI_GAA_PERF_GROSS_DEPE_CAPA_N) |
| Gross Max Capacity (G) (MI_GMCAPHST_G_MAXIM_CAPAC_N) | Gross Maximum Capacity (G) (MI_GAA_PERF_GROSS_MAX_CAPA_N) |
| Inactive Hours (MI_GMCAPHST_INACT_HRS_N) | Inactive Hours (MI_GAA_PERF_INAC_HRS_N) |
| MI_SM_STATE_ENTERED_D (MI_SM_STATE_ENTERED_D) | MI_SM_STATE_ENTERED_D (MI_SM_STATE_ENTERED_D) |
| MI_SM_STATE_ID_C (MI_SM_STATE_ID_C) | MI_SM_STATE_ID_C (MI_SM_STATE_ID_C) |
| MI_SM_STATE_KEY_N (MI_SM_STATE_KEY_N) | MI_SM_STATE_KEY_N (MI_SM_STATE_KEY_N) |
| MI_SM_STATE_OWNER_ID_C (MI_SM_STATE_OWNER_ID_C) | MI_SM_STATE_OWNER_ID_C (MI_SM_STATE_OWNER_ID_C) |
| Maint Outage Basic Hrs (MI_GMCAPHST_MNT_OUT_HRS_N) | Maintenance Outage Hours (MI_GAA_PERF_MAIN_OUT_HRS_N) |
| Maint Outage Factor (MI_GMCAPHST_MNT_OUT_FAC_N) | Maintenance Outage Factor (MI_GAA_PERF_MNT_OUT_FACT_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|--|---|
| Maint Outage Sched Ext Hrs (MI_GMCAPHST_MNT_OUT_SCHD_EX_N) | Maintenance Outage Schedule Extension Hours (MI_GAA_PERF_MNTOT_SCHEXT_HR_N) |
| Maint and Ext Outage Hrs (MI_GMCAPHST_MNT_AND_EXT_OT_N) | Maintenance and Extension Outage Hours (MI_GAA_PERF_MNT_ND_EXT_OT_HR_N) |
| Max Generation (G) (MI_GMCAPHST_MAX_G_GENER_N) | Max Generation (G) (MI_GAA_PERF_MAX_GENE_GROSS_N) |
| Max Generation (N) (MI_GMCAPHST_MAX_N_GENER_N) | Max Generation (N) (MI_GAA_PERF_MAX_GENE_NET_N) |
| Mean Forced Outage Duration (MI_GMCAPHST_MN_FORC_OUT_DUR_N) | Mean Forced Outage Duration (MI_GAA_PERF_MEAN_FORC_OT_DUR_N) |
| Mean Maintenance Outage Duration (MI_GMCAPHST_MN_MAIN_OUT_DUR_N) | Mean Maintenance Outage Duration (MI_GAA_PERF_MEAN_MAIN_OT_DUR_N) |
| Mean Planned Outage Duration (MI_GMCAPHST_MN_PLAN_OUT_DUR_N) | Mean Planned Outage Duration (MI_GAA_PERF_MEAN_PLAN_OT_DUR_N) |
| Mean Service Time To Forced Outage (MI_GMCAPHST_MN_SER_TM_FRC_OU_N) | Mean Service Time To Forced Outage (MI_GAA_PERF_MEAN_SER_TIME_OT_N) |
| Mean Service Time To Maintenance Outage (MI_GMCAPHST_MN_SER_TM_MAI_OU_N) | Mean Service Time To Maintenance Outage (MI_GAA_PERF_MN_SERTIM_MNT_OT_N) |
| Mean Service Time To Planned Outage (MI_GMCAPHST_MN_SER_TM_PL_OU_N) | Mean Service Time To Planned Outage (MI_GAA_PERF_MN_SERTIM_PLN_OT_N) |
| Mean Service Time To Unplanned Outage (MI_GMCAPHST_MN_SER_TM_UPL_OU_N) | Mean Service Time To Unplanned Outage (MI_GAA_PERF_MN_SERTM_UNPL_OT_N) |
| Mean Unplanned Outage Duration (MI_GMCAPHST_MN_UNPL_OUT_DUR_N) | Mean Unplanned Outage Duration (MI_GAA_PERF_MEAN_UNPL_OT_DUR_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|--|--|
| Net Actual Capacity (N) (MI_GMCAPHST_N_ACTUA_CAPAC_N) | Net Actual Capacity (N) (MI_GAA_PERF_NET_ACTU_CAPA_N) |
| Net Actual Generation (N) (MI_GMCAPHST_N_ACTUA_GENER_N) | Net Actual Generation (N) (MI_GAA_PERF_NET_ACTU_GENE_N) |
| Net Dependable Capacity (N) (MI_GMCAPHST_N_DEPEN_CAPAC_N) | Net Dependable Capacity (N) (MI_GAA_PERF_NET_DEPE_CAPA_N) |
| Net Maximum Capacity (N) (MI_GMCAPHST_N_MAXIM_CAPAC_N) | Net Maximum Capacity (N) (MI_GAA_PERF_NET_MAXI_CAPA_N) |
| NonCurtailing Event Hrs (MI_GMCAPHST_NONCU_EVT_HRS_NC_N) | Non Curtailing Event Hours (MI_GAA_PERF_NON_CURTEVNT_HRS_N) |
| Number Of Non Curtailing Events (MI_GMCAPHST_NUM_NC_EVE_N) | Number Of Non Curtailing Events (MI_GAA_PERF_NON_CURTEVNT_CNT_N) |
| Number of Forced Outages (MI_GMCAPHST_NUM_FRC_OUT_N) | Number of Forced Outages (MI_GAA_PERF_FORC_OUT_CNT_N) |
| Number of Maintenance Outages (MI_GMCAPHST_NUM_MNT_OUT_N) | Number of Maintenance Outages (MI_GAA_PERF_MAIN_OUT_CNT_N) |
| Number of Planned Outages (MI_GMCAPHST_NUM_PLN_OUT_N) | Number of Planned Outages (MI_GAA_PERF_PLAN_OUT_CNT_N) |
| Number of Unplanned Outages (MI_GMCAPHST_NUM_UPL_OUT_N) | Number of Unplanned Outages (MI_GAA_PERF_UNPL_OUT_CNT_N) |
| Override Reserve Shutdown Hours (MI_GMCAPHST_OV_RSRV_SHTD_HRS_F) | Override Reserve Shutdown Hours (MI_GAA_PERF_RSRVSHUT_HRS_FLG) |
| Period Hours (MI_GMCAPHST_PERIO_HRS_N) | Period Hours (MI_GAA_PERF_PERIOD_HRS_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|--|--|
| Planned Outage Basic Hrs (MI_GMCAPHST_PL_OUT_HRS_N) | Planned Outage Hours (MI_GAA_PERF_PLAN_OUT_HRS_N) |
| Planned Outage Factor (MI_GMCAPHST_PL_OUT_FAC_N) | Planned Outage Factor (MI_GAA_PERF_PLAN_OUT_FACT_N) |
| Planned and Ext Outage Hrs (MI_GMCAPHST_PL_AND_EXT_OT_N) | Planned and Extension Outage Hours (MI_GAA_PERF_PLN_EXT_OT_HRS_N) |
| Plant ID (MI_GMCAPHST_PLANT_ID_C) | Plant ID (MI_GAA_PERF_PLANT_ID_C) |
| Plant Name (MI_GMCAPHST_PLANT_NAME_C) | Plant Name (MI_GAA_PERF_PLANT_NAME_C) |
| Pln Outage Sched Ext Hrs (MI_GMCAPHST_PL_OUT_SCHD_EX_N) | Planned Outage Schedule Extension Hours (MI_GAA_PERF_PL_OT_SCHEXT_HRS_N) |
| Pumping Hrs (MI_GMCAPHST_PUMPI_HRS_N) | Pumping Hours (MI_GAA_PERF_PUMPING_HRS_N) |
| Report Date (MI_GMCAPHST_REPO_DATE_DT) | Report Date (MI_GAA_PERF_REPORT_DATE_DT) |
| Reporting Date (MI_GMCAPHST_REPOR_DATE_D) | Reporting Date (MI_GAA_PERF_REPORTING_DATE_DT) |
| Reporting Month (MI_GMCAPHST_REPOR_MONTH_C) | Reporting Month (MI_GAA_PERF_REPORTING_MONT_C) |
| Reporting Year (MI_GMCAPHST_REPOR_YEAR_C) | Reporting Year (MI_GAA_PERF_REPORTING_YEAR_C) |
| Reserve Shutdown Hrs (MI_GMCAPHST_RESER_SHUTD_HRS_N) | Reserve Shutdown Hours (MI_GAA_PERF_RESE_SHUT_HRS_N) |
| Revision (MI_GMCAPHST_REVIS_N) | Revision (MI_GAA_PERF_REVISION_N) |
| Sched Outage Hrs (MI_GMCAPHST_SCHED_OUTAG_HRS_N) | Scheduled Outage Hours (MI_GAA_PERF_SCH_OUT_HRS_N) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|--|--|
| Scheduled Outage Factor (MI_GMCAPHST_SCHED_OUT_FAC_N) | Scheduled Outage Factor (MI_GAA_PERF_SCH_OUT_FACT_N) |
| Service Factor (MI_GMCAPHST_SERVI_FAC_N) | Service Factor (MI_GAA_PERF_SERV_FACT_N) |
| Service Hrs (MI_GMCAPHST_SERVI_HRS_N) | Service Hours (MI_GAA_PERF_SERV_HRS_N) |
| Start Reliability (MI_GMCAPHST_STRT_RELIA_N) | Start Reliability (MI_GAA_PERF_STAR_RELI_N) |
| Startup Failure Hrs (MI_GMCAPHST_STRT_FAIL_HRS_SF_N) | Startup Failure Hours (MI_GAA_PERF_STAR_FAIL_HRS_N) |
| Synchronous Condensing Hrs (MI_GMCAPHST_SYNCR_CONDE_HRS_N) | Synchronous Condensing Hours (MI_GAA_PERF_SYNC_COND_HRS_N) |
| Typical Unit Loading (MI_GMCAPHST_TYPIC_UNIT_LOADI_C) | Typical Unit Loading (MI_GAA_PERF_TYPI_UNIT_LOAD_C) |
| U1 Unplanned Outage Hrs (MI_GMCAPHST_U1_HRS_N) | U1 Unplanned Outage Hours (MI_GAA_PERF_U1_UNPL_OUT_HRS_N) |
| U2 Unplanned Outage Hrs (MI_GMCAPHST_U2_HRS_N) | U2 Unplanned Outage Hours (MI_GAA_PERF_U2_UNPL_OUT_HRS_N) |
| U3 Unplanned Outage Hrs (MI_GMCAPHST_U3_HRS_N) | U3 Unplanned Outage Hours (MI_GAA_PERF_U3_UNPL_OUT_HRS_N) |
| Unavailability Factor (MI_GMCAPHST_UNAVA_FAC_N) | Unavailability Factor (MI_GAA_PERF_UNAV_FACT_N) |
| Unavailable Hrs (MI_GMCAPHST_UNAVA_HRS_N) | Unavailable Hours (MI_GAA_PERF_UNAV_HRS_N) |
| Unit ID (MI_GMCAPHST_UNIT_ID_C) | Unit ID (MI_GAA_PERF_UNIT_ID_C) |
| Unit Name (MI_GMCAPHST_UNIT_NAME_C) | Unit Name (MI_GAA_PERF_UNIT_NAME_C) |

| Fields in V3.6.0.0.0 | Fields in V4.3.0.0.0 |
|--|--|
| Unit Type (MI_GMCAPHST_NERC_UNIT_TYPE_C) | Unit Type (MI_GAA_PERF_UNIT_TYPE_C) |
| Unplanned Outage Factor (MI_GMCAPHST_UPL_OUT_FAC_N) | Unplanned Outage Factor (MI_GAA_PERF_UNPL_OUT_FACT_N) |
| Unplanned Outage Hrs (MI_GMCAPHST_UPL_OUT_HUR_UO_N) | Unplanned Outage Hours (MI_GAA_PERF_UNPL_OUT_HRS_N) |
| Verbal Description (MI_GMCAPHST_DESCR_C) | Verbal Description (MI_GAA_PERF_VERB_DESC_C) |
| YTD Actual Unit Starts (MI_GMCAPHST_YTD_CUM_ACT_STRT_N) | YTD Actual Unit Starts (MI_GAA_PERF_YTD_ACTUNIT_STAR_N) |
| YTD Attempted Unit Starts (MI_GMCAPHST_YTD_CUM_ATT_STRT_N) | YTD Attempted Unit Starts (MI_GAA_PERF_YTD_ATTUNIT_STAR_N) |
| YTD Start Reliability (MI_GMCAPHST_YTD_STRT_RELIA_N) | YTD Start Reliability (MI_GAA_PERF_YTD_STAR_RELI_N) |
| Zone (MI_GMCAPHST_ZONE_C) | Zone (MI_GAA_PERF_ZONE_C) |

Generation Availability Analysis (GAA) Security Groups and Roles

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

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

| Security Group | Roles |
|----------------------|---|
| MI GAA Viewer | MI APM Viewer MI GAA Administrator MI GAA Analyst MI GAA Operator MI GAA Supervisor |
| MI GAA Administrator | MI GAA Administrator |
| MI GAA Analyst | MI GAA Analyst MI GAA Operator MI GAA Supervisor |

Note: To [access the Health Summary page for an Asset](#), you must be member of one of the following [Asset Health Manager Security Groups](#):

- MI AHI Administrator
- MI AHI User
- MI AHI Viewer

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

| Family | MI GAA Viewer | MI GAA Administrator | MI GAA Analyst |
|-----------------|---------------|----------------------|----------------|
| Entity Families | | | |

| Family | MI GAA Viewer | MI GAA Administrator | MI GAA Analyst |
|-------------------------|---------------|------------------------------|----------------------|
| Amplification Codes | View | View, Update, Insert, Delete | View, Update, Insert |
| APM Event | View | View, Update, Insert, Delete | View, Update, Insert |
| Capacity Incident | View | View, Update, Insert, Delete | View, Update, Insert |
| Cause Codes | View | View, Update, Insert, Delete | View |
| Contributing Event | View | View, Update, Insert, Delete | View, Update, Insert |
| GAA Code Mapping | View | View, Update, Insert, Delete | View |
| GAA Company | View | View, Update, Insert, Delete | View |
| GAA Configuration | View | View, Update, Insert, Delete | View |
| GAA Event Categories | View | View, Update, Insert, Delete | View |
| GAA Event Transition | View | View, Update, Insert, Delete | View |
| GAA Event Types | View | View, Update, Insert, Delete | View, Update, Insert |
| GAA Fuel Types | View | View, Update, Insert, Delete | View, Update, Insert |
| GAA Performance | View | View, Update, Insert, Delete | View, Update, Insert |
| GAA Performance Fuel | View | View, Update, Insert, Delete | View, Update, Insert |
| GAA Performance Indexes | View | View, Update, Insert, Delete | View, Update, Insert |
| GAA Performance Summary | View | View, Update, Insert, Delete | View, Update, Insert |

| Family | MI GAA Viewer | MI GAA Administrator | MI GAA Analyst |
|--|---------------|------------------------------|------------------------------|
| GAA Plant | View | View, Update, Insert, Delete | View |
| GAA Report Details | View | View, Update, Insert, Delete | View, Update, Insert |
| GAA Supported Organizations | View | View, Update, Insert, Delete | View |
| GAA Unit | View | View, Update, Insert, Delete | View |
| GAA Unit Capacity | View | View, Update, Insert, Delete | View |
| GAA Unit Types | View | View, Update, Insert, Delete | View |
| GAA Unit States | View | View, Update, Insert, Delete | View |
| Generation Pool | View | View, Update, Insert, Delete | View |
| Primary Event | View | View, Update, Insert, Delete | View, Update, Insert |
| Primary Event Details | View | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Primary Event History | View | View, Update, Insert, Delete | View, Insert |
| RCA Analysis | View | View | View |
| Reference Document | View | View, Update, Insert, Delete | View, Update, Insert |
| Relationship Families | | | |
| Associated with APM Event | View | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Functional Location Has Generation Company | View | View, Update, Insert, Delete | View |
| Functional Location Has Generation Plant | View | View, Update, Insert, Delete | View |

| Family | MI GAA Viewer | MI GAA Administrator | MI GAA Analyst |
|---|---------------|------------------------------|------------------------------|
| Functional Location Has Generation Unit | View | View, Update, Insert, Delete | View |
| Has Capacity History | View | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Has Incident | View | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Has Plant | View | View, Update, Insert, Delete | View |
| Has Reference Documents | View | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Has Unit | View | View, Update, Insert, Delete | View |
| Log has Events | View | View, Update, Insert, Delete | View, Update, Insert |
| Primary Incident Has RCA Analysis | View | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Unit Has Records | View | View, Update, Insert, Delete | View |

Deploy Hazards Analysis

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

Deploy Hazards Analysis for the First Time

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

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

Note: If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

| Step | Task | Notes |
|------|--|---|
| 1 | Define alternate search queries. | This step is required only if you do not want to use the baseline search queries. |
| 2 | Manage the types of Deviations in a HAZOP Analysis. To do so, add a code to the MI_HAZOP_DEVIATIONS system code table. | This step is required only if you want to add another value to the list of default values in the Deviation/Guideword list in the HAZOP Deviation datasheet. |
| 3 | Activate the SIS Management license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 4 | Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 5 | Review the Hazards Analysis data model to determine which relationship definitions you will need to modify to include your custom equipment or location families. Modify any relationship definitions as needed via the Configuration Manager application. | This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families. |
| 6 | Assign Security Users to one or more of the Hazards Analysis Security Groups and Roles . | This step is required. |

Upgrade or Update Hazards Analysis to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the SIS Management license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

This module will be upgraded automatically when you upgrade the components in the basic GE Digital APM system architecture. Additionally, as needed, perform the following steps:

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the SIS Management license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

| Step | Task | Notes |
|------|---|---|
| 3 | Access the Safeguards and verify the mapping of IPL Checklist records to the existing Safeguards after upgrade. | <p>This step is optional.</p> <p>In V4.3.0.0.0, IPL Checklist records are used to store your selection for the criteria that are used to determine if a Safeguard is an IPL. When you upgrade to V4.3.0.0.0, for each of the previously existing Safeguards, IPL Checklist records are created and associated with the corresponding Safeguard.</p> |

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the SIS Management license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the SIS Management license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the SIS Management license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the SIS Management license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V3.5.1 through V3.5.1.12.1

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the SIS Management license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the SIS Management license . | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the SIS Management license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the SIS Management license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign Security Users to the MI SIS Administrator or MI SIS Engineer Security Group. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Related Information

Overview of Hazards Analysis

Hazards Analysis (Administrative User Help)

Hazards Analysis System Requirements

[Deploy Hazards Analysis](#)

[Deploy Modules and Features](#)

[GE Digital APM Installation and Upgrade](#)

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 Facilitator | MI Safety Admin MI Safety Power MI Safety User |
| MI HA Member | MI Safety Admin MI Safety Power MI Safety User |
| MI HA Owner | MI Safety Admin MI Safety Power |
| MI Hazards Viewer | MI APM Viewer 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.

Note: The [baseline family-level privileges available in the LOPA module](#) are also applicable to Security Groups in Hazards Analysis module.

| Family | MI HA Administrator | MI HA Facilitator | MI HA Member | MI HA Owner | MI Hazards Viewer |
|------------------------------|------------------------------|------------------------------|--------------|------------------------------|-------------------|
| Entity Families | | | | | |
| Alert | View, Update, Insert, Delete | View, Update, Insert, Delete | None | View, Update, Insert, Delete | View |
| Consequence | View, Update, Insert, Delete | View | View | View | View |
| Equipment | View | View | View | View | View |
| Functional Location | View | View | View | View | View |
| Hazards Analysis | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Hazards Analysis Cause | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Hazards Analysis Consequence | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Hazards Analysis Safeguard | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Hazards Analysis System/Node | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| HAZOP Deviation | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |

| Family | MI HA Administrator | MI HA Facilitator | MI HA Member | MI HA Owner | MI Hazards Viewer |
|--------------------------------|------------------------------|------------------------------|--------------|------------------------------|-------------------|
| Human Resource | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Initiating Event | View, Update, Insert, Delete | View | View | View | View |
| Instrumented Function | View | View | View | View | View |
| Probability | View, Update, Insert, Delete | View | View | View | View |
| Protection Level | View, Update, Insert, Delete | View, Insert | View, Insert | View, Insert | View |
| Reference Document | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Risk Assessment | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Risk Assessment Recommendation | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Risk Category | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Risk Matrix | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |

| Family | MI HA Administrator | MI HA Facilitator | MI HA Member | MI HA Owner | MI Hazards Viewer |
|---|------------------------------|------------------------------|--------------|------------------------------|-------------------|
| Risk Rank | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Risk Threshold | View, Update, Insert, Delete | View | View | View | View |
| Site Reference | View | View | View | View | View |
| What If | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Relationship Families | | | | | |
| Analysis Has Human Resource | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Cause Has Consequence | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Cause Revision Has Consequence Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Consequence Has Safeguard | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Consequence Revision Has Safeguard Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |

| Family | MI HA Administrator | MI HA Facilitator | MI HA Member | MI HA Owner | MI Hazards Viewer |
|---|------------------------------|------------------------------|--------------|------------------------------|-------------------|
| Deviation\What If Has Cause | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Deviation\What If Revision Has Cause Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Equipment Has Equipment | View | View | View | View | View |
| Functional Location Has Equipment | View | View | View | View | View |
| Functional Location Has Functional Location | View | View | View | View | View |
| Has Functional Location | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Hazards Analysis Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has HAZOP Reference | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has IF | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has LOPA | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View | View |

| Family | MI HA Administrator | MI HA Facilitator | MI HA Member | MI HA Owner | MI Hazards Viewer |
|--|------------------------------|------------------------------|--------------|------------------------------|-------------------|
| Has Recommendations | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Reference Documents | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Reference Values | View, Update, Insert, Delete | View | View | View | View |
| Has Risk | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Risk Category | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Risk Matrix | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Site Reference | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Hazards Analysis Has Assets | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Hazards Analysis Revision Has Systems/Nodes Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |

| Family | MI HA Administrator | MI HA Facilitator | MI HA Member | MI HA Owner | MI Hazards Viewer |
|--|------------------------------|------------------------------|--------------|------------------------------|-------------------|
| Is Independent Protection Layer | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Mitigates Risk | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Safety Analysis Has Equipment | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| System/Node Has Deviations/What Ifs | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| System/Node Has Deviations/What Ifs Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |

Deploy Inspection Management

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

Deploy Inspection Management for the First Time

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

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

Note: If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

| Step | Task | Notes |
|------|---|--|
| 1 | Review the Inspection Management data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed. | This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families. |
| 2 | Assign Security Users to one or more of the Security Roles used in IM. | This step is required. Security Users will need permissions to the Inspection Management families before they can use the Inspection Management features. |
| 3 | Modify baseline Application Configuration settings. | This step is required only if you want to modify Application Configurations. The following Application Configurations are defined in the baseline database: Asset Query Path; Associated Relationship Family; Published Query Path; Summary Query Path; Alerts Query Path; Asset Is Successor; Profile Configuration; Method Configuration; Strategy Rule Configuration. |

| | | |
|---|--|---|
| 4 | Define the Inspection Profile for each piece of equipment that you will inspect. | This step is required only if you plan to create Inspection records in baseline families other than the <i>Checklists</i> sub-families. |
| 5 | Modify the baseline Asset query. | This step is required only if you want Inspection records to be linked to records in a family other than the <i>Equipment</i> family. |
| 6 | Define Event Configurations for any new Inspection families that you have created. | This step is required only if you have created custom Inspection families that you want to use within Inspection Management. |
| 7 | Assign certifications to users. | This step is optional. |
| 8 | Group inspection work into Work Packs. | This step is optional. |
| 9 | Define Time-Based Inspection settings. | This step is optional. |

Upgrade or Update Inspection Management to V4.3.0.2.0


The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

| Step | Task | Notes |
|------|---|--|
| 1 | Revert the My Open Inspections Query to baseline. | <p>This step is required only if you have previously modified the My Open Inspections query. If you have, you will not have the ability to download inspections from the My Open Inspections section of the Inspections page until you revert the My Open Inspections query to baseline for the offline functionality to be enabled.</p> <div style="border: 1px solid yellow; padding: 5px;"> <p> Note: If you want to modify this query, you must have both the Inspection Lock and the Entity Key fields as selected fields in the customized query.</p> </div> |

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital 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 V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in

the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

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

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

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

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

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

Inspection Management Security Groups and Roles

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

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

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


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

| Family | MI Inspection | MI Inspection Viewer |
|--------------------|------------------------------|----------------------|
| Entity Families | | |
| Alert | View, Insert, Update, Delete | View |
| Certification | View, Insert, Update, Delete | View |
| Checklist Finding | View, Insert, Update, Delete | View |
| Conditional Alerts | View, Insert, Update, Delete | View |
| Corrosion | View, Insert, Update, Delete | View |
| Equipment | View, Insert, Update, Delete | View |

| Family | MI Inspection | MI Inspection Viewer |
|--|------------------------------|----------------------|
| Event | View, Insert, Update, Delete | View |
| Finding | View, Insert, Update, Delete | View |
| Human Resource | View | View |
| Inspection Method | View, Insert, Update, Delete | View |
| Inspection Profile | View, Insert, Update, Delete | View |
| Inspection Team Member | View, Insert, Update, Delete | View |
| Inventory Group Configuration | View | View |
| Potential Degradation Mechanisms | View | View |
| RBI Degradation Mechanisms | View | View |
| RBI Inspection Auto-Selection Criteria | View | View |
| Recommendation | View, Insert, Update, Delete | View |
| Reference Document | View, Insert, Update, Delete | View |
| Resource Role | View, Insert, Update, Delete | View |
| SAP System | View | View |
| Security User | View | View |
| Strategy | View, Update | View |
| Task | View, Insert, Update, Delete | View |
| Taxonomy References | View | View |
| Time Based Inspection Interval | View, Insert, Update, Delete | View |
| Time Based Inspection Setting | View, Insert, Update, Delete | View |


| Family | MI Inspection | MI Inspection Viewer |
|--------------------------------------|------------------------------|----------------------|
| Work Pack | View, Insert, Update, Delete | View |
| Relationship Families | | |
| Belongs to a Unit | View, Update, Insert, Delete | View |
| Checklist Has Finding | View, Insert, Update, Delete | View |
| Has Certifications | View, Insert, Update, Delete | View |
| Has Degradation Mechanisms | View | View |
| Has Findings | View, Insert, Update, Delete | View |
| Has Inspection Method | View, Insert, Update, Delete | View |
| Has Inspection Profile | View, Insert, Update, Delete | View |
| Has Inspection Scope | View, Insert, Update, Delete | View |
| Has Inspections | View, Insert, Update, Delete | View |
| Has Potential Degradation Mechanisms | View | View |
| Has Recommendations | View, Insert, Update, Delete | View |
| Has Reference Documents | View, Insert, Update, Delete | View |
| Has Roles | View, Insert, Update, Delete | View |
| Has Sub-Inspections | View, Insert, Update, Delete | View |
| Has Tasks | View, Insert, Update, Delete | View |

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

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

Note that:

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

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


Deploying Layers of Protection Analysis (LOPA)


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 LOPA 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 GE Digital APM system architecture.

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

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

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

Upgrade or Update Layers of Protection Analysis (LOPA) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

LOPA 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 Facilitator | MI Safety Admin MI Safety Power MI Safety User |
| MI HA Member | MI Safety Admin MI Safety Power MI Safety User |
| MI HA Owner | MI Safety Admin MI Safety Power |
| MI Hazards Viewer | MI APM Viewer MI Safety Admin MI Safety Power MI Safety User |
| MI SIS Administrator | MI Safety Admin |
| MI SIS Engineer | MI Safety Admin MI Safety Power MI Safety User |

| Security Group | Roles |
|----------------|--|
| MI SIS User | MI Safety Admin MI Safety Power MI Safety User |
| MI SIS Viewer | MI APM Viewer MI Safety Admin MI Safety Power MI Safety User MI SIS Engineer |

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

| Family | MI HA Administrator | MI HA Facilitator | MI HA Member | MI - H-A Owner | MI Hazards Viewer | MI SIS Administrator | MI SIS Engineer | MI SIS User | MI SIS Viewer |
|------------------------------------|------------------------------|-------------------|--------------|----------------|-------------------|------------------------------|-----------------|-------------|---------------|
| Entity Families | | | | | | | | | |
| Active IPL | View, Update, Insert, Delete | View | View | View | View | View, Update, Insert, Delete | View | View | View |
| Asset Safety Preferences | View, Update, Insert, Delete | View | View | View | View | View, Update, Insert, Delete | View | View | View |
| Consequence Adjustment Probability | View, Update, Insert, Delete | View | View | View | View | View, Update, Insert, Delete | View | View | View |

| Family | MI HA Administrator | MI HA Facilitator | MI HA Member | MI - H-A Owner | MI Hazards Viewer | MI SIS Administrator | MI SIS Engineer | MI SIS User | MI SIS Viewer |
|-------------------------------------|------------------------------|------------------------------|--------------|------------------------------|-------------------|------------------------------|------------------------------|-------------|---------------|
| Consequence Modifier | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Consequence Modifier Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Hazards Analysis Safeguard | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Hazards Analysis Safeguard Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Human IPL | View, Update, Insert, Delete | View | View | View | View | View, Update, Insert, Delete | View | View | View |

| Family | MI HA Administrator | MI HA Facilitator | MI HA Member | MI H-A Owner | MI Hazards Viewer | MI SIS Administrator | MI SIS Engineer | M-I-S-I-S User | MI SIS Viewer |
|------------------------|------------------------------|------------------------------|--------------|--------------|-------------------|------------------------------|------------------------------|----------------|---------------|
| Initiating Event | View, Update, Insert, Delete | View | View | View | View | View, Update, Insert, Delete | View | View | View |
| IPL Checklist | View, Update, Insert, Delete | View | View | View | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| IPL Checklist Revision | View, Update, Insert, Delete | View | View | View | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| LOPA | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| LOPA Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Passive IPL | View, Update, Insert, Delete | View | View | View | View | View, Update, Insert, Delete | View | View | View |
| Safety Integrity Level | None | None | None | None | None | View, Update, Insert, Delete | View | View | View |

Relationship Families

| Family | MI HA Administrator | MI HA Facilitator | MI HA Member | MI - H-A Owner | MI Hazards Viewer | MI SIS Administrator | MI SIS Engineer | MI SIS User | MI SIS Viewer |
|---|------------------------------|------------------------------|--------------|------------------------------|-------------------|------------------------------|------------------------------|-------------|---------------|
| Consequence Revision Has Safeguard Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Consequence Modifier | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Consequence Modifier Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Functional Location | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |

| Family | MI HA Administrator | MI HA Facilitator | MI HA Member | MI - H-A Owner | MI Hazards Viewer | MI SIS Administrator | MI SIS Engineer | M-I-S-I-S User | MI SIS Viewer |
|----------------------------------|------------------------------|------------------------------|--------------|------------------------------|-------------------|------------------------------|------------------------------|----------------|---------------|
| Has Independent Protection Layer | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has IPL Checklist Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has LOPA | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has LOPA Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Risk | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |

Deploy Modules and Features

| Family | MI HA Administrator | MI HA Facilitator | MI HA Member | MI - H-A Owner | MI Hazards Viewer | MI SIS Administrator | MI SIS Engineer | M-I-S-I-S User | MI SIS Viewer |
|---------------------------------|------------------------------|------------------------------|--------------|------------------------------|-------------------|------------------------------|------------------------------|----------------|---------------|
| Is Independent Protection Layer | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |


Deploy Life Cycle Cost Analysis (LCC)

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

Deploy Life Cycle Cost Analysis (LCC) for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

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

Upgrade or Update Life Cycle Cost Analysis (LCC) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Life Cycle Cost Analysis Security Groups and Roles

Note: To [import Production Event costs](#) from Production Loss Analysis as Operating Costs, you must be a member of the [MI Production Loss Accounting User](#) Security Group. To [import Strategy Action costs](#) as Operating Costs, you must be a member of the [MI ASM Viewer](#) Security Group.

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

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

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

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

| Family | LCC Administrator | LCC User | LCC Viewer |
|-----------------|------------------------------|------------------------------|------------|
| Entity Families | | | |
| LCC Analysis | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| LCC Cost | View, Update, Insert, Delete | View, Update, Insert, Delete | View |

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


Deploy Management of Change (MoC)

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 Management of Change (MOC) 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 GE Digital APM system architecture.

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

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

Upgrade or Update Management of Change (MoC) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Management of Change 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 MOC Administrator | MI Safety Admin |
| MI MOC Approver | MI Safety Power |
| MI MOC User | MI Safety User |
| MI MOC Viewer | MI Safety User MI Safety Power MI Safety Admin MI APM Viewer |

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

| Family | MI MOC Administrator | MI MOC Approver | MI MOC User | MI MOC Viewer |
|---------------------------|------------------------------|-----------------|------------------------------|---------------|
| Entity Families | | | | |
| General Recommendation | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| MI MOC Answer Option | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| MI MOC Change Project | View, Update, Insert, Delete | View, Update | View, Update, Insert, Delete | View |
| MI MOC Checklist | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| MI MOC Checklist Question | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |

| Family | MI MOC Administrator | MI MOC Approver | MI MOC User | MI MOC Viewer |
|-------------------------------|------------------------------|-----------------|------------------------------|---------------|
| MI MOC Exception | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Operation Tasks | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Reference Document | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Relationship Families | | | | |
| Analysis Has Human Resource | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Change Project Has Checklist | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Change Project Has Elements | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Change Project Has Exception | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Checklist has Questions | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Functional Location | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Reference Documents | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Tasks | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| MOC Answer Has MOC Exception | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| MOC Question Has MOC Answer | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Has Recommendations | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |
| Safety Analysis Has Equipment | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View |


Deploy Metrics and Scorecards

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

Deploy Metrics and Scorecards for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

| Step | Task | Notes |
|------|--|---|
| 1 | <p>Deploy SQL Server Analysis Services 2012 or Microsoft SQL Server Analysis Services 2014. Ensure that the SQL Server Analysis Services machine meets the system requirements.</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"> a. Install SQL Server Analysis Services. b. Deploy the Work History Analysis Services database. <p>This Work History cube is a replacement for the <i>Equipment</i> and <i>Functional Location Work History</i> cubes in the <i>Meridium_Event_Analysis</i> database.</p> <ol style="list-style-type: none"> c. 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 GE Digital APM 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 (e.g., <i>meridium_ssas_user</i>). <ol style="list-style-type: none"> d. Add the user created in Step c to a role on all SQL Analysis Services databases you want to access in GE Digital APM software. <p>The role should have read and drill through permissions. The 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 Per-</p> | <p>This step is required.</p> <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 | Notes |
|------|--|---|
| | <p>missions for Analysis Services.</p> <p>e. 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 | Verify that your event and asset criticality data meet the standard classification requirements, and modify the views for the Work History cube as needed. | This step is required. |
| 3 | Localize the event and asset criticality values in the application. | This step is optional. |
| 4 | Schedule cubes for processing on the SQL Server Analysis Server. | This step is required. |
| 5 | Assign Security Users to one or more of the Metrics and Scorecards Security Groups and Roles . | This step is required. |
| 6 | <p>Create Analysis Services Cube records for each cube that has been defined in SQL Server Analysis Services.</p> <p>Since GE Digital APM uses HTTP connection to connect to the cube, in addition to server address, you need to provide credentials of the user created in Step 1 Task 3.</p> | This step is required. |
| 7 | Grant Security Users and Groups access rights to Analysis Services Cube records. | This step is required. |
| 8 | Configure privileges for KPI. | This step is required. |
| 9 | Configure privileges for Scorecards. | This step is required. |
| 10 | Configure a cube for usage metrics tracking on the SQL Server Analysis Server. | This step is required only if you use Metrics and Scorecards to view the usage metrics in a cube. |

Upgrade or Update Metrics and Scorecards to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

| Step | Task | Notes |
|------|---|--|
| 1 | Deploy the new Work History cube. | <div style="border: 1px solid red; padding: 5px; margin-bottom: 10px;"> <p>⚠ IMPORTANT: Before deploying the new Work History cube, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted <i>View</i> permissions to the cubes associated with the Metric Views, and that the cubes are active.</p> </div> <p>This step is required, and the baseline work history cube must be redeployed.</p> <p>The baseline Work History cube was modified such that even if the event or equipment data do not meet the standard classification defined for Work History cube, with minor modifications to SQL views used by the cube, the cube can still work with the non-standard event and equipment data.</p> |
| 2 | <p>If you have made modifications in the previous version of the cube, then you must manually make the same modifications to the current Work History cube.</p> | <p>This step is required only if you had made any modifications to the previously provided Work History cube.</p> <p>If you had made any modifications to the Work History cube, then you must manually make those updates again.</p> |

| Step | Task | Notes |
|------|--|---|
| 3 | Verify that your event and asset criticality data meet the standard classification requirements , and modify the views for the Work History cube as needed . | This step is required. |
| 4 | Localize the event and equipment values in the GE Digital APM . | This step is required only if you want to localize the event and equipment values in the Work History cube. |
| 5 | Schedule cubes for processing on the SQL Server Analysis Server. | This step is required. |

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

| Step | Task | Notes |
|------|--|--|
| 1 | Deploy the new Work History cube . | <div style="border: 1px solid red; padding: 5px; margin-bottom: 10px;"> <p>⚠ IMPORTANT: Before deploying the new Work History cube, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted <i>View</i> permissions to the cubes associated with the Metric Views, and that the cubes are active.</p> </div> <p>This step is required, and the baseline work history cube must be redeployed.</p> <p>The baseline Work History cube was modified such that even if the event or equipment data do not meet the standard classification defined for Work History cube, with minor modifications to SQL views used by the cube, the cube can still work with the non-standard event and equipment data.</p> |

| Step | Task | Notes |
|------|--|--|
| 2 | If you have made modifications in the previous version of the cube, then you must manually make the same modifications to the current Work History cube. | This step is required only if you had made any modifications to the previously provided Work History cube. If you had made any modifications to the Work History cube, then you must manually make those updates again. |
| 3 | Verify that your event and asset criticality data meet the standard classification requirements , and modify the views for the Work History cube as needed . | This step is required. |
| 4 | Localize the event and equipment values in the GE Digital APM . | This step is required only if you want to localize the event and equipment values in the Work History cube. |
| 5 | Schedule cubes for processing on the SQL Server Analysis Server. | This step is required. |

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

| Step | Task | Notes |
|------|---|--|
| 1 | Deploy the new Work History cube. | <div style="border: 1px solid red; padding: 5px; margin-bottom: 10px;"> <p>⚠ IMPORTANT: Before deploying the new Work History cube, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted <i>View</i> permissions to the cubes associated with the Metric Views, and that the cubes are active.</p> </div> <p>This step is required, and the baseline work history cube must be redeployed.</p> <p>The baseline Work History cube was modified such that even if the event or equipment data do not meet the standard classification defined for Work History cube, with minor modifications to SQL views used by the cube, the cube can still work with the non-standard event and equipment data.</p> |
| 2 | <p>If you have made modifications in the previous version of the cube, then you must manually make the same modifications to the current Work History cube.</p> | <p>This step is required only if you had made any modifications to the previously provided Work History cube.</p> <p>If you had made any modifications to the Work History cube, then you must manually make those updates again.</p> |
| 3 | <p>Verify that your event and asset criticality data meet the standard classification requirements, and modify the views for the Work History cube as needed.</p> | <p>This step is required.</p> |
| 4 | <p>Localize the event and equipment values in the GE Digital APM.</p> | <p>This step is required only if you want to localize the event and equipment values in the Work History cube.</p> |
| 5 | <p>Schedule cubes for processing on the SQL Server Analysis Server.</p> | <p>This step is required.</p> |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| Step | Task | Notes |
|------|---|--|
| 1 | Deploy the new Work History cube. | <div style="border: 1px solid red; padding: 5px; margin-bottom: 10px;"> <p>⚠ IMPORTANT: Before deploying the new Work History cube, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted <i>View</i> permissions to the cubes associated with the Metric Views, and that the cubes are active.</p> </div> <p>This step is required, and the baseline work history cube must be redeployed.</p> <p>The baseline Work History cube was modified such that even if the event or equipment data do not meet the standard classification defined for Work History cube, with minor modifications to SQL views used by the cube, the cube can still work with the non-standard event and equipment data.</p> |
| 2 | <p>If you have made modifications in the previous version of the cube, then you must manually make the same modifications to the current Work History cube.</p> | <p>This step is required only if you had made any modifications to the previously provided Work History cube.</p> <p>If you had made any modifications to the Work History cube, then you must manually make those updates again.</p> |
| 3 | <p>Verify that your event and asset criticality data meet the standard classification requirements, and modify the views for the Work History cube as needed.</p> | <p>This step is required.</p> |
| 4 | <p>Localize the event and equipment values in the GE Digital APM.</p> | <p>This step is required only if you want to localize the event and equipment values in the Work History cube.</p> |
| 5 | <p>Schedule cubes for processing on the SQL Server Analysis Server.</p> | <p>This step is required.</p> |


Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

| Step | Task | Notes |
|------|--|--|
| 1 | <p>Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions:</p> <ul style="list-style-type: none"> • 2012 • 2014 | <p>This step is required only if you were previously using SQL Server Analysis Services 2008 R2.</p> |
| 2 | <p>Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication.</p> | <p>This step is required.</p> |
| 3 | <p>Deploy Work History Analysis Services database.</p> <p>This Work History cube is a replacement for the <i>Equipment</i> and <i>Functional Location Work History</i> cubes in the <i>Meridium_Event_Analysis</i> database.</p> | <div style="border: 1px solid red; padding: 5px;"> <p>⚠ IMPORTANT: Before executing this step, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted <i>View</i> permissions to the cubes associated with the Metric Views, and that the cubes are active.</p> </div> <p>This step is required.</p> |
| 4 | <p>Create a Windows User on the Analysis Server or in your organization's Active Directory.</p> <p>The user name requires minimum privileges and will only be used by the GE Digital APM 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 (e.g., meridium_ssas_user). | <p>This step is required.</p> |

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

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

| Step | Task | Notes |
|------|--|---|
| 1 | <p>Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions:</p> <ul style="list-style-type: none"> • 2012 • 2014 | This step is required only if you were previously using SQL Server Analysis Services 2008 R2. |

| Step | Task | Notes |
|------|--|--|
| 2 | Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication . | This step is required. |
| 3 | <p>Deploy Work History Analysis Services database.</p> <p>This Work History cube is a replacement for the <i>Equipment</i> and <i>Functional Location Work History</i> cubes in the <i>Meridium_Event_Analysis</i> database.</p> | <div style="border: 1px solid red; padding: 5px;"> <p> IMPORTANT: Before executing this step, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted <i>View</i> permissions to the cubes associated with the Metric Views, and that the cubes are active.</p> </div> <p>This step is required.</p> |

| Step | Task | Notes |
|------|--|---|
| 4 | <p>Create a Windows User on the Analysis Server or in your organization's Active Directory.</p> <p>The user name requires minimum privileges and will only be used by the GE Digital APM 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 (e.g., meridium_ssas_user). | This step is required. |
| 5 | <p>Add the user created in Step 4 to a role on all SQL Analysis Services databases that you want to access in GE Digital APM.</p> <p>The role should have read and drill-through permissions. If the Work History database already has a <i>View</i> role defined, then you should add the user to this role. For more information, consult the MSDN documentation regarding Roles and Permissions for Analysis Services.</p> | This step is required. |
| 6 | <p>Verify that your event and asset criticality data meet the standard classification requirements, and modify the views for the Work History cube as needed.</p> | This step is required. |
| 7 | <p>Localize the event and equipment values in GE Digital APM.</p> | This step is required only if you want to localize the event and equipment values in the Work History cube. |
| 8 | <p>Schedule cubes for processing on the SQL Server Analysis Server.</p> | This step is required. |
| 9 | <p>Update the existing Analysis Services Cube records so that GE Digital APM connects to the cube using the HTTP/HTTPS access.</p> | This step is required. |

Upgrade from any version V3.5.1 through V3.5.1.12.1

| Step | Task | Notes |
|------|--|--|
| 1 | <p>Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions:</p> <ul style="list-style-type: none"> • 2012 • 2014 | <p>This step is required only if you were previously using SQL Server Analysis Services 2008 R2.</p> |
| 2 | <p>Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication.</p> | <p>This step is required.</p> |
| 3 | <p>Deploy Work History Analysis Services database.</p> <p>This Work History cube is a replacement for the <i>Equipment</i> and <i>Functional Location Work History</i> cubes in the <i>Meridium_Event_Analysis</i> database.</p> | <div style="border: 1px solid red; padding: 5px;"> <p>⚠ IMPORTANT: Before executing this step, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted <i>View</i> permissions to the cubes associated with the Metric Views, and that the cubes are active.</p> </div> <p>This step is required.</p> |
| 4 | <p>Create a Windows User on the Analysis Server or in your organization's Active Directory.</p> <p>The user name requires minimum privileges and will only be used by the GE Digital APM 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 (e.g., meridium_ssas_user). | <p>This step is required.</p> |

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

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

| Step | Task | Notes |
|------|--|---|
| 1 | <p>Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions:</p> <ul style="list-style-type: none"> • 2012 • 2014 | This step is required only if you were previously using SQL Server Analysis Services 2008 R2. |

| Step | Task | Notes |
|------|---|--|
| 2 | <p>Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication.</p> | <p>This step is required.</p> |
| 3 | <p>Deploy Work History Analysis Services database.</p> <p>This Work History cube is a replacement for the <i>Equipment</i> and <i>Functional Location Work History</i> cubes in the <i>Meridium_Event_Analysis</i> database.</p> | <div style="border: 1px solid red; padding: 5px;"> <p>⚠ IMPORTANT: Before executing this step, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted <i>View</i> permissions to the cubes associated with the Metric Views, and that the cubes are active.</p> </div> <p>This step is required.</p> |
| 4 | <p>Create a Windows User on the Analysis Server or in your organization's Active Directory.</p> <p>The user name requires minimum privileges and will only be used by the GE Digital APM 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 (e.g.,meridium_ssas_user). | <p>This step is required.</p> |

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

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

| Step | Task | Notes |
|------|--|---|
| 1 | <p>Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions:</p> <ul style="list-style-type: none"> • 2012 • 2014 | This step is required only if you were previously using SQL Server Analysis Services 2008 R2. |

| Step | Task | Notes |
|------|--|---|
| 2 | Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication . | This step is required. |
| 3 | Deploy Work History Analysis Services database . This Work History cube is a replacement for the <i>Equipment</i> and <i>Functional Location Work History</i> cubes in the <i>Meridium_Event_Analysis</i> database. | <div style="border: 1px solid red; padding: 5px; margin-bottom: 5px;"> <p>⚠ IMPORTANT: Before executing this step, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted <i>View</i> permissions to the cubes associated with the Metric Views, and that the cubes are active.</p> </div> This step is required. |
| 4 | Create a Windows User on the Analysis Server or in your organization's Active Directory. The user name requires minimum privileges and will only be used by the GE Digital APM Server to connect to the cubes. It is recommended that: <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 (e.g.,meridium_ssas_user). | This step is required. |

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

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Notes |
|------|--|---|
| 1 | <p>Migrate your SQL Server Analysis Services database and cubes to the following supported SQL Server Analysis Services versions:</p> <ul style="list-style-type: none"> • 2012 • 2014 | This step is required only if you were previously using SQL Server Analysis Services 2008 R2. |

| Step | Task | Notes |
|------|---|--|
| 2 | <p>Configure SQL Server Analysis Server for HTTP or HTTPS access using basic authentication.</p> | <p>This step is required.</p> |
| 3 | <p>Deploy Work History Analysis Services database.</p> <p>This Work History cube is a replacement for the <i>Equipment</i> and <i>Functional Location Work History</i> cubes in the <i>Meridium_Event_Analysis</i> database.</p> | <div style="border: 1px solid red; padding: 5px;"> <p>⚠ IMPORTANT: Before executing this step, ensure that the Security User who will run the Analysis Services Deployment Wizard has been granted <i>View</i> permissions to the cubes associated with the Metric Views, and that the cubes are active.</p> </div> <p>This step is required.</p> |
| 4 | <p>Create a Windows User on the Analysis Server or in your organization's Active Directory.</p> <p>The user name requires minimum privileges and will only be used by the GE Digital APM 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 (e.g.,meridium_ssas_user). | <p>This step is required.</p> |

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

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 GE Digital 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 GE Digital 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 GE Digital APM. Usage metrics are not recorded for activities performed in the GE Digital 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 GE Digital 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 GE Digital 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 GE Digital 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 GE Digital or from a third-party vendor, depending upon the licensing options you selected when you purchased the GE Digital 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 GE Digital 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 GE Digital 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 GE Digital APM objects.

- If you have SQL Server Server 2008 cubes, you must migrate them to SQL Server 2012.
- If you have SQL Server 2012 cubes, you can migrate them to SQL Server 2014.

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

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

Steps

1. On the SQL Server Analysis Services Server where the older version of SQL Server Analysis Services is installed, open the **SQL Server Management Studio** window.
2. Connect to the SQL 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** box, select the **Browse** button, and specify the location where the database will be backed up.
5. Specify any additional settings, and then select **OK**.

The selected database is saved to an .ABF file in the specified location.

6. Open the **SQL Server Management Studio** window for the new version of SQL Server Analysis Services.
7. In the **Object Explorer** pane, right-click **Databases**, and select **New Database**.

The **New Database** window appears.

8. In the **Database name** box, enter a name for the database that you are migrating to the new version of SQL Server Analysis Services.
9. Specify any additional settings, and then select **OK**.

The specified database is created, and a corresponding node appears in the **Object Explorer** pane.

10. Right-click the node representing the new database, and then select **Restore**.

The **Restore Database** window appears.

11. In the **Backup** file, enter the file path or select the **Browse** button and navigate to the database file that you backed up in step 5.
12. Specify an additional settings, and then select **OK**.

Your SQL Server Analysis Services database is migrated to the new SQL Server Analysis Services version.

13. In the GE Digital APM, in the **Metrics and Scorecards** module, modify the remaining properties of each Analysis Services Cube record, including selecting the appropriate new SQL Server Analysis Server. You can do by using the **Manage Cubes** page in the **Metrics and Scorecards** module.
14. View existing objects (e.g. Metric Views and KPIs) that are based upon the migrated cubes to ensure that the correct data is being displayed. If the correct data is not displayed, rebuild the cubes and the objects that are based upon them. For details on rebuilding cubes, see your SQL Server documentation.

Deploy the Work History Cube

Steps

1. Create a copy of the **Cubes** folder from the Release CD to a folder in SQL Server Analysis Services Server.
2. In the copied **Cubes** folder, select the **Work History** folder.

The folder contains following files:

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

3. Run the **Analysis Services Deployment Wizard** program.

The **Welcome** page appears.

4. Select **Next**.
5. When the wizard prompts you to choose the database file, navigate to the **Work History** folder, and then select the file **Work History.asdatabase**.
6. Run through all steps of the wizard to deploy the Work History database to SQL Server Analysis Services Server.

For more information, consult the MSDN documentation regarding Analysis Services Deployment Wizard.

About Modifying the Work History Cube

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

- Event Type
 - Standard Event Types
 - ID: Miscellaneous; Caption: Miscellaneous
 - ID: PM/PdM; Caption: PM/PdM
 - ID: Repair; Caption: Repair
 - ID: Unknown; Caption: Unknown
- Event Breakdown Indicator
 - Standard Event Breakdown Indicators
 - ID: N, Caption: N
 - ID: Y, Caption: Y
 - ID: Unknown, Caption: Unknown
- Event Priority
 - Standard Event Priorities
 - ID: 1, Caption: Very Low
 - ID: 2, Caption: Low
 - ID: 3, Caption: Medium
 - ID: 4, Caption: High
 - ID: 5, Caption: Emergency
 - ID: Unknown, Caption: Unknown
- Event Detection Method
 - Standard Event Detection Methods
 - ID: 0001, Caption: Continuous Condition Monitoring
 - ID: 0002, Caption: Corrective Maintenance
 - ID: 0003, Caption: Formal Inspection
 - ID: 0004, Caption: Operator Routine Observation
 - ID: 0005, Caption: Periodic Condition Monitoring
 - ID: 0006, Caption: Preventive Maintenance
 - ID: 0007, Caption: Production Interference
 - ID: 0008, Caption: Radar Operator Observation
 - ID: Unknown, Caption: Unknown

- Asset Criticality Data
 - Standard Asset Criticality Data
 - ID: A, Caption: High
 - ID: B, Caption: Medium
 - ID: C, Caption: Low
 - ID: Unknown, Caption: Unknown

Modify the Views for Work History Cube

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

Before You Begin

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

Modify the Non Standard Event Type Data

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

```
SELECT distinct MI_EVENT_TYP_CHR from MI_EVENT
```

2. Verify if the results match the [standard event type IDs defined by the Work History cube.](#)
3. If the results do not match, then modify the case statement CASE MI_EVENT_TYP_CHR in the view to display the standard event type IDs.

Example:

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

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

Modify the Non Standard Event Breakdown Data

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

```
SELECT distinct MI_EVWKHIST_BRKDN_IND_F from MI_EVWKHIST
```

2. Verify if the results match the [standard event breakdown IDs defined by the Work History cube.](#)

3. If the results do not match, then modify the case statement CASE MI_EVWKHIST_BRKDN_IND_F in the view to display the standard event breakdown IDs.

Example:

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

```
CASE MI_EVWKHIST_BRKDN_IND_F
  WHEN 'Y' THEN 'Y'
  WHEN 'N' THEN 'N'
  WHEN 'No' THEN 'N'
  ELSE 'Unknown'
END AS Breakdown
```

Modify the Non Standard Event Priority Data

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


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

Example:

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

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



```

    WHEN 'M' THEN '3'
    ELSE 'Unknown'
END AS Priority

```

Modify the Non Standard Event Detection Method Data

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

```
SELECT distinct MI_EVWKHIST_DETCT_MTHD_CD_C from MI_EVWKHIST
```

2. Verify if the results match the [standard event detection method IDs defined by the Work History cube](#).
3. If the results do not match, then modify the case statement CASE MI_EVWKHIST_DETCT_MTHD_CD_C in the view to display standard event detection method IDs.

Example:

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

```

CASE MI_EVWKHIST_DETCT_MTHD_CD_C
    WHEN 'Continuous Condition Monitoring' THEN '0001'
    WHEN 'Corrective Maintenance' THEN '0002'
    WHEN 'Formal Inspection' THEN '0003'
    WHEN 'Operator Routine Observation' THEN '0004'
    WHEN 'Periodic Condition Monitoring' THEN '0005'
    WHEN 'Preventive Maintenance' THEN '0006'
    WHEN 'Production Interference' THEN '0007'
    WHEN 'Radar operator Observation' THEN '0008'
    WHEN '0001' THEN '0001'
    WHEN '0002' THEN '0002'
    WHEN '0003' THEN '0003'
    WHEN '0004' THEN '0004'
    WHEN '0005' THEN '0005'
    WHEN '0006' THEN '0006'
    WHEN '0007' THEN '0007'
    WHEN '0008' THEN '0008'
    WHEN '0009' THEN '0001'
    ELSE 'Unknown'
END AS DetectionMethod

```

Modify the Non Standard Equipment Criticality Data

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

```
SELECT distinct MI_EQUIP000_CRITI_MTHD_IND_C from MI_EQUIP000
```

2. Verify if the results match the [standard event detection method IDs defined by the Work History cube](#).
3. If the results do not match, then modify the case statement CASE MI_EQUIP000_CRITI_IND_C in the view to display standard event detection method IDs.

Example:

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

```
CASE MI_EQUIP000_CRITI_IND_C
  WHEN 'HIGH' THEN 'A'
  WHEN 'Medium' THEN 'B'
  WHEN 'Low' THEN 'C'
  WHEN 'A' THEN 'A'
  WHEN 'B' THEN 'B'
  WHEN 'C' THEN 'C'
  WHEN 'H' THEN 'A'
  ELSE 'Unknown'
END AS EquipmentCriticality
```

Modify the Non Standard Functional Location Equipment Criticality Data

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

```
SELECT distinct MI_FNCLOC00_CRTCAL_IND_C from MI_FNCLOC00
```

2. Verify if the results match the [standard event detection method IDs defined by the Work History cube](#).
3. If the results do not match, then modify the case statement CASE A.MI_FNCLOC00_CRTCAL_IND_C in the view to display standard functional location criticality IDs.

Example:

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

```
CASE A.MI_FNCLOC00_CRTCAL_IND_C
  WHEN 'HIGH' THEN 'A'
  WHEN 'Medium' THEN 'B'
  WHEN 'Low' THEN 'C'
  WHEN 'A' THEN 'A'
  WHEN 'B' THEN 'B'
  WHEN 'C' THEN 'C'
  WHEN 'M' THEN 'B'
  ELSE 'Unknown'
END AS FunctionalLocationCriticality
```

Localize the Event or Asset Criticality Values

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

Before You Begin

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

Example: Localize the Event Type Values

1. In the **Tables**, select the table MI_DIM_EVENT_TYPE.

The table values appear, displaying the event type ID and the event caption.

2. In the **EventTypeCaption** column, select the cell for the event type that you want to localize, and then manually modify the caption.
3. Save the modification, and then process the cube.

4. Log in to the GE Digital APM.

5. Access the Metrics and Scorecards page and create a new Metric View.

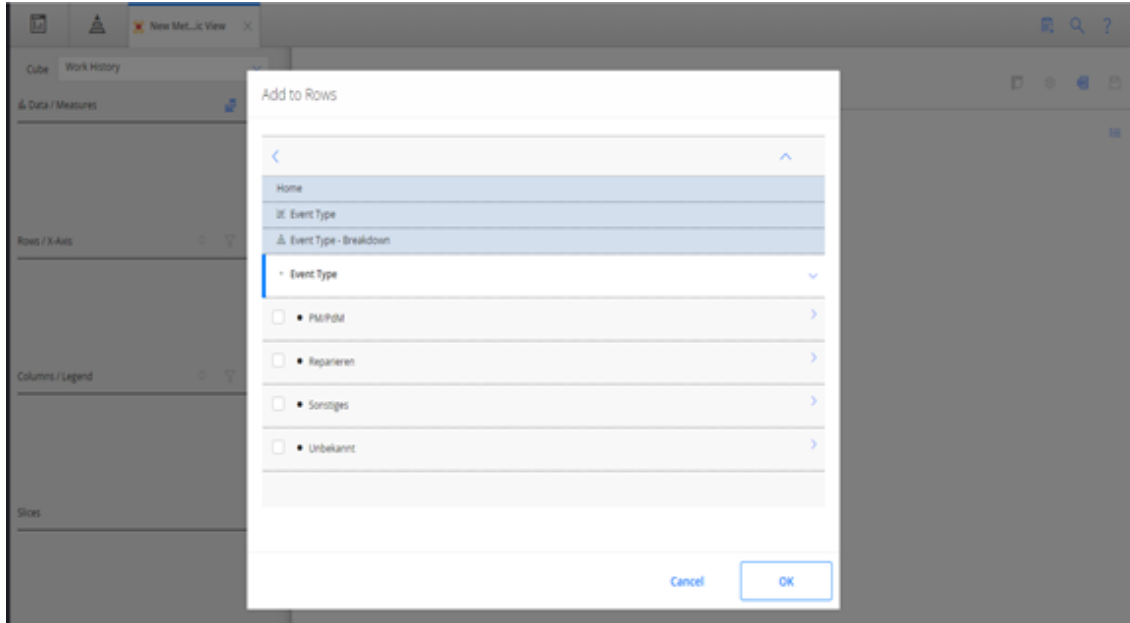
The design page for the Metric View appears.

6. In the Metric Views design page, in the **Rows/X-Axis** subsection, select **+**.

The **Add to Rows** window appears.

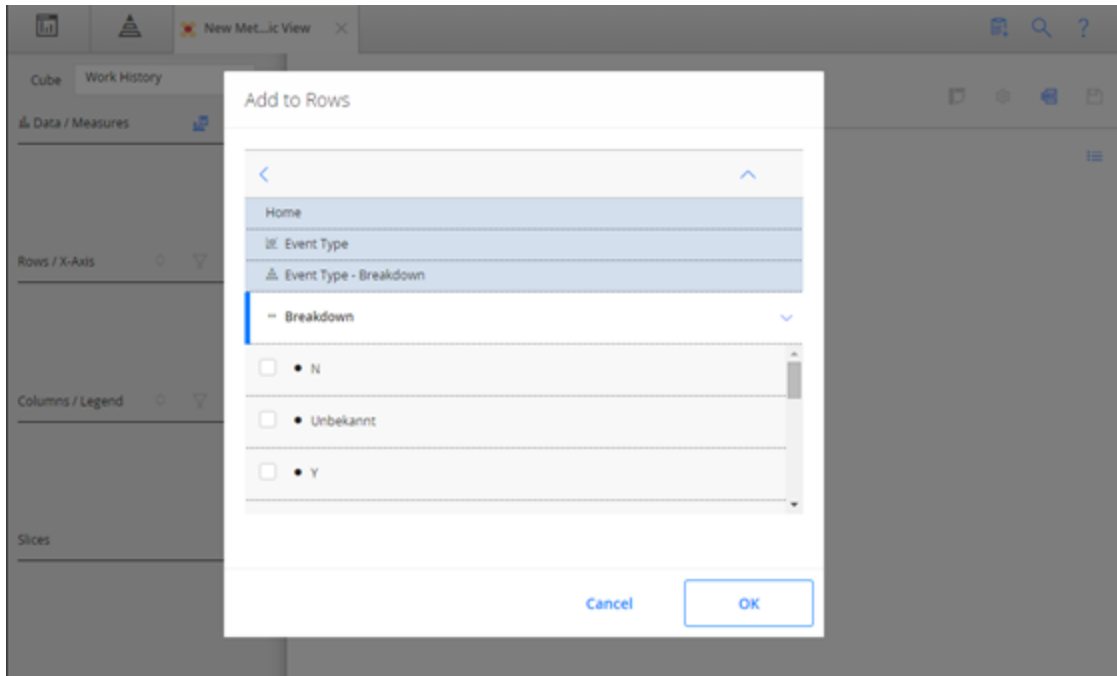
7. In the **Event Type**, select **Event Type-Breakdown**, and then select **Event Type**.

The caption for the event type values appears in the language to which you have modified.



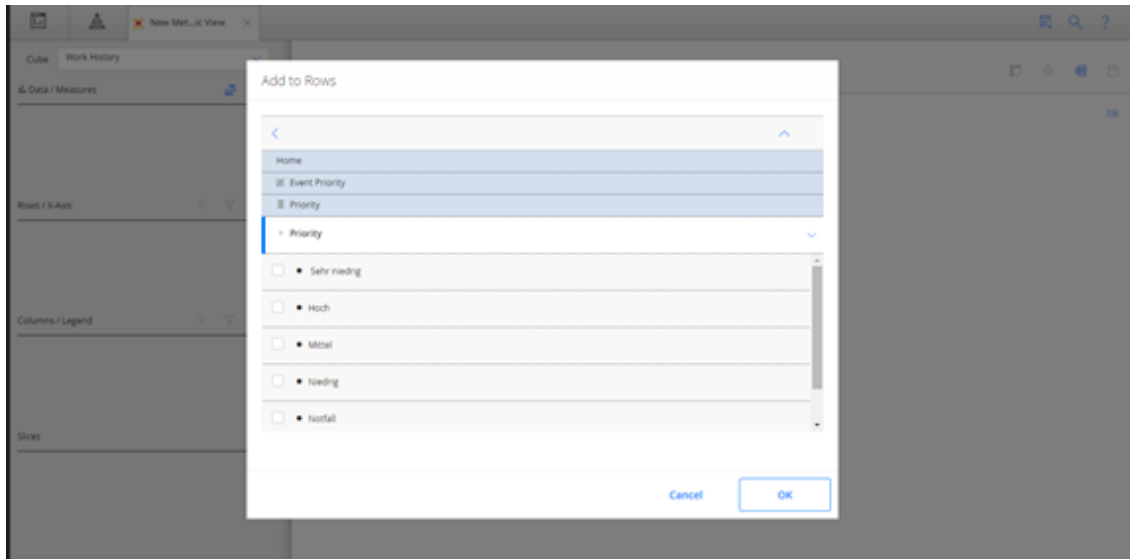
Example: Localize the Event Breakdown Values

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



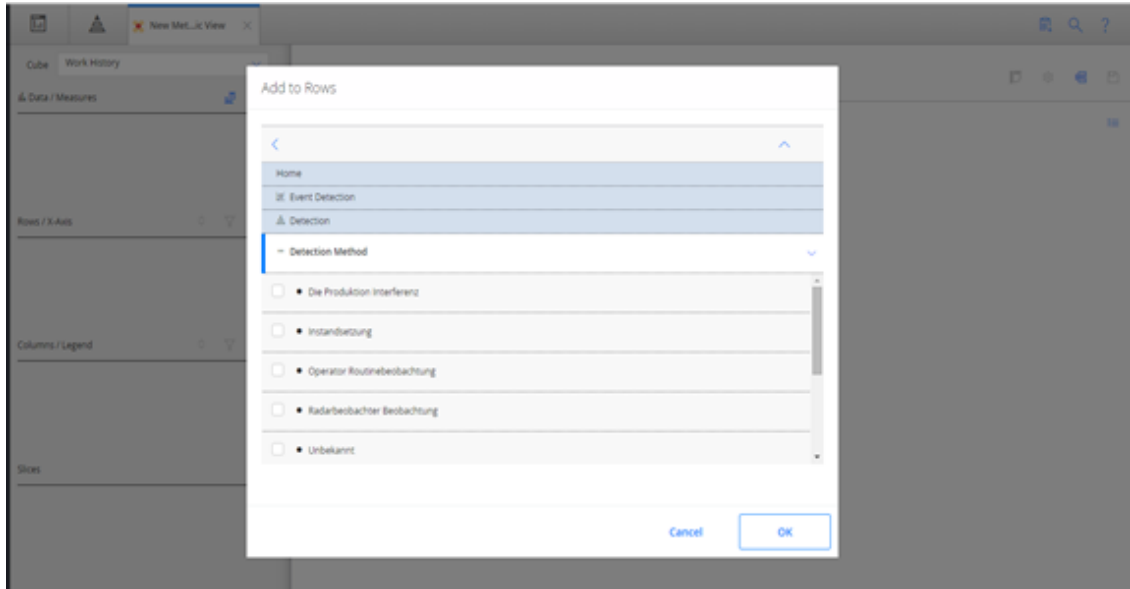
Example: Localize the Event Priority Values

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



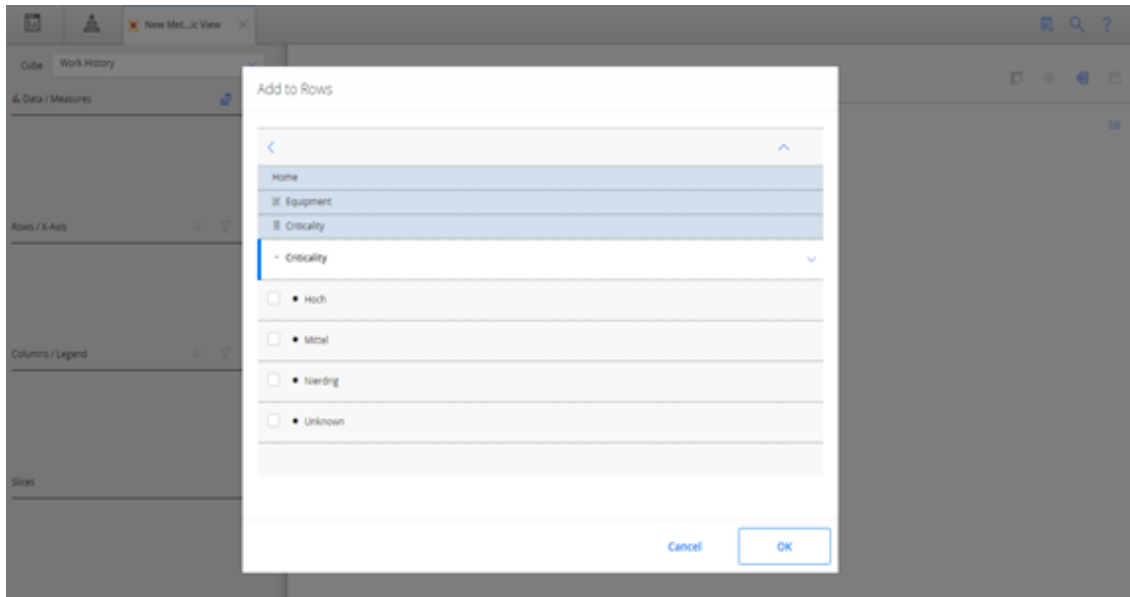
Example: Localize Event Detection Method Values

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



Example: Localize Equipment Criticality Values

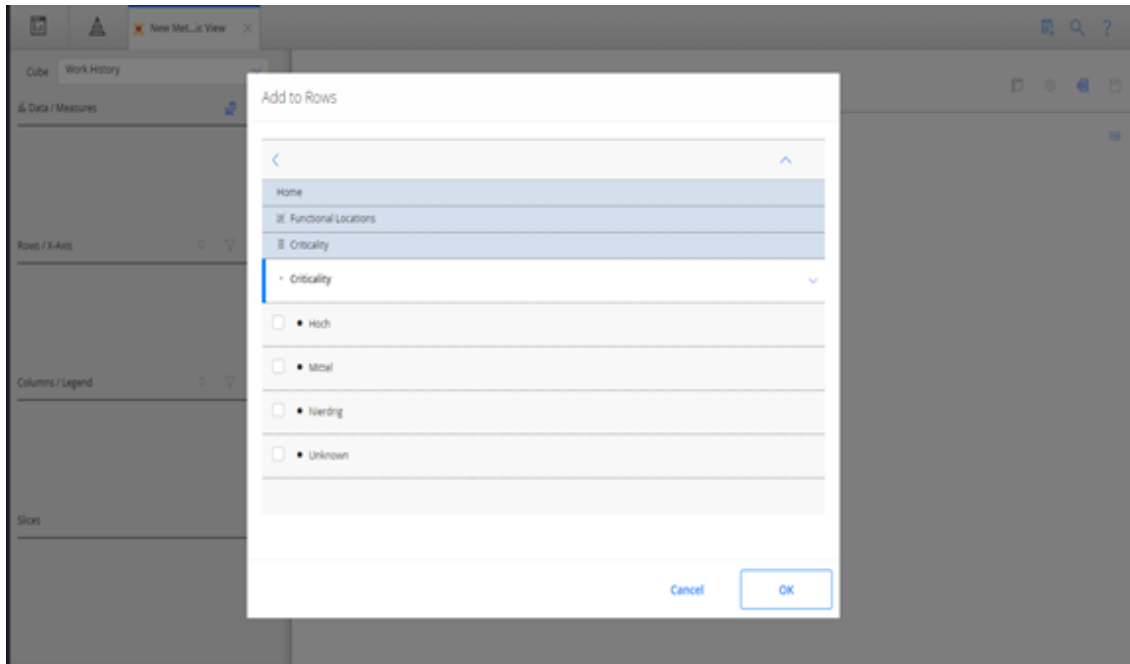
1. In the **Tables**, select the table MI_DIM_ASSET_CRITICALITY.
The table values appear, displaying the Criticality ID and the Criticality caption.
2. In the **CriticalityCaption** column, select the cell for the caption that you want to localize, and then manually modify the caption.
3. Save the modifications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



Example: Localize Functional Location Criticality Values

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

Deploy Modules and Features



Metrics and Scorecards Security Groups and Roles

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

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

| Security Group | Roles |
|--------------------------|--|
| MI Metrics Administrator | MI Foundation Admin MI APMNow Admin |
| MI Metrics User | MI Foundation Power MI Foundation User |
| MI Metrics Viewer | MI APM Viewer |
| 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 | MI Metrics Viewer |
|------------------------|------------------------------|------------------------------|-------------------|
| Entity Families | | | |
| Analysis Services Cube | View, Update, Insert, Delete | View | View |
| KPI | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| KPI Measurement | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Scorecard | View, Update, Insert, Delete | View, Update, Insert, Delete | View |

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

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 GE Digital APM.

Deploy Policy Designer

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

Deploy Policy Designer for the First Time

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

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

Note: If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

| Step | Task | Notes |
|------|---|---|
| 1 | Assign Security Users to one or more of the Policy Designer Security Groups and Roles . | This step is required. |
| 2 | Review the Policy Designer data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed. | This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families. |
| 3 | On the GE Digital APM Server, start the Policy Execution Service. | This step is required. If your system architecture contains more than one GE Digital 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:\ProgramData\Meridium\Logs . |
| 4 | On the GE Digital APM Server, start the Policy Trigger Service. | This step is required. If your system architecture contains more than one GE Digital APM Server, you must configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |

| Step | Task | Notes |
|------|---|---|
| 5 | On the GE Digital APM Server, reset IIS. | This step is required. |
| 6 | On the GE Digital APM Process Data Integration Server, start or restart the Process Data Integration Service. | This step is required only if you want to use OPC Tag records in your policies. |

Upgrade or Update Policy Designer to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

| Step | Task | Notes | | | | | | | | | | | | | | |
|--------------------|---|--------------------|--------------------|-----------------|-----------|--------|-----------|--------------|------------|------|----------|---------|------------------|------------|------------|--|
| 1 | <p>If you are upgrading from V4.1.5.x <i>and</i> you used Policy Recommendations for the first time in V4.1.5.x, after you upgrade your database, use the State Management option in the Revert to Baseline feature to apply the correct State Configuration for the Policy Recommendation Family.</p> <p>When you do so, you will need to provide mappings from the incorrect states to the corresponding correct states, as shown in the following table:</p> <table border="1"> <thead> <tr> <th>Custom (incorrect)</th> <th>Baseline (correct)</th> </tr> </thead> <tbody> <tr> <td>Accepted by ASM</td> <td>Completed</td> </tr> <tr> <td>Closed</td> <td>Completed</td> </tr> <tr> <td>Consolidated</td> <td>Superseded</td> </tr> <tr> <td>Open</td> <td>Proposed</td> </tr> <tr> <td>Pending</td> <td>Pending Approval</td> </tr> <tr> <td>Superseded</td> <td>Superseded</td> </tr> </tbody> </table> | Custom (incorrect) | Baseline (correct) | Accepted by ASM | Completed | Closed | Completed | Consolidated | Superseded | Open | Proposed | Pending | Pending Approval | Superseded | Superseded | <p>This step is necessary because an incorrect baseline State Configuration was delivered for the Policy Recommendation family in V4.1.5.0. The baseline configuration was corrected in V4.1.6.0.</p> <p>The correct baseline state configuration must be applied for various queries and lists in GE Digital APM to function as expected.</p> <p>You do <i>not</i> need to complete this step if:</p> <ul style="list-style-type: none"> You never used V4.1.5.x -or- You never used Policy Recommendations -or- You used Policy Recommendations in a version <i>prior</i> to V4.1.5.x |
| Custom (incorrect) | Baseline (correct) | | | | | | | | | | | | | | | |
| Accepted by ASM | Completed | | | | | | | | | | | | | | | |
| Closed | Completed | | | | | | | | | | | | | | | |
| Consolidated | Superseded | | | | | | | | | | | | | | | |
| Open | Proposed | | | | | | | | | | | | | | | |
| Pending | Pending Approval | | | | | | | | | | | | | | | |
| Superseded | Superseded | | | | | | | | | | | | | | | |

| Step | Task | Notes |
|------|---|--|
| 2 | On the GE Digital APM Server, start or restart the Policy Execution Service. | This step is required. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 3 | If your system architecture contains more than one GE Digital APM Server, you must configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution. | This step is required. |
| 4 | Start or restart the Policy Trigger Service. | This step is required. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 5 | On the GE Digital APM Server, reset IIS. | This step is required. |
| 6 | On the Process Data Integration Server, start (or restart if it is already started) the Meridium Process Data Integration Service. | This step is required <i>only</i> if you want to use OPC Tag records in your policies. |

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

| Step | Task | Notes | | | | | | | | | | | | | | |
|--------------------|--|--|--------------------|-----------------|-----------|--------|-----------|--------------|------------|------|----------|---------|------------------|------------|------------|--|
| 1 | <p>If you are upgrading from V4.1.5.x <i>and</i> you used Policy Recommendations for the first time in V4.1.5.x, after you upgrade your database, use the State Management option in the Revert to Baseline feature to apply the correct State Configuration for the Policy Recommendation Family.</p> <p>When you do so, you will need to provide mappings from the incorrect states to the corresponding correct states, as shown in the following table:</p> <table border="1" data-bbox="331 747 954 1205"> <thead> <tr> <th data-bbox="331 747 651 821">Custom (incorrect)</th> <th data-bbox="651 747 954 821">Baseline (correct)</th> </tr> </thead> <tbody> <tr> <td data-bbox="331 821 651 884">Accepted by ASM</td> <td data-bbox="651 821 954 884">Completed</td> </tr> <tr> <td data-bbox="331 884 651 947">Closed</td> <td data-bbox="651 884 954 947">Completed</td> </tr> <tr> <td data-bbox="331 947 651 1010">Consolidated</td> <td data-bbox="651 947 954 1010">Superseded</td> </tr> <tr> <td data-bbox="331 1010 651 1073">Open</td> <td data-bbox="651 1010 954 1073">Proposed</td> </tr> <tr> <td data-bbox="331 1073 651 1136">Pending</td> <td data-bbox="651 1073 954 1136">Pending Approval</td> </tr> <tr> <td data-bbox="331 1136 651 1205">Superseded</td> <td data-bbox="651 1136 954 1205">Superseded</td> </tr> </tbody> </table> | Custom (incorrect) | Baseline (correct) | Accepted by ASM | Completed | Closed | Completed | Consolidated | Superseded | Open | Proposed | Pending | Pending Approval | Superseded | Superseded | <p>This step is necessary because an incorrect baseline State Configuration was delivered for the Policy Recommendation family in V4.1.5.0. The baseline configuration was corrected in V4.1.6.0.</p> <p>The correct baseline state configuration must be applied for various queries and lists in GE Digital APM to function as expected.</p> <p>You do <i>not</i> need to complete this step if:</p> <ul style="list-style-type: none"> • You never used V4.1.5.x -or- • You never used Policy Recommendations -or- • You used Policy Recommendations in a version <i>prior</i> to V4.1.5.x |
| Custom (incorrect) | Baseline (correct) | | | | | | | | | | | | | | | |
| Accepted by ASM | Completed | | | | | | | | | | | | | | | |
| Closed | Completed | | | | | | | | | | | | | | | |
| Consolidated | Superseded | | | | | | | | | | | | | | | |
| Open | Proposed | | | | | | | | | | | | | | | |
| Pending | Pending Approval | | | | | | | | | | | | | | | |
| Superseded | Superseded | | | | | | | | | | | | | | | |
| 2 | <p>On the GE Digital APM Server, start or restart the Policy Execution Service.</p> | <p>This step is required.</p> <p>You may review the log files for this service at C:\ProgramData\Meridium\Logs.</p> | | | | | | | | | | | | | | |
| 3 | <p>If your system architecture contains more than one GE Digital APMServer, you must configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution.</p> | <p>This step is required.</p> | | | | | | | | | | | | | | |

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

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

| Step | Task | Notes | | | | | | | | | | | | | | |
|--------------------|---|--------------------|--------------------|-----------------|-----------|--------|-----------|--------------|------------|------|----------|---------|------------------|------------|------------|--|
| 1 | <p>If you are upgrading from V4.1.5.x <i>and</i> you used Policy Recommendations for the first time in V4.1.5.x, after you upgrade your database, use the State Management option in the Revert to Baseline feature to apply the correct State Configuration for the Policy Recommendation Family.</p> <p>When you do so, you will need to provide mappings from the incorrect states to the corresponding correct states, as shown in the following table:</p> <table border="1"> <thead> <tr> <th>Custom (incorrect)</th> <th>Baseline (correct)</th> </tr> </thead> <tbody> <tr> <td>Accepted by ASM</td> <td>Completed</td> </tr> <tr> <td>Closed</td> <td>Completed</td> </tr> <tr> <td>Consolidated</td> <td>Superseded</td> </tr> <tr> <td>Open</td> <td>Proposed</td> </tr> <tr> <td>Pending</td> <td>Pending Approval</td> </tr> <tr> <td>Superseded</td> <td>Superseded</td> </tr> </tbody> </table> | Custom (incorrect) | Baseline (correct) | Accepted by ASM | Completed | Closed | Completed | Consolidated | Superseded | Open | Proposed | Pending | Pending Approval | Superseded | Superseded | <p>This step is necessary because an incorrect baseline State Configuration was delivered for the Policy Recommendation family in V4.1.5.0. The baseline configuration was corrected in V4.1.6.0.</p> <p>The correct baseline state configuration must be applied for various queries and lists in GE Digital APM to function as expected.</p> <p>You do <i>not</i> need to complete this step if:</p> <ul style="list-style-type: none"> You never used V4.1.5.x -or- You never used Policy Recommendations -or- You used Policy Recommendations in a version <i>prior</i> to V4.1.5.x |
| Custom (incorrect) | Baseline (correct) | | | | | | | | | | | | | | | |
| Accepted by ASM | Completed | | | | | | | | | | | | | | | |
| Closed | Completed | | | | | | | | | | | | | | | |
| Consolidated | Superseded | | | | | | | | | | | | | | | |
| Open | Proposed | | | | | | | | | | | | | | | |
| Pending | Pending Approval | | | | | | | | | | | | | | | |
| Superseded | Superseded | | | | | | | | | | | | | | | |

| Step | Task | Notes |
|------|--|--|
| 2 | On the GE Digital APM Server, start or restart the Policy Execution Service. | This step is required. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 3 | If your system architecture contains more than one GE Digital APMServer, you must configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution. | This step is required. |
| 4 | Start or restart the Policy Trigger Service. | This step is required. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 5 | On the GE Digital APM Server, reset IIS. | This step is required. |
| 6 | On the Process Data Integration Server, start (or restart if it is already started) the Meridium Process Data Integration Service. | This step is 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 | Notes |
|------|--|--|
| 1 | On the GE Digital APM Server, start or restart the Policy Execution Service. | This step is required. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 2 | If your system architecture contains more than one GE Digital APMServer, you must configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution. | This step is required. |

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

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

| Step | Task | Notes |
|------|--|--|
| 1 | On the GE Digital APM Server, start or restart the Policy Execution Service. | This step is required. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 2 | If your system architecture contains more than one GE Digital APMServer, you must configure the Policy Trigger Service on each server to specify the name of the load-balanced server cluster that you want to use for policy execution. | This step is required. |
| 3 | Start or restart the Policy Trigger Service. | This step is required. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 4 | On the GE Digital APM Server, reset IIS. | This step is required. |
| 5 | On the Process Data Integration Server, start (or restart if it is already started) the Meridium Process Data Integration Service. | This step is 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 V3.6.0.12.8

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

Upgrade from any version V3.5.1 through V3.5.1.12.1

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

| Step | Task | Notes |
|------|--|--|
| 3 | Start or restart the Policy Trigger Service. | This step is required. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 4 | On the GE Digital APM Server, reset IIS. | This step is required. |
| 5 | On the Process Data Integration Server, start (or restart if it is already started) the Meridium Process Data Integration Service. | This step is 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 V3.5.0.1.10.0

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

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

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

| Step | Task | Notes |
|------|--|--|
| 3 | Start or restart the Policy Trigger Service. | This step is required. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 4 | On the GE Digital APM Server, reset IIS. | This step is required. |
| 5 | On the Process Data Integration Server, start (or restart if it is already started) the Meridium Process Data Integration Service. | This step is 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.

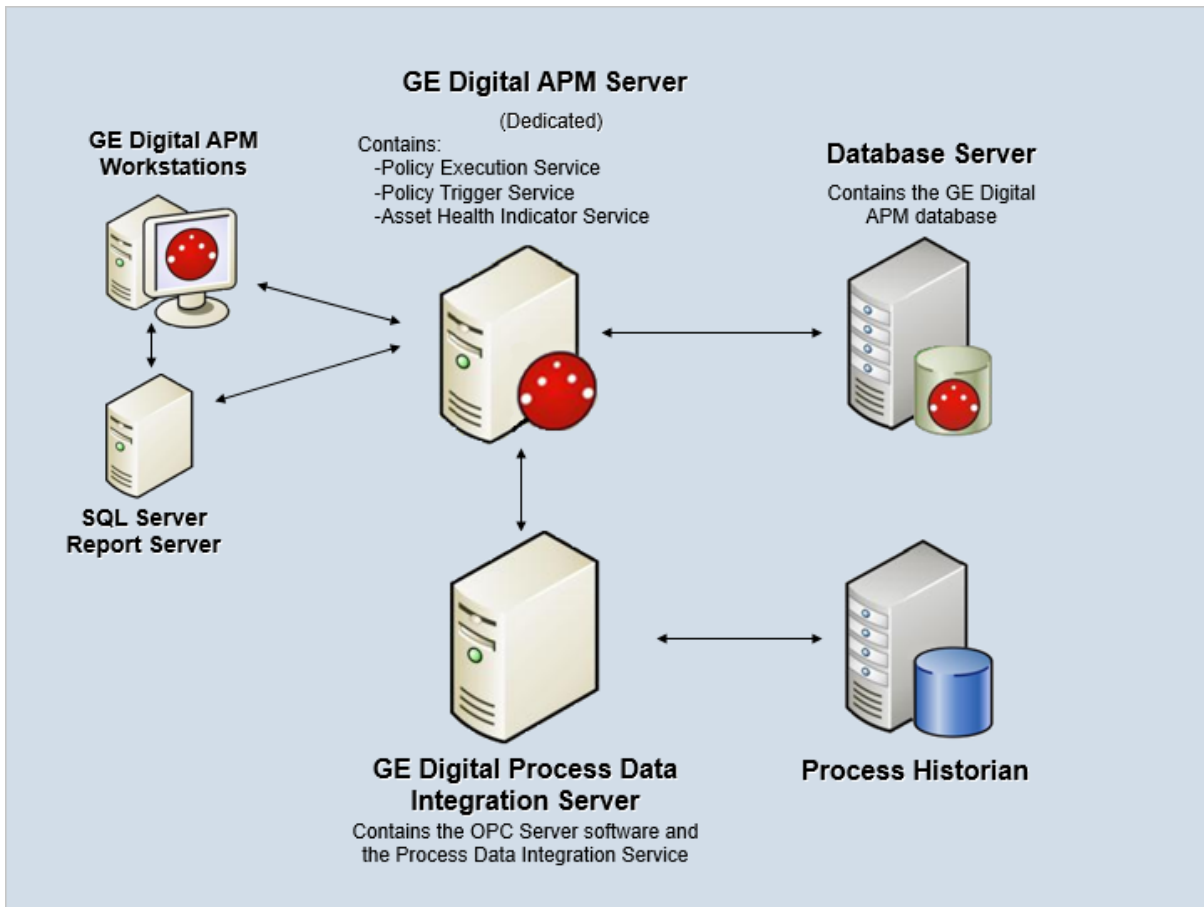
- **Policy Trigger Service:** When an input to a policy (i.e., an associated record in the GE Digital APM database or reading value in the process historian) changes or when a policy schedule is due, a message is added to the policy trigger queue. The Policy Trigger Service monitors this queue and sends these messages to an appropriate policy execution queue.
- **Policy Execution Service:** The Meridium 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 GE Digital APM database) and, when data changes occur on these tags, adds messages to the appropriate queues. This service also facilitates the automatic import and synchronization of tags from a configured process historian.

Example: Standard System Architecture Configuration

The following diagram illustrates the machines in the GE Digital 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 GE Digital APM Servers, [multiple OPC Servers](#), or [multiple GE Digital 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](#), [Process Data Integration](#), and [Policy Designer](#).

| Machine | Software Installed | Asset Health Service Installed Automatically with Service Software |
|-----------------------|--------------------------------|--|
| GE Digital APM Server | GE Digital APM Server software | Asset Health Indicator Service |
| | | Policy Trigger Service |
| | | Policy Execution Service |

| Machine | Software Installed | Asset Health Service Installed Automatically with Service Software |
|--|---|--|
| Process Data Integration Server, which also acts as the OPC Server | Process Data Integration Service software | Process Data Integration Service |
| | OPC Server software | N/A |
| Process Historian | Process historian software | N/A |

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 GE Digital 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 GE Digital 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 GE Digital APM Server in your system architecture, accept the default value (i.e., *localhost*).
 - or-
 - If you have [more than one GE Digital 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 GE Digital APM Servers for Policy Execution

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

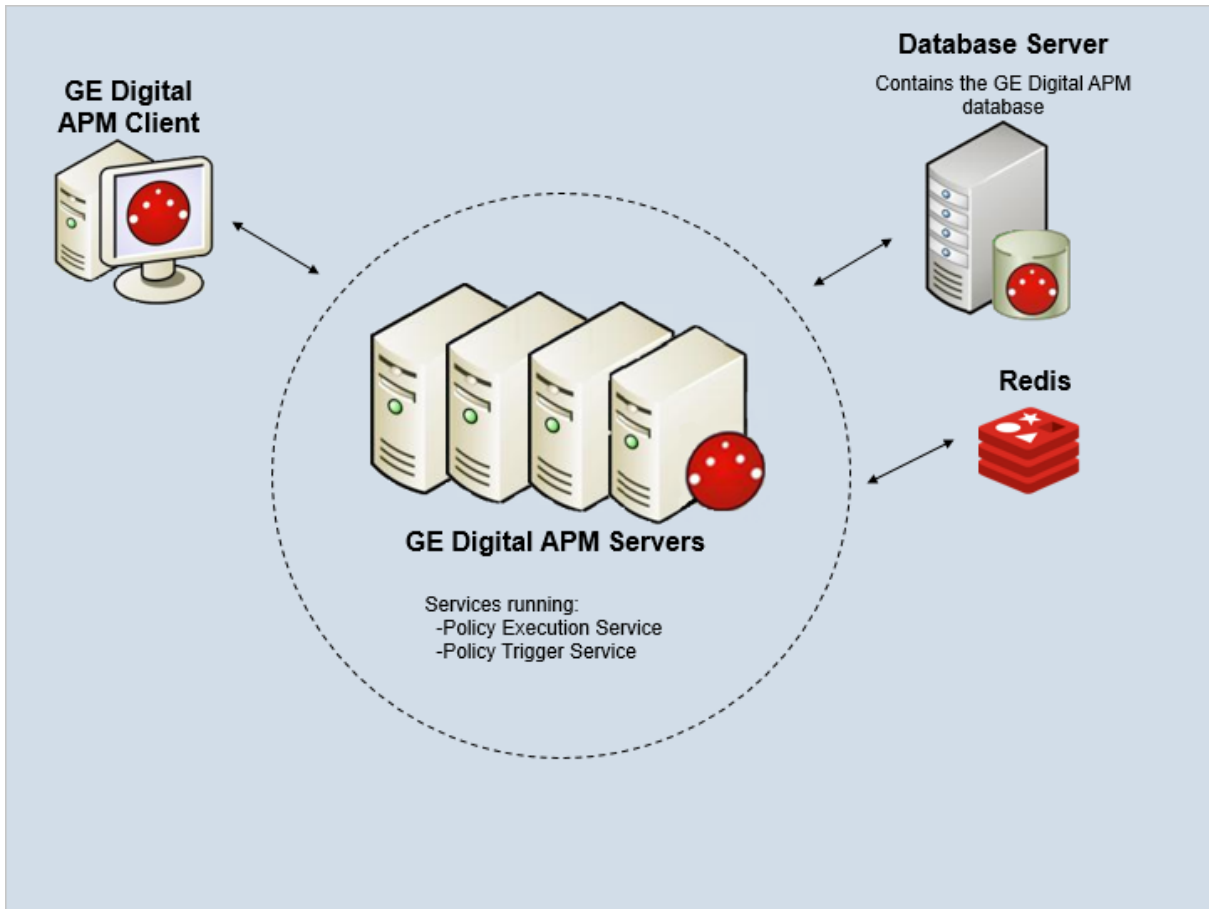
Regardless of the approach you use, you must fully configure each GE Digital APM Server according to the steps for deploying the basic GE Digital APM system architecture. In addition, each GE Digital APM Server must be configured to use the same instance of Redis.

Global Load Balancing

In global load balancing, you configure all GE Digital 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 GE Digital APM Servers to specify the name of the cluster.
- Start the Policy Execution Service on all GE Digital APM Servers.

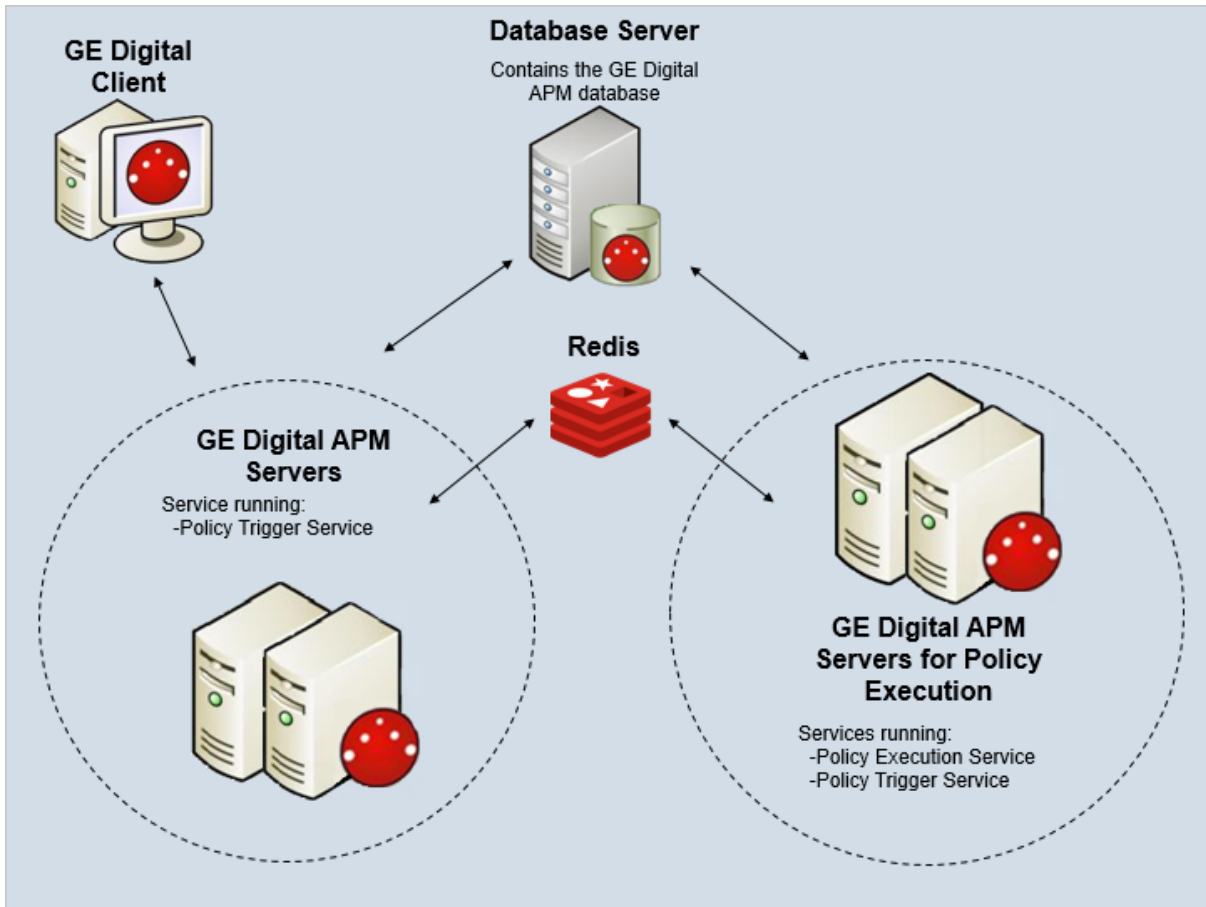


Isolated Load Balancing

In isolated load balancing, you configure designated GE Digital APM Server(s) to process policy executions in a *separate* load-balanced cluster from other GE Digital APM Server(s). In this scenario, the policy execution processes are isolated from the GE Digital 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 GE Digital APM Servers to specify the name of the cluster used for policy executions.
- Start the Policy Execution Service on *only* the GE Digital APM Servers in the cluster designated to process policy executions.



Policy Designer Security Groups and Roles

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

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

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

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

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


Deploy Process Data Integration (PDI)


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

Deploy Process Data Integration (PDI) for the First Time

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

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

 **Note:** This GE Digital APM module is not available in the APM Now environment.

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

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

| Step | Task | Notes |
|------|---|--|
| 6 | On the Process Data Integration Server, modify the Process Data Integration Service configuration file to specify your OPC Server, the GE Digital APM Server, GE Digital APM database, and login credentials. | This step is required. |
| 7 | On the Process Data Integration Server, start the Process Data Integration Service. | This step is required. When you start the service, tags from the configured process historian are imported automatically into the GE Digital APM database as OPC Tag records. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 8 | On the GE Digital APM Server, configure the Meridium Notification Service for PDI. | This step is required. |
| 9 | On the GE Digital APM Server, start or restart the Meridium Notification Service. | This step is required. You may review the log files for this service at C:\ProgramData\Meridium\Logs . |
| 10 | Review the Process Data Integration data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. | This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families. |
| 11 | In GE Digital APM, link OPC Tags to related assets (i.e., equipment and functional locations). | This step is required. |
| 12 | Complete various PDI administrative user tasks as necessary to manage the OPC Tags imported into GE Digital APM. | This step is required. |

Upgrade or Update Process Data Integration (PDI) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

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

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

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

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

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

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

Upgrade from any version V4.0.0.0 through V4.0.1.0

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

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

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

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

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

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

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

Upgrade from any version V3.5.1 through V3.5.1.12.1

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

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

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

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

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

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

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


Upgrade from any version V3.4.5 through V3.4.5.0.1.4

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

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

Process Data Integration Server Roles

The following server roles are configured on the Process Data Integration Server in the GE Digital 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.

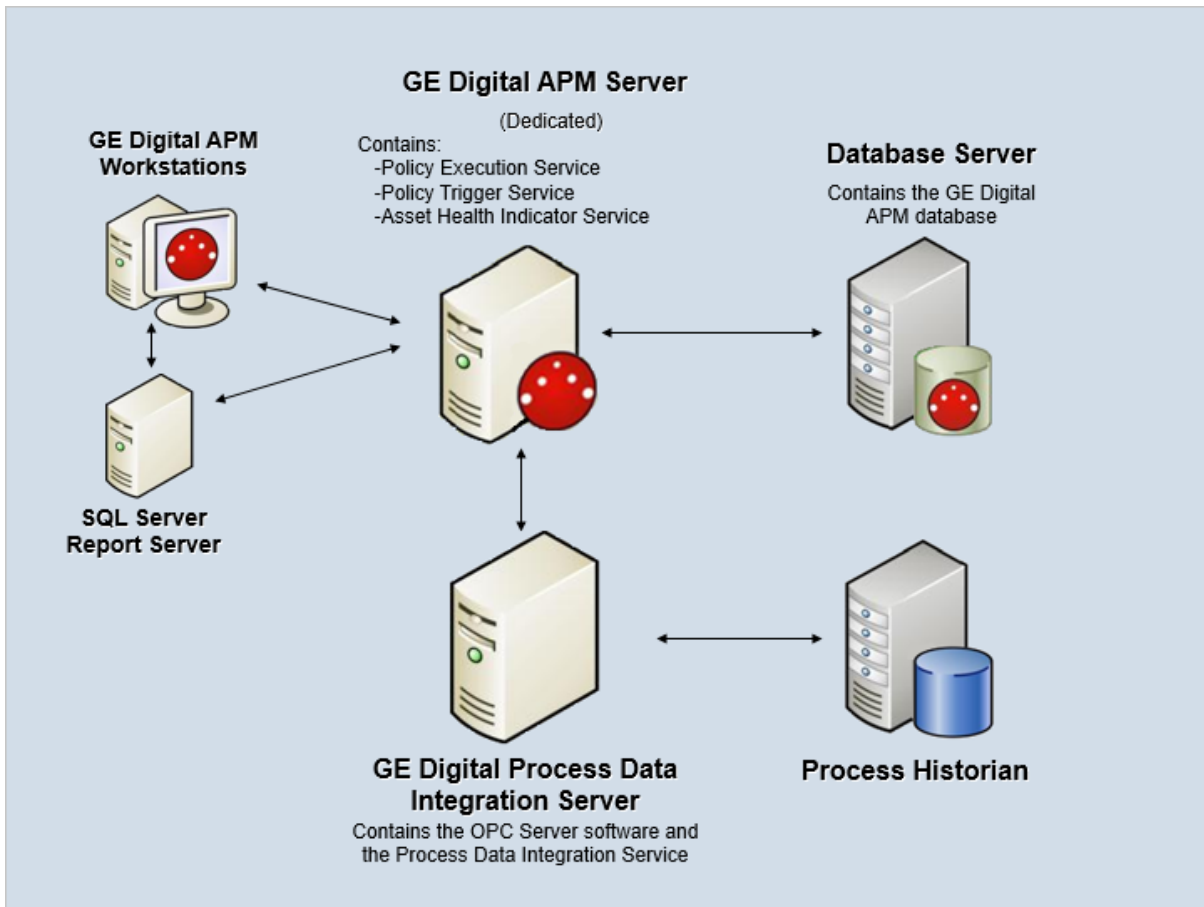
- **Policy Trigger Service:** When an input to a policy (i.e., an associated record in the GE Digital APM database or reading value in the process historian) changes or when a policy schedule is due, a message is added to the policy trigger queue. The Policy Trigger Service monitors this queue and sends these messages to an appropriate policy execution queue.
- **Policy Execution Service:** The Meridium 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 GE Digital APM database) and, when data changes occur on these tags, adds messages to the appropriate queues. This service also facilitates the automatic import and synchronization of tags from a configured process historian.

Example: Standard System Architecture Configuration

The following diagram illustrates the machines in the GE Digital 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 GE Digital APM Servers, [multiple OPC Servers](#), or [multiple GE Digital 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](#), [Process Data Integration](#), and [Policy Designer](#).

| Machine | Software Installed | Asset Health Service Installed Automatically with Service Software |
|-----------------------|--------------------------------|--|
| GE Digital APM Server | GE Digital APM Server software | Asset Health Indicator Service |
| | | Policy Trigger Service |
| | | Policy Execution Service |

| Machine | Software Installed | Asset Health Service Installed Automatically with Service Software |
|--|---|--|
| Process Data Integration Server, which also acts as the OPC Server | Process Data Integration Service software | Process Data Integration Service |
| | OPC Server software | N/A |
| Process Historian | Process historian software | N/A |

Install the Process Data Integration Service

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

Steps

1. On the machine that will serve as the Meridium Process Data Integration Server, access the GE Digital APMM distribution package, and then navigate to the folder **\\Setup\Meridium 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 GE Digital APM System Administration Tool will also be installed automatically.

7. Select **Next**.

GE Digital 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**.

The installation is complete.

What's Next?

- [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

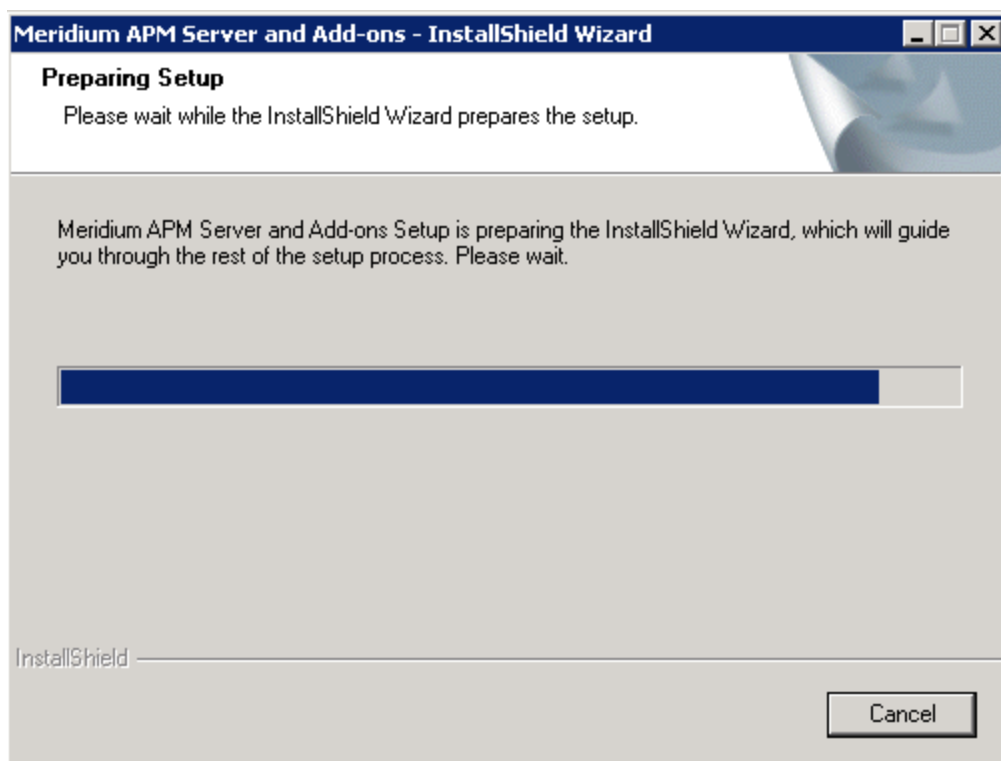
1. On the machine that will serve as the Meridium Process Data Integration Server, access the GE Digital APM distribution package, and then navigate to the folder **\\Setup\Meridium APM Server and Add-ons**.

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 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**.

The upgrade is complete.

What's Next?

- [Refer back to the upgrade checklist.](#)

Configure the Meridium Notification Service for PDI

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 GE Digital APM Server.

Steps

1. On the GE Digital 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" binding="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

To use Process Data Integration, you must configure the Process Data Integration Service by modifying the file *Meridium.PDI.Service.exe.config* on the GE Digital APM 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 GE Digital APM Server. You should ensure that your firewalls are configured to allow this access.

Steps

1. On the GE Digital APM Process Data Integration Server, access the APM System Administration tool.
2. In the **APM System Administration** window, in the **Configuration** section, select 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 GE Digital. We recommend, however, that you contact the third-party distributor of your process historian software to confirm the values that you should use for your system configuration.

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


*In the GE Digital 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, select 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. Select 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 GE Digital APM Server on which the data source specified in the datasource attribute is configured. | None |
| datasource | Replace DATASOURCE_NAME with the name of the GE Digital APMM 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 GE Digital APM Server in the Data Sources section of Operations Manager. |
| userId | Replace SERVICE_USER_NAME with the User ID of the Security User whose credentials should be used to log in to the specified GE Digital APM database. | The user you specify should be a member of the MI Process Data Integration Service Security Group. |

| Within this attribute... | Make this change | Notes |
|--------------------------|---|--|
| password | Replace PaSsWoRd with the password for the specified user. | <p>Do not delete the ! in front of the password. This symbol is not part of the password itself. Instead, this symbol will cause the password to be encrypted automatically when the service is restarted.</p> <div style="border: 1px solid red; padding: 5px;"> <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 System 1 with the value that exists in the OPC System ID field in an OPC System record in the GE Digital 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 GE Digital 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 GE Digital 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.

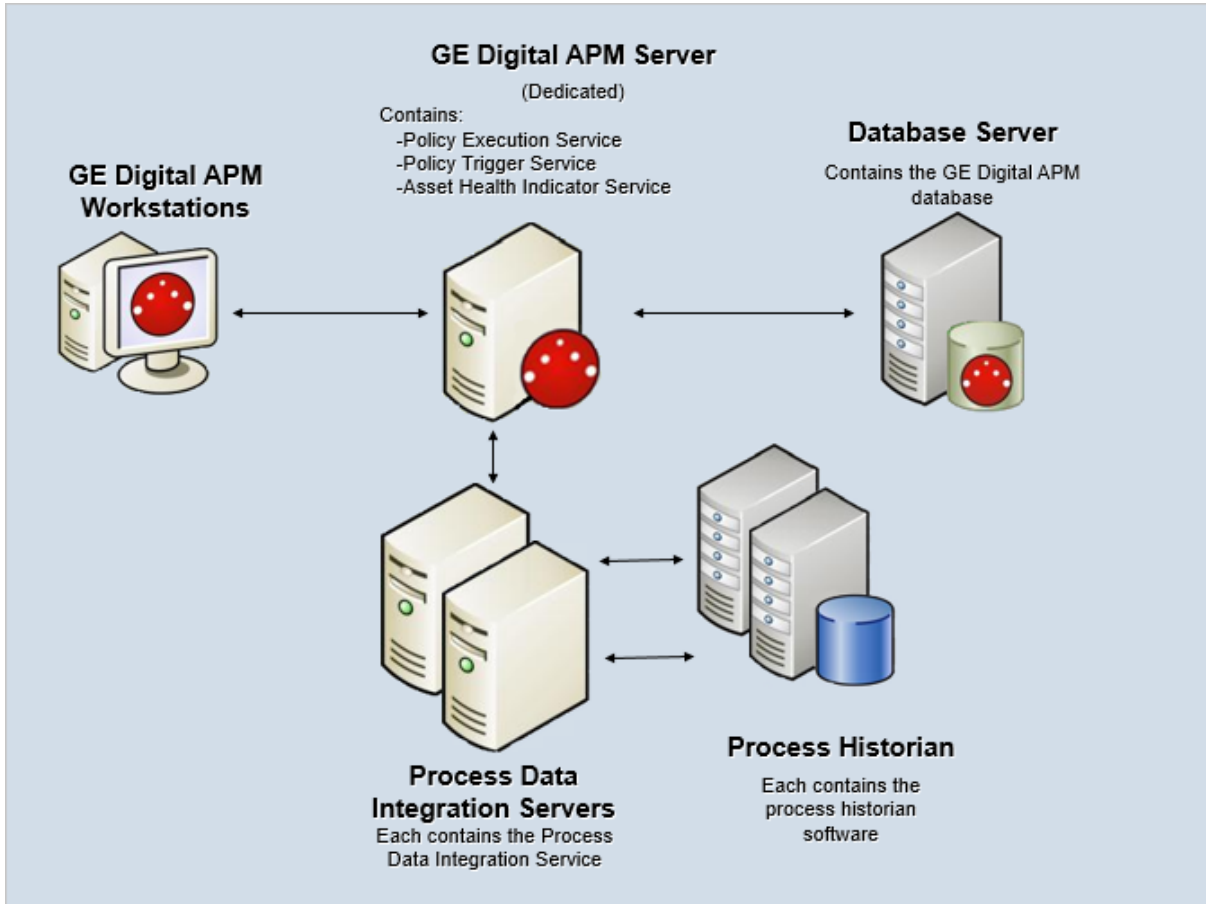
 **Note:** The connection name that you specify in each connection string must be unique.

5. Repeat these steps for each required connection.

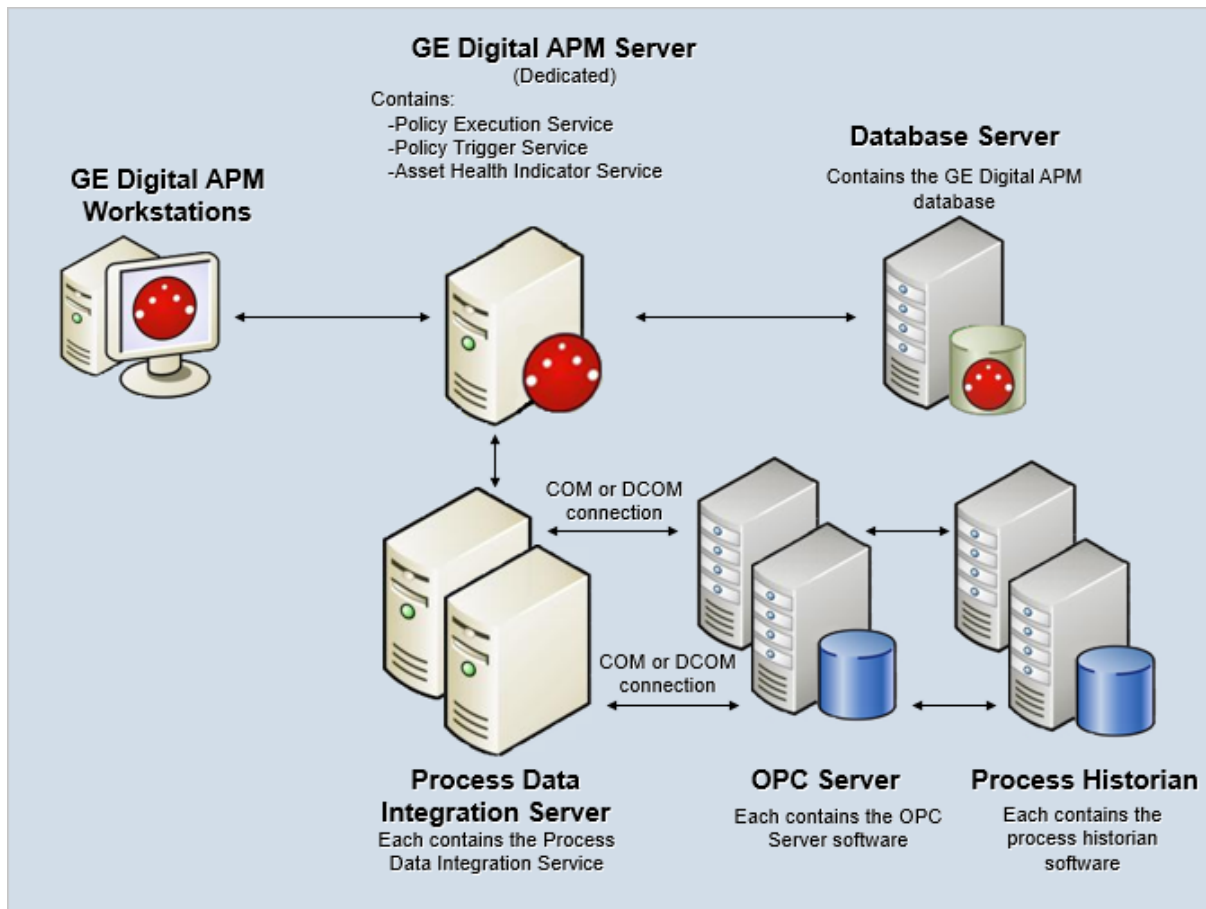
Configure Multiple Process Data Integration and OPC Servers

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 GE Digital APM application, you will create an OPC System record for each OPC Server (e.g., OPCServer1 and OPCServer2). Then, when you [configure the Process Data Integration Service](#), you must specify the appropriate OPC Server record in the **xiServers** attribute within the **meridumConnections** tags. For example, the connection string on each machine might look like this:

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

Process Data Integration Security Groups and Roles

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

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

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

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

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

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

Deploy Production Loss Analysis (PLA)

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

Deploy Production Loss Analysis (PLA) for the First Time

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

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

Note: If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

| Step | Task | Notes |
|------|---|--|
| 1 | Review the PLA data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed. | This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families. |
| 2 | Assign Security Users to one or more of the Production Loss Analysis Security Groups and Roles . | This step is required. Users must have permissions to the PLA families to use the PLA functionality. |
| 3 | Change the default currency symbol . Change the default currency symbol. | This step is optional. By default, the currency symbol is set to \$ and displayed in the following places: <ul style="list-style-type: none"> • Default Margin field on the Production Profile data-sheet. • Production Summary workspace. |

| Step | Task | Notes |
|------|-----------------------------|---|
| 4 | Define all products. | <p>This step 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.</p> |
| 5 | Define Production Units. | <p>This step is required. You must identify the Production Units that produce the products you defined in the previous task. A single product can be produced by more than one Production Unit. A single Production Unit can also produce more than one product.</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 step is required. For each Production Unit that you defined in the previous step, you must identify all the products that it produces and information about those products, such as the maximum demonstrated rate of production and the amount of profit one of those products yields. The combination of data about a product and the corresponding Production Unit is the Production Profile for that Production Unit. A Production Unit will have one Production Profile for each product it produces.</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 GE Digital 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 GE Digital 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> |
| 9 | Define OEE Codes. | <p>The baseline GE Digital 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.</p> |
| 10 | Define values that will be mapped to a Production Analysis. | <p>This step is optional. By default, certain PLA values are mapped to the production data in a Production Analysis. If you want to map different or additional PLA values, you can do so by modifying the All Production Data query.</p> |

| Step | Task | Notes |
|------|---|---|
| 11 | <p>Configure PLA for PDI integration:</p> <ul style="list-style-type: none"> • Link Production Profile records to OPC Tag records. | <p>This step is required if you want to use the integration between PLA and the Process Data Integration feature where Production Data records are created automatically.</p> |
| 12 | <p>Replace the Top 10 Bad Actors query for the PLA Overview page.</p> | <p>This step is optional. The Top 10 Bad Actors query is used by GE Digital 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.</p> |

Upgrade or Update Production Loss Analysis (PLA) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.


Upgrade from any version V4.1.0.0 through V4.1.7.4.0

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

Upgrade from any version V4.0.0.0 through V4.0.1.0


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

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1


| Step | Task | Notes |
|------|---|--|
| 1 | Confirm the deployment of the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server. | This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server in V3.6.0.0.0. |
| 2 | Set the timezones for the Production Units. | <p>This step is required. If the timezones for the Production Units are set, all the Production Plan records, Plan Data records, and Production Target records will be updated based on the timezone for the respective Production Unit.</p> <div style="border: 1px solid yellow; padding: 5px;"> <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, then the Production Plan records, Plan Data records, and Production Target records will be updated based on the timezone of the user who last modified the Production Plan record. • If you do not set the timezones for the Production Units, and if the Production Plan records do not exist in the database, then the timezone for the Production Unit will be updated based on the timezone of the user who last modified the Production Unit record. </div> |

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

| Step | Task | Notes |
|------|---|--|
| 1 | Confirm the deployment of the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server. | This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server in V3.6.0.0.0. |

| Step | Task | Notes |
|------|---|--|
| 2 | Set the timezones for the Production Units. | <p>This step is required. If the timezones for the Production Units are set, all the Production Plan records, Plan Data records, and Production Target records will be updated based on the timezone for the respective Production Unit.</p> <div style="border: 1px solid yellow; padding: 5px;"> <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, then the Production Plan records, Plan Data records, and Production Target records will be updated based on the timezone of the user who last modified the Production Plan record. • If you do not set the timezones for the Production Units, and if the Production Plan records do not exist in the database, then the timezone for the Production Unit will be updated based on the timezone of the user who last modified the Production Unit record. </div> |

Upgrade from any version V3.5.1 through V3.5.1.12.1

| Step | Task | Notes |
|------|--|---|
| 1 | On the GE Digital APM Server, import the required baseline rules . | <div style="border: 1px solid red; padding: 5px;"> <p> IMPORTANT: This step is required and must be completed <i>before</i> upgrading the GE Digital APM Server and Add Ons software on the GE Digital APM(s). After completing this step, you should return to the upgrade GE Digital APM workflow. Then, after completing the remainder of the upgrade GE Digital APM workflow, when you are ready to upgrade PLA, proceed to step 2 in this workflow.</p> </div> |

| Step | Task | Notes |
|------|---|--|
| 2 | Confirm the deployment of the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server. | This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server in V3.5.1. |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

| Step | Task | Notes |
|------|---|--|
| 1 | On the GE Digital APM Server, import the required baseline rules . | ⚠ IMPORTANT: This step is required and must be completed <i>before</i> upgrading the GE Digital APM Server and Add Ons software on the GE Digital APM(s). After completing this step, you should return to the upgrade GE Digital APM workflow. Then, after completing the remainder of the upgrade GE Digital APM workflow, when you are ready to upgrade PLA, proceed to step 2 in this workflow. |
| 2 | Confirm the deployment of the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server. | This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server in V3.5.0. SP1 LP. |

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

| Step | Task | Notes |
|------|---|--|
| 1 | On the GE Digital APM Server, import the required baseline rules . | ⚠ IMPORTANT: This step is required and must be completed <i>before</i> upgrading the GE Digital APM Server and Add Ons software on the GE Digital APM(s). After completing this step, you should return to the upgrade GE Digital APM workflow. Then, after completing the remainder of the upgrade GE Digital APM workflow, when you are ready to upgrade PLA, proceed to step 2 in this workflow. |
| 2 | Confirm the deployment of the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server. | This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server in V3.5.0. |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Notes |
|------|--|--|
| 1 | On the GE Digital APM Server, import the required baseline rules . | ⚠ IMPORTANT: This step is required and must be completed <i>before</i> upgrading the GE Digital APM Server and Add Ons software on the GE Digital APM(s). After completing this step, you should return to the upgrade GE Digital APM workflow. Then, after completing the remainder of the upgrade GE Digital APM workflow, when you are ready to upgrade PLA, proceed to step 2 in this workflow. |
| 2 | Define OEE codes | This step is required only if you want to use custom OEE Code records instead of or in addition to the baseline OEE Code records that are provided in the GE Digital APM database. If you do, you will need to create custom OEE codes to identify the types of losses you can incur. Each OEE code will be stored in an OEE Code record. |
| 3 | Define values that will be mapped to a Production Analysis | By default, certain PLA values are mapped to the production data in a Production Analysis. This step is required only if you want to map different or additional PLA values. If you do, you will need to modify the All Production Data query. |

| Step | Task | Notes |
|------|---|--|
| 4 | Confirm the deployment of the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server. | This step is required only if you did not deploy the Production Data cube and Equipment Costs Data cube on the SQL Server Analysis Server in V3.4.5. |

Import Baseline Rules

Note: If you are upgrading Production Loss Analysis from a starting version that is earlier than V3.6.0.0.0, this procedure must be completed *before* upgrading the Meridium Enterprise APM Server and Add Ons software on the Meridium Enterprise APM Server(s). This procedure is part of the upgrade Meridium Enterprise APM and [upgrade Production Loss Analysis](#) workflows.

Before You Begin

- Acquire a copy of the baseline GE Digital 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 GE Digital Professional Services department.

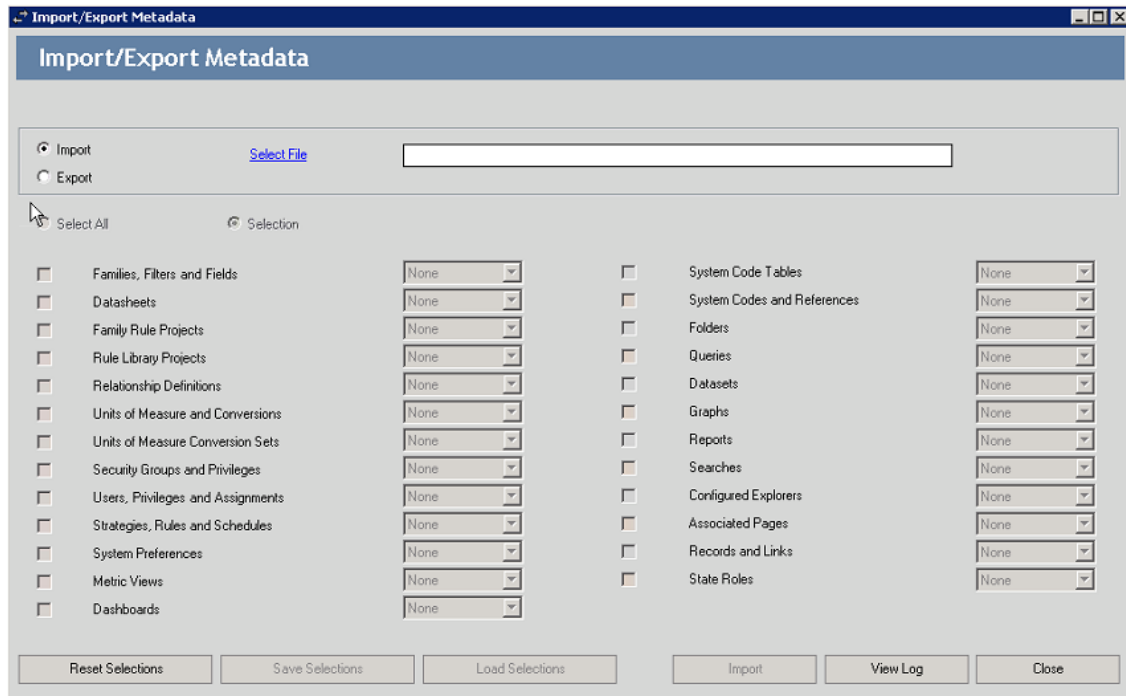
Steps

1. On the GE Digital APM Server, via the Windows start button, access Configuration Manager.

The **Meridium APM Login** window appears.

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

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



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

The **Save As** window appears.

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

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

Deploy Modules and Features

Import/Export Metadata

Import [Select File](#)

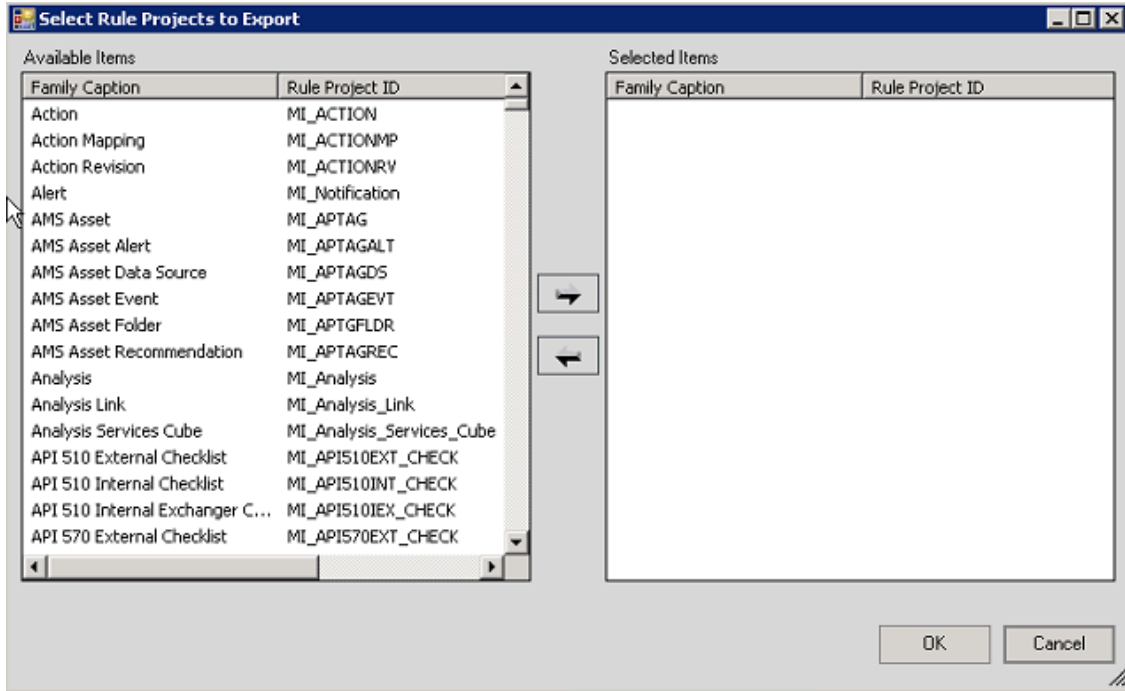
Export


Select All Selection Include underlying Query/Dataset for Reports and Graphs

| | | | |
|--|------|--|------|
| <input type="checkbox"/> Families, Filters and Fields | None | <input type="checkbox"/> System Code Tables | None |
| <input type="checkbox"/> Datasheets | None | <input type="checkbox"/> System Codes and References | None |
| <input type="checkbox"/> Family Rule Projects | None | <input type="checkbox"/> Folders | None |
| <input type="checkbox"/> Rule Library Projects | None | <input type="checkbox"/> Queries | None |
| <input type="checkbox"/> Relationship Definitions | None | <input type="checkbox"/> Datasets | None |
| <input type="checkbox"/> Units of Measure and Conversions | None | <input type="checkbox"/> Graphs | None |
| <input type="checkbox"/> Units of Measure Conversion Sets | None | <input type="checkbox"/> Reports | None |
| <input type="checkbox"/> Security Groups and Privileges | None | <input type="checkbox"/> Searches | None |
| <input type="checkbox"/> Users, Privileges and Assignments | None | <input type="checkbox"/> Configured Explorers | None |
| <input type="checkbox"/> Strategies, Rules and Schedules | None | <input type="checkbox"/> Associated Pages | None |
| <input type="checkbox"/> System Preferences | None | <input type="checkbox"/> Records and Links | None |
| <input type="checkbox"/> Metric Views | None | <input type="checkbox"/> State Roles | None |
| <input type="checkbox"/> Dashboards | None | | |


Reset Selections Save Selections Load Selections Export View Log Close

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

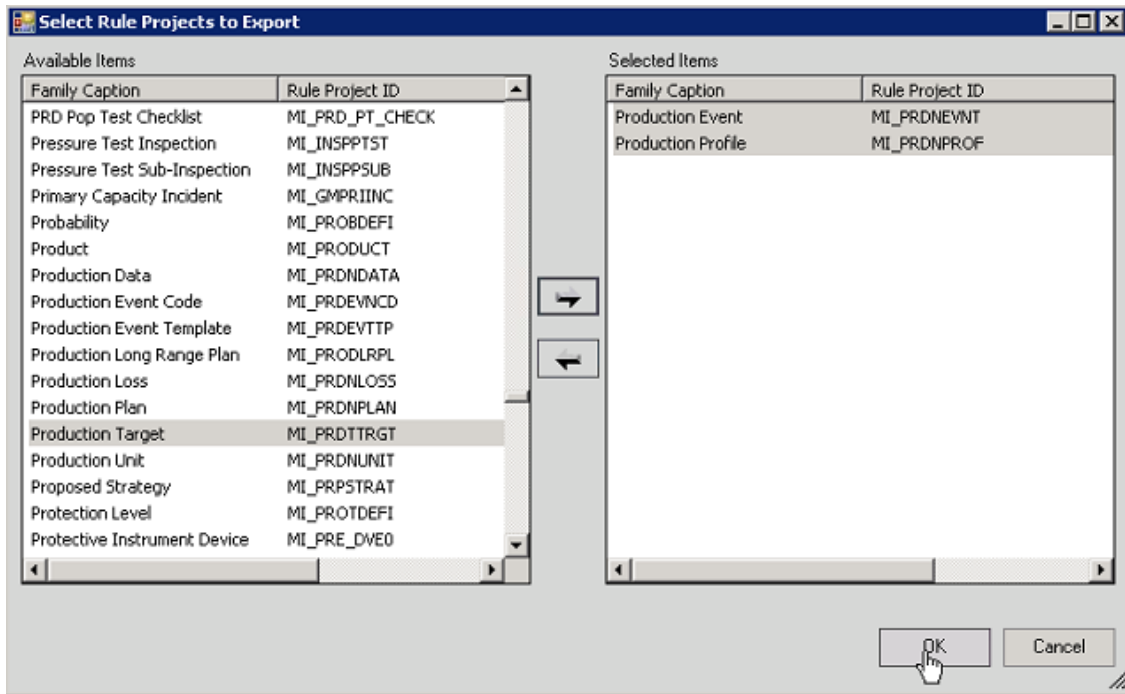


9. In the **Available Items** section, select the item whose Family Caption is Production Event, and then select .

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

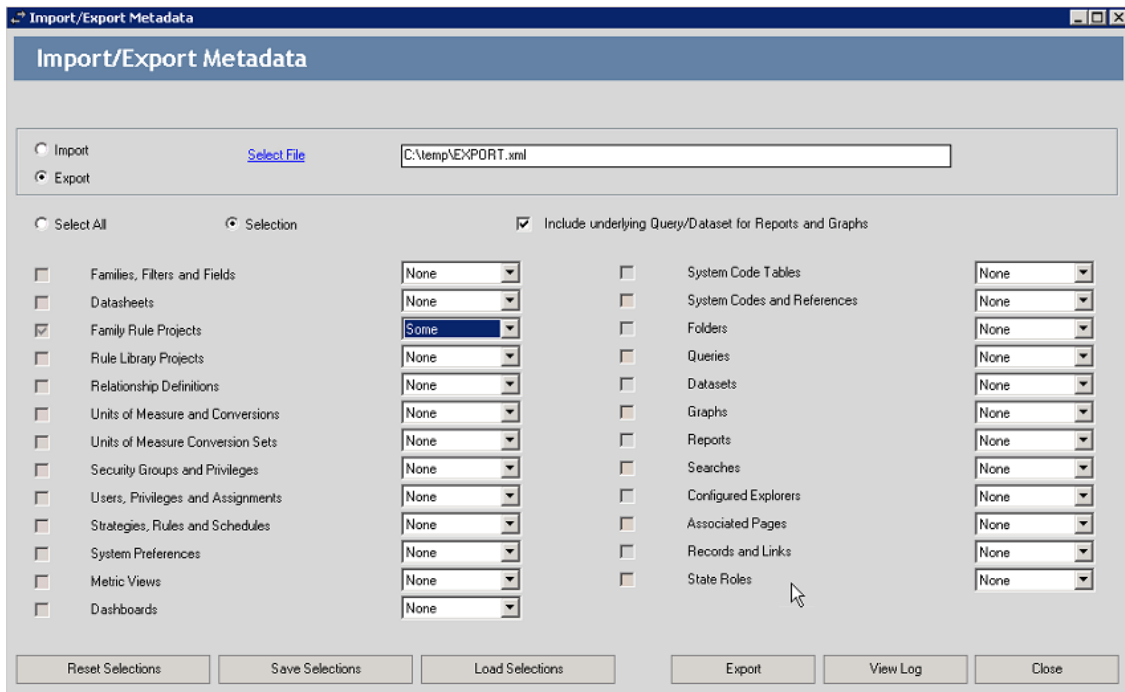
10. In the **Available Items** section, select the item whose Family Caption is Production Profile, and then select .

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



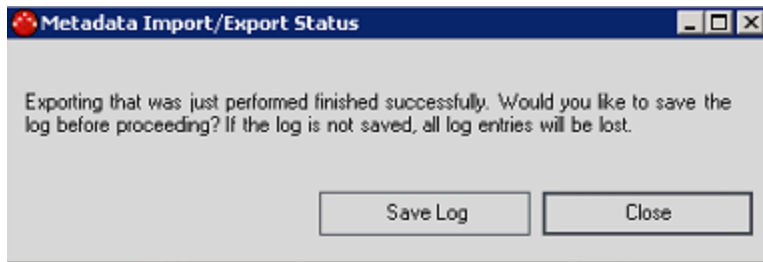
11. Select OK.

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



12. Select **Export**.

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



13. Select **Save Log**.

The **Save As** window appears.

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

The **Save As** window closes.

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

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

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

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

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

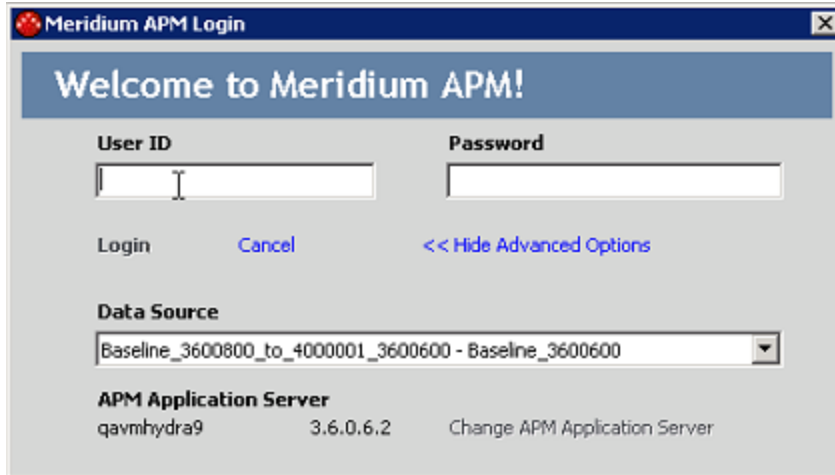
A dialog box appears, asking if you are sure that you want to log off.

18. Select **OK**.

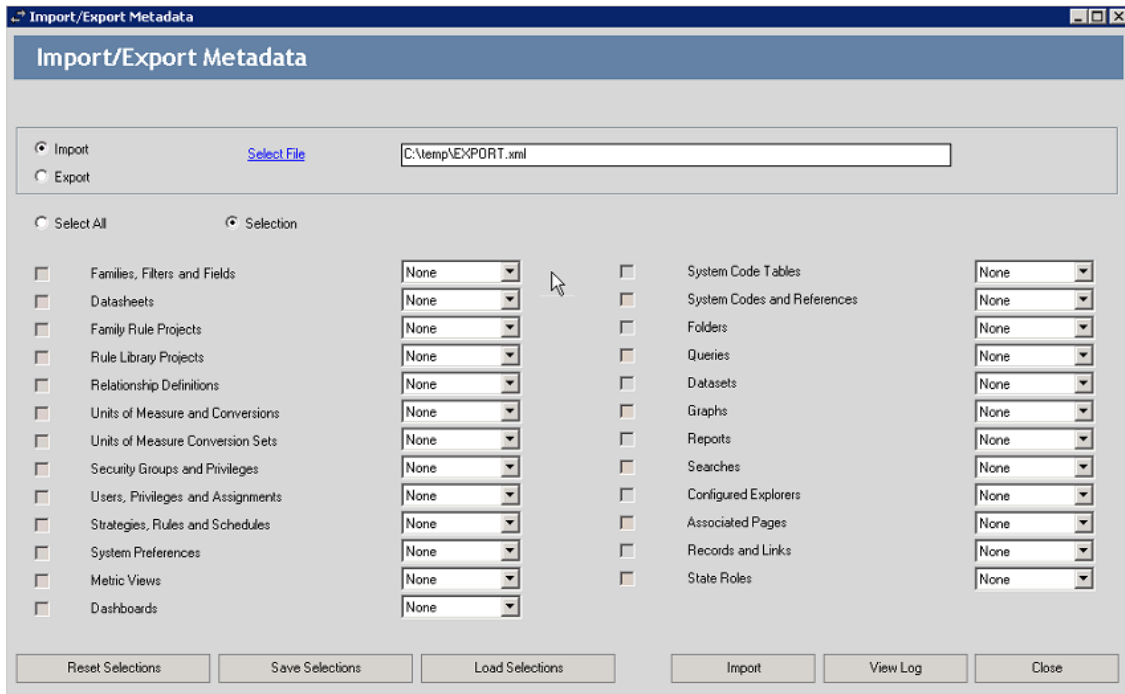
Configuration Manager closes.

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

The **Meridium APM Login** window appears.

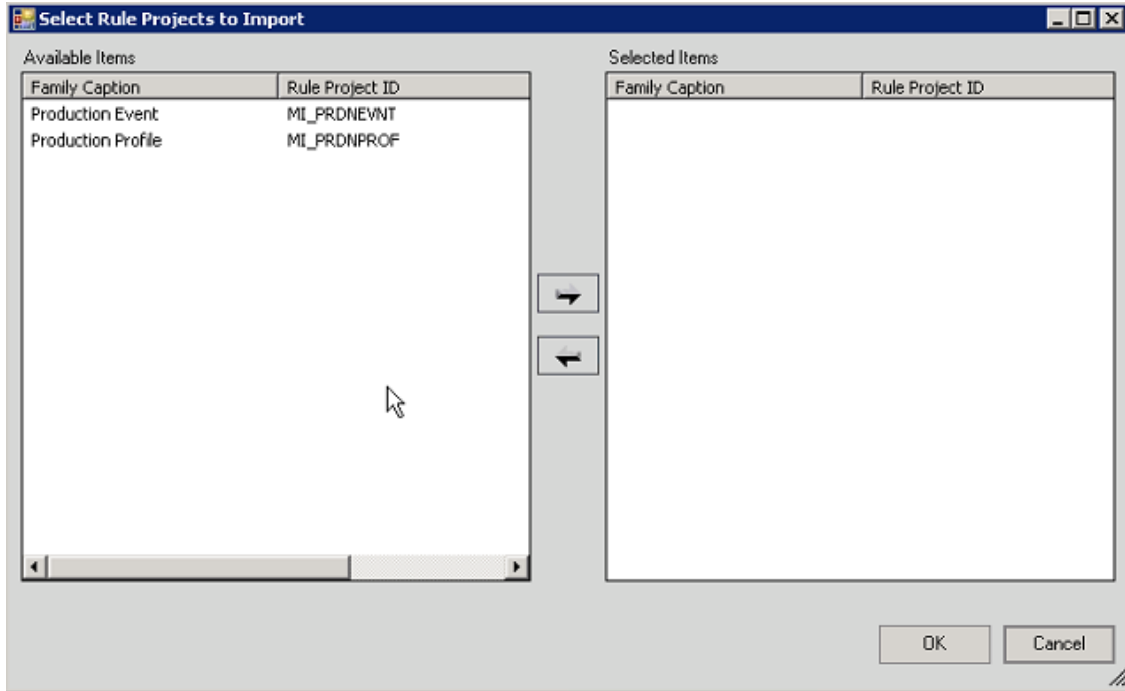



20. Enter your User ID and Password into the appropriate boxes, and then, in the **Data Source** box, select your current, pre-upgraded database.
21. Select **Login**.
Configuration Manager opens.
22. On the top navigation bar, select **Tools**, and then select **Import/Export Meridium Metadata**.
The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




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

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

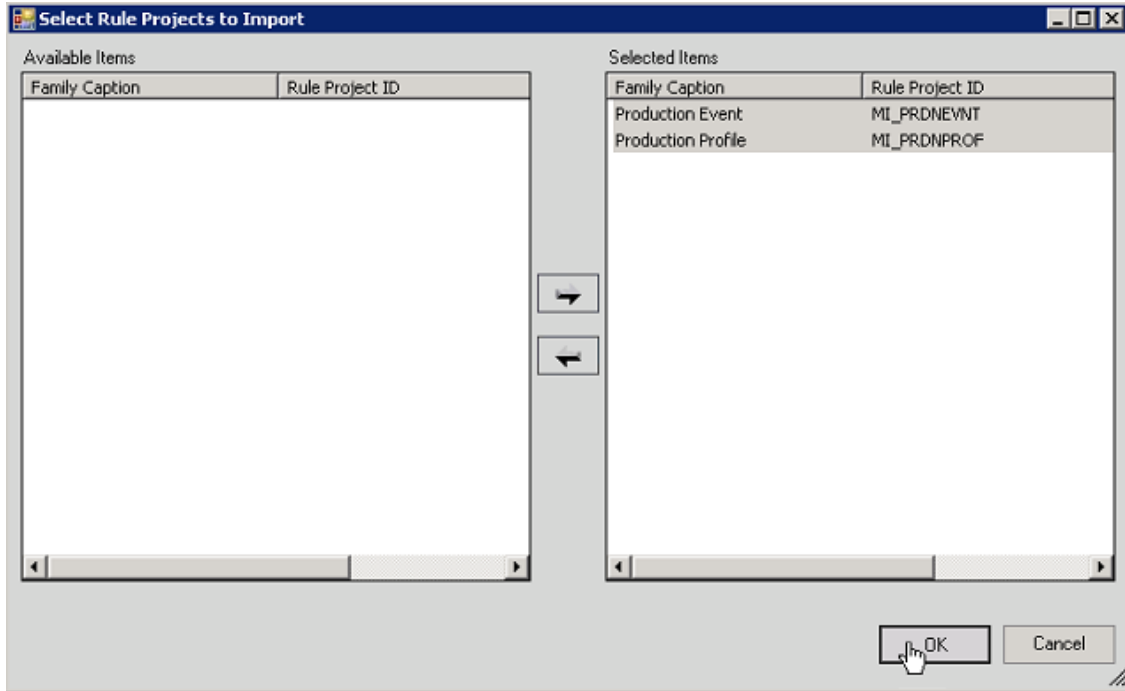


27. In the **Available Items** section, select the item whose Family Caption is Production Event, and then select .

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

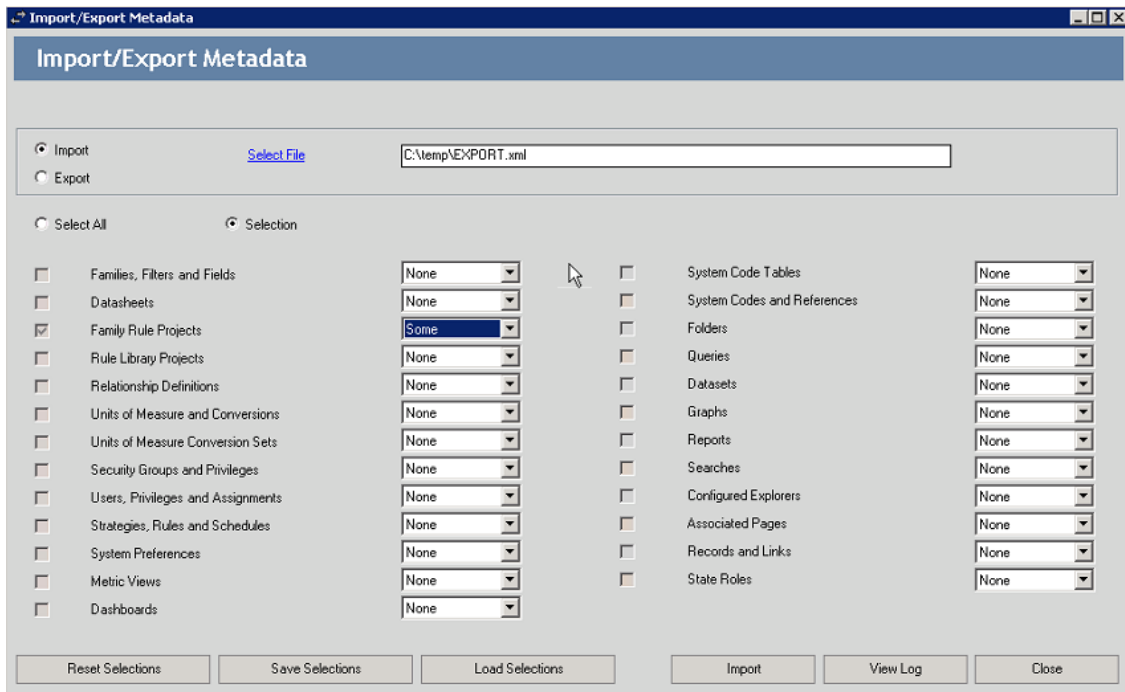
28. In the **Available Items** section, select the item whose Family Caption is Production Profile, and then select .

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



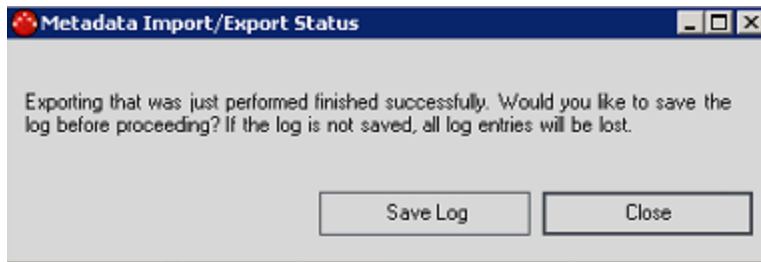
29. Select OK.

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



30. Select **Import**.

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



31. Select **Save Log**.

The **Save As** window appears.

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

The **Save As** window closes.

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

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

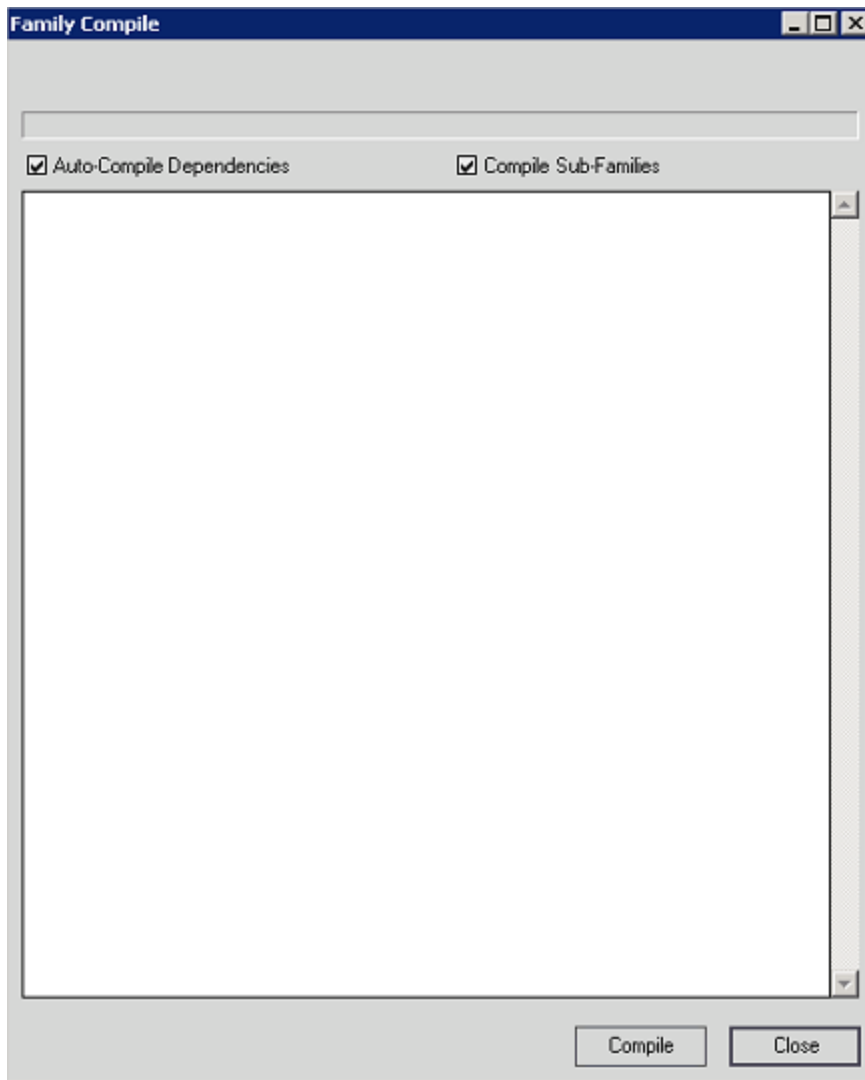
34. On the **Import/Export Metadata** window, select **Close**.

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

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

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

The **Family Compile** window appears.



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

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


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

The **Family Compile** window closes.

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

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

Replace the Top 10 Bad Actors Query

 **Note:** The steps in this section are required only if you are upgrading from a version of Meridium Enterprise APM between V4.0.0.0 and V4.1.7.4.0.

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

Errors ×

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

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

Steps

1. Access the **Query** page .
2. In the heading of the **Query** page, select **Browse**.
The **Select a query from the catalog** window appears.

Select a query from the catalog

| Name | Caption |
|---------------------------------------|---------------------------------------|
| AllProductionEvents | AllProductionEvents |
| EventList | EventList |
| EventList for the given unit | EventList for the given unit |
| Get Production Event | Get Production Event |
| GetDifferenceFromOriginalToFilterData | GetDifferenceFromOriginalToFilterData |
| GetEventCodeForGivenUnit | GetEventCodeForGivenUnit |
| GetEventKeyAssociatedLossAmount | GetEventKeyAssociatedLossAmount |
| GetEventOtherCostWithLossAmount | GetEventOtherCostWithLossAmount |
| GetMaxProductionDataEndDateByEventKey | GetMaxProductionDataEndDateByEventKey |
| GetProductionDataCountByEventDates | GetProductionDataCountByEventDates |
| GetProductionDataCountByEventKey | GetProductionDataCountByEventKey |
| GetProductionEventCode | GetProductionEventCode |
| GetProductionEventCodeByUnitKey | GetProductionEventCodeByUnitKey |

Open Cancel

- 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

Period


Asset Hierarchy

Home 

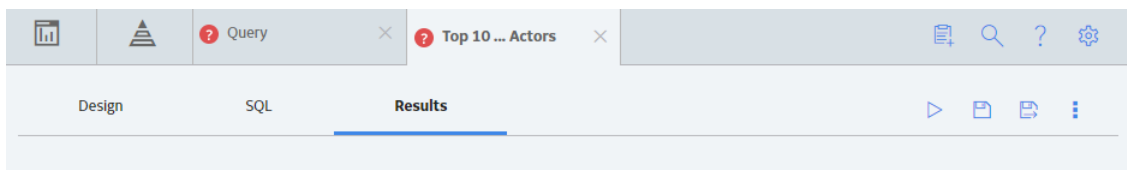
Cancel

Done

4. Select OK.

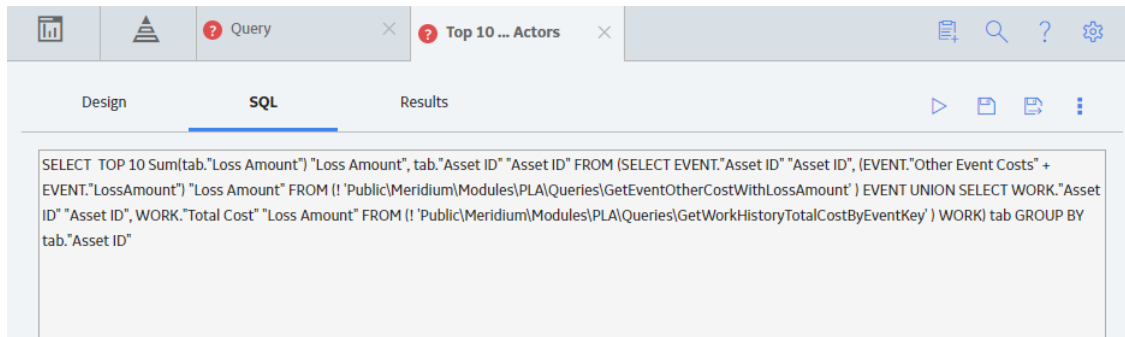
 **Note:** For the purposes of these instructions, you do not need to complete any fields in the **Enter Parameter Values** window.

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_FNCLOC000].[MI_FNCLOC000_FNC_LOC_C]
"AssetID" FROM [MI_FNCLOC000], [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_FNCLOC000].ENTY_KEY =
[MI_PRDNEVNT].[MI_PRDNEVNT_CAUSE_EQP_KEY_N]) and [MI_FNCLOC000].[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.

Related Information

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 APM Viewer |
| MI Production Loss Accounting Service | MI FE Admin |
| MI Production Loss Accounting User | MI FE Admin MI FE PowerUser MI FE User |

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

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

| 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 |
| Relationship Families | | | | |

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

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

Related Information


Deploy R Scripts

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

Deploy R Scripts for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

| Step | Task | Notes |
|------|---|------------------------|
| 1 | Ensure that your R Server is configured according to the R Scripts system requirements. | This step is required. |
| 2 | In GE Digital APM, specify the R Server credentials. | This step is required. |

Upgrade or Update R Scripts to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

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

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

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

Upgrade from any version V4.0.0.0 through V4.0.1.0

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

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1


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

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

| Step | Task | 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 . | This step is required only if you are upgrading from V3.6.0.8.0. This step is not required if you are upgrading from any V3.x version that is covered by this section. |
| 2. | Ensure that your R Server is configured according to the R scripts system requirements. | This step is required. |
| 3. | In GE Digital APM, specify the R Server credentials. | This step is required. |

Upgrade R Script Metadata

If you are upgrading *directly* from V3.6.0.8.0, after upgrading your database to V4.3.0.2.0, 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 GE Digital.

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.

The R script metadata is upgraded.


Deploy Recommendation Management

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

Deploy Recommendation Management for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

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

Upgrade or Update Recommendation Management to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital 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 V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital 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 V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Recommendation Management Security Groups and Roles

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

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

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

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

| Family | MI Recommendation Management User |
|------------------------------|-----------------------------------|
| Entity Families | |
| Action | View |
| Equipment | View |
| Hazards Analysis Consequence | View |
| Instrumented Function | View |
| Protective Instrument Loop | View |
| RCA Analysis | View |
| RCA Team Member | View |
| RCM FMEA Analysis | View |
| Recommendation | View, Update, Insert, Delete |
| SIS Proof Test | View |
| SIS Proof Test Template | View |

| Family | MI Recommendation Management User |
|-----------------------------------|-----------------------------------|
| Relationship Families | |
| Has Asset Strategy | View, Update, Insert, Delete |
| Has Associated Recommendation | View, Update, Insert, Delete |
| Has Consolidated Recommendations | View, Update, Insert, Delete |
| Has Driving Recommendation | View, Update, Insert, Delete |
| Has Recommendations | View, Update, Insert, Delete |
| Has RCM FMEA Recommendation | View, Update, Insert, Delete |
| Has Strategy | View, Update, Insert, Delete |
| Has Superseded Recommendations | View, Update, Insert, Delete |
| Is RCM FMEA Asset | View, Update, Insert, Delete |
| Production Event Has RCA Analysis | View |
| RCA Analysis Relationships | View |


Deploy Reliability Analytics

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

Deploy Reliability Analytics for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

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

Upgrade or Update Reliability Analytics to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital 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 V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.1

Reliability Analytics will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

Reliability Analytics will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Notes |
|------|---|---|
| 1 | Configure the ability for users to create Reliability Distribution and Reliability Growth Analyses from Associated Pages. | This step is optional. This feature is new in V3.5.0, so even if you have deployed Reliability Analytics in V3.4.5, you will not have completed this step. You need to complete this step, however, only if you want to implement this functionality. |

Reliability Analytics Security Groups and Roles

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

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

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

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

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

| Family | MI Reliability Administrator | MI Reliability User | MI Reliability Viewer |
|------------------------------|------------------------------|------------------------------|-----------------------|
| Normal | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| 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 |

| Family | MI Reliability Administrator | MI Reliability User | MI Reliability Viewer |
|---------------------------------|------------------------------|------------------------------|-----------------------|
| System Analysis | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| 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 |

| Family | MI Reliability Administrator | MI Reliability User | MI Reliability Viewer |
|----------------------------------|------------------------------|------------------------------|-----------------------|
| System Sensor | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| 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 |

| Family | MI Reliability Administrator | MI Reliability User | MI Reliability Viewer |
|-------------------------------|------------------------------|------------------------------|-----------------------|
| Has System Actions | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| 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 |

Related Information


Deploy Reliability Centered Maintenance (RCM)

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

Deploy Reliability Centered Maintenance (RCM) for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

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

Upgrade or Update Reliability Centered Maintenance (RCM) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

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

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital 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 V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

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

Reliability Centered Maintenance (RCM) Security Groups and Roles

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

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

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

Associating RCM Analyses with a Specific Site


Some companies that use the GE Digital 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 GE Digital 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 |
| RCM FMEA Template | View, Update, Insert, Delete | View |
| RCM FMEA Task | View, Update, Insert, Delete | View |

| Family Caption | MI RCM User | MI RCM Viewer |
|---|------------------------------|---------------|
| 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 style="border: 1px solid yellow; padding: 5px;">  Note: The Task History relationship family is inactive in the baseline GE Digital 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 |
| Has RCM Functional Failure | View, Update, Insert, Delete | View |
| Has RCM FMEA Failure Mode | View, Update, Insert, Delete | View |

| Family Caption | MI RCM User | MI RCM Viewer |
|---|------------------------------|---------------|
| 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 |
| <div style="border: 1px solid black; padding: 5px; background-color: #ffffcc;">  Note: The Has Task History relationship family is inactive in the baseline GE Digital APM database. </div> | | |
| 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.


Deploy Reports

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

Deploy Reports for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

| Step | Task | Notes |
|------|--|------------------------|
| 1 | | This step is required. |
| 2 | Set up the Reports Designer. | This step is required. |

Upgrade or Update Reports to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital 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 V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital 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 V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Install the APM Reports Designer

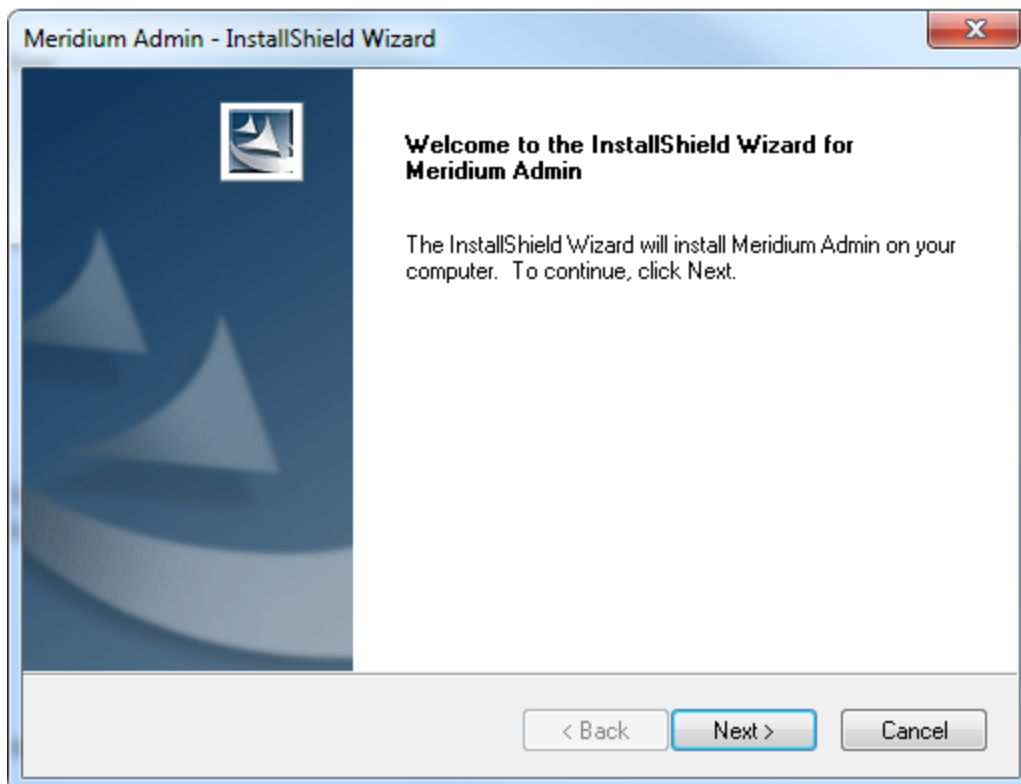
Before You Begin

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

Steps

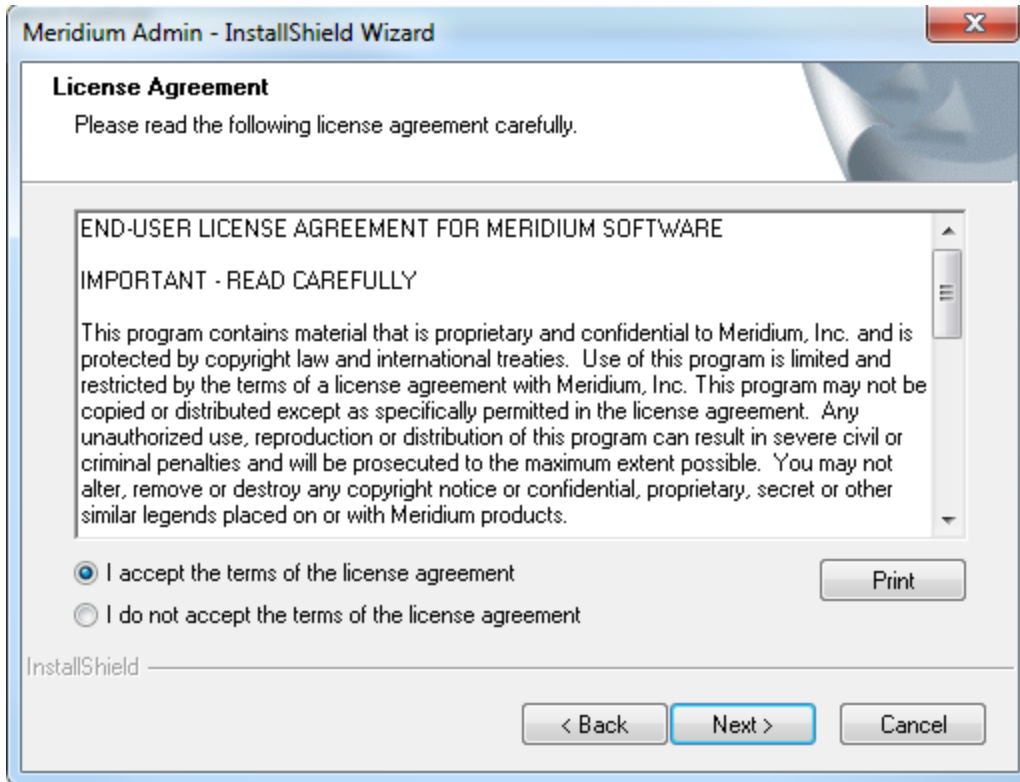
1. On the machine that will serve as the APM Reports Designer, access the GE Digital APM Distribution package, and then navigate to the **Admin** folder.
2. Run the file **Setup.exe**.

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



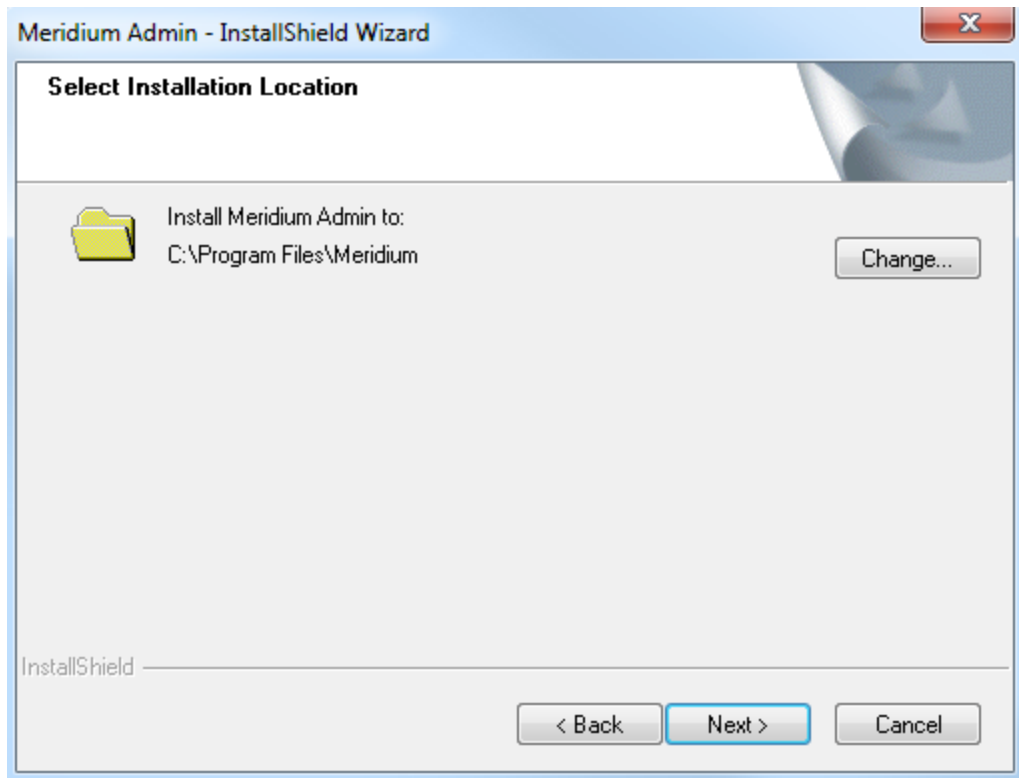
3. Select **Next**.

The **License Agreement** window appears.



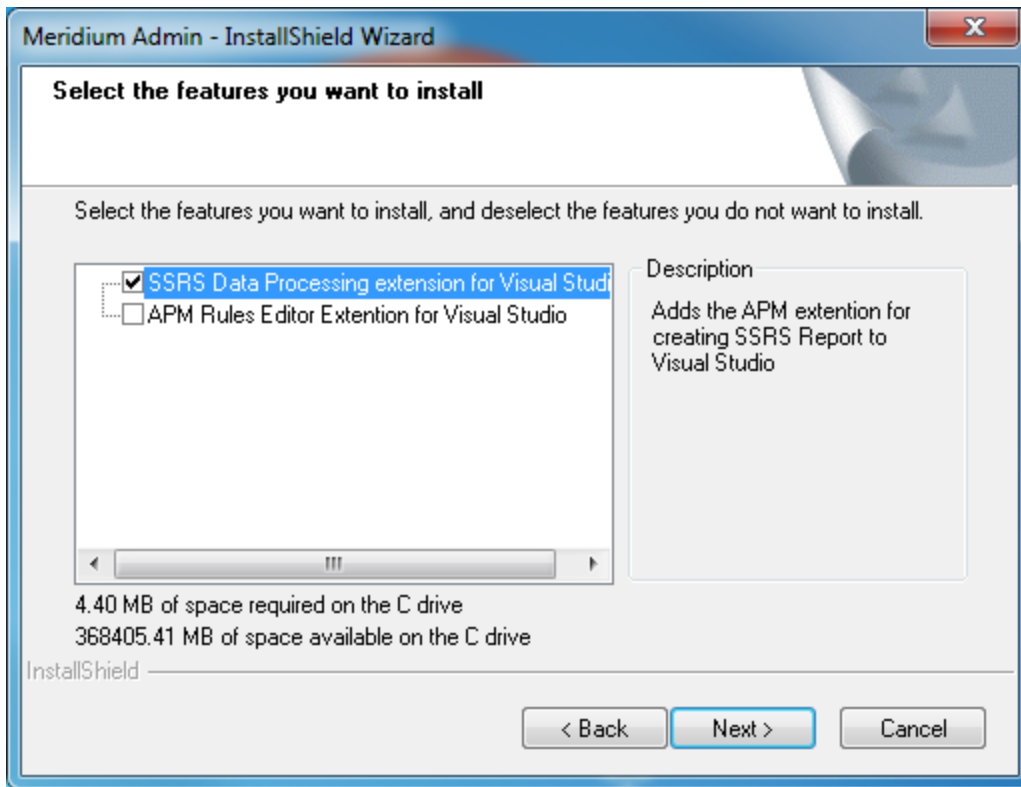
4. Read the License Agreement and, if you agree, select the **I accept the terms of the license agreement** check box, and then select **Next**.

The **Select Installation Location** window appears.

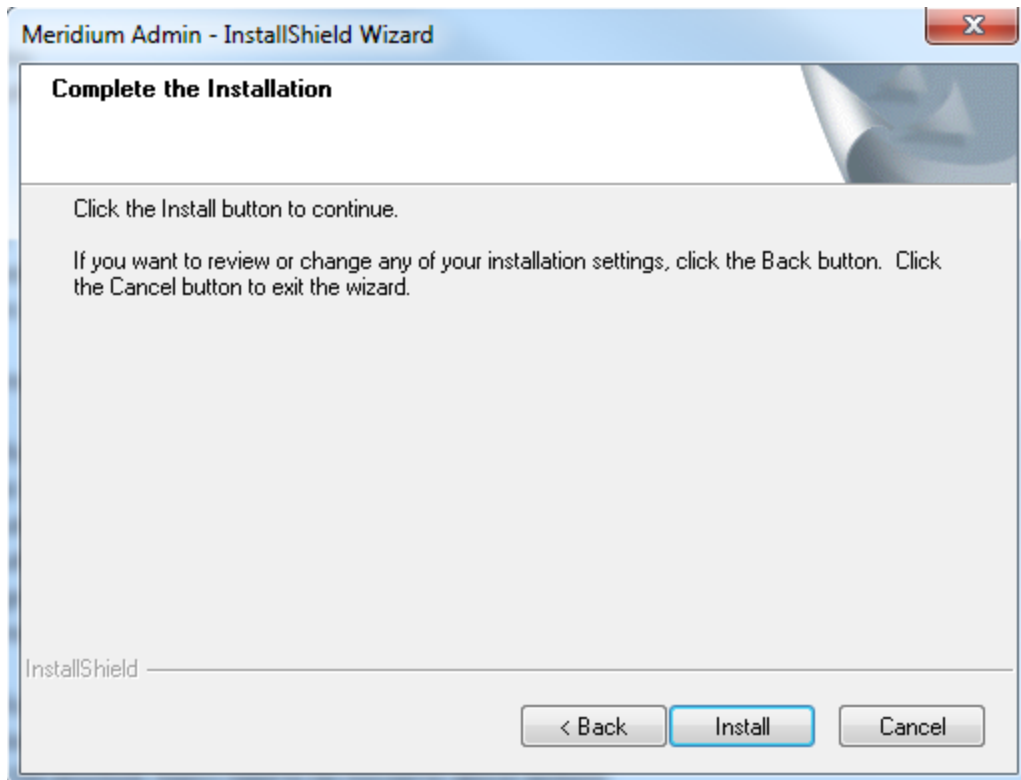


5. Select **Next** to accept the default location.

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

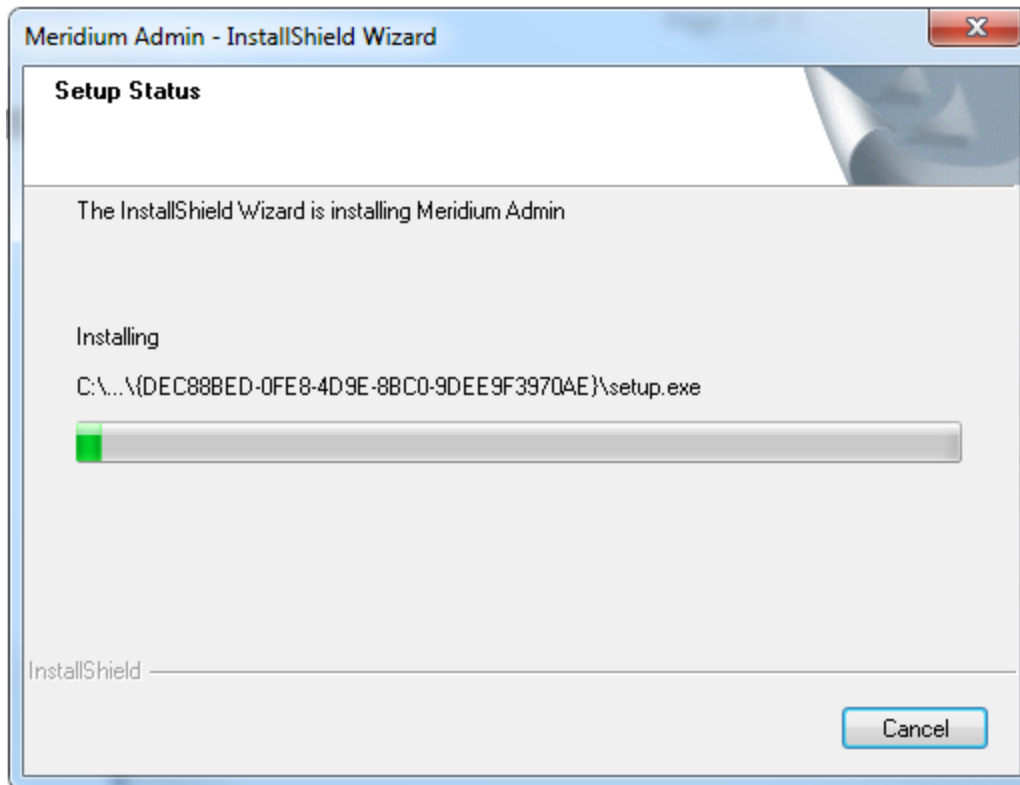


6. Select **SSRS Data Processing extension for Visual Studio**, and then select **Next**. The **Complete the Installation** window appears.

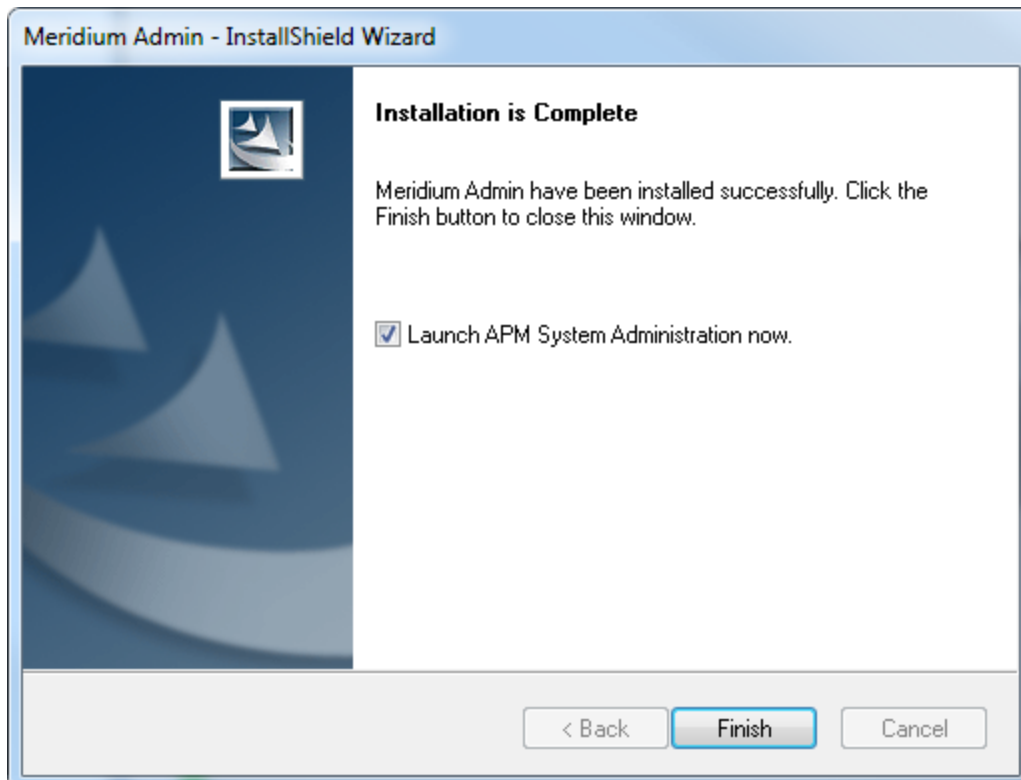



7. Select **Install**.

The **Setup Status** window appears, displaying a progress bar that shows the progress of the installation process. After the progress bar reaches the end, a message appears, indicating that the installation was successful.

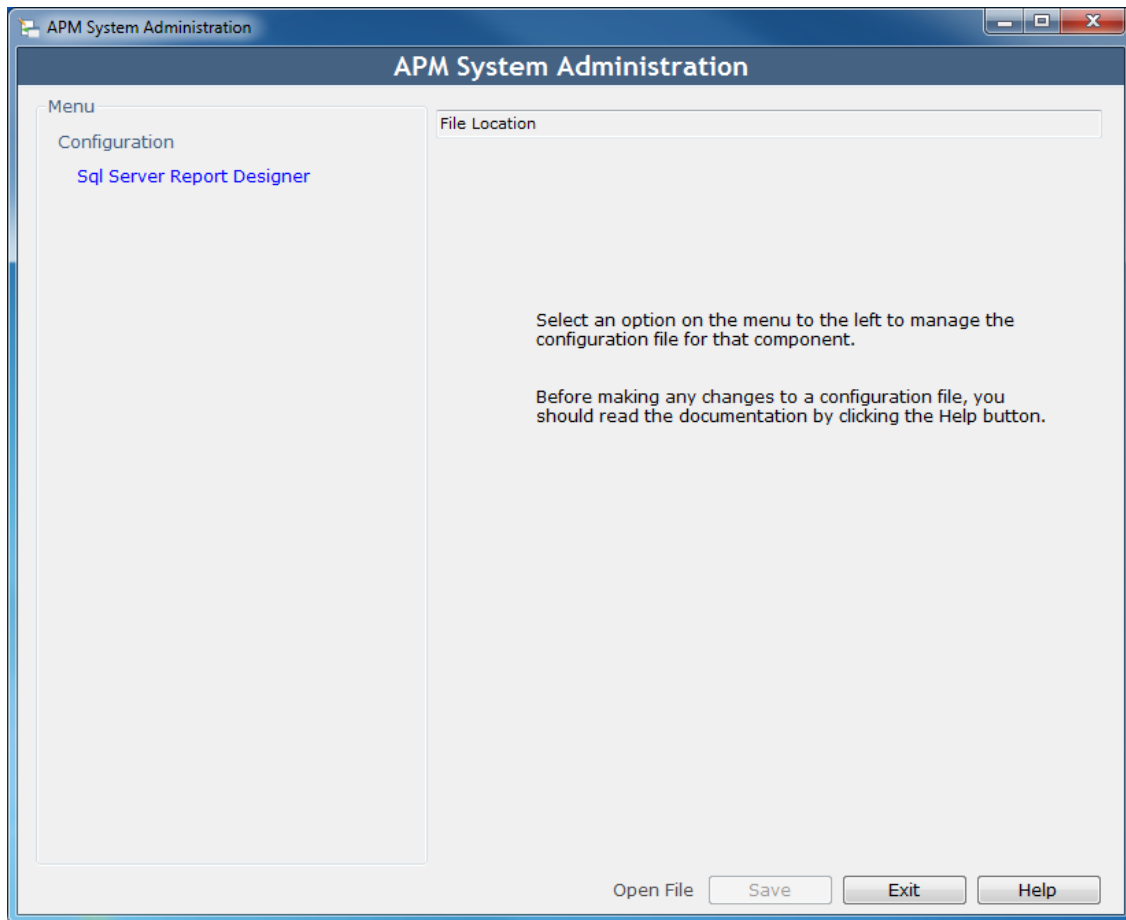


8. Clear the **Launch APM System Administration now** box, and then select **Finish**.



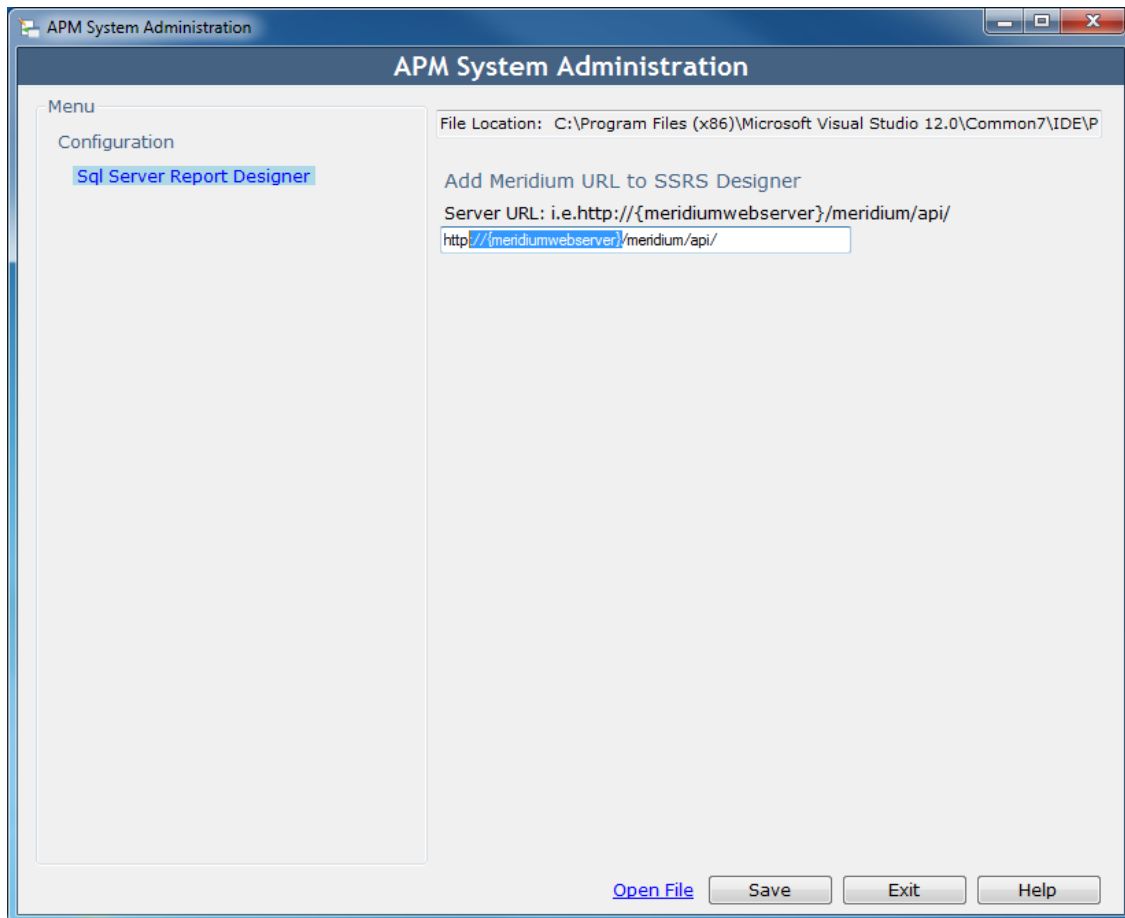
 **Note:** You may be asked to restart your system for the changes to take effect.

The **APM System Administration** window appears.



9. Select **Sql Server Report Designer**.

The **Add Meridium URL to SSRS Designer** box appears.



10. In the **Add Meridium URL to SSRS Designer** box, enter the server URL .

11. Select **Save**.

The Meridium Server URL is added.

12. Select **Exit**.

The APM Report Designer is installed.

Set Up the APM Report Designer

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

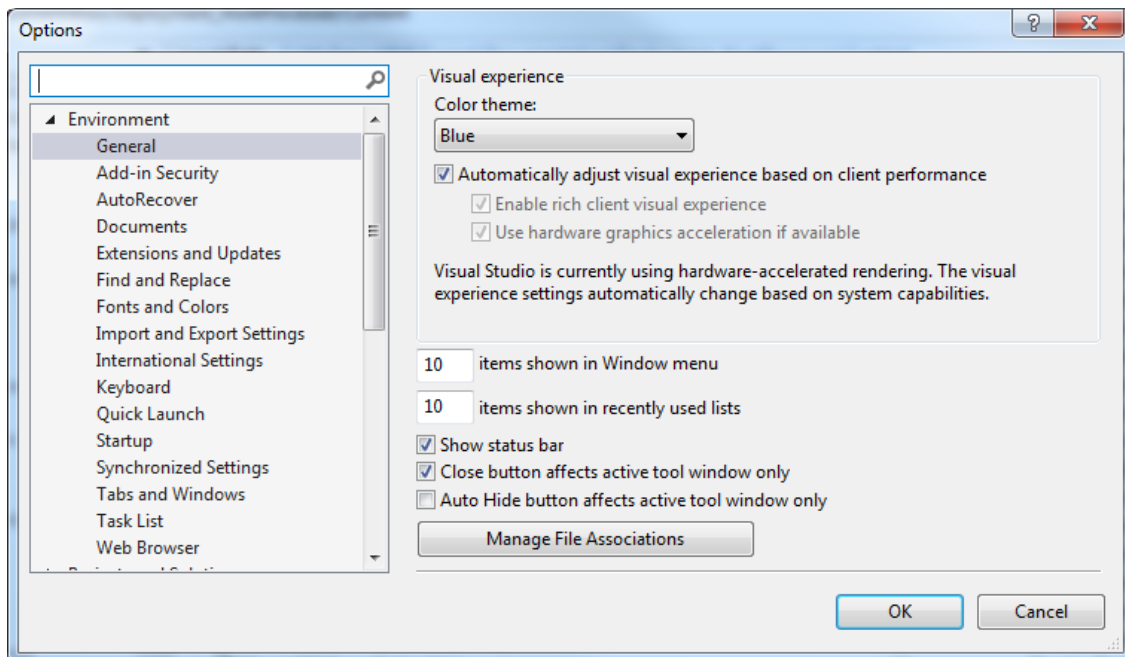
Before You Begin

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

Steps

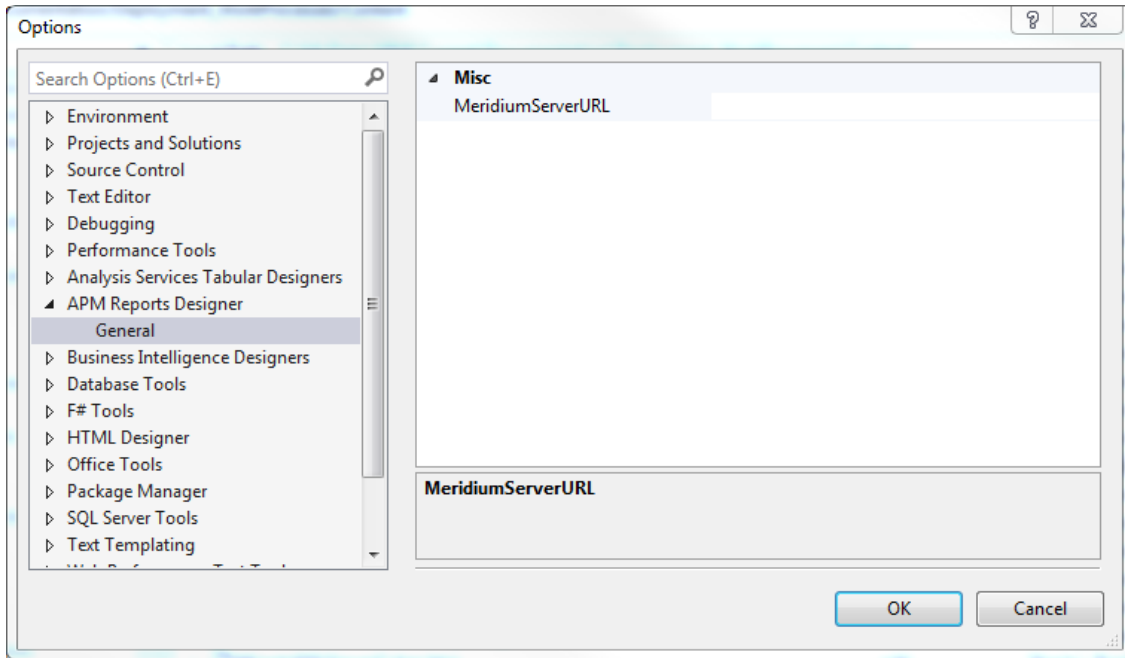
1. On the GE Digital APM Server, open Microsoft Visual Studio.
2. On the **Tools** menu, select **Options**.

The **Options** window appears.



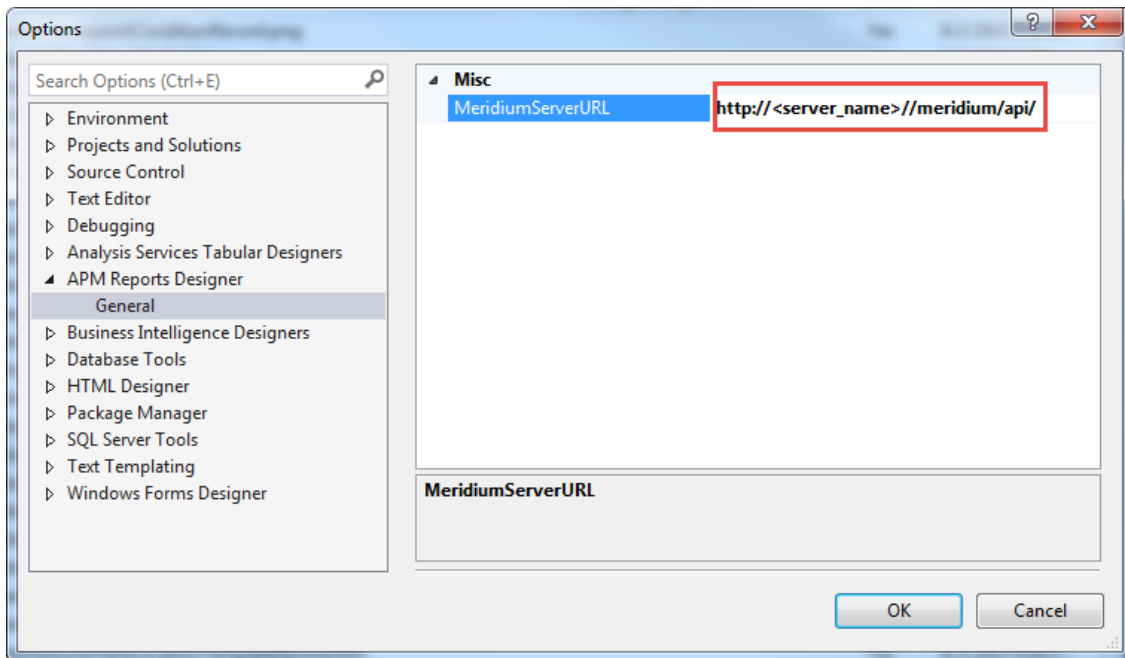
3. On the **Options** window, in the left section, select **APM Report Designer**, and then select **General**.

The **MeridiumServerURL** box appears in the right section.



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

`http://<server_name>//meridium/api/`



The APM Report Designer setup is complete.


Deploy RBI 581

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

Deploy RBI 581 for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

| Step | Task | Notes |
|------|---|--|
| 1 | Review and complete the steps required for deploying R Scripts. | This step is required. This will install R Scripts and other third-party software that is used by the RBI 581 module. |
| 2 | Review the RBI data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed. | This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families. |
| 3 | Assign Security Users to one or more of the Security Roles used in RBI. | This step is required. |

| Step | Task | Notes |
|------|--|--|
| 4 | <p>Add the following types of RBI 581 users to at least one TM Security Group:</p> <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. | <p>This step is required only if you are using the integration between the RBI 581 and Thickness Monitoring modules.</p> |
| 5 | <p>Select the Is a Unit? check box in Functional Location records that represent units in your facility.</p> | <p>This step is required, and marks Functional Location records as Process Units.</p> |
| 6 | <p>Using the Belongs to a Unit relationship, link Equipment records to Functional Location records representing units to which that equipment belongs (i.e., the Is a Unit? check box is selected).</p> | <p>This step is optional.</p> |

| Step | Task | Notes |
|------|---|---|
| 7 | <p>Add the RBI-581 tab to the datasheet of the following families:</p> <ul style="list-style-type: none"> • 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 | <p>This step is required only for families for which you have customized the datasheet.</p> |
| 8 | <p>Using Configuration Management, import the following files located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks folder:</p> <ul style="list-style-type: none"> • 06_MI_DATA_GRP.xml • 07_MI_MPPG_QRY.xml • 08_MI_CLMND_PR.xml | <p>This step is required only if you are deploying RBI 581 on an <i>existing</i> database. This will create data mappings between families in RBI 581.</p> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p>⚠ IMPORTANT: These data mapping records are used in RBI 581 <i>and</i> Risk Based Inspection. After you complete this step, <i>all existing changes</i> to data mapping in the RBI 581 and Risk Based Inspection will be reverted to baseline. All customization for data mappings will be lost. Do <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> </div> |

| Step | Task | Notes |
|------|--|---|
| 9 | <p>Using Configuration Manager, import the following files located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks folder:</p> <ul style="list-style-type: none"> • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml | <p>This step is required. This will update the RBI Strategy Mapping Composite entities, overwriting the existing ones.</p> |
| 10 | <p>Using Configuration Manager, import the MI_REPFLUID_581.xml file located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\IEU_ManualImports folder.</p> | <p>This step is required to import the Representative Fluids that are used in RBI 581.</p> <p>If you want to use <i>only</i> RBI 581 (i.e., you do <i>not</i> want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 representative fluids.</p> <p>If you want to verify that the file has been imported successfully, run the following query:</p> <pre data-bbox="699 1073 1395 1150">SELECT Count([MI_REPFLUID].[MI_REPFLUID_FLUID_C]) "Fluid" FROM [MI_REPFLUID]</pre> <p>This will return a list of 30 records.</p> <p>If you want to use <i>both</i> RBI 580 and RBI 581, import these files <i>without</i> deleting the existing content. In this case, the aforementioned query returns a list of 111 records.</p> |

| Step | Task | Notes |
|------|---|---|
| 11 | <p>Using Configuration Manager, import the MI_CMT_FLE0.xml file located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\IEU_ManualImports folder.</p> | <p>This step is required to import the Component Damage Flammable records.</p> <p>If you want to use only RBI 581 (i.e., you do not want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Component Damage Flammable records. This will ensure that the content in this table is as per API 3rd Edition table 4.8.</p> <p>If you want to verify that the file has been imported successfully, run the following query:</p> <pre data-bbox="704 680 1393 751">SELECT Count([MI_CMT_FLE0].[MI_CMT_FLE0_FLUID_C]) "Fluid" FROM [MI_CMT_FLE0]</pre> <p>This will return a list of 64 records. If you want to use <i>both</i> RBI 580 and RBI 581, import these files <i>without</i> deleting the existing content.</p> |
| 12 | <p>Using Configuration Manager, import the MI_FLD_VSCY_581.xml file located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\IEU_ManualImports folder.</p> | <p>This step is required to import the Fluid Viscosity records.</p> <p>If you want to use <i>only</i> RBI 581 (i.e., you do <i>not</i> want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Fluid Viscosity tables. This will ensure that the content in this table is as per API 3rd Edition table 6.1.</p> <p>If you want to verify that the file has been imported successfully, run the following query:</p> <pre data-bbox="704 1314 1393 1386">SELECT Count([MI_FLD_VSCY].[MI_FLD_VSCY_FLUID_C]) "Fluid" FROM [MI_FLD_VSCY]</pre> <p>This will return a list of 5 records. If you want to use <i>both</i> RBI 580 and RBI 581, import these files <i>without</i> deleting the existing content. In this case, the aforementioned query returns a list of 10 records.</p> |

| Step | Task | Notes |
|------|--|---|
| 13 | Using Configuration Manager, import the MI_PRL_CNS0.xml file located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\IEU_ManualImports folder. | <p>This step is required to import the Personal Injury Flammable CE Constants records.</p> <p>If you want to use <i>only</i> RBI 581 (i.e., you do not want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Fluid Viscosity records. This will ensure that the content in this table is as per API 3rd Edition table 4.9.</p> <p>If you want to verify that the file has been imported successfully, run the following query:</p> <pre data-bbox="704 680 1393 751">SELECT Count([MI_PRL_CNS0].[MI_PRL_CNS0_FLUID_C]) "Fluid" FROM [MI_PRL_CNS0]</pre> <p>This will return a list of 62 records. If you want to use <i>both</i> RBI 580 and RBI 581, import these files <i>without</i> deleting the existing content. In this case, the aforementioned query returns a list of 62 records.</p> |
| 14 | On the GE Digital APM Server, restart Redis. | This step is required, and has to be performed after you complete all the previous steps. |
| 15 | On the GE Digital APM Server, reset IIS. | This step is required, and has to be performed after you complete all the previous steps. |

Upgrade or Update RBI 581 to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

| Step | Task | Notes |
|------|---|---|
| 1 | <p>Using the Query tool, run the following query:</p> <pre>UPDATE [MI_RMMPG] SET [MI_RMMPG].[MI_RMMPG_ SOURCE_FLD_C] = 'MI_ RBDEMECH_TOTAL_PF_RBI_ DTE_N' WHERE [MI_RMMPG]. [MI_RMMPG_SOURCE_FLD_C] = 'MI_RBDEMECH_POF_N'</pre> | <p>This step is required. This will update the RBI Risk Matrix Mapping records such that the <i>Total POF - RBI Date</i> value is used to plot probability of failure (POF) on the risk matrix, instead of the <i>Total POF With Plan</i> value.</p> <div style="border: 1px solid red; padding: 5px;"> <p>⚠ IMPORTANT: After you complete this step, any customization done on the POF data mapping will be lost. 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 query.</p> </div> |

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

| Step | Task | Notes |
|------|---|--|
| 1 | <p>Using Configuration Manager, import the MI_REPFLUID_581.xml file located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\IEU_ManualImports folder.</p> | <p>This step is required to import the Representative Fluids that are used in RBI 581.</p> <p>If you want to use <i>only</i> RBI 581 (i.e., you do <i>not</i> want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 representative fluids.</p> <p>If you want to verify that the file has been imported successfully, run the following query:</p> <pre data-bbox="678 663 1393 762">SELECT Count([MI_REPFLUID].[MI_REPFLUID_FLUID_C]) "Fluid" FROM [MI_REPFLUID]</pre> <p>This will return a list of 30 records.</p> <p>If you want to use both RBI 580 and RBI 581, import these files <i>without</i> deleting the existing content. In this case, the aforementioned query returns a list of 111 records.</p> |
| 2 | <p>Using Configuration Manager, import the MI_CMT_FLE0.xml file located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\IEU_ManualImports folder.</p> | <p>This step is required to import the Component Damage Flammable records.</p> <p>If you want to use only RBI 581 (i.e., you do not want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Component Damage Flammable records. This will ensure that the content in this table is as per API 3rd Edition table 4.8.</p> <p>If you want to verify that the file has been imported successfully, run the following query:</p> <pre data-bbox="678 1461 1393 1560">SELECT Count([MI_CMT_FLE0].[MI_CMT_FLE0_FLUID_C]) "Fluid" FROM [MI_CMT_FLE0]</pre> <p>This will return a list of 64 records. If you want to use both RBI 580 and RBI 581, import these files <i>without</i> deleting the existing content.</p> |

| Step | Task | Notes |
|------|---|---|
| 3 | <p>Using Configuration Manager, import the MI_FLD_VSCY_581.xml file located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\IEU_ManualImports folder.</p> | <p>This step is required to import the Fluid Viscosity records.</p> <p>If you want to use <i>only</i> RBI 581 (i.e., you do <i>not</i> want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Fluid Viscosity tables. This will ensure that the content in this table is as per API 3rd Edition table 6.1.</p> <p>If you want to verify that the file has been imported successfully, run the following query:</p> <pre data-bbox="678 701 1395 800">SELECT Count([MI_FLD_VSCY].[MI_FLD_VSCY_FLUID_C]) "Fluid" FROM [MI_FLD_VSCY]</pre> <p>This will return a list of 5 records. If you want to use both RBI 580 and RBI 581, import these files without deleting the existing content. In this case, the aforementioned query returns a list of 10 records.</p> |
| 4 | <p>Using Configuration Manager, import the MI_PRL_CNS0.xml file located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\IEU_ManualImports folder.</p> | <p>This step is required to import the Personal Injury Flammable CE Constants records.</p> <p>If you want to use <i>only</i> RBI 581 (i.e., you do not want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Fluid Viscosity records. This will ensure that the content in this table is as per API 3rd Edition table 4.9.</p> <p>If you want to verify that the file has been imported successfully, run the following query:</p> <pre data-bbox="678 1478 1395 1556">SELECT Count([MI_PRL_CNS0].[MI_PRL_CNS0_FLUID_C]) "Fluid" FROM [MI_PRL_CNS0]</pre> <p>This will return a list of 62 records. If you want to use both RBI 580 and RBI 581, import these files without deleting the existing content. In this case, the aforementioned query returns a list of 62 records.</p> |

| Step | Task | Notes |
|------|--|---|
| 5 | <p>Using Configuration Manager, import the following files located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks folder:</p> <ul style="list-style-type: none"> • 06_MI_DATA_GRP.xml • 07_MI_MPPG_QRY.xml • 08_MI_CLMND_PR.xml | <p>This step is required only if you have not performed it during a previous upgrade. This will create data mappings between families in RBI 581.</p> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p>⚠ IMPORTANT: After you complete this 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. Do not perform this step unless your organization will be satisfied with the baseline data mappings, or you are prepared to customize the records again following the execution of the script.</i></p> </div> |
| 6 | <p>Using Configuration Manager, import the following files located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks folder:</p> <ul style="list-style-type: none"> • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml | <p>This step is required. This will update the RBI Strategy Mapping Composite entities, overwriting the existing ones.</p> |

| Step | Task | Notes |
|------|---|--|
| 7 | <p>Add the RBI-581 tab to the datasheet of the following families:</p> <ul style="list-style-type: none"> • 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 | <p>This step is required only for families for which you have customized the datasheet and if you have not performed it during a previous upgrade.</p> |
| 8 | <p>Review and complete the steps required for deploying R Scripts.</p> | <p>This step is required. This will install R-Script and other third-party software that is used by the RBI 581 module.</p> |

| Step | Task | Notes |
|------|---|---|
| 9 | <p>Using the Query tool, run the following query:</p> <pre>UPDATE [MI_RMMPG] SET [MI_RMMPG].[MI_RMMPG_ SOURCE_FLD_C] = 'MI_ RBDEMECH_TOTAL_PF_ RBI_DTE_N' WHERE [MI_ RMMPG].[MI_RMMPG_ SOURCE_FLD_C] = 'MI_ RBDEMECH_POF_N'</pre> | <p>This step is required. This will update the RBI Risk Matrix Mapping records such that <i>Total POF - RBI Date</i> value is used to plot probability of failure (POF) on the risk matrix, instead of the <i>Total POF With Plan</i> value.</p> <div style="border: 1px solid red; padding: 5px;"> <p>⚠ IMPORTANT: After you complete this step, any customization done on the POF data mapping will be lost. 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 query.</p> </div> |
| 10 | <p>On the GE Digital APM Server, reset IIS.</p> | <p>This step is required, and has to be performed after you complete all the aforementioned steps.</p> |

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

| Step | Task | Notes |
|------|---|---|
| 1 | <p>Using Configuration Manager, import the MI_REPFLUID_581.xml file located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\IEU_ManualImports folder.</p> | <p>This step is required to import the Representative Fluids that are used in RBI 581.</p> <p>If you want to use <i>only</i> RBI 581 (i.e., you do <i>not</i> want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 representative fluids.</p> <p>If you want to verify that the file has been imported successfully, run the following query:</p> <pre>SELECT Count([MI_REPFLUID].[MI_REPFLUID_FLUID_C]) "Fluid" FROM [MI_REPFLUID]</pre> <p>This will return a list of 30 records.</p> <p>If you want to use both RBI 580 and RBI 581, import these files <i>without</i> deleting the existing content. In this case, the aforementioned query returns a list of 111 records.</p> |

| Step | Task | Notes |
|------|---|---|
| 2 | <p>Using Configuration Manager, import the MI_CMT_FLE0.xml file located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\IEU_ManualImports folder.</p> | <p>This step is required to import the Component Damage Flammable records.</p> <p>If you want to use only RBI 581 (i.e., you do not want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Component Damage Flammable records. This will ensure that the content in this table is as per API 3rd Edition table 4.8.</p> <p>If you want to verify that the file has been imported successfully, run the following query:</p> <pre data-bbox="678 743 1395 842">SELECT Count([MI_CMT_FLE0].[MI_CMT_FLE0_FLUID_C]) "Fluid" FROM [MI_CMT_FLE0]</pre> <p>This will return a list of 64 records. If you want to use both RBI 580 and RBI 581, import these files <i>without</i> deleting the existing content.</p> |
| 3 | <p>Using Configuration Manager, import the MI_FLD_VSCY_581.xml file located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\IEU_ManualImports folder.</p> | <p>This step is required to import the Fluid Viscosity records.</p> <p>If you want to use <i>only</i> RBI 581 (i.e., you do <i>not</i> want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Fluid Viscosity tables. This will ensure that the content in this table is as per API 3rd Edition table 6.1.</p> <p>If you want to verify that the file has been imported successfully, run the following query:</p> <pre data-bbox="678 1436 1395 1535">SELECT Count([MI_FLD_VSCY].[MI_FLD_VSCY_FLUID_C]) "Fluid" FROM [MI_FLD_VSCY]</pre> <p>This will return a list of 5 records. If you want to use both RBI 580 and RBI 581, import these files without deleting the existing content. In this case, the aforementioned query returns a list of 10 records.</p> |

| Step | Task | Notes |
|------|---|---|
| 4 | <p>Using Configuration Manager, import the MI_PRL_CNS0.xml file located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\IEU_ManualImports folder.</p> | <p>This step is required to import the Personal Injury Flammable CE Constants records.</p> <p>If you want to use <i>only</i> RBI 581 (i.e., you do not want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Fluid Viscosity records. This will ensure that the content in this table is as per API 3rd Edition table 4.9.</p> <p>If you want to verify that the file has been imported successfully, run the following query:</p> <pre data-bbox="678 743 1395 842">SELECT Count([MI_PRL_CNS0].[MI_PRL_CNS0_FLUID_C]) "Fluid" FROM [MI_PRL_CNS0]</pre> <p>This will return a list of 62 records. If you want to use both RBI 580 and RBI 581, import these files without deleting the existing content. In this case, the aforementioned query returns a list of 62 records.</p> |
| 5 | <p>Using Configuration Manager, import the following files located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks folder:</p> <ul style="list-style-type: none"> • 06_MI_DATA_GRP.xml • 07_MI_MPPG_QRY.xml • 08_MI_CLMND_PR.xml | <p>This step is required only if you have not performed it during a previous upgrade. This will create data mappings between families in RBI 581.</p> <div data-bbox="678 1255 1395 1591" style="border: 1px solid red; padding: 5px;"> <p>⚠ IMPORTANT: After you complete this 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 not perform this step unless your organization will be satisfied with the baseline data mappings, or you are prepared to customize the records again following the execution of the script.</p> </div> |

| Step | Task | Notes |
|------|---|--|
| 6 | <p>Using Configuration Manager, import the following files located in the C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks folder:</p> <ul style="list-style-type: none"> • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml | <p>This step is required. This will update the RBI Strategy Mapping Composite entities, overwriting the existing ones.</p> |
| 7 | <p>Add the RBI-581 tab to the datasheet of the following families:</p> <ul style="list-style-type: none"> • 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 | <p>This step is required only for families for which you have customized the datasheet and if you have not performed it during a previous upgrade.</p> |

| Step | Task | Notes |
|------|---|---|
| 8 | Review and complete the steps required for deploying R Scripts. | This step is required. This will install R-Script and other third-party software that is used by the RBI 581 module. |
| 9 | <p>Using the Query tool, run the following query:</p> <pre>UPDATE [MI_RMMPG] SET [MI_RMMPG].[MI_RMMPG_SOURCE_FLD_C] = 'MI_RBDEMECH_TOTAL_PF_RBI_DTE_N' WHERE [MI_RMMPG].[MI_RMMPG_SOURCE_FLD_C] = 'MI_RBDEMECH_POF_N'</pre> | <p>This step is required. This will update the RBI Risk Matrix Mapping records such that <i>Total POF - RBI Date</i> value is used to plot probability of failure (POF) on the risk matrix, instead of the <i>Total POF With Plan</i> value.</p> <div style="border: 1px solid red; padding: 5px; margin-top: 10px;"> <p>⚠ IMPORTANT: After you complete this step, any customization done on the POF data mapping will be lost. 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 query.</p> </div> |
| 10 | On the GE Digital APM Server, reset IIS. | This step is required, and has to be performed after you complete all the aforementioned steps. |

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

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

| Step | Task | Notes |
|------|--|--|
| 1 | Review and complete the steps required for deploying R Scripts. | This step is required. This will install R-Script and other third-party software that is used by the RBI 581 module. |
| 2 | Copy your customized SQL code from the Review Analyses by Asset query to the Review Analyses by Asset 580 query, and then replace the Review Analyses by Asset query with its baseline version. | This step is required <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, and only if you will have the RBI 581 and Risk Based Inspection modules active at the same time. |

| Step | Task | Notes |
|------|---|---|
| 3 | <p>Add the RBI-581 tab to the datasheet of the following families:</p> <ul style="list-style-type: none"> • 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 | <p>This step is required only for families for which you have customized the datasheet.</p> |

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

RBI 581 has been introduced in GE Digital APM V3.6.0.8.0. Therefore, if you have an earlier version of GE Digital APM, then you must follow the steps in the [first-time deployment of RBI 581](#). If you have deployed RBI 581 in GE Digital APM V3.6.0.8.0 or later, you must follow the steps outlined in the following table.

| Step | Task | Notes |
|------|---|---|
| 1 | <p>Review and complete the steps required for deploying R Scripts.</p> | <p>This step is required. This will install R-Script and other third-party software that is used by the RBI 581 module.</p> |
| 2 | <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> | <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, and only if you will have the RBI 581 and Risk Based Inspection modules active at the same time.</p> |

| Step | Task | Notes |
|------|---|---|
| 3 | <p>Add the RBI-581 tab to the datasheet of the following families:</p> <ul style="list-style-type: none"> • 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 | <p>This step is required only for families for which you have customized the datasheet.</p> |

Add the RBI-581 Tab to Criticality RBI Component Datasheets

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

| Caption | Field ID | Criticality RBI Component - Cylindrical Shell | Criticality RBI Component - Exchanger Bundle | Criticality RBI Component - Exchanger Header | Criticality RBI Component - Exchanger Tube | Criticality RBI Component - Piping | Criticality RBI Component - Tank Bottom |
|-------------------|----------------------------------|---|--|--|--|------------------------------------|---|
| Base Material | MI_CCRBIC-OM_BASE_MATERIAL_C | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Cladding Material | MI_CCRBIC-OM_CLADDING_MATERIAL_C | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Cladding Present | MI_CCRBIC-OM_CLADDING_PRESENT_L | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Caption | Field ID | Criticality RBI Component - Cylindrical Shell | Criticality RBI Component - Exchanger Bundle | Criticality RBI Component - Exchanger - Header | Criticality RBI Component - Exchanger Tube | Criticality RBI Component - Piping | Criticality RBI Component - Tank Bottom |
|------------------------|-----------------------------------|---|--|--|--|------------------------------------|---|
| CM Corrosion Rate | MI_CCRBIC-OM_CM_COR_RT_C | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Coefficient Y Material | MI_CCRBIC-OM_COEFFICIENT_Y_MTRL_C | × | × | × | × | ✓ | × |
| Corrosion Allow | MI_RBICOMPO_CORRO_ALLOW_N | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Detection System | MI_CCRBIC-OM_DETECTION_SYSTEM_C | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Fluid Velocity | MI_CCRBIC-OM_FLUID_VELOCITY_N | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Caption | Field ID | Criticality RBI Component - Cylindrical Shell | Criticality RBI Component - Exchanger Bundle | Criticality RBI Component - Exchanger - Header | Criticality RBI Component - Exchanger Tube | Criticality RBI Component - Piping | Criticality RBI Component - Tank Bottom |
|-----------------------------------|-------------------------------------|---|--|--|--|------------------------------------|---|
| Furnished Cladding Thk | MI_CCRBIC-OM_FRNSHD_CLDDG_THK_N | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Geometry Type | MI_CCRBIC-OM_GEOMETRY_TYPE_C | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| GFF Component Type | MI_CCRBIC-OM_GFF_COMPONENT_TYPE_CHR | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Has Release Prevention - Barrier? | MI_CCRBIC-TB_HAS_RELEASE_PREVENTION | × | × | × | × | × | ✓ |

| 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 |
|------------------------------|--------------------------------|---|--|--|--|------------------------------------|---|
| Is Intrusive? | MI_RBICOM-PO_IS_INTRU_CHR | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Isolation System | MI_CCRBICOM_ISOLA_SYSTE_CHR | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Liner Present | MI_CCRBICOM_LINER_PRESE_CHR | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Liner Type | MI_CCRBICOM_LINER_TP_C | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Minimum Structural Thickness | MI_CCRBICOM_MNMM_STRCTRL_THS_N | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

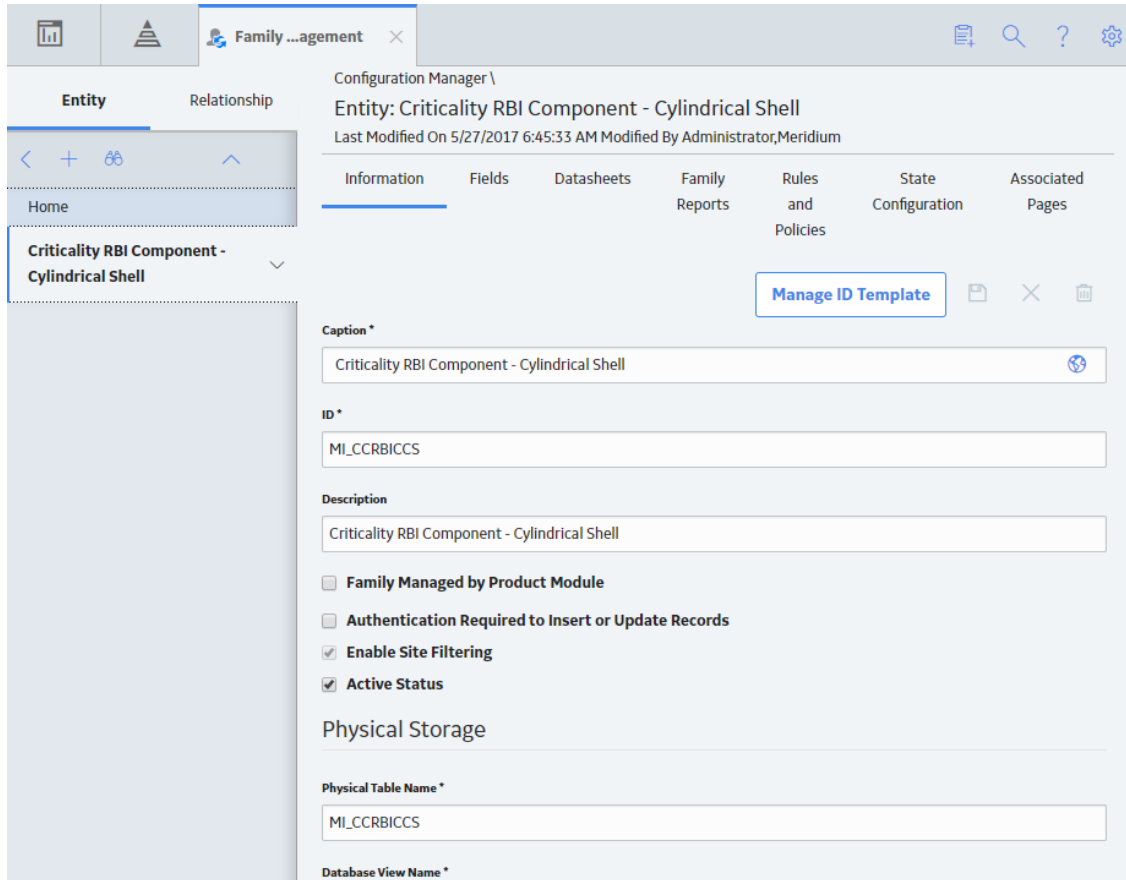
| Caption | Field ID | Criticality RBI Component - Cylindrical Shell | Criticality RBI Component - Exchanger Bundle | Criticality RBI Component - Exchanger - Header | Criticality RBI Component - Exchanger Tube | Criticality RBI Component - Piping | Criticality RBI Component - Tank Bottom |
|-----------------------|----------------------------------|---|--|--|--|------------------------------------|---|
| Mitigation System | MI_CCRBIC-OM_MITIGATION_SYSTM_C | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Percent Liquid Volume | MI_RBICOMPO_PER_LIQ_VOL_N | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| pH of Water | MI_CCRBIC-OM_PH_OF_WATER_N | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Specified Tmin | MI_CCRBIC-OM_SPECIFIED_TMIN_N | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Total Acid Number | MI_CCRBIC-OM_TOTAL_ACID_NUMB-R_N | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Steps

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

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

In the workspace, the corresponding Criticality RBI Component family appears, displaying the **Information** section.



3. In the workspace, select the **Datasheets** tab, and then select **Manage Datasheets**.

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

Deploy Modules and Features

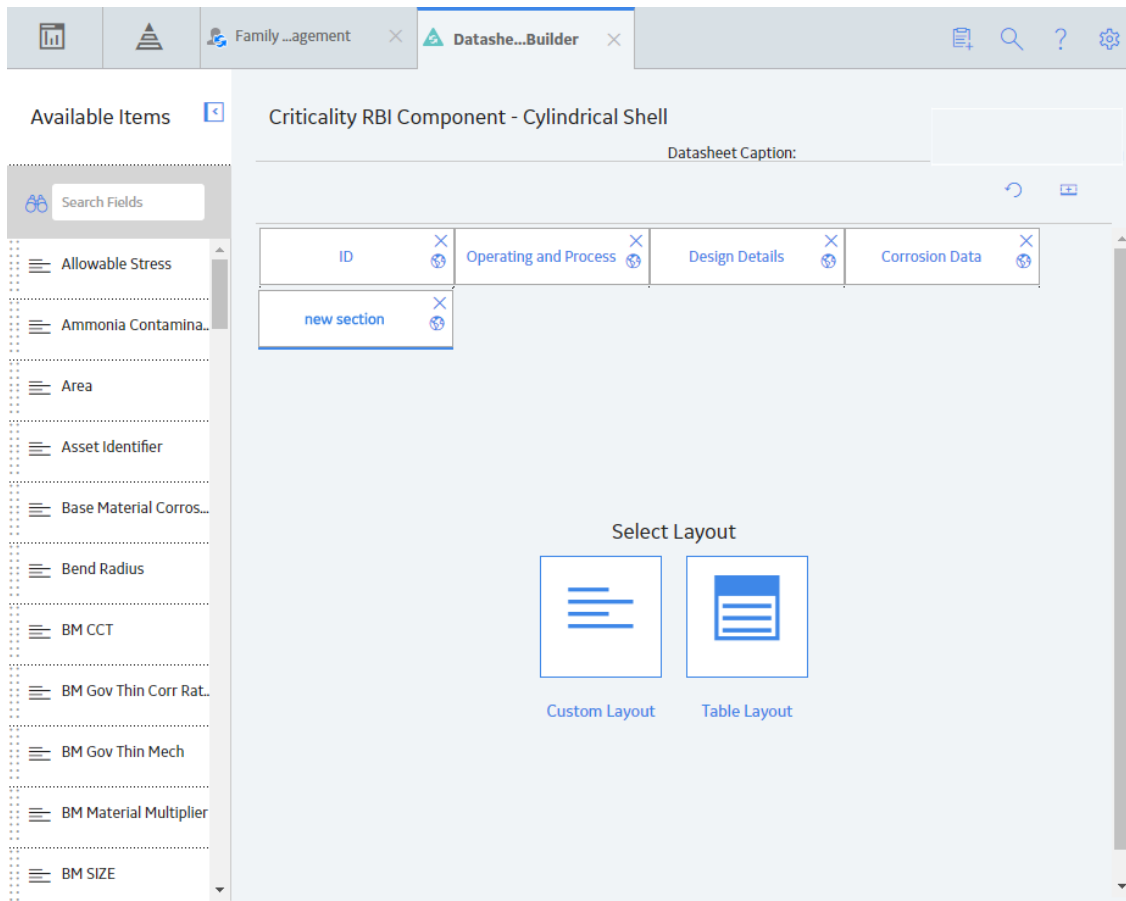
The screenshot shows the 'Dashes...Builder' window with a workspace titled 'Criticality RBI Component - Cylindrical Shell'. The workspace contains a table with four columns: 'ID', 'Operating and Process', 'Design Details', and 'Corrosion Data'. Below the table, there is a 'Values(s)' section with several rows, each containing a label and a text input field:


| | Values(s) |
|-----------------------|--|
| Equipment | <input type="text" value="Equipment"/> |
| Equipment Family | <input type="text" value="Equipment Family"/> |
| Function Location | <input type="text" value="Function Location"/> |
| Component | <input type="text" value="Component"/> |
| Component Description | <input type="text" value="Component Description"/> |
| Component Type | <input type="text" value="Component Type"/> |


On the left side, there is an 'Available Items' panel with a search bar and a list of items including: Allowable Stress, Ammonia Contamina..., Area, Asset Identifier, Base Material Corros..., Bend Radius, BM CCT, BM Gov Thin Corr Rat..., BM Gov Thin Mech, BM Material Multiplier, and BM SIZE.

4. In the upper-right corner of the page, select .

A **new section** tab appears at the top of the workspace, displaying a blank section.



5. On the new tab, rename *new section* to *RBI-581*.
6. In the **RBI-581** section, select .
7. In the right column, in the top cell, enter *Value(s)*.
8. In the left pane, locate a field that corresponds to [the table at the beginning of this topic](#), and then add that field into the empty cell in the **Value(s)** column using the drag-and-drop method.

In the cell, an input box that corresponds to the selected field appears.
9. In the left column, enter the caption that corresponds to the field. For example, if you added the Coefficient Y Material field to the **Value(s)** column, then enter *Coefficient Y Material* in the corresponding cell in the left column.
10. In the upper-right corner of the page, select .

In the **RBI-581** section, in the table, a new row appears.
11. Repeat steps 8 to 10 for each of the fields specified in [the table at the beginning of this topic](#).
12. In the upper-right corner of the page, select **Save**.

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

RBI 581 Security Groups and Roles

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

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

| Security Group | Roles |
|---------------------------------------|--|
| RBI Security Groups | |
| MI RBI Administrator | MI Mechanical Integrity Administrator |
| MI RBI Analyst | MI Mechanical Integrity Administrator MI Mechanical Integrity Power |
| MI RBI Viewer | MI APM Viewer MI Mechanical Integrity Viewer |
| RBI Policy Security Groups | |
| MI RBI Calculation Policy Designer | None |
| MI RBI Calculation Policy Viewer | MI Mechanical Integrity Administrator MI Mechanical Integrity Power |
| MI RBI Recommendation Policy Designer | None |
| MI RBI Recommendation Policy Viewer | MI Mechanical Integrity Administrator MI Mechanical Integrity Power |
| MI RBI Risk Mapping Policy Designer | None |
| MI RBI Risk Mapping Policy Viewer | MI Mechanical Integrity Administrator MI Mechanical Integrity Power |

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

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

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

Note: If you have activated only the *RBI 581* license (and not the *Risk Based Inspection* license), then privileges to some of the following families do not exist for the MI RBI Administrator, MI RBI Analyst, and MI RBI Viewer Security Groups.

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


| Family | MI RBI Administrator | MI RBI Analyst | MI RBI Viewer |
|---|------------------------------|------------------------------|---------------|
| Criticality RBI Component - Cylindrical Shell | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Criticality RBI Component - Exchanger Bundle | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Criticality RBI Component - Exchanger Header | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Criticality RBI Component - Exchanger Tube | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Criticality RBI Component - Piping | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Criticality RBI Component - Tank Bottom | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Data Mapping Column-Field Pair | View, Update, Insert, Delete | View | View |
| Data Mapping Group | View, Update, Insert, Delete | View | View |
| Data Mapping Query | View, Update, Insert, Delete | View | View |
| Degradation Mechanisms Evaluation Factors | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Equipment | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Functional Location | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Grouping Element | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Inspection Task | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Inventory Group Configuration | View, Update, Insert, Delete | View | View |
| General Recommendation | View | View, Update, Insert, Delete | View |

| Family | MI RBI Administrator | MI RBI Analyst | MI RBI Viewer |
|--|------------------------------|------------------------------|---------------|
| Meridium Reference Tables | View, Update, Insert, Delete | View | View |
| Policy | View | View | View |
| Potential Degradation Mechanisms | View, Update, Insert, Delete | View | View |
| RBI 581 Admin Options | View, Update, Insert, Delete | View | View |
| RBI 581 Brittle Fracture Damage Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 Consequence Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 Cracking Damage Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 Damage Mechanism Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 External Cracking Damage Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 External Damage Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 HTHA Damage Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 Mechanical Fatigue Damage Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 Risk Analysis | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 Thinning and Lining Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI Criticality Analysis | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI Custom DM Evaluation Configuration | View, Update, Insert, Delete | View | View |

| Family | MI RBI Administrator | MI RBI Analyst | MI RBI Viewer |
|--|------------------------------|------------------------------|---------------|
| RBI Custom DM Evaluation Configuration Details | View, Update, Insert, Delete | View | View |
| RBI Custom DM Evaluation Validation | View, Update, Insert, Delete | View | View |
| RBI Custom DM Evaluation Validation Details | View, Update, Insert, Delete | View | View |
| RBI Degradation Mechanisms | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI Inspection Auto-Selection Criteria | View, Update, Insert, Delete | View | View |
| RBI Recommendation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI Risk Matrix Mapping | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI Strategy Mapping Configuration | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI Strategy Mapping Details | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI System | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Reference Document | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Risk Assessment | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Risk Rank | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Risk Translation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| SAP System | View | View | View |
| Strategy Logic Case | View, Update, Insert, Delete | View | View |

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

| Family | MI RBI Admin- istrator | MI RBI Analyst | MI RBI Viewer |
|--|---------------------------------|---------------------------------|------------------|
| Has Inspections | View | View, Update, Insert, Delete | View |
| Has Inspection Scope | View | View | View |
| Has Potential Degradation Mechanisms | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has RBI Components | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has RBI Criticality Analysis | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has RBI Custom DME Configuration | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has RBI Custom DME Validation | View, Update, Insert, Delete | View | View |
| Has RBI Degradation Mechanisms Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has RBI Strategy Mapping Con- figuration | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has RBI Systems | View, Update, Insert, Delete | View, Update, Insert, Delete | View |

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

The following families are *not* used elsewhere in the RBI module. Privileges to these families support integration with the Inspection Management module:

- Has Inspection Scope
- Has Time Based Inspection Interval
- Time Based Inspection Interval
- Time Based Inspection Setting

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


Deploy Risk Based Inspection (RBI)

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

Deploy Risk Based Inspection (RBI) for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

| Step | Task | Notes |
|------|---|--|
| 1 | Review the RBI data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Modify any relationship definitions as needed via Configuration Manager. | This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families. |
| 2 | Assign Security Users to one or more of the Security Roles used in RBI. | This step is required. |
| 3 | On the GE Digital APM Server, using Configuration Manager, import the following files <ul style="list-style-type: none"> 101_MI_STMPCNFG.xml 102_MI_STRMAPP.xml These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks . You must extract the 4030000 archive from the MI_DB_MASTER_4300000 archive. | This step is required only if you are deploying Risk Based Inspection on an <i>existing</i> GE Digital APM database. These data mapping records are used in RBI 581 <i>and</i> Risk Based Inspection. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 2888 . |

| Step | Task | Notes |
|------|---|---|
| 4 | <p>Assign the following types of RBI users to at least one TM Security Group:</p> <ul style="list-style-type: none"> Users who are responsible for completing the steps necessary to use TM Analysis values to calculate RBI 580 corrosion rates. Users who should be able to navigate to TM via RBI 580. | This step is required only if you are using the integration between the RBI and Thickness Monitoring modules. |
| 5 | Modify the MI_DEGRADATION_MECHANISM_TYPES System Code Table. | This step is required only if you want to create your own Potential Degradation Mechanisms records. |
| 6 | Select the Recommendation Creation Enabled check box in the Global Preferences workspace. | This step is required only if you do not want to create Recommendations in RBI, but want to use the Asset Strategy Management (ASM) module to recommend actions and manage mitigated risk. This check box is selected by default. |
| 7 | Select the Enable Recommendations to be Generated at Created State check box in the Global Preferences workspace. | This step is required only if you want to create RBI Recommendation records while RBI Analysis records are in the <i>Created</i> state. This check box is cleared by default. |
| 8 | Select the Allow Override of Calculated Unmitigated Risk Values check box in the Global Preferences workspace. | This step is required only if you want to override the calculated values of unmitigated risk because you use a custom calculator. This check box is cleared by default. |
| 9 | Select the Consider Half-Life when Determining Inspection Task Interval check box in the Global Preferences workspace. | This step is required only if you want additional values such as half-life to determine the inspection task interval. This check box is cleared by default. |

| Step | Task | Notes |
|------|--|---|
| 10 | Select the Is a Unit? check box in Functional Location records that represent units in your facility. | This step is required to mark Functional Location records as Process Units. |
| 11 | Using the Belongs to a Unit relationship, link Equipment records to Functional Location records representing units to which that equipment belongs (i.e., the Is a Unit? check box is selected). | This step is optional. |
| 12 | Configure the GE Digital APM system to generate RBI Recommendation records automatically. | This step is optional. |
| 13 | Create Potential Degradation Mechanisms records. | This step is required only if you want to use additional Potential Degradation Mechanisms records that are not provided in the baseline GE Digital APM database. |
| 14 | Assign a ranking to all Qualitative Potential Degradation Mechanisms records. | This step is required only if you want the Probability Category field in certain Criticality Degradation Mech Evaluation records to be populated automatically based on this ranking. |

Upgrade or Update Risk Based Inspection (RBI) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

| Step | Task | Notes |
|------|--|---|
| 1 | <p>Modify the Data Mapping Query record RBI-CNAFC MI_CCRBICTB-MI_CRCOEVAL by Component as follows:</p> <ul style="list-style-type: none"> In the related Data Mapping Column-Field Pair record where the Source Query Field is set to <i>Toxic Mixture</i>, ensure the Target Field(s) field is also set to <i>Toxic Mixture</i>. In the related Data Mapping Column-Field Pair record where the Source Query Field is set to <i>Toxic Model</i>, ensure the Target Field(s) field is set to <i>Toxic Fluid</i>. | <p>This step is required only if you have not completed it while upgrading RBI 581.</p> |

| Step | Task | Notes |
|------|---|---|
| 2 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 09_MI_RRSKMAP.xml • 10_MI_RRSKMDT.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities.</p> |
| 3 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 2888.</p> |

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

| Step | Task | Notes |
|------|--|---|
| 1 | <p>Modify the Data Mapping Query record RBI-CNAFC MI_CCRBICTB-MI_CRCOEVAL by Component as follows:</p> <ul style="list-style-type: none"> • In the related Data Mapping Column-Field Pair record where the Source Query Field is set to <i>Toxic Mixture</i>, ensure the Target Field(s) field is also set to <i>Toxic Mixture</i>. • In the related Data Mapping Column-Field Pair record where the Source Query Field is set to <i>Toxic Model</i>, ensure the Target Field(s) field is set to <i>Toxic Fluid</i>. | <p>This step is required only if you have not completed it while upgrading RBI 581.</p> |
| 2 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 09_MI_RRSKMAP.xml • 10_MI_RRSKMDT.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities.</p> |

| Step | Task | Notes |
|------|--|---|
| 3 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 2888.</p> |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| Step | Task | Notes |
|------|--|---|
| 1 | <p>Modify the Data Mapping Query record RBI-CNAFC MI_CCRBICTB-MI_CRCOEVAL by Component as follows:</p> <ul style="list-style-type: none"> • In the related Data Mapping Column-Field Pair record where the Source Query Field is set to <i>Toxic Mixture</i>, ensure the Target Field(s) field is also set to <i>Toxic Mixture</i>. • In the related Data Mapping Column-Field Pair record where the Source Query Field is set to <i>Toxic Model</i>, ensure the Target Field(s) field is set to <i>Toxic Fluid</i>. | <p>This step is required only if you have not completed it while upgrading RBI 581.</p> |

| Step | Task | Notes |
|------|---|--|
| 2 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 09_MI_RRSKMAP.xml • 10_MI_RRSKMDT.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities.</p> |
| 3 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • Select Protected Assets • Unlinked Corrosion Loops <p>These files should be located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000_IEU_CatalogItems_Queries. You must zip any files together that you need to import into the system. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required only if you have modified the queries that were delivered in baseline. After you complete this step, Site Filtering is enabled.</p> |

| Step | Task | Notes |
|------|---|---|
| 4 | <p>On the GE Digital APM Application Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 2888.</p> |

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

| Step | Task | Notes |
|------|--|--|
| 1 | <p>Import Policy records that GE Digital modified in order to fix issues in the associated policy diagrams. This includes the following Policy records:</p> <ul style="list-style-type: none"> • Appendix G • Appendix H • Appendix I | <p>This step is required only if you use Policy records to generate RBI Recommendations.</p> |

| Step | Task | Notes |
|------|--|---|
| 2 | <p>Modify the Data Mapping Query record RBI-CNAFC MI_CCRBICTB-MI_CRCOEVAL by Component as follows:</p> <ul style="list-style-type: none"> • In the related Data Mapping Column-Field Pair record where the Source Query Field is set to <i>Toxic Mixture</i>, ensure the Target Field(s) field is also set to <i>Toxic Mixture</i>. • In the related Data Mapping Column-Field Pair record where the Source Query Field is set to <i>Toxic Model</i>, ensure the Target Field(s) field is set to <i>Toxic Fluid</i>. | <p>This step is required only if you have not completed it while upgrading RBI 581.</p> |
| 3 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 09_MI_RRSKMAP.xml • 10_MI_RRSKMDT.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities.</p> |

| Step | Task | Notes |
|------|---|---|
| 4 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 2888.</p> |

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

| Step | Task | Notes |
|------|--|--|
| 1 | <p>Import Policy records that GE Digital modified in order to fix issues in the associated policy diagrams. This includes the following Policy records:</p> <ul style="list-style-type: none"> • Appendix G • Appendix H • Appendix I | <p>This step is required only if you use Policy records to generate RBI Recommendations.</p> |

| Step | Task | Notes |
|------|--|---|
| 2 | <p>Modify the Data Mapping Query record RBI-CNAFC MI_CCRBICTB-MI_CRCOEVAL by Component as follows:</p> <ul style="list-style-type: none"> • In the related Data Mapping Column-Field Pair record where the Source Query Field is set to <i>Toxic Mixture</i>, ensure the Target Field(s) field is also set to <i>Toxic Mixture</i>. • In the related Data Mapping Column-Field Pair record where the Source Query Field is set to <i>Toxic Model</i>, ensure the Target Field(s) field is set to <i>Toxic Fluid</i>. | <p>This step is required only if you have not completed it while upgrading RBI 581.</p> |
| 3 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 09_MI_RRSKMAP.xml • 10_MI_RRSKMDT.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities.</p> |

| Step | Task | Notes |
|------|---|---|
| 4 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 2888.</p> |

Upgrade from any version V3.5.1 through V3.5.1.12.1

| Step | Task | Notes |
|------|--|--|
| 1 | <p>Import Policy records that GE Digital modified in order to fix issues in the associated policy diagrams. This includes the following Policy records:</p> <ul style="list-style-type: none"> • Appendix G • Appendix H • Appendix I | <p>This step is required only if you use Policy records to generate RBI Recommendations.</p> |

| Step | Task | Notes |
|------|--|---|
| 2 | <p>Import the Inspection Strategy records that GE Digital modified in order to fix issues in existing Inspection Strategy records. To do so:</p> <ol style="list-style-type: none"> Using the Import/Export Metadata window, navigate to the following location on the GE Digital APM Server machine: C:\Meridium\DbUpg\MI_DB_Master_4030000\4030000\20_IEU\50_Other\2_RecordsLinks Import the file MI_INSP_STRAT.xml from the aforementioned location. | <p>This step is required. This will replace the Inspection Strategy records with new ones.</p> |
| 3 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> 09_MI_RRSKMAP.xml 10_MI_RRSKMDT.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities.</p> |

| Step | Task | Notes |
|------|---|---|
| 4 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 2888.</p> |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

| Step | Task | Notes |
|------|--|--|
| 1 | <p>Import Policy records that GE Digital modified in order to fix issues in the associated policy diagrams. This includes the following Policy records:</p> <ul style="list-style-type: none"> • Appendix G • Appendix H • Appendix I | <p>This step is required only if you use Policy records to generate RBI Recommendations.</p> |
| 2 | <p>Import the Inspection Strategy records that GE Digital 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 GE Digital APM Server machine: C:\Meridium\DbUpg\MI_DB_Master_4030000\4030000\20_IEU\50_Other\2_RecordsLinks 2. Import the file MI_INSP_STRAT.xml from the aforementioned location. | <p>This step is required. This will replace the Inspection Strategy records with new ones.</p> |

| Step | Task | Notes |
|------|---|---|
| 3 | In Functional Location records that represent units in your facility, select the Is a Unit? check box. | This step is required. |
| 4 | Using the <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>). | This step is optional. |
| 5 | Select the Enable Recommendations to be Generated at Created State check box in the RBI Global Preferences workspace. | This step is required only if you want to create RBI Recommendation records while RBI Analysis records are in the <i>Created</i> state. This check box is cleared by default. |
| 6 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 09_MI_RRSKMAP.xml • 10_MI_RRSKMDT.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | This step is required. This will overwrite the existing Strategy Mapping Composite Entities. |

| Step | Task | Notes |
|------|---|---|
| 7 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 2888.</p> |

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

| Step | Task | Notes |
|------|--|--|
| 1 | <p>Import Policy records that GE Digital modified in order to fix issues in the associated policy diagrams. This includes the following Policy records:</p> <ul style="list-style-type: none"> • Appendix G • Appendix H • Appendix I | <p>This step is required only if you use Policy records to generate RBI Recommendations.</p> |
| 2 | <p>Import the Inspection Strategy records that GE Digital 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 GE Digital APM Server machine: C:\Meridium\DbUpg\MI_DB_Master_4030000\4030000\20_IEU\50_Other\2_RecordsLinks 2. Import the file MI_INSP_STRAT.xml from the aforementioned location. | <p>This step is required. This will replace the Inspection Strategy records with new ones.</p> |

| Step | Task | Notes |
|------|--|---|
| 3 | In Functional Location records that represent units in your facility, select the Is a Unit? check box. | This step is required. |
| 4 | Using the <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>). | This step is optional. |
| 5 | Select the Enable Recommendations to be Generated at Created State check box in the RBI Global Preferences workspace. | This check box is cleared by default. This step is required only if you want to create RBI Recommendation records while RBI Analysis records are in the <i>Created</i> state. |
| 6 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 09_MI_RRSKMAP.xml • 10_MI_RRSKMDT.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | This step is required. This will overwrite the existing Strategy Mapping Composite Entities. |

| Step | Task | Notes |
|------|---|---|
| 7 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 2888.</p> |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Notes |
|------|--|--|
| 1 | <p>Import Policy records that GE Digital modified in order to fix issues in the associated policy diagrams. This includes the following Policy records:</p> <ul style="list-style-type: none"> • Appendix G • Appendix H • Appendix I | <p>This step is required only if you use Policy records to generate RBI Recommendations.</p> |

| Step | Task | Notes |
|------|--|--|
| 2 | <p>Import the Inspection Strategy records that GE Digital modified in order to fix issues in existing Inspection Strategy records. To do so:</p> <ol style="list-style-type: none"> Using the Import/Export Metadata window, navigate to the following location on the GE Digital APM Server machine: C:\Meridium\DbUpg\MI_DB_Master_4030000\4030000\20_IEU\50_Other\2_RecordsLinks Import the file MI_INSP_STRAT.xml from the aforementioned location. | <p>This step is required. This will replace the Inspection Strategy records with new ones.</p> |
| 3 | <p>In Functional Location records that represent units in your facility, select the Is a Unit? check box.</p> | <p>This step is required.</p> |
| 4 | <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> | <p>This step is optional.</p> |
| 5 | <p>Select the Enable Recommendations to be Generated at Created State check box in the RBI Global Preferences workspace.</p> | <p>This step is required only if you want to create RBI Recommendation records while RBI Analysis records are in the <i>Created</i> state. This check box is cleared by default.</p> |

| Step | Task | Notes |
|------|---|---|
| 6 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 09_MI_RRSKMAP.xml • 10_MI_RRSKMDT.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities.</p> |
| 7 | <p>On the GE Digital APM Server, using Configuration Manager, import the following files:</p> <ul style="list-style-type: none"> • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml <p>These files are located in the following folder: C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks. You must extract the 4030000 archive from the MI_DB_MASTER_4030000 archive.</p> | <p>This step is required. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in KBA 2888.</p> |

Risk Based Inspection Security Groups and Roles

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

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

| Security Group | Roles |
|---------------------------------------|--|
| RBI Security Groups | |
| MI RBI Administrator | MI Mechanical Integrity Administrator |
| MI RBI Analyst | MI Mechanical Integrity Administrator MI Mechanical Integrity Power |
| MI RBI Viewer | MI APM Viewer MI Mechanical Integrity Viewer |
| RBI Policy Security Groups | |
| MI RBI Calculation Policy Designer | None |
| MI RBI Calculation Policy Viewer | MI Mechanical Integrity Administrator MI Mechanical Integrity Power |
| MI RBI Recommendation Policy Designer | None |
| MI RBI Recommendation Policy Viewer | MI Mechanical Integrity Administrator MI Mechanical Integrity Power |
| MI RBI Risk Mapping Policy Designer | None |
| MI RBI Risk Mapping Policy Viewer | MI Mechanical Integrity Administrator MI Mechanical Integrity Power |

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

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

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

Note: If you have activated only the *Risk Based Inspection* license (and not the *RBI 581* license), then privileges to some of the following families do not exist for the MI RBI Administrator, MI RBI Analyst, and MI RBI Viewer Security Groups.

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

| Family | MI RBI Administrator | MI RBI Analyst | MI RBI Viewer |
|---|------------------------------|------------------------------|---------------|
| Criticality RBI Component - Cylindrical Shell | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Criticality RBI Component - Exchanger Bundle | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Criticality RBI Component - Exchanger Header | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Criticality RBI Component - Exchanger Tube | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Criticality RBI Component - Piping | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Criticality RBI Component - Tank Bottom | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Data Mapping Column-Field Pair | View, Update, Insert, Delete | View | View |
| Data Mapping Group | View, Update, Insert, Delete | View | View |
| Data Mapping Query | View, Update, Insert, Delete | View | View |
| Degradation Mechanisms Evaluation Factors | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Equipment | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Functional Location | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Grouping Element | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Inspection Task | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Inventory Group Configuration | View, Update, Insert, Delete | View | View |
| General Recommendation | View | View, Update, Insert, Delete | View |


| Family | MI RBI Administrator | MI RBI Analyst | MI RBI Viewer |
|--|------------------------------|------------------------------|---------------|
| Meridium Reference Tables | View, Update, Insert, Delete | View | View |
| Policy | View | View | View |
| Potential Degradation Mechanisms | View, Update, Insert, Delete | View | View |
| RBI 581 Admin Options | View, Update, Insert, Delete | View | View |
| RBI 581 Brittle Fracture Damage Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 Consequence Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 Cracking Damage Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 Damage Mechanism Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 External Cracking Damage Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 External Damage Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 HTHA Damage Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 Mechanical Fatigue Damage Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 Risk Analysis | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI 581 Thinning and Lining Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI Criticality Analysis | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI Custom DM Evaluation Configuration | View, Update, Insert, Delete | View | View |

| Family | MI RBI Administrator | MI RBI Analyst | MI RBI Viewer |
|--|------------------------------|------------------------------|---------------|
| RBI Custom DM Evaluation Configuration Details | View, Update, Insert, Delete | View | View |
| RBI Custom DM Evaluation Validation | View, Update, Insert, Delete | View | View |
| RBI Custom DM Evaluation Validation Details | View, Update, Insert, Delete | View | View |
| RBI Degradation Mechanisms | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI Inspection Auto-Selection Criteria | View, Update, Insert, Delete | View | View |
| RBI Recommendation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI Risk Matrix Mapping | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI Strategy Mapping Configuration | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI Strategy Mapping Details | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| RBI System | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Reference Document | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Risk Assessment | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Risk Rank | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Risk Translation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| SAP System | View | View | View |
| Strategy Logic Case | View, Update, Insert, Delete | View | View |

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

| Family | MI RBI Administrator | MI RBI Analyst | MI RBI Viewer |
|---|------------------------------|------------------------------|---------------|
| Has Inspections | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Inspection Scope | View | View | View |
| Has Potential Degradation Mechanisms | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has RBI Components | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has RBI Criticality Analysis | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has RBI Custom DME Configuration | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has RBI Custom DME Validation | View, Update, Insert, Delete | View | View |
| Has RBI Degradation Mechanisms Evaluation | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has RBI Strategy Mapping Configuration | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has RBI Systems | 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 |
| Has Reference Values | View | View | View |
| Has SAP System | View | View | View |
| Has Superseded Recommendations | View | View, Update, Insert, Delete | View |
| Has Task Revision | View | View, Update, Insert, Delete | View |
| Has Tasks | View, Update, Insert, Delete | View, Update, Insert, Delete | View |

| Family | MI RBI Administrator | MI RBI Analyst | MI RBI Viewer |
|--|------------------------------|------------------------------|---------------|
| Has Time Based Inspection Interval | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Unmitigated Risk | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Is Based on RBI Degradation Mechanisms | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Is Mitigated | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Is Part of Group | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Mapped to RBI Component | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Represents Inspections | View, Update, Insert, Delete | View, Update, Insert, Delete | View |

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

The following families are *not* used elsewhere in the RBI module. Privileges to these families support integration with the Inspection Management module:

- Has Inspection Scope
- Has Time Based Inspection Interval
- Time Based Inspection Interval
- Time Based Inspection Setting

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

Deploy Root Cause Analysis (RCA)

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

Deploy Root Cause Analysis (RCA) for the First Time

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

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

Note: If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

| Step | Task | Notes |
|------|--|--|
| 1 | Review the RCA data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Modify any relationship definitions as required. | This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families. |
| 2 | Assign Security Users to one or more of the RCA Security Groups and Roles . | This step is required. Users will not be able to access Root Cause Analysis unless they belong to an RCA Security Group . |
| 3 | Specify the Team Charter after you create a new Root Cause Analysis record. | This step is optional. A default Team Charter exists in the baseline GE Digital APM database. You can select the default Team Charter or define your own. |
| 4 | Specify the Critical Success Factors after you create a new Root Cause Analysis record. | This step is optional. Default Critical Success Factors exist in the baseline GE Digital APM database. You can select one or more default Critical Success Factors or define your own. |

Upgrade or Update Root Cause Analysis (RCA) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital 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 V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.1 through V3.5.1.12.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

This module will be upgraded to V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital 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 V4.3.0.2.0 automatically when you upgrade the components in the basic GE Digital 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 MI APM Viewer |

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

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

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

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

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

Deploy Rounds

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

Deploy Rounds for the First Time

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

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


Note: If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

APM Sync Server


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

| Step | Task | Notes |
|------|---|--|
| 1 | <p>Configure the APM Sync Server. Configuring the APM Sync Server includes completing the following steps.</p> <ol style="list-style-type: none"> Install GE Digital 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. | <p>This step is required only if you want to use Operator Rounds on Windows Mobile handheld devices.</p> |
| 2 | <p>Configure security for the MeridiumSyncService Service.</p> | <p>This step is required only if you want to use Operator Rounds on Windows Mobile handheld devices.</p> |

Module-level Configuration Tasks

| Step | Task | Notes |
|------|--|---|
| 1 | <p>Review the Rounds data model to determine which relationship definitions you will need to modify to include your custom asset families. Modify any relationship definitions as needed. For example, if you have created a new asset family, create a relationship definition as follows:</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 | <p>This step is required only if you have asset data in families outside of the baseline Equipment and Functional Location families.</p> |
| 2 | <p>Assign Security Users to the following Rounds Security Groups and Roles:</p> <ul style="list-style-type: none"> • MI Operator Rounds Administrator • MI Operator Rounds Mobile User | <p>This step is required.</p> <div style="border: 1px solid yellow; padding: 5px;"> <p> Note: The MAPM Security Group that has been provided with GE Digital 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.</p> </div> |
| 3 | <p>Manage Measurement Location Template mappings.</p> | <p>This step is required only if you added fields to the Measurement Location Template family via Configuration Manager.</p> |
| 4 | <p>Install the GE Digital APM application on the mobile device that you plan to use for data collection.</p> | <p>This step is required only if you want to use a mobile device for data collection.</p> |
| 5 | <p>Set the local time zone on the mobile device that you will use for data collection, typically the user time zone.</p> | <p>This step is required only if you will use a mobile device for data collection.</p> |

| Step | Task | Notes |
|------|--|--|
| 6 | Set up the Scheduled Compliance task. | This step is required. The scheduled compliance task should be configured to start as soon as the Rounds module is deployed and set to run continuously as long as Rounds in use. |
| 7 | Configure automatic synchronization of Measurement Location and Measurement Location Template Records with Allowable Values. | This step is optional. |

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

Windows Mobile Handheld Device

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

| Step | Task | Notes |
|------|---|------------------------|
| 1 | Ensure that all the Windows Mobile handheld devices that you want to use with Operator Rounds meet the software requirements. | This step is required. |
| 2 | Install the .NET Compact Framework. | This step is required. |
| 3 | Install Microsoft SQL CE. Install Microsoft SQL CE. | This step is required. |
| 4 | Install Microsoft Sync Services for ADO.NET. | This step is required. |
| 5 | Install the GE Digital APM Mobile Framework. | This step is required. |
| 6 | Access Device Settings Screen. | This step is required. |
| 7 | Identify the Sync Server within the APM Mobile Framework. | This step is required. |
| 8 | Specify the security query to be used with the APM Mobile Framework. | This step is required. |
| 9 | Modify the user time-out value. | This step is required. |
| 10 | Install Operator Rounds. | This step is required. |

| Step | Task | Notes |
|------|---|--|
| 11 | <p>Configure barcode scanning. Configuring barcode scanning includes the following steps:</p> <ul style="list-style-type: none"> • Install the Barcode add-on. • Enable barcode scanning. | <p>This step is required only if you will use an Barcode scanner with Operator Rounds.</p> |
| 12 | <p>Configure RFID tag scanning. Configuring RFID scanning includes the following steps:</p> <ul style="list-style-type: none"> • Install the RFID add-on. • Enable RFID tag scanning. | <p>This step is required only if you will use an RFID scanner with Operator Rounds.</p> |
| 13 | <p>Install translations for Operator Rounds.</p> | <p>This step is required only if you are using translations.</p> |

Upgrade or Update Rounds to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

This module will be updated to V4.3.0.2.0 automatically when you update the components in the basic GE Digital APM system architecture. No additional steps are required.

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

| Step | Task | Notes |
|------|---|--|
| 1 | Prior to upgrading your database, complete the pre-upgrade steps for lubrication . | <p>This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 2 | After upgrading your database, complete the post-upgrade steps for lubrication . | <p>This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 3 | Depending on the type of mobile device you use for data collection, install the APM mobile application on tablet devices or upgrade the components on Windows Mobile handheld devices . | This step is required only if you will use a mobile device for data collection. |
| 4 | Set the local time zone on the mobile device that you will use for data collection. | This step is required only if you will use a mobile device for data collection. |

| Step | Task | Notes |
|------|---|------------------------|
| 5 | Create the initial default sequencing schedule by accessing the Rounds Designer administration page . | This step is required. |

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

| Step | Task | Notes |
|------|---|--|
| 1 | Prior to upgrading your database, complete the pre-upgrade steps for lubrication . | <p>This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 2 | After upgrading your database, complete the post-upgrade steps for lubrication . | <p>This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 3 | Depending on the type of mobile device you use for data collection, install the APM mobile application on tablet devices or upgrade the components on Windows Mobile handheld devices . | This step is required only if you will use a mobile device for data collection. |
| 4 | Set the local time zone on the mobile device that you will use for data collection. | This step is required only if you will use a mobile device for data collection. |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| Step | Task | Notes |
|------|---|--|
| 1 | Prior to upgrading your database, complete the pre-upgrade steps for lubrication . | <p>This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 2 | After upgrading your database, complete the post-upgrade steps for lubrication . | <p>This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 3 | Depending on the type of mobile device you use for data collection, install the APM mobile application on tablet devices or upgrade the components on Windows Mobile handheld devices . | This step is required only if you will use a mobile device for data collection. |
| 4 | Set the local time zone on the mobile device that you will use for data collection. | This step is required only if you will use a mobile device for data collection. |

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

| Step | Task | Notes |
|------|--|--|
| 1 | Prior to upgrading your database, complete the pre-upgrade steps for lubrication . | <p>This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |

| Step | Task | Notes |
|------|---|--|
| 2 | Prior to upgrading your database, modify checkpoints linked to multiple assets so that they are only linked to one asset. | This step is necessary because a checkpoint can now be linked to only one asset. |
| 3 | Prior to upgrading your database, complete specific steps to upgrade records with schedules containing end dates. | This step is required only if you have any records with schedules containing end dates. |
| 4 | After upgrading your database, complete the post-upgrade steps for lubrication. | <p>This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 5 | Install the APM mobile application, or the APM Mobile Framework , on the mobile device that you will use for data collection. | This step is required only if you will use a mobile device for data collection. |
| 6 | Set the local time zone on the mobile device that you will use for data collection. | This step is required only if you will use a mobile device for data collection. |
| 7 | Confirm the assignment of Security Users for the existing route subscriptions and make additional assignments if needed. | <p>This step is required.</p> <p>Routes that a user was subscribed to via the Meridium V3.6 mobileAPM application will be assigned to that user automatically through the database upgrade process.</p> |

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

| Step | Task | Notes |
|------|---|--|
| 1 | Prior to upgrading your database, complete the pre-upgrade steps for lubrication . | <p>This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 2 | Prior to upgrading your database, modify checkpoints linked to multiple assets so that they are only linked to one asset . | This step is necessary because a checkpoint can now be linked to only one asset. |
| 3 | Prior to upgrading your database, complete specific steps to upgrade records with schedules containing end dates . | This step is required only if you have any records with schedules containing end dates. |
| 4 | After upgrading your database, complete the post-upgrade steps for lubrication . | <p>This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 5 | Depending on the type of mobile device you use for data collection, install the APM mobile application on tablet devices or upgrade the components on Windows Mobile handheld devices . | This step is required only if you will use a mobile device for data collection. |
| 6 | Set the local time zone on the mobile device that you will use for data collection. | This step is required only if you will use a mobile device for data collection. |
| 7 | Confirm the assignment of Security Usrs for the existing route subscriptions and make additional assignments if needed . | <p>This step is required.</p> <p>Routes that a user was subscribed to via the Meridium V3.6 mobileAPM application will be assigned to that user automatically through the database upgrade process.</p> |

Upgrade from any version V3.5.1 through V3.5.1.12.1

| Step | Task | Notes |
|------|---|--|
| 1 | Prior to upgrading your database, complete the pre-upgrade steps for lubrication . | <p>This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 2 | Prior to upgrading your database, modify checkpoints linked to multiple assets so that they are only linked to one asset . | This step is necessary because a checkpoint can now be linked to only one asset. |
| 3 | Prior to upgrading your database, complete specific steps to upgrade records with schedules containing end dates . | This step is required only if you have any records with schedules containing end dates. |
| 4 | After upgrading your database, complete the post-upgrade steps for lubrication . | <p>This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 5 | Depending on the type of mobile device you use for data collection, install the APM mobile application on tablet devices or upgrade the components on Windows Mobile handheld devices . | This step is required only if you will use a mobile device for data collection. |
| 6 | Set the local time zone on the mobile device that you will use for data collection. | This step is required only if you will use a mobile device for data collection. |
| 7 | Assign mobile device users to Routes. | This step is required only if you will use a mobile device for data collection. |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

| Step | Task | Notes |
|------|---|--|
| 1 | Prior to upgrading your database, complete the pre-upgrade steps for lubrication . | <p>This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 2 | Prior to upgrading your database, modify checkpoints linked to multiple assets so that they are only linked to one asset . | This step is necessary because a checkpoint can now be linked to only one asset. |
| 3 | Prior to upgrading your database, complete specific steps to upgrade records with schedules containing end dates . | This step is required only if you have any records with schedules containing end dates. |
| 4 | After upgrading your database, complete the post-upgrade steps for lubrication . | <p>This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 5 | Depending on the type of mobile device you use for data collection, install the APM mobile application on tablet devices or upgrade the components on Windows Mobile handheld devices . | This step is required only if you will use a mobile device for data collection. |
| 6 | Set the local time zone on the mobile device that you will use for data collection. | This step is required only if you will use a mobile device for data collection. |
| 7 | Assign mobile device users to Routes. | This step is required only if you will use a mobile device for data collection. |

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

| Step | Task | Notes |
|------|--|--|
| 1 | <p>Prior to upgrading your database, complete the pre-upgrade steps for lubrication.</p> | <p>This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 2 | <p>Prior to upgrading your database, modify checkpoints linked to multiple assets so that they are only linked to one asset.</p> | <p>This step is necessary because a checkpoint can now be linked to only one asset.</p> |
| 3 | <p>Prior to upgrading your database, complete specific steps to upgrade records with schedules containing end dates.</p> | <p>This step is required only if you have any records with schedules containing end dates.</p> |

| Step | Task | Notes |
|------|---|--|
| 4 | After upgrading your database, complete the post-upgrade steps for lubrication . | <p>This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 5 | Depending on the type of mobile device you use for data collection, install the APM mobile application on tablet devices or upgrade the components on Windows Mobile handheld devices . | This step is required only if you will use a mobile device for data collection. |
| 6 | Set the local time zone on the mobile device that you will use for data collection. | This step is required only if you will use a mobile device for data collection. |

| Step | Task | Notes |
|------|---------------------------------------|---|
| 7 | Assign mobile device users to Routes. | This step is required only if you will use a mobile device for data collection. |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Notes |
|------|--|--|
| 1 | Prior to upgrading your database, complete the pre-upgrade steps for lubrication . | <p>This step is required only if you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |
| 2 | Prior to upgrading your database, modify checkpoints linked to multiple assets so that they are only linked to one asset . | This step is necessary because a checkpoint can now be linked to only one asset. |
| 3 | Prior to upgrading your database, complete specific steps to upgrade records with schedules containing end dates . | This step is required only if you have any records with schedules containing end dates. |
| 4 | After upgrading your database, complete the post-upgrade steps for lubrication . | <p>This step is required only if you have Lubrication Requirement or Lubrication Requirement Template records in your database.</p> <p>This step is necessary due to various changes in the data model for records related to lubrication.</p> |

| Step | Task | Notes |
|------|---|---|
| 5 | Depending on the type of mobile device you use for data collection, install the APM mobile application on tablet devices or upgrade the components on Windows Mobile handheld devices . | This step is required only if you will use a mobile device for data collection. |
| 6 | Set the local time zone on the mobile device that you will use for data collection. | This step is required only if you will use a mobile device for data collection. |
| 7 | Assign mobile device users to Routes. | This step is required only if you will use a mobile device for data collection. |

Manage the Measurement Location Template Mappings

The Measurement Location Template family and the Measurement Location family are provided as part of the baseline Rounds data model. If you create a Measurement Location Template in the GE Digital 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.

APM Sync Services Tasks

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

Install APM Sync Services

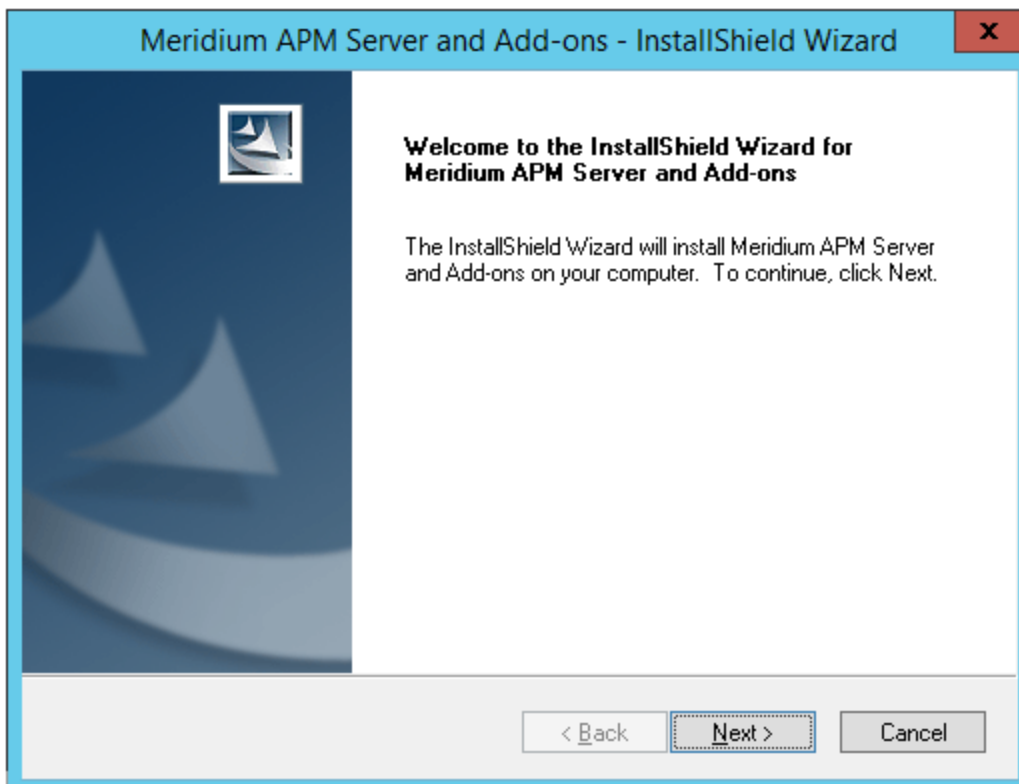
Before You Begin

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

Steps

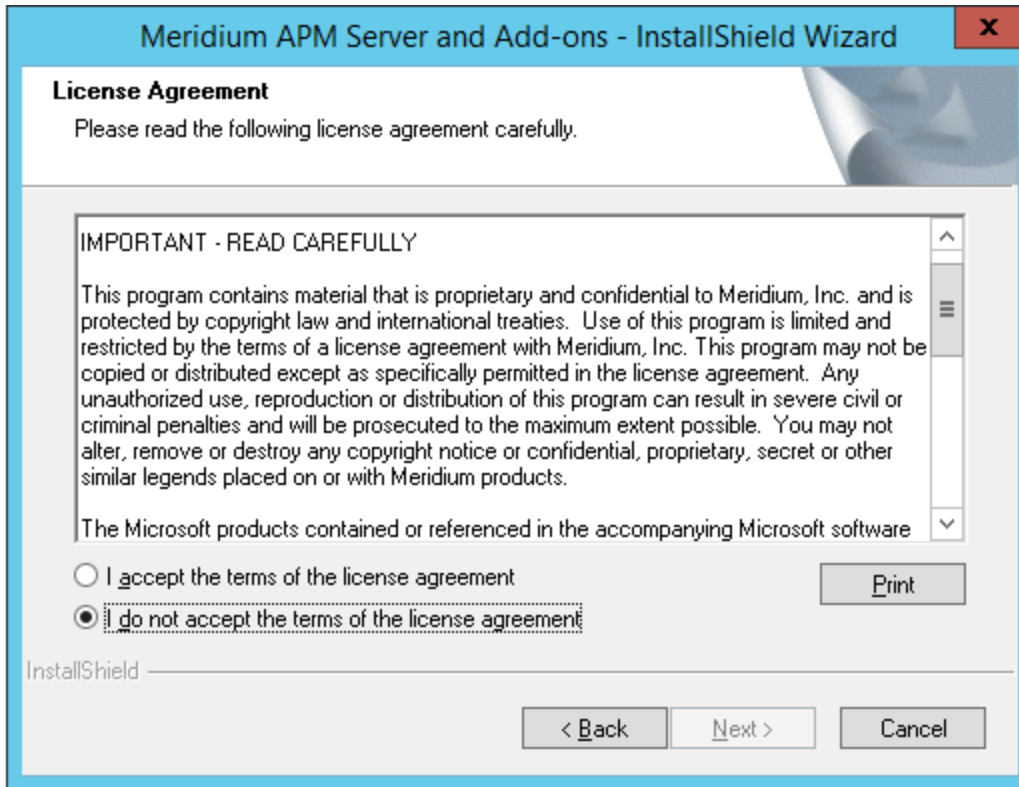
1. On the APM Sync Server machine, access the GE Digital APM distribution package, and then navigate to the **Meridium APM Server and Add-ons** folder.
2. Open the file **Setup.exe**.

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



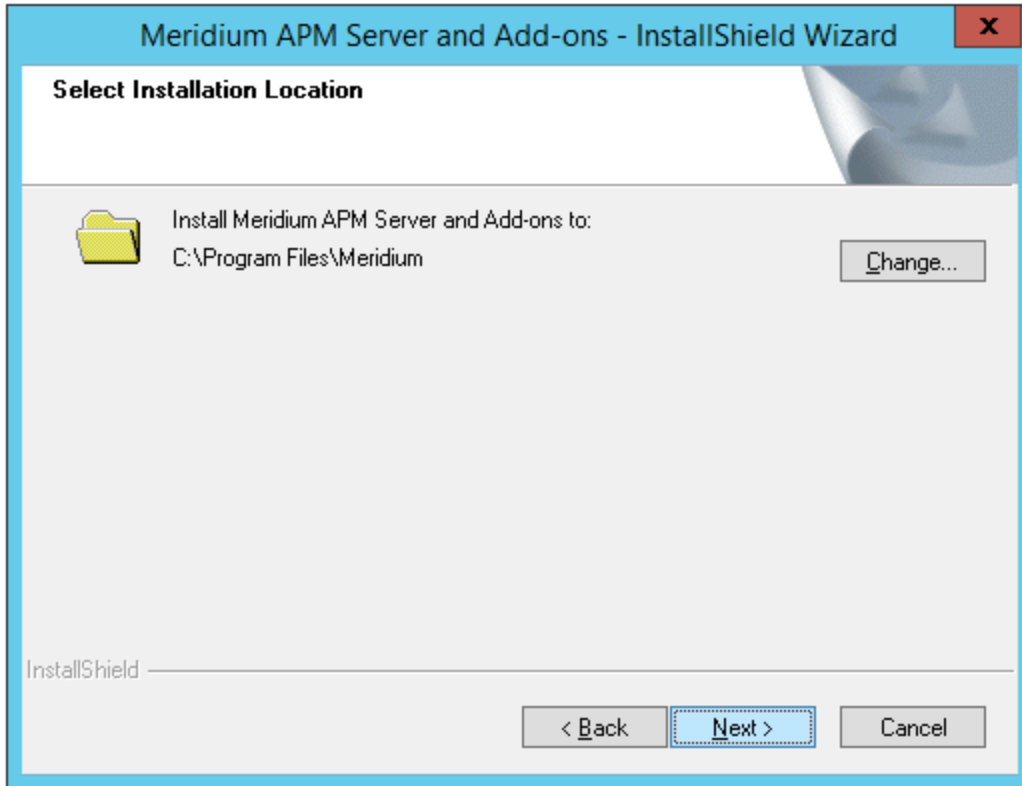
3. Select **Next**.

The **License Agreement** screen appears.



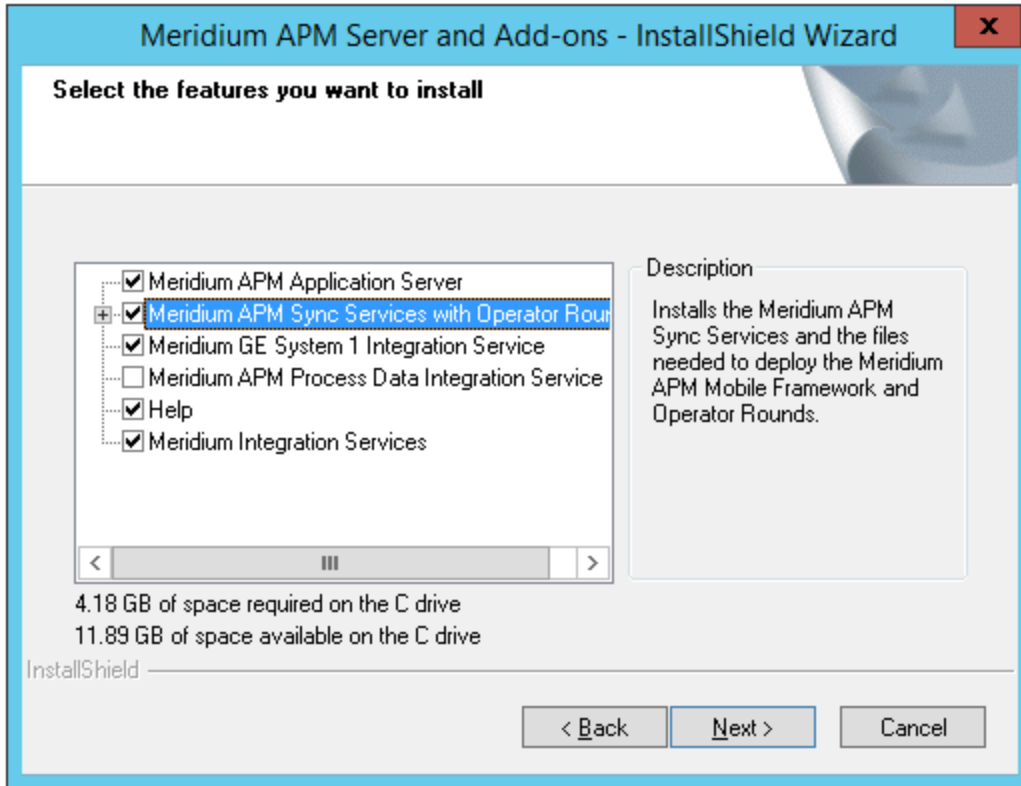
4. Read the License Agreement and, if you agree, select the **I accept the terms of the license agreement** option. Then, select **Next** button.

The **Select Installation Location** screen appears.



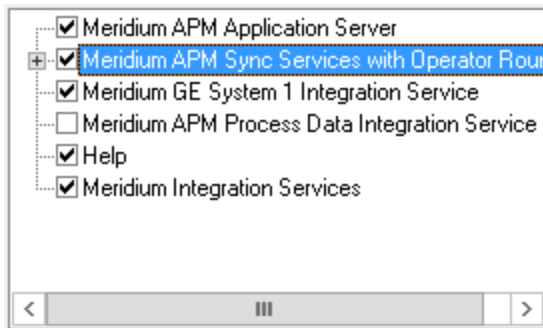
5. Select **Next** to accept the default location.

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 APM Sync Server machine.

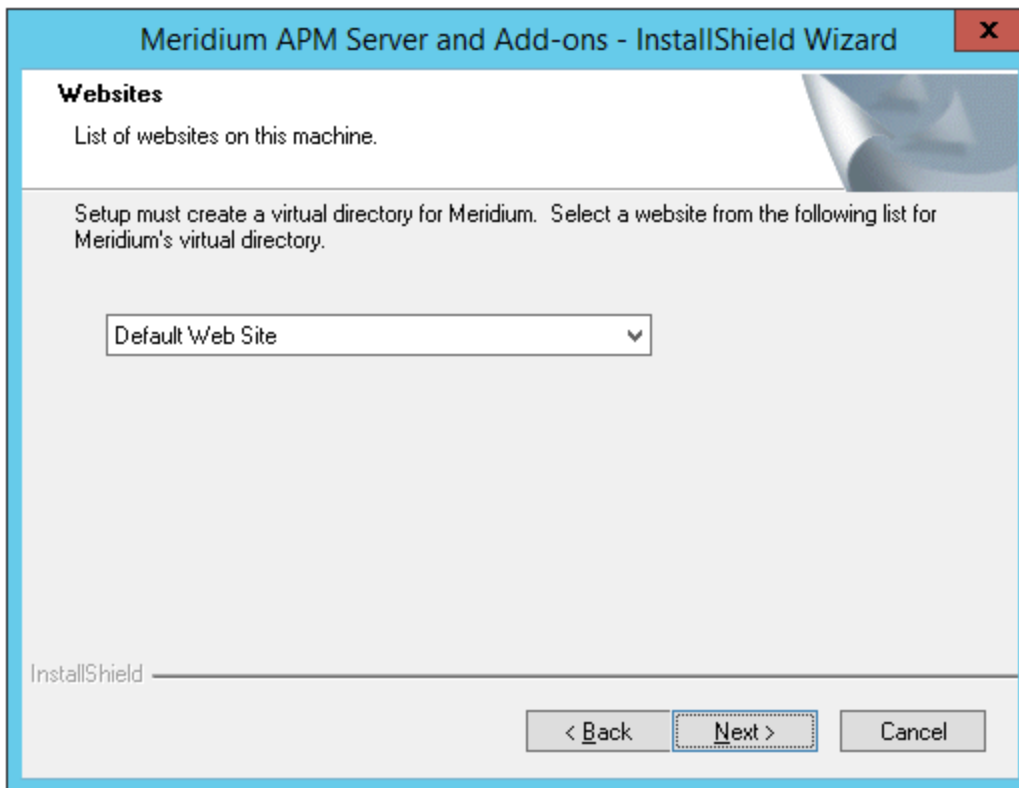
6. Select the **Meridium APM Application Server** and **Meridium Sync Services with Operator Rounds** check boxes. All the subnodes that appear below these nodes become selected automatically.




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

7. Select **Next**.

The **websites** screen appears.

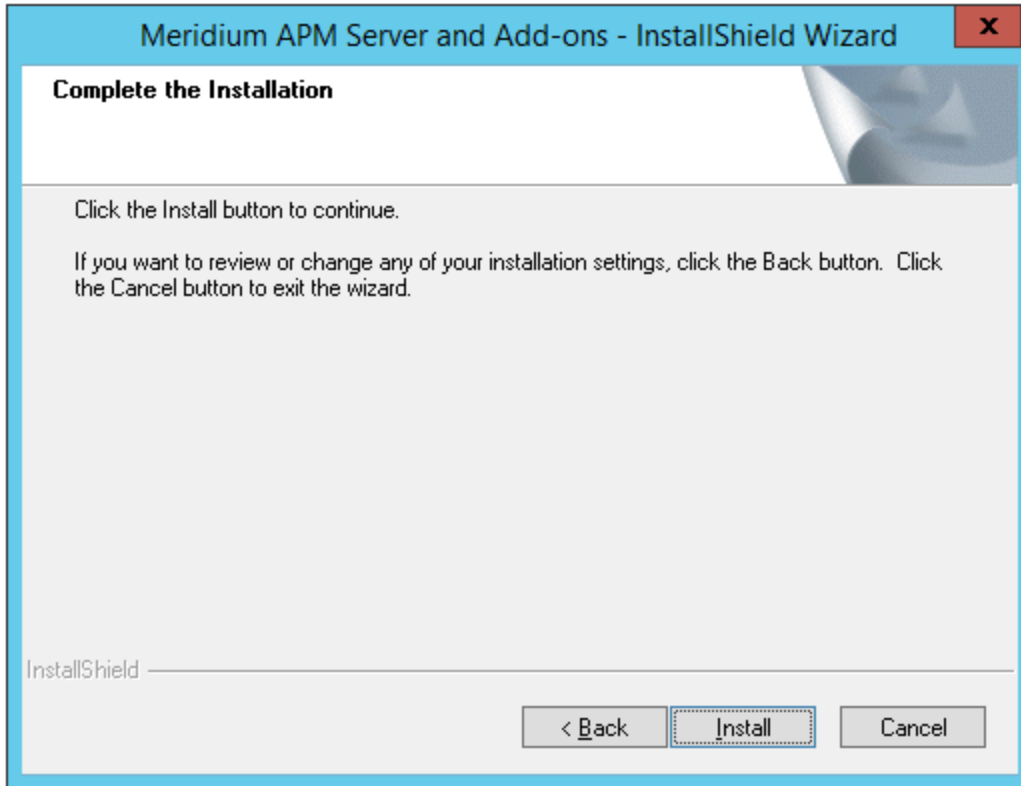


8. Select the website where you want to create a virtual directory for APM Sync Services.

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

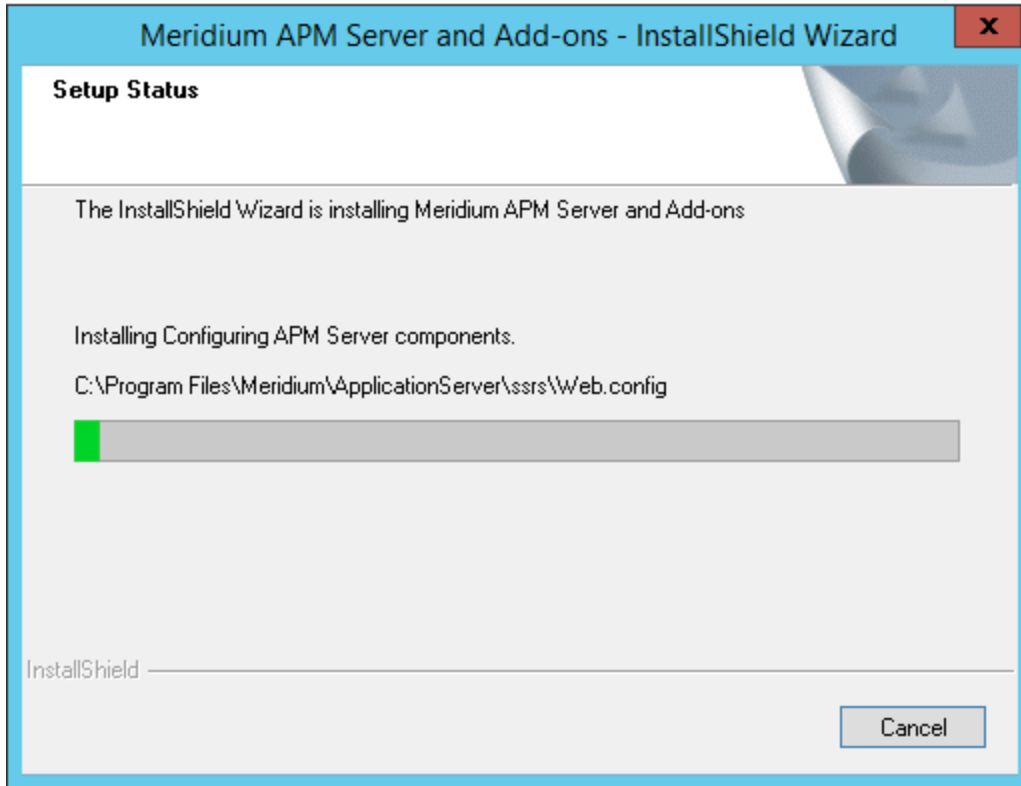
9. Select **Next**.

The **Complete the Installation** screen appears.

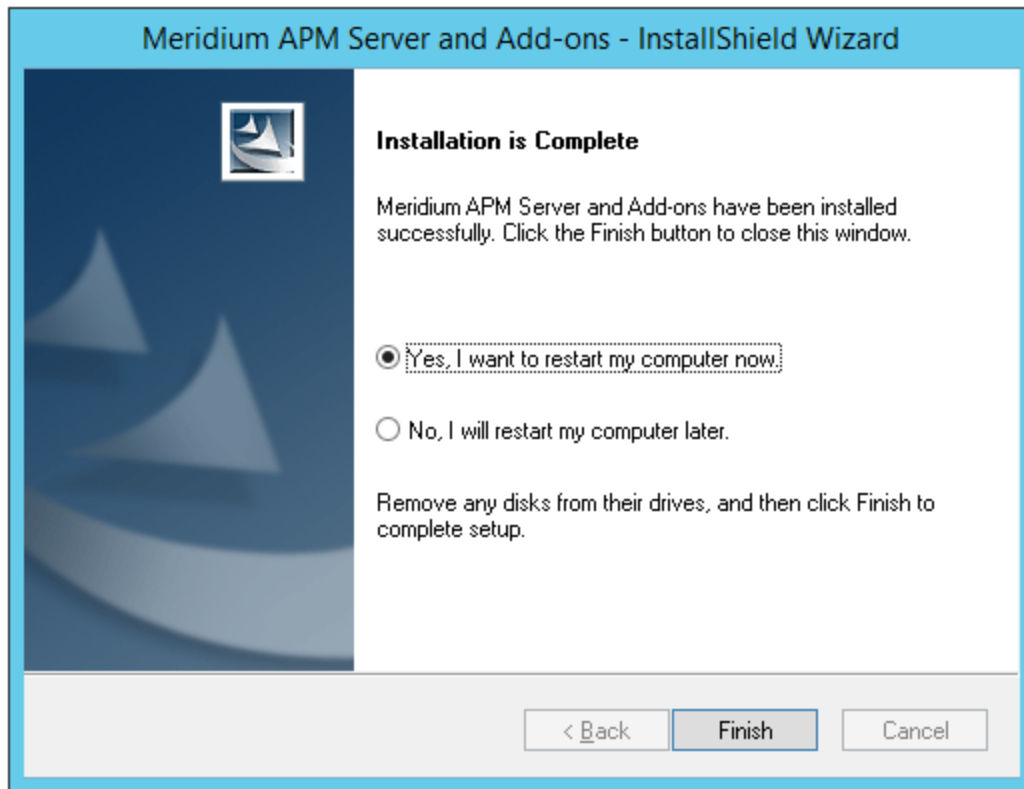


10. Select **Install**.

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 APM Sync Services

Steps

1. On the 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 APM Sync Services is installed.

The following page appears, indicating that 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 APM Sync Server machine, access the GE Digital 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 GE Digital 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:

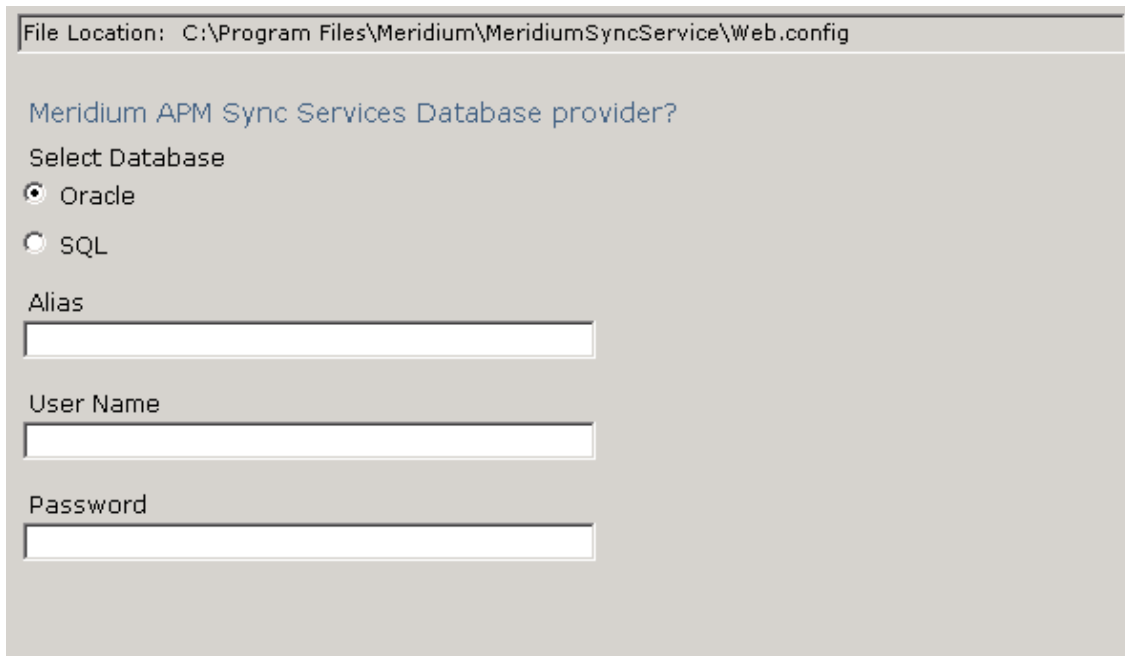
- The Oracle database that will contain the database tables for the APM Sync Services already exists.
- You have accessed the APM System Administration tool on the APM Sync Server machine.

 **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 GE Digital 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 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:

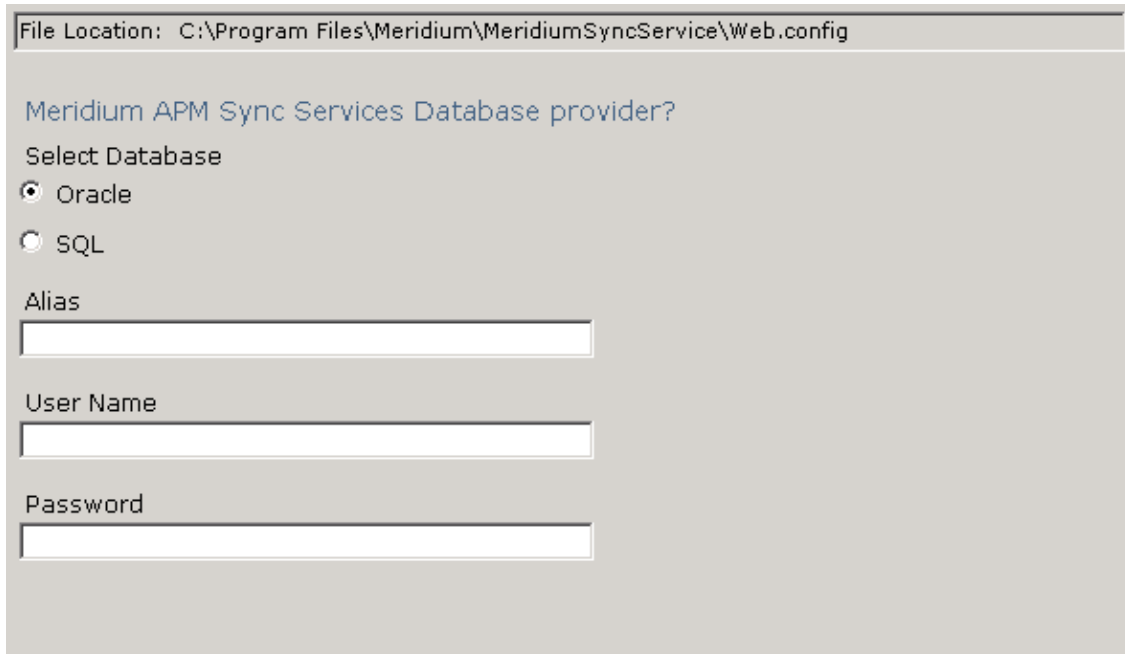
- The SQL database that will contain the database tables for the APM Sync Services already exists.
- You have accessed the APM System Administration tool on the APM Sync Server machine.

 **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 GE Digital 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 APM Sync Services.



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

Meridium APM Sync Services Database provider?

Select Database

Oracle

SQL

Alias

User Name

Password

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

The SQL settings appear and replace the Oracle settings.

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

Meridium APM Sync Services Database provider?

Select Database

Oracle

SQL

DB Server

DB Name

User Name

Password

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

Modify APM Sync Config

When you perform a sync operation in the APM Mobile Framework, the device connects to the APM Sync Server, which in turn connects to the specified GE Digital 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 APM Sync Server:

- The GE Digital APM Server
- The GE Digital APM data source
- The APM Sync Services Security User credentials that will be used to connect the APM Sync Server to the GE Digital 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 APM Sync Server machine.

The following instructions provide details on defining the GE Digital 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 APM Sync Services server machine.

Steps

1. Access the GE Digital 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 APM Server machine that you want to use with Sync Services.
4. In the **Data Source** box, enter the name of the GE Digital 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 GE Digital 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 GE Digital 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 APM Sync Service

When you install APM Sync Services, the service MeridiumSyncService is created under the Default Web Site in IIS on the 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 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 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 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 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 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 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 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 APM Sync Services is installed.

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

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

2. Select **MFX.APM.<version>.ARM4.CAB**, where **<version>** is the corresponding version of GE Digital APM.

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

3. Select **Yes**.

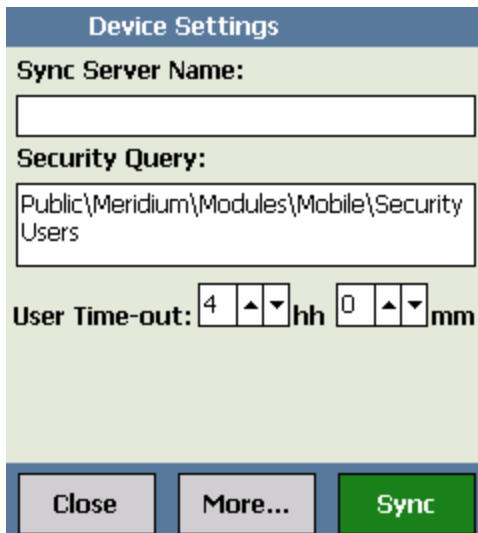
The file is downloaded, and the APM Mobile Framework is installed. When the installation is complete, a message will appear, indicating that the installation is successful.

The **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 **APM Mobile Framework** screen appears.
3. Select **Settings**.
The **Device Settings** screen appears.



Identify the Sync Server Within the APM Mobile Framework on Windows Mobile Device

Steps

1. [Access the Device Settings screen.](#)
2. In the **Sync Server Name** box, type the name or IP address of the server on which APM Sync Services is installed.

 **Note:** At this point, you can also specify the security query.

3. 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.

4. When the process is complete, select **Close**.

Specify the Security Query on Windows Mobile Device

Steps

1. [Access the Device Settings screen.](#)

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 GE Digital APM Catalog folder `\\Public\Meridium\Modules\Mobile`.

2. 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 GE Digital 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 GE Digital 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 GE Digital APM Catalog folder `\\Public\Meridium\Modules\Operator Rounds\Queries\Download Queries`, enter Chicago Users.

Likewise, if the Chicago Users query is stored in the GE Digital APM Catalog folder `\\Public\Meridium\Modules\Operator Rounds\Queries\Download Queries\Users\Chicago`, enter `Users\Chicago\Chicago Users`.

3. 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 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 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 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 APM Mobile Framework](#).

Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** screen appears.

2. Select **APM Mobile Framework**.

The **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 **APM Mobile Framework** closes, and the **Operator Rounds** application is installed.

 **Note:** After the installation is complete, the APM Mobile Framework will reopen automatically and return you to the **APM Mobile Framework** screen.

Install the Barcode Add-on on Windows Mobile Device

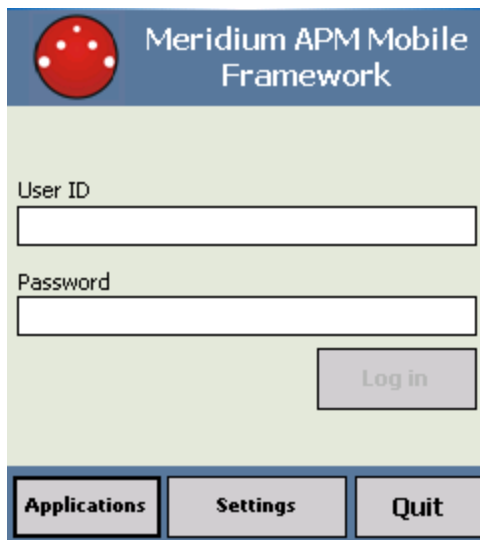
Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** window appears.

2. Select **APM Mobile Framework**.

The **Meridium APM Mobile Framework** window appears.



The screenshot shows the Meridium APM Mobile Framework application window. At the top left is a red circular logo with four white dots. To its right, the text "Meridium APM Mobile Framework" is displayed in white on a blue background. Below this, the main area has a light green background. It contains two text input fields: "User ID" and "Password". To the right of the "Password" field is a grey "Log in" button. At the bottom of the window, there is a dark blue bar with three buttons: "Applications" (highlighted), "Settings", and "Quit".

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 APM Mobile Framework closes, and the Barcode add-on is installed.

 **Note:** After the installation is complete, the APM Mobile Framework will reopen automatically, and the APM Mobile Framework screen appears and you can enable Barcode scanning.

Enable Barcode Scanning on Windows Mobile Device

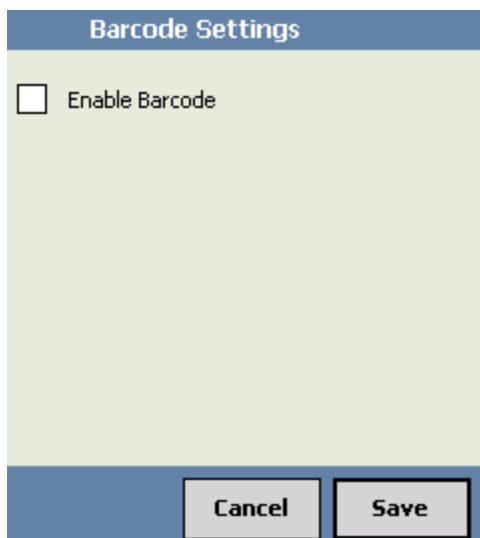
Before You Begin

- [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

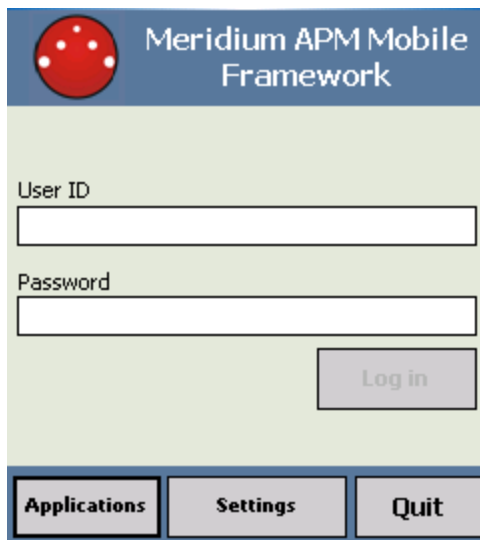
Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** screen appears.

2. Select **APM Mobile Framework**.

The **Meridium APM Mobile Framework** screen appears.



Meridium APM Mobile Framework

User ID

Password

Log in

Applications Settings Quit

3. Select **Applications**.

The **Add/Remove Applications** screen appears.



4. In the list of applications, select the **Install** button that appears to the right of **RFID**.

A message appears, asking if you want to install the RFID add-on.

5. Select **Yes**.

The installation process begins. During this process, the **APM Mobile Framework** closes, and the RFID add-on is installed.

Note: After the installation process is complete, the **APM Mobile Framework** reopens automatically, and the 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.](#)



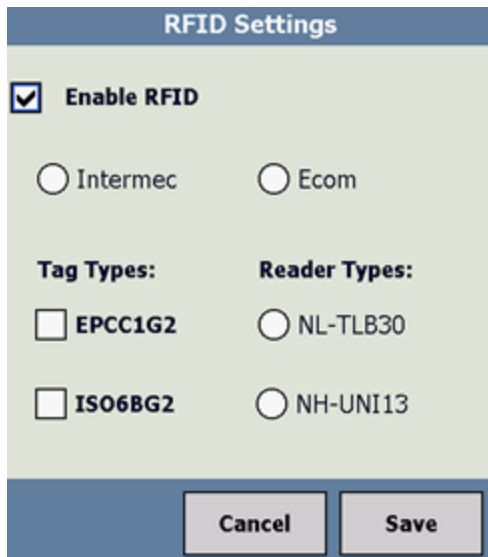
2. Select **More**.

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 blue header bar with the text "RFID Settings". Below the header, there is a section with a checked checkbox labeled "Enable RFID". Underneath, there are two radio button options: "Intermec" and "Ecom". Below these, there are two columns of settings. The first column is labeled "Tag Types:" and contains two checkboxes: "EPCC1G2" and "ISO6BG2". The second column is labeled "Reader Types:" and contains two radio buttons: "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 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 **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. **APM Mobile Framework** closes, and the translations are installed.

 **Note:** After the installation is complete, the APM Mobile Framework will reopen automatically and return you to the APM Mobile Framework screen.

Uninstall 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 APM Mobile Framework is removed from the Windows Mobile handheld device.

Uninstall then RFID Add-on on Windows Mobile Device

Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** screen appears.

2. Select **APM Mobile Framework**.

The **Meridium APM Mobile Framework** screen appears.



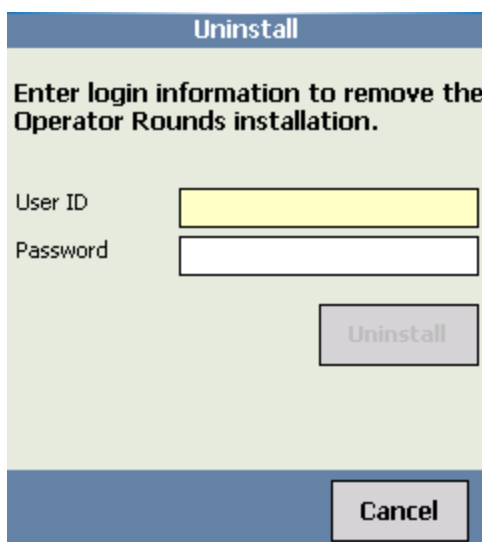
3. Select **Applications**.

The **Add/Remove Applications** screen appears. This following image shows an example of the **Add/Remove Applications** screen.




4. In the list of available applications, to the right of **RFID** , select **Uninstall**.

The **Uninstall** screen appears, prompting you to enter your username and password.



5. In the **User ID** box, enter your username.
The **Uninstall** button is enabled.
6. In the **Password** box, enter your password.

 **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 APM Mobile Framework closes, and the **RFID** add-on is uninstalled.

Uninstall the Barcode Add-on on Windows Mobile Device

Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** screen appears.

2. Select **APM Mobile Framework**.

The **Meridium APM Mobile Framework** screen appears.



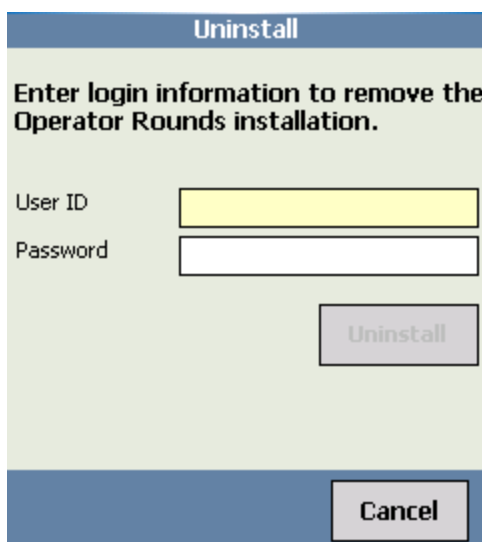
3. Select **Applications**.

The **Add/Remove Applications** screen appears. This following image shows an example of the **Add/Remove Applications** screen.




4. In the list of available applications, to the right of **Barcode**, select **Uninstall**.

The **Uninstall** screen appears, prompting you to enter your username and password.



5. In the **User ID** box, enter your username.
The **Uninstall** button is enabled.
6. In the **Password** box, enter your password.

 **Note:** If the credentials that you enter are not associated with a Security User who is a Super User or member of the MI Operator Rounds Administrator Security Group, a message will appear, indicating that you do not have the privileges required to uninstall the application.

7. Select **Uninstall**.

The uninstallation process begins. The APM Mobile Framework closes, and the Barcode add-on is uninstalled.

Uninstall Translations for Operator Rounds on Windows Mobile Device

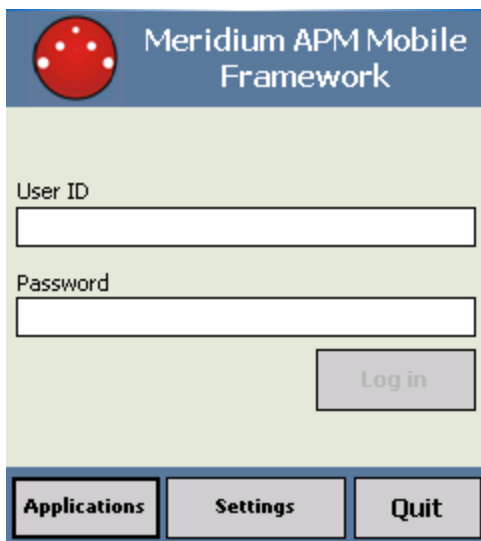
Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** screen appears.

2. Select **APM Mobile Framework**.

The **Meridium APM Mobile Framework** screen appears.



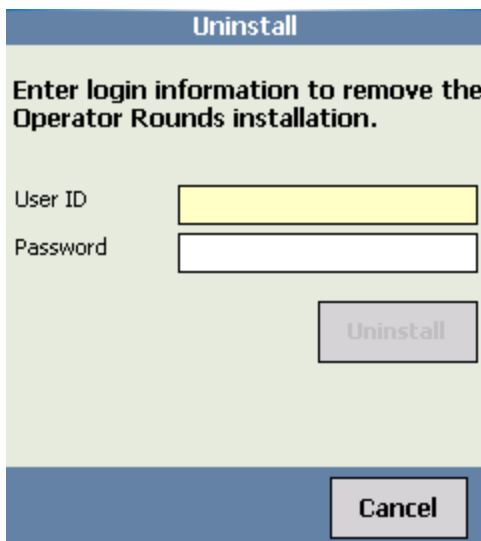
3. Select **Applications**.

The **Add/Remove Applications** screen appears. This following image shows an example of the **Add/Remove Applications** screen.




4. In the list of available applications, to the right of the language whose translation you want to uninstall, select **Uninstall**.

The **Uninstall** screen appears, prompting you to enter your username and password.



5. In the **User ID** box, enter your username.
The **Uninstall** button is enabled.
6. In the **Password** box, enter your password.

 **Note:** If the credentials that you enter are not associated with a Security User who is a Super User or member of the MI Operator Rounds Administrator Security Group, a mes-

sage will appear, indicating that you do not have the privileges required to uninstall the application.

7. Select **Uninstall**.

The uninstallation process begins. The APM Mobile Framework closes, and the translations add-on for a language is uninstalled.

Uninstall Operator Rounds on Windows Mobile Device

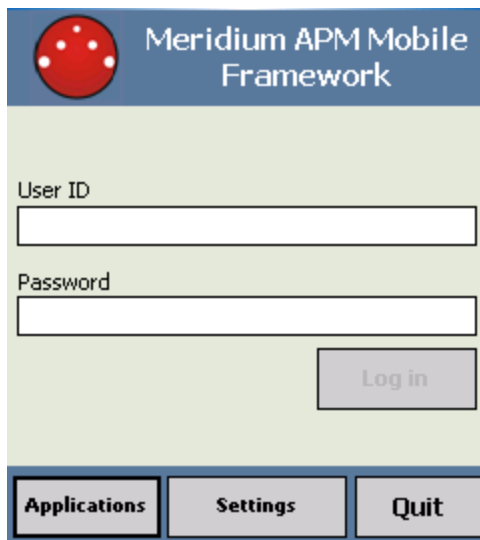
Steps

1. On the Windows Start menu, select **Programs**.

The **Programs** screen appears.

2. Select **APM Mobile Framework**.

The **Meridium APM Mobile Framework** screen appears.



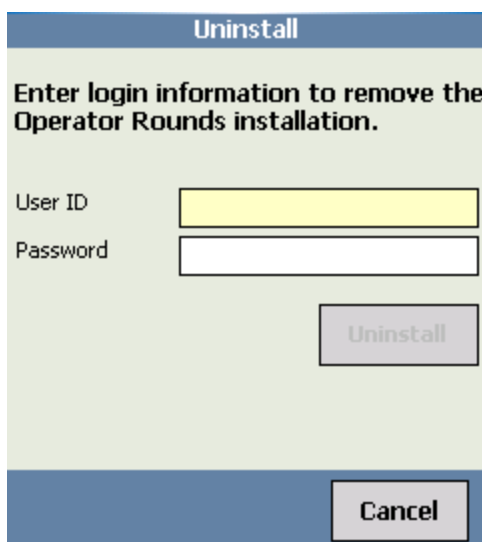
The screenshot shows the Meridium APM Mobile Framework interface. At the top, there is a blue header with a red circular logo on the left and the text "Meridium APM Mobile Framework" on the right. Below the header is a light green area containing two text input fields: "User ID" and "Password". To the right of the "Password" field is a grey button labeled "Log in". At the bottom of the screen, there is a blue bar with three buttons: "Applications", "Settings", and "Quit".

3. Select **Applications**.


The **Add/Remove Applications** screen appears. This following image shows an example of the **Add/Remove Applications** screen.



4. In the list of available applications, to the right of the **Operator Rounds**, select **Uninstall**.
The **Uninstall** screen appears, prompting you to enter your username and password.



5. In the **User ID** box, enter your username.
The **Uninstall** button is enabled.
6. In the **Password** box, enter your password.

 **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 APM Mobile Framework closes, and the **Operator Rounds** is uninstalled.

Upgrade Windows Mobile Handheld Device

After you upgrade the 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 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 GE Digital 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., 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 APM Mobile Framework closes automatically to allow the upgrade process to be completed.

When the upgrade process is complete, some of the 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. You will then need to go to the **Add/Remove Applications** window and upgrade any remaining add-ons.

 **Note:** You are not required to update Windows Mobile Devices all at once or within a specific timeframe after upgrading the GE Digital APM Sync Server. If desired, you can simply allow the update to occur automatically the next time users synchronize with the server.

Upgrade Steps for Lubrication


If you have Lubricant, Lubrication Requirement, or Lubrication Requirement Template records in your database, complete these steps.


Pre-Upgrade Steps

Complete these steps prior to upgrading your database.

| Step | Task | Notes |
|------|--|---|
| 1 | <p>Review the values in the Manufacturer field in Lubricant records and consolidate any near-matches.</p> <p>For example, if some of your existing records contain the value “ABC Company” and others contain “A B C Company” to refer to the same manufacturer, you should modify one or the other so that the values match exactly.</p> <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;"> <p>i Tip: You can use the following query, which returns a list of manufacturers in alphabetical order, to review the values:</p> <pre>SELECT DISTINCT [MI_LUBRICANT].[MI_LUBRICANT_MFR_C] "Lubricant Manufacturer" FROM [MI_LUBRICANT] ORDER BY [MI_LUBRICANT].[MI_LUBRICANT_MFR_C] Asc</pre> </div> | <p>This step is required only if you have Lubricant records in your database.</p> <p>This step is necessary because a new Lubricant Manufacturer record will be created during the upgrade for each value in the Manufacturer field in Lubricant records prior to upgrading (and the value will be replaced with a reference to the corresponding Lubricant Manufacturer record).</p> |

| Step | Task | Notes |
|------|---|--|
| 2 | <p>Review the values in the Priority field in Lubrication Requirement and Lubrication Requirement Template records and consolidate any near-matches.</p> <p>For example, if some of your existing records contain the value "High" and others contain "Hihg" to refer to the same level of priority, you should modify one or the other so that the values match exactly.</p> <div data-bbox="332 682 852 1081" style="border: 1px solid #0070C0; padding: 5px;"> <p>i Tip: You can use the following query, which returns a list of priority values in alphabetical order, to review the values:</p> <pre>SELECT DISTINCT [MI_LUBR_REQ].[MI_LUBR_REQ_PRIOR_C] "Priority" FROM [MI_LUBR_REQ] ORDER BY [MI_LUBR_REQ].[MI_LUBR_REQ_PRIOR_C] ASC</pre> </div> | <p>This step is required only if you have Lubrication Requirement and Lubrication Requirement Template records in your database.</p> <p>This step is necessary because a new entry in the system code table MI_LUBR_PRIORITY will be added during the upgrade for each value in the Priority field in Lubrication Requirement and Lubrication Requirement Template records prior to upgrading.</p> |

| Step | Task | Notes |
|------|--|--|
| 3 | <p>Review the values in the Component field in Lubrication Requirement and Lubrication Requirement Template records and consolidate any near-matches.</p> <p>For example, if some of your existing records contain the value "Bearing" and others contain "Bearings" to refer to the component, you should modify one or the other so that the values match exactly.</p> <div data-bbox="331 680 852 1081" style="border: 1px solid #0070C0; padding: 5px;"> <p> Tip: You can use the following query, which returns a list of components in alphabetical order, to review the values:</p> <pre>SELECT DISTINCT [MI_LUBR_REQ].[MI_LUBR_REQ_COMP_C] "Component" FROM [MI_LUBR_REQ] ORDER BY [MI_LUBR_REQ].[MI_LUBR_REQ_COMP_C] ASC</pre> </div> | <p>This step is required only if you have Lubrication Requirement and Lubrication Requirement Template records in your database.</p> <p>This step is necessary because a new Lubrication Component record will be created during the upgrade for each value in the Component field in Lubrication Requirement and Lubrication Requirement Template records prior to upgrading (and the Component Type field will be updated with a reference to the corresponding Lubrication Component record).</p> |

| Step | Task | Notes |
|------|---|--|
| 4 | <p>Review the values in the Method field in Lubricant records and consolidate any near-matches.</p> <p>For example, if some of your existing records contain the value "Grease Gun" and others contain "greasegun" to refer to the method, you should modify one or the other so that the values match exactly.</p> <div data-bbox="334 642 850 1041" style="border: 1px solid #0070C0; padding: 5px;"> <p> Tip: You can use the following query, which returns a list of methods in alphabetical order, to review the values:</p> <pre data-bbox="345 800 794 1026">SELECT DISTINCT [MI_LUBRICANT].[MI_LUBRICANT_METHOD_C] "Method" FROM [MI_LUBRICANT] ORDER BY [MI_LUBRICANT].[MI_LUBRICANT_METHOD_C] Asc</pre> </div> | <p>This step is required only if you have Lubricant records in your database.</p> <p>This step is necessary because a new Lubrication Method record will be created during the upgrade for each unique value in the Method field in Lubricant records prior to upgrading (and the Method field will be deprecated). In addition, the new Method Type field in Lubrication Requirement and Lubrication Requirement Template records will be populated with the Entity Key of the corresponding Lubrication Method record.</p> |

| Step | Task | Notes |
|------|---|---|
| 5 | <p>Review the values in the Capacity Unit of Measure field in Lubrication Requirement and Lubrication Requirement Template records and consolidate any near-matches. Then, ensure that each value matches exactly the system code <i>Description</i> value for an entry in the MI_LM_REFERENCES System Code Table. If a corresponding entry does not exist, and you want to use the value in your upgraded database, add an entry.</p> <div data-bbox="332 737 850 1075" style="border: 1px solid red; padding: 5px;"> <p>⚠ IMPORTANT: You can add an entry directly to the MI_LM_REFERENCES System Code Table or you can add a <i>reference</i> to an entry in the global UOME System Code Table. However, <i>do not</i> add a given value to the MI_LM_REFERENCES System Code Table using both methods.</p> </div> <div data-bbox="332 1100 850 1759" style="border: 1px solid blue; padding: 5px;"> <p>📘 Tip: You can use the following queries, which return a list of Capacity Unit of Measure values in alphabetical order, to review the values:</p> <ul style="list-style-type: none"> • Lubrication Requirement records: <pre>SELECT DISTINCT [MI_LUBR_REQ].[MI_LUBR_REQ_CAPTY_UOM_C] "Capacity Unit of Measure" FROM [MI_LUBR_REQ] WHERE [MI_LUBR_REQ].[MI_LUBR_REQ_CAPTY_UOM_C] IS NOT NULL ORDER BY [MI_LUBR_REQ].[MI_LUBR_REQ_CAPTY_UOM_C] Asc</pre> </div> | <p>This step is required only if you have Lubrication Requirement and Lubrication Requirement Template records in your database.</p> <p>This step is necessary because the new Capacity Unit of Measure field in Lubrication Requirement and Lubrication Requirement Template records will be populated automatically with a reference to the unit of measure that corresponds to the value in the deprecated Capacity Unit of Measure field.</p> <p>If the deprecated Capacity Unit of Measure field contains a value that does not correspond to an entry in the MI_LM_REFERENCES System Code Table, no value will be added to the new field.</p> |

| Step | Task | Notes |
|------|---|-------|
| | <ul style="list-style-type: none"> • Lubrication Requirement Template records: <pre>SELECT DISTINCT [MI_LR_TMPLT].[MI_LR_TMPLT_CAPTY_UOM_C] "Capacity Unit of Measure" FROM [MI_LR_TMPLT] WHERE [MI_LR_TMPLT].[MI_LR_TMPLT_CAPTY_UOM_C] IS NOT NULL ORDER BY [MI_LR_TMPLT].[MI_LR_TMPLT_CAPTY_UOM_C] Asc</pre> | |

Post-Upgrade Steps

Complete this step after upgrading your database.

| Step | Task | Notes |
|------|--|--|
| 1 | <p>Confirm that appropriate the Lubricant Manufacturer records were created. Add or remove records as necessary.</p> <p>i Tip: You can use the following query, which returns a list of the Lubricant Manufacturer records in your upgraded database, to review the values:</p> <pre>SELECT DISTINCT [MI_LUBR_MANU].[MI_LUBR_MANU_MANU_ID_C] "Manufacturer ID" FROM [MI_LUBR_MANU] ORDER BY [MI_LUBR_MANU].[MI_LUBR_MANU_MANU_ID_C] Asc</pre> | See notes for Step 1 in the pre-upgrade steps. |
| 2 | <p>Confirm that appropriate entries were created in the system code table MI_LUBR_PRIORITY.</p> <p>i Tip: View the MI_LUBR_PRIORITY system code table in Configuration Manager to confirm the entries.</p> | See notes for Step 2 in the pre-upgrade steps. |

| Step | Task | Notes |
|------|--|---|
| 3 | <p>Confirm that appropriate Lubrication Component records were created. Add or remove records as necessary.</p> <div data-bbox="332 380 1265 659" style="border: 1px solid #0070C0; padding: 5px;"> <p>i Tip: You can use the following query, which returns a list of the Lubrication Component records in your upgraded database, to review the values:</p> <pre>SELECT DISTINCT [MI_LUBR_COMP].[MI_LUBR_COMP_ID_C] "ID" FROM [MI_LUBR_COMP] ORDER BY [MI_LUBR_COMP].[MI_LUBR_COMP_ID_C] Asc</pre> </div> | <p>See notes for Step 3 in the pre-upgrade steps.</p> |
| 4 | <p>Confirm that appropriate Lubrication Method records were created. Add or remove records as necessary.</p> <div data-bbox="332 793 1265 1031" style="border: 1px solid #0070C0; padding: 5px;"> <p>i Tip: You can use the following query, which returns a list of the Lubrication Method records in your upgraded database, to review the values:</p> <pre>SELECT DISTINCT [MI_LUBR_METH].[MI_LUBR_METH_ID_C] "Method ID" FROM [MI_LUBR_METH] ORDER BY [MI_LUBR_METH].[MI_LUBR_METH_ID_C] Asc</pre> </div> | <p>See notes for Step 4 in the pre-upgrade steps.</p> |

| Step | Task | Notes |
|------|--|---|
| 5 | <p>For all Lubrication Requirement and Lubrication Requirement Template records that contained a value in the deprecated Capacity Unit of Measure field, confirm that the new Capacity Unit of Measure field contains a reference to the corresponding unit of measure.</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> <p>i Tip: You can use the following queries to locate records where the deprecated field contains a value, but the new field does not.</p> <ul style="list-style-type: none"> Lubrication Requirement records: <pre>SELECT [MI_LUBR_REQ].[MI_LUBR_REQ_CAPTY_UOM_C] "Capacity Unit of Measure(Depr", [MI_LUBR_REQ].[MI_LUBR_REQ_CAPACITY_UOM_C] "Capacity Unit of Measure", [MI_LUBR_REQ].ENTY_KEY "ENTY_KEY", [MI_LUBR_REQ].[MI_LUBR_REQ_COMP_TYPE_N] "Component Type", [MI_LUBR_REQ].[MI_MEAS_LOC_DESC_C] "Description" FROM [MI_LUBR_REQ] WHERE ([MI_LUBR_REQ].[MI_LUBR_REQ_CAPTY_UOM_C] IS NOT NULL AND [MI_LUBR_REQ].[MI_LUBR_REQ_CAPACITY_UOM_C] IS NULL) ORDER BY [MI_LUBR_REQ].[MI_LUBR_REQ_CAPTY_UOM_C] Asc</pre> Lubrication Requirement Template records: <pre>SELECT DISTINCT [MI_LR_TMPLT].[MI_LR_TMPLT_CAPTY_UOM_C] "Capacity Unit of Measure(Depr", [MI_LR_TMPLT].[MI_LR_TMPLT_CAPACITY_UOM_C] "Capacity Unit of Measure_", [MI_LR_TMPLT].ENTY_KEY "ENTY_KEY", [MI_LR_TMPLT].[MI_LR_TMPLT_COMP_TYPE_N] "Component Type", [MI_LR_TMPLT].[MI_LR_TMPLT_DESC_C] "Description" FROM [MI_LR_TMPLT] WHERE ([MI_LR_TMPLT].[MI_LR_TMPLT_CAPTY_UOM_C] IS NOT NULL AND [MI_LR_TMPLT].[MI_LR_TMPLT_CAPACITY_UOM_C] IS NULL) ORDER BY [MI_LR_TMPLT].[MI_LR_TMPLT_CAPTY_UOM_C] Asc</pre> </div> | <p>See notes for Step 5 in the pre-upgrade steps.</p> |

Modify Checkpoints Linked to Multiple Assets

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

In GE Digital APM V4.3.0.2.0, a Checkpoint can be linked to *one* asset. During upgrade from versions V3.x to V4.3.0.2.0, the related asset entity key is added to a field on the Checkpoint family. Therefore, if you have Checkpoints that are linked to more than one asset, then you must remove the links to the additional assets *prior to upgrading*.

Steps

1. Using an appropriate database management tool, prior to upgrading your database to V4.3.0.2.0, run a query to locate checkpoints that are linked to multiple assets.

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 GE Digital APM.

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

3. Unlink the additional assets from the Checkpoint so that it is linked only to one asset (e.g., either a Functional Location *or* an Equipment if you are using the default asset families).

Upgrade Records with Schedules Containing End Dates

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

When upgrading from any V3.x version to a V4.x version, follow these steps to ensure that schedules for the following record types are upgraded successfully:

- Checkpoint Task
- Measurement Location
- Lubrication Requirement
- Measurement Location Template
- Lubrication Requirement Template

These steps are required to ensure that any records containing schedules with end dates are upgraded successfully.

Note: If preferred, instead of completing the following steps prior to upgrading, you can instead upgrade your database as normal. When you do so, the log for the Rounds upgrade utility will record entries for schedules that failed to upgrade. You can then use this information to recreate the schedules in V4.2.0.0.

Steps

Prior to Upgrading

1. Review the affected record types to determine if there are any schedules containing end dates.

You can use the following queries to locate these records:

- Checkpoint Templates (i.e., Measurement Template and Lubrication Requirement Template records)

```
SELECT ENTY_KEY, ENTY_ID, MI_ML_TMPLT_SCHEDULE_C FROM MIV_MI_CP_TMPLT
WHERE MI_ML_TMPLT_SCHEDULE_C LIKE '<?xml%' AND MI_ML_TMPLT_SCHEDULE_C NOT
LIKE '%<EndDate xsi:nil="true" />%'
```

- Checkpoints (i.e., Measurement Location and Lubrication Requirement records)

```
SELECT MI_MEAS_LOC_SCHEDULE_C FROM MIV_MI_CHECK_PT WHERE MI_MEAS_LOC_
SCHEDULE_C LIKE '<?xml%' AND MI_MEAS_LOC_SCHEDULE_C NOT LIKE '%<EndDate
xsi:nil="true" />%'
```

- Checkpoint Tasks


```
SELECT ENTY_KEY, ENTY_ID, MI_TASK_SCHEDULE_C FROM MIV_MI_CP_TASK0 WHERE  
MI_TASK_SCHEDULE_C LIKE '<?xml%' AND MI_TASK_SCHEDULE_C NOT LIKE  
'%<EndDate xsi:nil="true" />%'
```

2. For each record with a schedule containing an end date:
 - a. Note the record and the end date value.
 - b. In the **Schedule** field, select the [...] button to open the **Schedule** window.
 - c. In the **Range of recurrence** section, select **No end date**, and then select **OK**.
3. Proceed with the database upgrade as normal.

After upgrading:

1. In GE Digital APM, locate the records you noted in the previous section.
2. In each record, update the schedule to set the required end date.

Rounds Security Groups and Roles

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

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

| Security Group | Roles |
|---|--|
| MI Operator Rounds Administrator | MI Health Admin |
| MI Operator Rounds Mobile User | MI Health Admin MI Health Power MI Health User |
| MI Lubrication Management Administrator | MI Health Admin |
| MI Lubrication Management User | MI Health Admin MI Health Power MI Health User |
| MI Rounds Designer Viewer | MI APM Viewer |

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

Notes:

- Users who should be able to run Rounds queries to view the Rounds data after it has been uploaded from a tablet or a mobile device will need a combination of the privileges listed in the following table, depending on the families included in the queries they want to run.

- To create work requests via Operator Rounds Recommendations, users must also have the appropriate privileges to create EAM notifications (e.g., be a member of the MI SAP Interface User Security Group).
- The privileges assigned to the members of the MAPM Security Group, which was provided in the baseline Rounds module in Meridium Enterprise APM V3.6.0, are also assigned to the members of the MI Operator Rounds Mobile User Security Group. We recommend that you use the MI Operator Rounds User Security Group instead of the MAPM Security Group.

| Family | MI Operator Rounds Administrator | MI Operator Rounds Mobile User | MAP-M Security Group | MI Rounds Designer Viewer | MI Lubrication Management Administrator | MI Lubrication Management User |
|--|----------------------------------|--------------------------------|----------------------|---------------------------|---|--------------------------------|
| Entity Families | | | | | | |
| Checkpoint Condition | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Checkpoint Task | View, Update, Insert, Delete | View, Update | View, Update | View | View, Update, Insert, Delete | View, Update |
| Health Indicator | View | View | View | View | View | View |
| Health Indicator Mapping | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Hierarchy Item Child Definition (Deprecated) | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Hierarchy Item Definition (Deprecated) | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |

| Family | MI Operator Rounds Administrator | MI Operator Rounds Mobile User | MAP-M Security Group | MI Rounds Designer Viewer | MI Lubrication Management Administrator | MI Lubrication Management User |
|---------------------------------------|----------------------------------|--------------------------------|------------------------------|---------------------------|---|--------------------------------|
| Lubricant | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Lubrication Component | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Lubrication Management Recommendation | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Lubricant Manufacturer | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Lubrication Method | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Lubrication Requirement | View, Update, Insert, Delete | View, Update | View, Update | View | View, Update, Insert, Delete | View |
| Lubrication Requirement Template | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Measurement Location | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |

| Family | MI Operator Rounds Administrator | MI Operator Rounds Mobile User | MAP-M Security Group | MI Rounds Designer Viewer | MI Lubrication Management Administrator | MI Lubrication Management User |
|----------------------------------|----------------------------------|--------------------------------|------------------------------|---------------------------|---|--------------------------------|
| Measurement Location Template | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Operator Rounds Allowable Values | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Operator Rounds Recommendation | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Reading | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Reference Document | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Route | View, Update, Insert, Delete | View, Update | View, Update | View | View, Update, Insert, Delete | View, Update |
| Route History | View, Update, Insert, Delete | View, Insert, Update, Delete | View, Insert, Update, Delete | View | View, Update, Insert, Delete | View, Insert, Update, Delete |

| Family | MI Operator Rounds Administrator | MI Operator Rounds Mobile User | MAP-M Security Group | MI Rounds Designer Viewer | MI Lubrication Management Administrator | MI Lubrication Management User |
|-------------------------------|----------------------------------|--------------------------------|----------------------|---------------------------|---|--------------------------------|
| Rounds Allowable Value | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Rounds Category | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Rounds Sequence Information | View, Update, Insert, Delete | View | View | None | View, Update, Insert, Delete | View |
| Task | None | View, Update | View, Update | View | | View, Update |
| Template Group | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Relationship Families | | | | | | |
| Condition Has ML | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Condition Has LR | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Category Has Allowable Values | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |

| Family | MI Operator Rounds Administrator | MI Operator Rounds Mobile User | MAP-M Security Group | MI Rounds Designer Viewer | MI Lubrication Management Administrator | MI Lubrication Management User |
|-------------------------|----------------------------------|--------------------------------|------------------------------|---------------------------|---|--------------------------------|
| Has Checkpoint | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Has Checkpoint Template | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Has Health Indicators | View | View | View | View | View | View |
| Has History | View, Insert, Delete | View, Insert, Delete | View, Insert, Delete | View | View, Update, Insert, Delete | View, Insert, Delete |
| Has Readings | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Has Recommendations | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Has Reference Documents | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete |

| Family | MI Operator Rounds Administrator | MI Operator Rounds Mobile User | MAP-M Security Group | MI Rounds Designer Viewer | MI Lubrication Management Administrator | MI Lubrication Management User |
|------------------------------|----------------------------------|--------------------------------|------------------------------|---------------------------|---|--------------------------------|
| Has Route | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Has Tasks | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Health Indicator Has Mapping | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Lubricant Has Method | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| Health Indicator Has Source | View | View | View | View | View | View |
| ML Has Condition | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |
| ML Has OPR Recommendation | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View, Update, Insert, Delete | View, Update, Insert, Delete |
| Route Has Checkpoint | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |

| Family | MI Operator Rounds Administrator | MI Operator Rounds Mobile User | MAP-M Security Group | MI Rounds Designer Viewer | MI Lubrication Management Administrator | MI Lubrication Management User |
|--------------------------|----------------------------------|--------------------------------|----------------------|---------------------------|---|--------------------------------|
| Route Has Human Resource | View, Update, Insert, Delete | Insert | Insert | View | View, Update, Insert, Delete | Insert |
| Template Has Checkpoint | View, Update, Insert, Delete | View | View | View | View, Update, Insert, Delete | View |

Deploy Rules

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

Install the GE Digital APM Rules Editor

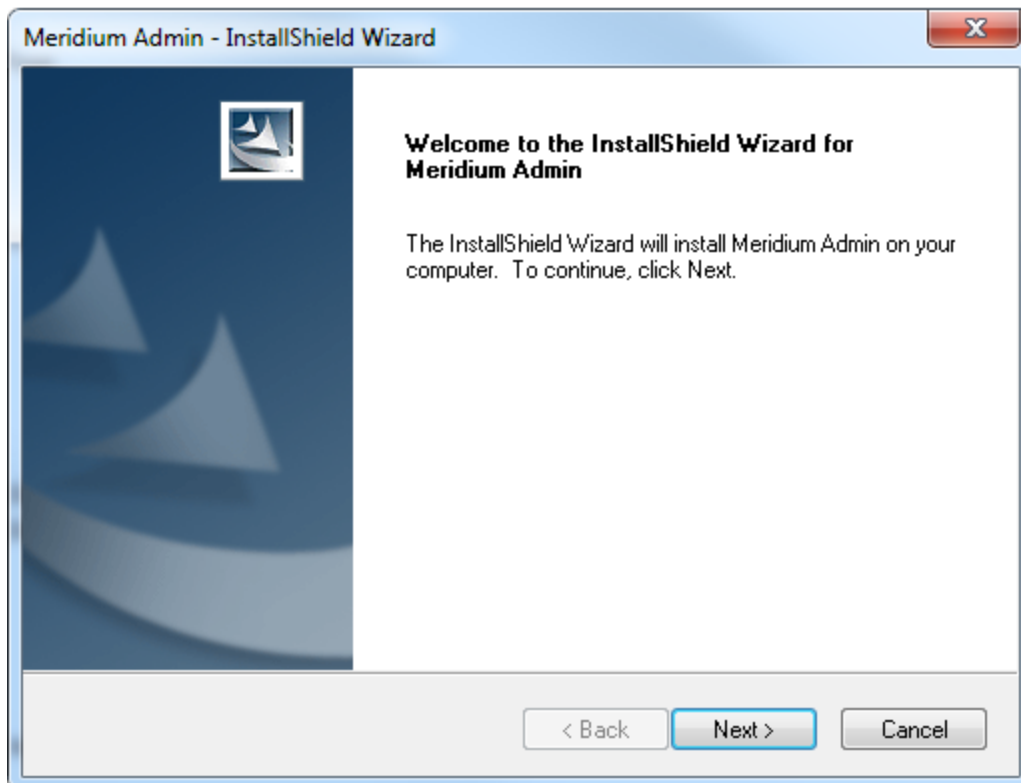
Before You Begin

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

Steps

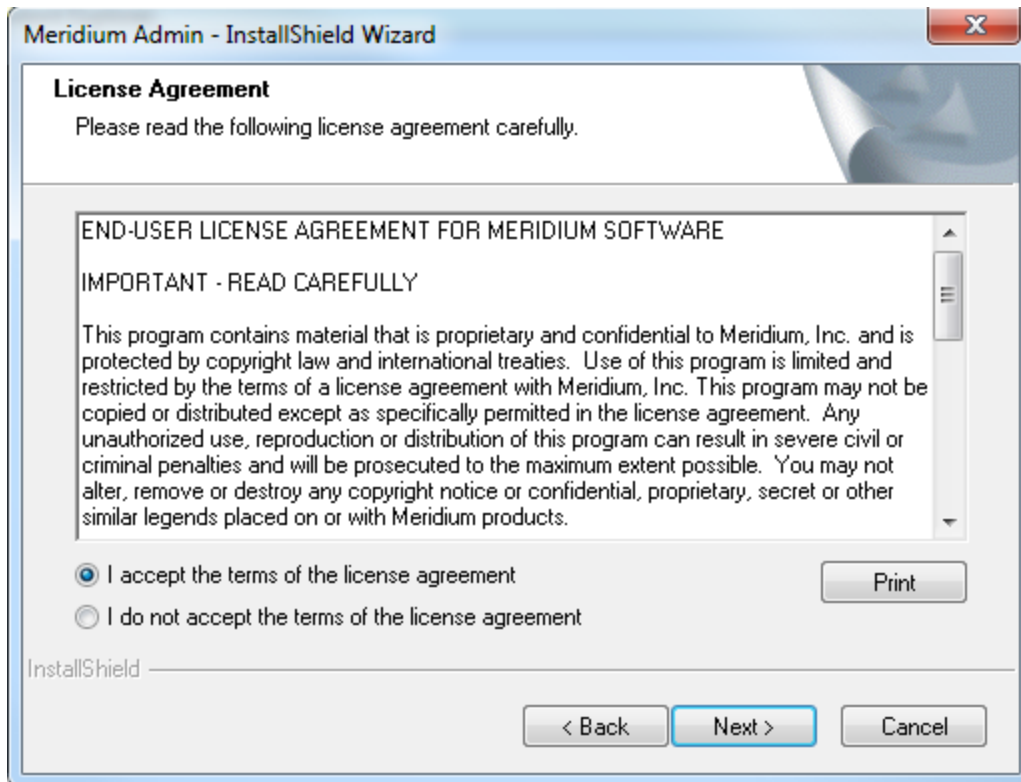
1. On the machine that will serve as the Meridium rules editor, access the GE Digital APM distribution package, and then navigate to the folder **\\General Release\Meridium APM Setup\Setup\Admin**.
2. Open the file **Setup.exe**.

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



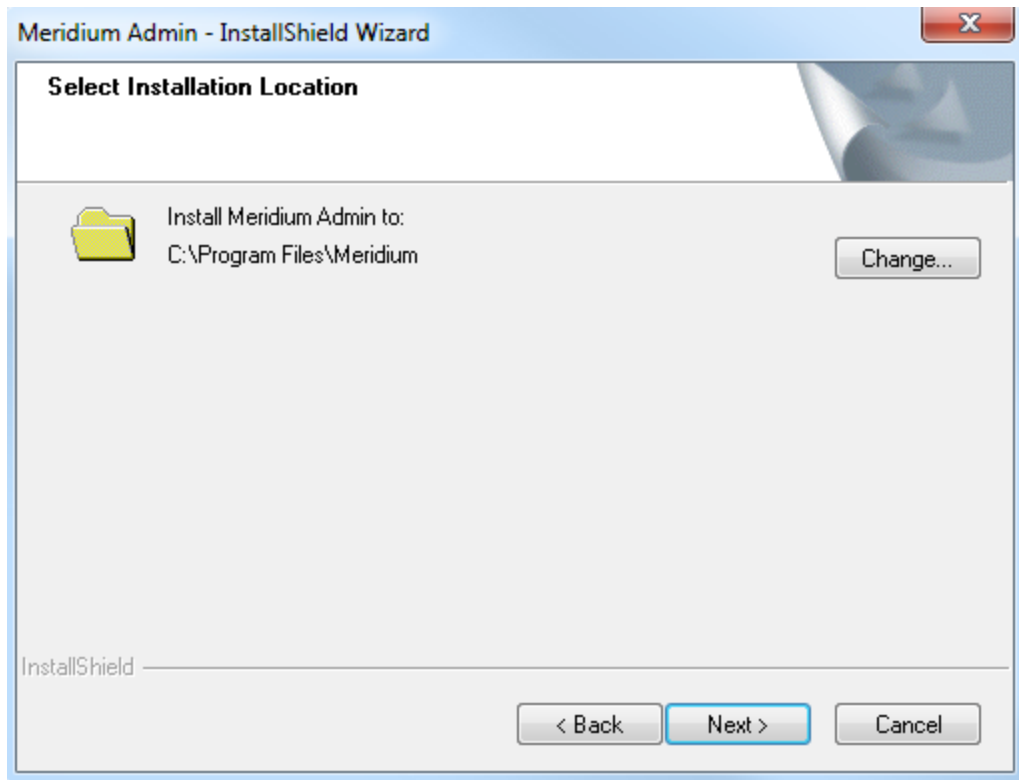
3. Select **Next**.

The **License Agreement** screen appears.



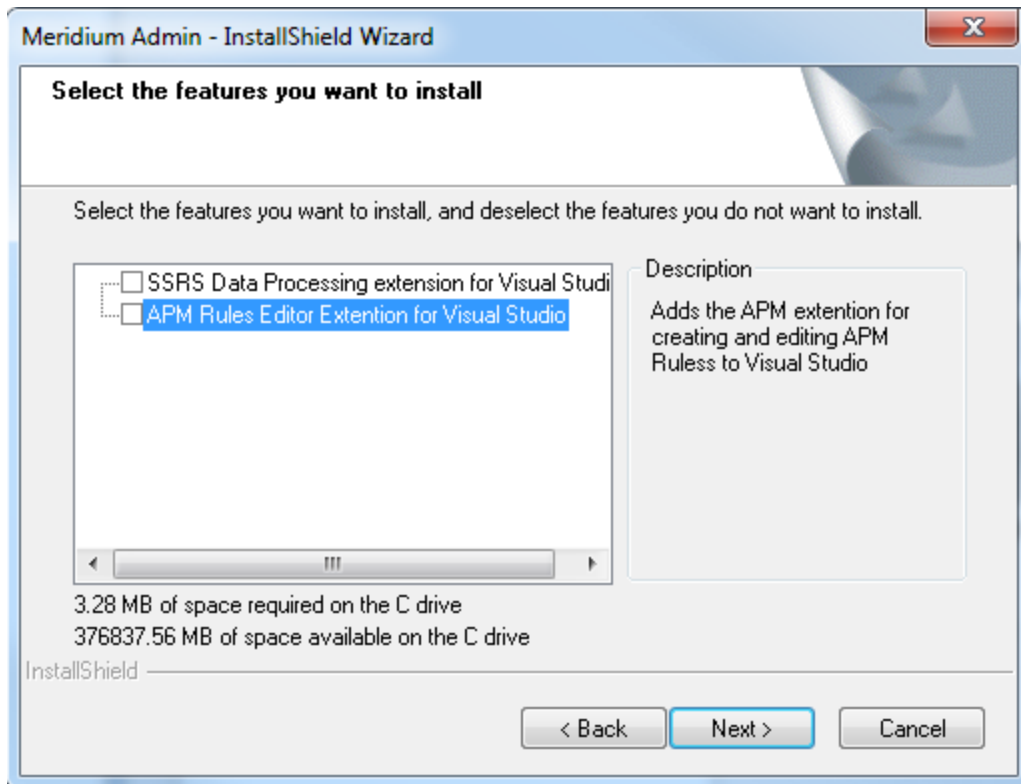
4. Read the License Agreement and, if you agree, select the **I accept the terms of the license agreement** option. Then, select **Next** button.

The **Select Installation Location** screen appears.



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

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

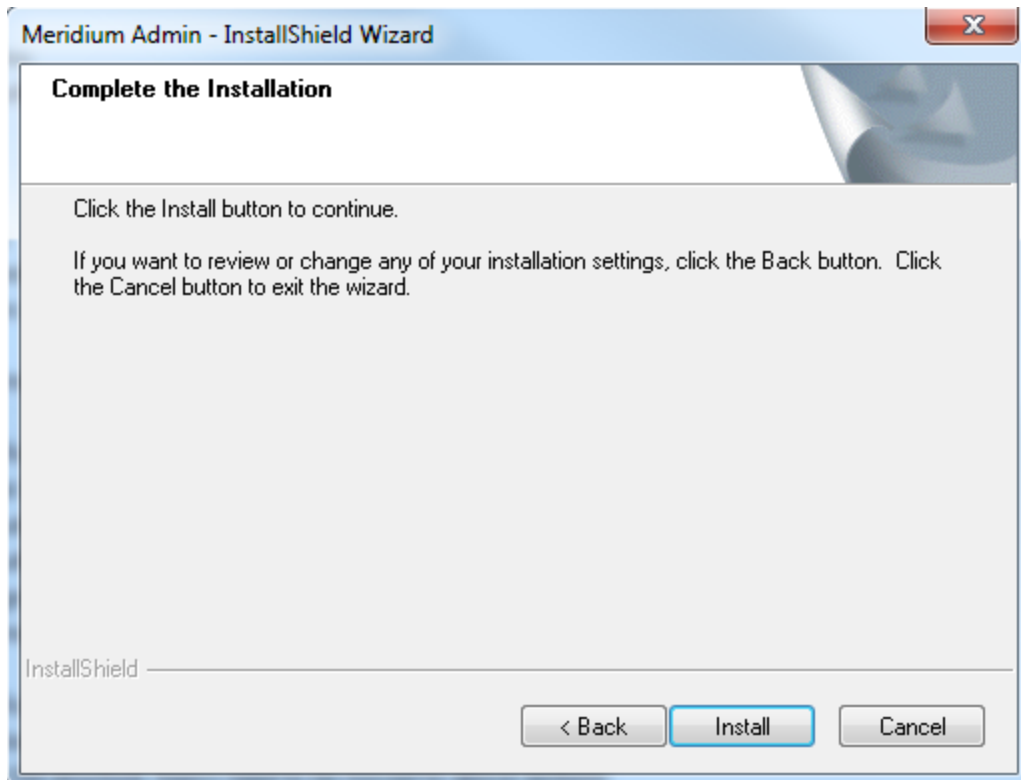


6. Select the **APM Rules Editor Extension for Visual Studio** option.

GE Digital APM performs a check to make sure that your machine contains the required prerequisites for the features that you want to install. If one or more prerequisites are missing or there is not enough space on the machine, a dialog box will appear, explaining which prerequisites are missing or asking to free up space. If this occurs, close the installer, install the missing prerequisite or free up some space, and then run the installer again.

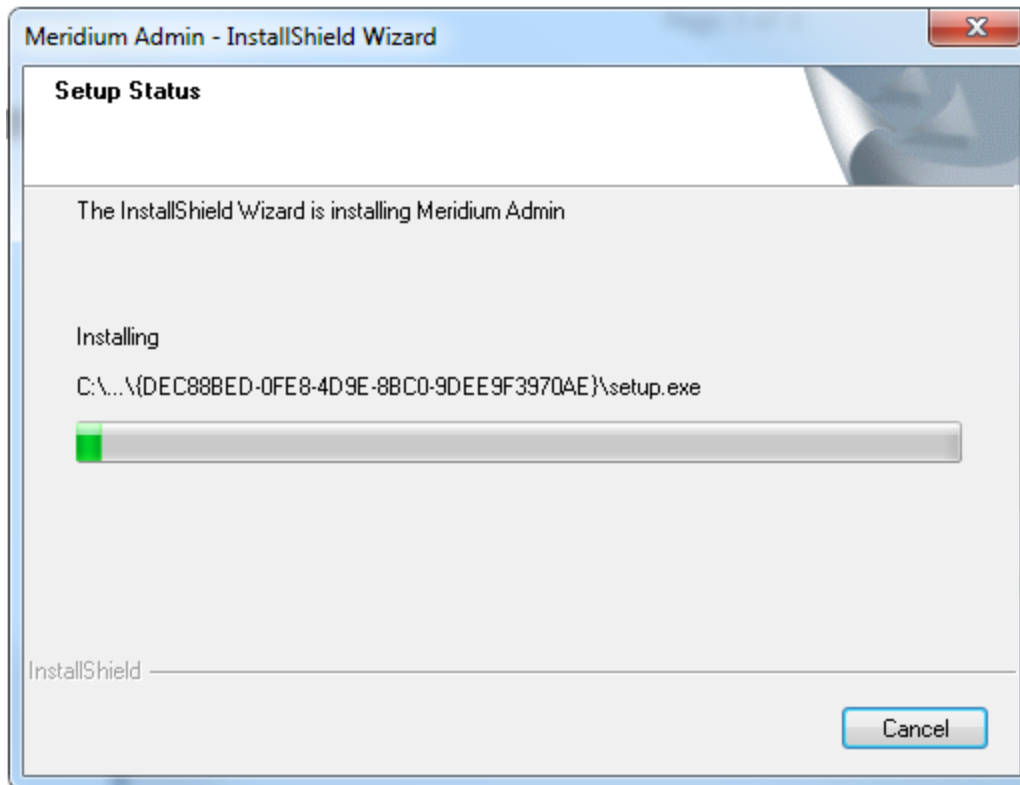
7. Select **Next**.

The **Complete the Installation** screen appears.

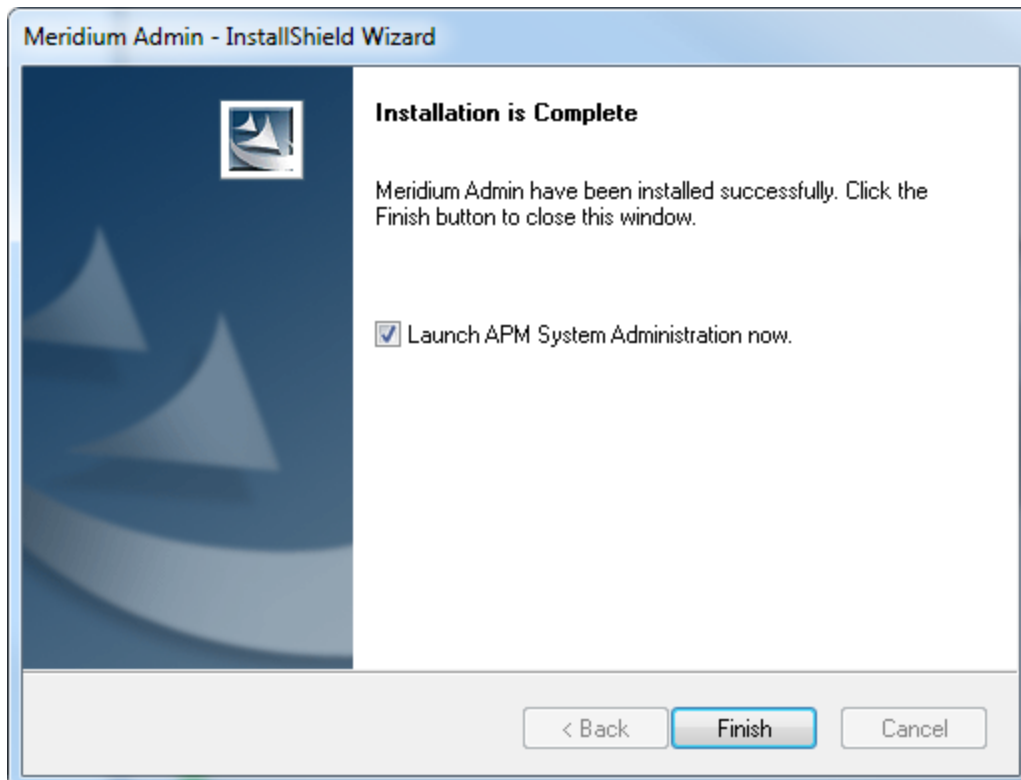


8. Select **Install**.

The **Setup Status** screen appears, which displays a progress bar that shows the progress of the installation process. After the progress bar reaches the end, a message appears, indicating that Meridium Admin is installed successfully. Optionally, you can select to launch the APM System Administration tool when the installer window closes.



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



Results

- The Meridium Rules Editor is installed.

What's Next?

- Access the Meridium Rules Editor.


Deploy SIS Management

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


Deploy SIS Management for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

| Step | Task | Notes |
|------|----------------------------------|---|
| 1 | Define alternate search queries. | This step is required only if you do not want to use the baseline search queries. |

| Step | Task | Notes |
|------|--|--|
| 2 | Modify threshold values in the SIL Threshold family. | <p>This step is required only if you want to modify the default boundary values specified in the SIL Threshold family.</p> <div data-bbox="1073 464 1398 1199" style="border: 1px solid #00aaff; padding: 5px;"> <p> Hint: To prevent ambiguity in SIL values for driving risk ranks that fall on the boundary value of two SIL thresholds, avoid specifying contiguous boundary values where the lower boundary value of one threshold is the upper boundary value of the preceding SIL threshold. For example, for the SIL value of 1, if you have specified a SIL threshold of 10 through 100, then, for a SIL value of 2 you can specify the SIL threshold of 100.1 through 1000.</p> </div> |
| 3 | Import data from an Exida project file. | This step is required only if you want to create SIL Analyses using an Exida project file. |
| 4 | Export data from an Exida project file. | This step is optional. |
| 5 | Activate the Hazards Analysis license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

| Step | Task | Notes |
|------|--|--|
| 6 | Assign <i>View</i> permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager . As needed, you can assign additional privileges. | This step is required only for Security Groups that will be used in the integration between the SIS Management module and Hazards Analysis. |
| 7 | Review the SIS Management data model to determine which relationship definitions you will need to modify to include your custom equipment or location families. Modify any relationship definitions as needed using the Configuration Manager. | This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families. |
| 8 | Assign Security Users to one or more of the SIS Management Security Groups and Roles . | This step is required. |

Upgrade or Update SIS Management to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the Hazards Analysis license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign <i>View</i> permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

This module will be upgraded automatically when you upgrade the components in the basic GE Digital APM system architecture. Additionally, as needed, perform the following steps:

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the Hazards Analysis license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign <i>View</i> permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 3 | Verify the LOPA Assessment records that are linked to Instrumented Functions after upgrade. | This step is optional. |

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the Hazards Analysis license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign <i>View</i> permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the Hazards Analysis license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign <i>View</i> permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the Hazards Analysis license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign <i>View</i> permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the Hazards Analysis license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign <i>View</i> permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V3.5.1 through V3.5.1.12.1

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the Hazards Analysis license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign <i>View</i> permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the Hazards Analysis license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign <i>View</i> permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V3.5.0 through V3.5.0.0.7.1

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the Hazards Analysis license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign <i>View</i> permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Notes |
|------|--|---|
| 1 | Activate the Hazards Analysis license. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |
| 2 | Assign <i>View</i> permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges. | This step is required only if you want to take advantage of the integration between the SIS Management module and Hazards Analysis. |

About Upgrade of LOPA and Safeguards to V4.3.0.0.0

In versions prior to V4.3.0.0.0, you could create a LOPA to assess SIL value for an Instrumented Function from the SIL Analysis. In V4.3.0.0.0, you can create and manage LOPAs using the Layers of Protection Analysis module. To assess the SIL value for an Instrumented Function using LOPA, you can create a LOPA Assessment record for the Instrumented Function by linking the LOPA.

When you upgrade the module to V4.3.0.0.0, LOPA Assessment records are created automatically by copying values from the existing LOPAs. The LOPA Assessments are then linked to the corresponding Instrumented Functions and LOPAs. The following table contains the fields in LOPA that are mapped to fields in LOPA Assessment:

| Values in the Following Fields in the LOPA... | Copied to the following fields in the LOPA Assessment |
|---|---|
| LOPA ID | LOPA Assessment ID |
| LOPA ID | Linked LOPA ID |
| Entity Key | Linked LOPA Key |
| Frequency of Initiating Event | Frequency of Initiating Event |
| Mitigated Consequence Frequency | Mitigated Consequence Frequency |
| Required Mitigated Consequence Frequency | Required Mitigated Consequence Frequency |
| Required PIF PFD | Required Probability of Failure |
| Required PIF Risk Reduction Factor | Risk Reduction Factor (RRF) |
| Unmitigated Consequence Frequency | Unmitigated Consequence Frequency |
| Total IPL PFD | Total IPL PFD |
| Calculated SIL | Selected SIL Level |

Also, in V4.3.0.0.0, the Hazards Analysis Safeguard records is used to store the details of Independent Layer of Protection. Hence, when you upgrade to V4.3.0.0.0, Hazards Analysis Safeguards records are created by copying values from the Independent Layer of Protection records associated with the existing LOPA records. The Safeguards created are then associated with the corresponding LOPA.

| Values in the Following Fields in the Independent Layer of Protection ... | Copied to the following fields in the associated Hazards Analysis Safeguard |
|---|---|
| PFD | PFD |

| Values in the Following Fields in the Independent Layer of Protection ... | Copied to the following fields in the associated Hazards Analysis Safeguard |
|---|---|
| IPL ID | Safeguard ID |
| Type | IPL Type |

In V4.3.0.0.0, for each Safeguard, [IPL Checklist records](#) are created to store your selection for the criteria that are used to determine if a Safeguard is an IPL. When you upgrade to V4.3.0.0.0, for each previously existing Independent Layer of Protection record, IPL Checklist records are created and associated with the corresponding Safeguard in V4.3.0.0.0.

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 |
| MI SIS Viewer | MI APM Viewer MI Safety Admin MI Safety Power MI Safety User MI SIS Engineer |

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

Note: The [baseline family-level privileges available in the LOPA module](#) are also applicable to Security Groups in SIS Management module.

| Family | MI SIS Administrator | MI SIS Engineer | MI SIS User | MI SIS Viewer |
|-----------------|----------------------|-----------------|-------------|---------------|
| Entity Families | | | | |

| Family | MI SIS Administrator | MI SIS Engineer | MI SIS User | MI SIS Viewer |
|---------------------------------------|------------------------------|------------------------------|------------------------------|---------------|
| Asset Criticality Analysis | View | None | None | View |
| Asset Criticality Analysis System | View | None | None | View |
| Consequence | View, Update, Insert, Delete | View | View | View |
| Equipment | View | View | View | View |
| External Assessment | View, Update, Insert, Delete | View, Update, Insert, Delete | None | View |
| Functional Location | View | View | View | View |
| Functional Systems | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Functional Test Detail | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Human Resource | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Instrumented Function | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| LOPA Assessment | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Proven In Use Justification | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Safety Integrity Level | View, Update, Insert, Delete | View | View | View |
| Relationship Families | | | | |
| Analysis Has Human Resource | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Asset Criticality Analysis Has System | View | None | View | View |

| Family | MI SIS Administrator | MI SIS Engineer | MI SIS User | MI SIS Viewer |
|---|------------------------------|------------------------------|------------------------------|---------------|
| Equipment Has Equipment | View | View | View | View |
| Functional Location Has Equipment | View | View | View | View |
| Functional Location Has Functional Location | View | View | View | View |
| Has Equipment | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Functional Location | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Functional Location Detail | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Functional Test | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has_Functional_Test_Detail | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Hazard Event | View, Update, Insert, Delete | View, Update, Insert, Delete | View | 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 | View |
| Has Instrumented Function Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Instrument Loop | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |

| Family | MI SIS Administrator | MI SIS Engineer | MI SIS User | MI SIS Viewer |
|---------------------------------|------------------------------|------------------------------|--------------|---------------|
| Has Instrument Loop Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has LOPA | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has LOPA Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has PIL Device | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has PIL Device Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has PIL Group | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has PIL Group Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has PIL Subsystem | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has PIL Subsystem Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Proven In Use Justification | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has RBI Components | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Recommendations | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Reference Documents | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Insert | View |
| Has Reference Values | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Risk | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Risk Category | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |

| Family | MI SIS Administrator | MI SIS Engineer | MI SIS User | MI SIS Viewer |
|------------------------------------|------------------------------|------------------------------|--------------|---------------|
| Has Risk Matrix | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has SIF Common Cause Failures | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has SIL Assessment | View, Update, Insert, Delete | View, Update, Insert, Delete | None | View |
| Has SIS Analysis Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has SIS Revision | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has SIS Trip Report Detail | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Site Reference | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Task History | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Insert | View |
| Has Tasks | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Task Revision | View | View | View | View |
| Has Template Detail | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Templates | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Has Time Based Inspection Interval | View | View | View | View |
| Migrates Risk | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Was Promoted to ASM | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |


Deploy Thickness Monitoring (TM)

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

Deploy Thickness Monitoring (TM) for the First Time

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

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

 **Note:** If you are deploying this module in APM Now, before you begin completing these tasks, review the [system requirements for this module](#) to identify the supported features for this module in APM Now. Unless noted, all deployment tasks in the following table are applicable for the deployment of this module in APM Now.

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

| Step | Task | Notes |
|------|---|---|
| 3 | Configure Family Preference Application Settings. | <p>This step is required.</p> <p>You must configure preferences for the families that will be used to store equipment data in Thickness Monitoring.</p> <p>The following relationships <i>must</i> be defined:</p> <ul style="list-style-type: none"> • For the <i>Equipment</i> family, the Asset to Subcomponent Relationship field must be set to Has TML Group, and the Component ID field must be set to Equipment ID. The Subcomponent to Asset Relationship field should be left <i>blank</i>. • For the <i>TML Group</i> family, the Subcomponent to Asset Relationship field must be set to Has TML Group, and the Component ID field must be set to TML Group ID. The Asset to Subcomponent Relationship field should be left <i>blank</i>. |
| 4 | Configure Global Preference Application Settings. | <p>This step is required only if you want to use custom reading preferences and Nominal T-Min preferences. Baseline reading preferences and Nominal T-Min preferences will be used if you do not define your own. You can also define additional, optional global preferences that are not defined in the baseline GE Digital APM database.</p> |
| 5 | Configure the system to use custom TML Types. | <p>This step is required only if you want to use custom TML Types. You can define additional TML Types to use in your Corrosion Analyses.</p> |
| 6 | Manage Thickness Monitoring Rules Lookup records. | <p>This step is required only if you want to view or modify Thickness Monitoring Rules Lookup records whose values are used to perform certain TM calculations.</p> |
| 7 | Define additional fields that will be displayed in the header section of the TM Measurement Data Entry. | <p>This step is required only if default Thickness Measurement fields are displayed on the headings of these pages in the baseline GE Digital APM database. You can specify that additional fields be displayed in the header section of these pages.</p> |
| 8 | Disable the Auto Manage Tasks setting. | <p>This step is required only if you are using both the RBI and the TM modules.</p> |

| Step | Task | Notes |
|------|---|---|
| 9 | Install the Meridium Device Service on all of the machines that will connect to devices that will be used with Thickness Monitoring. | This step is required only if you will use any device to collect data that you transfer to Thickness Monitoring. If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 2850 . |
| 10 | Install the drivers and supporting files for any devices on all of the machines that will connect to devices that will be used with Thickness Monitoring. | This step is required only if you will use these devices to collect data that you transfer to Thickness Monitoring. |

Upgrade or Update Thickness Monitoring (TM) to V4.3.0.2.0

The following tables outline the steps that you must complete to upgrade this module to V4.3.0.2.0. These instructions assume that you have completed the steps for upgrading the basic GE Digital APM system architecture.

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

Update from any version V4.3.0.0.0 through V4.3.0.1.0

| Step | Task | Notes |
|------|--|---|
| 1 | Uninstall the previous version of the GE Digital APM Device Service on all of the machines that will connect to devices that will be used with Thickness Monitoring. | This step is required only if you will use any device to collect data that you transfer to Thickness Monitoring. |
| 2 | Install the GE Digital APM Device Service on all of the machines that will connect to devices that will be used with Thickness Monitoring. | This step is required only if you will use any device to collect data that you transfer to Thickness Monitoring. If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 2850 . |

Upgrade from any version V4.2.0.0 through V4.2.0.9.1

| Step | Task | Notes |
|------|--|------------------------|
| 1 | If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 2850 . | This step is required. |

Upgrade from any version V4.1.0.0 through V4.1.7.4.0

| Step | Task | Notes |
|------|--|------------------------|
| 1 | If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 2850 . | This step is required. |

Upgrade from any version V4.0.0.0 through V4.0.1.0

| Step | Task | Notes |
|------|--|------------------------|
| 1 | If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 2850 . | This step is required. |

Upgrade from any version V3.6.1.0.0 through V3.6.1.5.1

| Step | Task | Notes |
|------|--|------------------------|
| 1 | If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 2850 . | This step is required. |

Upgrade from any version V3.6.0.0.0 through V3.6.0.12.8

| Step | Task | Notes |
|------|--|------------------------|
| 1 | If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 2850 . | This step is required. |


Upgrade from any version V3.5.1 through V3.5.1.12.1

| Step | Task | Notes |
|------|--|------------------------|
| 1 | If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 2850 . | This step is required. |

Upgrade from any version V3.5.0 SP1 LP through V3.5.0.1.10.0

| Step | Task | Notes |
|------|--|------------------------|
| 1 | If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 2850 . | This step is required. |


Upgrade from any version V3.5.0 through V3.5.0.0.7.1

| Step | Task | Notes |
|------|--|---|
| 1 | <p>Manually update TM Analyses for which you used custom corrosion rates. To do so:</p> <ol style="list-style-type: none"> <li data-bbox="380 386 964 1314"> <p>Locate the records that you will need to update by running the following query:</p> <pre data-bbox="423 485 964 1314">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> <li data-bbox="380 1346 964 1493"> <p>Use the Bulk Analyze tool to update TM Analyses associated with the Equipment and TML Group records returned by this query.</p> <div data-bbox="423 1520 964 1766" style="border: 1px solid yellow; padding: 5px;"> <p> Note: These instructions assume that you are using the baseline Equipment and TML Group families. If you use custom equipment families, you must replace the following values before running the query in order to identify the records</p> </div> | <p>This step is required only if, in previous versions of Meridium APM, you used custom corrosion rates in your TM Analyses. If you did so, certain fields in the associated TML Corrosion Analysis records were populated with values using the unit of measure (UOM) inches per day instead of IN/YR (TM) (i.e., inches per year), which is the UOM that is specified in the properties of the fields. To correct this issue in existing records, you must perform this step to manually update TM Analyses. For more information about this issue, see the V3.5.1 Release Notes.</p> |

| Step | Task | Notes |
|------|---|-------|
| | <p>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>c. Run the Bulk Analyze tool using your custom records.</p> | |
| 2 | If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 2850 . | |

Upgrade from any version V3.4.5 through V3.4.5.0.1.4

| Step | Task | Notes |
|------|---|------------------------|
| 1 | <p>Update certain TM Analyses to correct TML Corrosion Analyses for which you performed measurement variance evaluation prior to V4.3.0.2.0. To do so:</p> <ol style="list-style-type: none"> 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. Use the Bulk Analyze tool to update TM Analyses that are associated with TML Corrosion Analyses returned by the query you created in step a. | This step is required. |

| Step | Task | Notes |
|------|--|---|
| 2 | <p>Manually update TM Analyses for which you used custom corrosion rates. To do so:</p> <ol style="list-style-type: none"> 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 Data-points} 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> Use the Bulk Analyze tool to update TM Analyses associated with the Equipment and TML Group records returned by this query. <div data-bbox="412 1440 959 1766" style="border: 1px solid black; background-color: #ffffcc; padding: 5px;"> <p> Note: These instructions assume that you are using the baseline Equipment and TML Group families. If you use custom equipment families, you must replace the following values before running the query in order to identify the records requiring update:</p> <ul style="list-style-type: none"> MI_EQUIP000 and MI_ </div> | <p>This step is required only if, in previous versions of Meridium APM, you used custom corrosion rates in your TM Analyses. If you did so, certain fields in the associated TML Corrosion Analysis records were populated with values using the unit of measure (UOM) inches per day instead of IN/YR (TM) (i.e., inches per year), which is the UOM that is specified in the properties of the fields. To correct this issue in existing records, you must perform this step to manually update TM Analyses. For more information about this issue, see the V3.5.1 Release Notes.</p> |

| Step | Task | Notes |
|------|---|-------|
| | <p>TMLGROUP with your custom family IDs.</p> <ul style="list-style-type: none"> MI_EQUIP000_EQUIP_ID_C and MI_TMLGROUP_ID_C with the field IDs used to identify these custom equipment records. <p>c. Run the Bulk Analyze tool using your custom records.</p> | |
| 2 | <p>If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 2850.</p> | |

Use Custom TML Analysis Types

The baseline GE Digital APM database includes the Thickness Measurement Location family, which contains the TML Analysis Type field. This field is used to classify TMLs based upon the collection method that will be used for recording Thickness Measurements at that location.

The TML Analysis Type field contains a list of values that is populated with the Corrosion Inspection Type values from all Corrosion Analysis Settings records that are associated with the asset or TML Group to which the Thickness Measurement Location record is linked.

The values that are used to populate the Corrosion Inspection Type field in the Corrosion Analysis Settings family are stored in the System Code Table CITP (Corrosion Inspection Type). In the baseline GE Digital APM database, this table contains three System Codes: UT, RT, and TML. You can only create Thickness Measurement Location records with a given TML Analysis Type value if an associated Corrosion Analysis Settings record contains the same value in the Corrosion Inspection Type field.

Using the baseline functionality, you can separate Corrosion Analysis calculations into groups based upon TML Analysis Type. If you want to use this functionality, you will want to classify your TMLs as UT (measurements collected using ultrasonic thickness) or RT (measurements collected using radiographic thickness). This separation will be desirable for some implementations. Other implementations will prefer not to separate TMLs according to collection method and instead perform calculations on the entire group of TMLs that exists for an asset. For these implementations, you will want to classify all TMLs using the TML Analysis Type TML.

Depending upon your preferred implementation, you may choose to make one or more of the following changes to the System Code Table CITP (Corrosion Inspection Type):

- Add System Codes if you want to classify TMLs using methods in addition to UT and RT.
- Delete System Codes that you do not want to use.
- Modify the IDs and descriptions of the System Codes so that the classification options are more intuitive to your users.

If you make changes to this System Code Table, keep in mind that the analysis types that are stored in the System Code Table CITP (Corrosion Inspection Type) will be used when you create Corrosion Analysis Settings records, and therefore, will determine the analysis types for which you can create Thickness Measurement Location records.

Additionally, in Thickness Measurement Location records, the TML Analysis Type field has a baseline Default Value rule that is coded to present UT as the default value when you have defined the UT TML Analysis Type in your Corrosion Analysis (i.e., you have created a Corrosion Analysis Settings record with a Corrosion Inspection Type of UT). You could modify this rule if, for example, you wanted RT to be presented as the default value when you have defined the RT TML Analysis Type in your Corrosion Analysis (i.e., you have created a Corrosion Analysis Settings record with a Corrosion Inspection Type of RT). To do this, you would modify the MI_TML_TYPE_CHR class as follows:

```
<MetadataField("MI_TML_TYPE_CHR")> _
Public Class MI_TML_TYPE_CHR
    Inherits Baseline.MI_Thickness_Measurement_Location.MI_TML_TYPE_CHR
```

```
Public Sub New(ByVal record As Meridium.Core.DataManager.DataRecord, ByVal field
As Meridium.Core.DataManager.DataField)
    MyBase.New(record, field)
End Sub
Public Overrides Function GetDefaultInitialValue() As Object
    Return CStr("RT")
End Function
End Class
```

More information on customizing baseline rules is available [here](#).

Install the Meridium Device Service

⚠ IMPORTANT: This procedure needs to be repeated on every machine to which a datalogger will be connected.

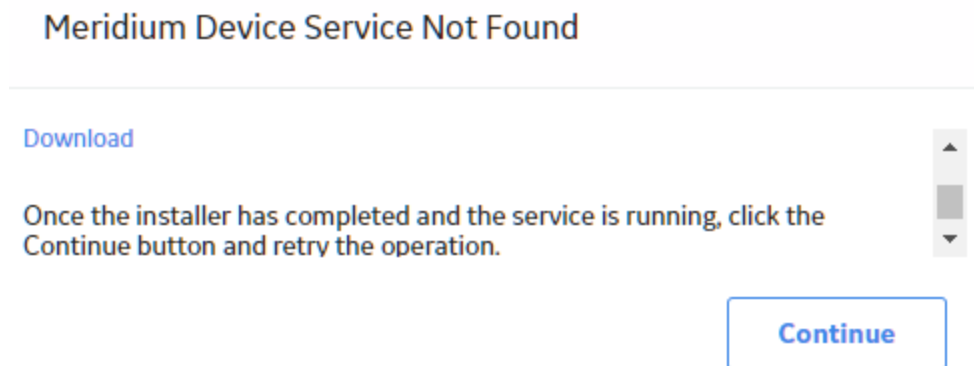
The Meridium Device Service can be installed in the normal workflow when using dataloggers with Thickness Monitoring.

Steps

1. Access Dataloggers for the any asset or TML Group.
2. Select **Send**.

Note: A datalogger does not need to be connected.

The **Meridium Device Service Not Found** window appears.




3. Select the **Download** link.
MeridiumDevices.exe is downloaded.
4. Run **MeridiumDevices.exe** and follow the instructions in the installer.
The Meridium Device Service is installed.
5. In the **Meridium Device Service Not Found** window, select **Continue**.
Dataloggers can now be used with Thickness Monitoring.

Configure the Meridium Device Service

After installing the Meridium Device Service, you can make changes to certain configuration settings. The Meridium Device Service is designed to function without additional configuration. 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 GE Digital 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

GE Digital 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 GE Digital APM is determined by membership in these Security Groups. Note that in addition to the baseline family-level privileges that exist for these Security Groups, users will also need at least *View* privileges for all customer-defined predecessor or successor families that participate in the Thickness Monitoring relationships. Keep in mind that:

- Users who will need to *create* new records in TM will need *Insert* privileges to these families.
- Users who will need to *modify* records will need *Update* privileges to these families.
- Any user who should be allowed to delete TM records will need *Delete* privileges to these families.

The following table summarizes the *functional* privileges associated with each group.

| Function | Can be done by members of the MI Thickness Monitoring Administrator Group? | Can be done by members of the MI Thickness Monitoring Inspector Group? | Can be done by members of the MI Thickness Monitoring User Group? |
|---|--|--|---|
| Configure Global Preferences | Yes | No | No |
| Configure Family Preferences | Yes | No | No |
| Use the T-Min Calculator | No | Yes | No |
| Archive Corrosion Rates | No | Yes | No |
| Reset the Maximum Historical Corrosion Rate | Yes | No | No |
| Exclude TMLs | No | Yes | No |

Deploy Modules and Features

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

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 |
| MI Thickness Monitoring Viewer | MI APM Viewer MI Mechanical Integrity Viewer |

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

| Family | MI Thickness Monitoring Administrator | MI Thickness Monitoring Inspector | MI Thickness Monitoring User | MI Thickness Monitoring Viewer |
|-----------------------|---------------------------------------|-----------------------------------|------------------------------|--------------------------------|
| Entity Families | | | | |
| Corrosion | View, Update, Insert | View, Update, Insert | View, Update, Insert | View |
| Datapoint | View, Update, Insert | View, Update, Insert | View, Update, Insert | View |
| Datapoint Measurement | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert | View |
| Equipment | View | View | View | View |

| Family | MI Thickness Monitoring Administrator | MI Thickness Monitoring Inspector | MI Thickness Monitoring User | MI Thickness Monitoring Viewer |
|--|---------------------------------------|-----------------------------------|------------------------------|--------------------------------|
| Human Resource | View, Update, Insert, Delete | View | View | View |
| Inspection Task | View | View, Update | View | View |
| Inventory Group Configuration | View | View | View | View |
| Materials of Construction | View | View | View | View |
| Meridium Reference Tables | View, Update, Insert, Delete | View | View | View |
| RBI Inspection Auto-Selection Criteria | View | View | View | View |
| Resource Role | View, Update, Insert, Delete | View | View | View |
| Security Group | View | View | View | View |
| Security User | View | View | View | View |
| Settings | View, Update, Insert | View, Update, Insert | View | View |
| Task Execution | View, Insert | View, Insert | View | View |
| Thickness Monitoring Task | View, Update, Insert, Delete | View, Update, Insert | View, Update, Insert | View |
| TML Group | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Relationship Families | | | | |
| Belongs to a Unit | View, Update, Insert, Delete | View, Update, Insert | View, Update, Insert | View |
| Equipment Has Equipment | View | View | View | View |

| Family | MI Thickness Monitoring Administrator | MI Thickness Monitoring Inspector | MI Thickness Monitoring User | MI Thickness Monitoring Viewer |
|--|---------------------------------------|-----------------------------------|------------------------------|--------------------------------|
| Group Assignment | View | View | View | View |
| Has Archived Corrosion Analyses | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Archived Corrosion Analysis Settings | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Archived Subcomponent Analysis Settings | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Archived Subcomponent Corrosion Analyses | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Corrosion Analyses | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Corrosion Analysis Settings | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Data-points | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Inspections | None | None | None | View |
| Has Measurements | View, Update, Insert, Delete | View, Update, Insert, Delete | View, Update, Insert, Delete | View |
| Has Roles | View, Update, Insert, Delete | View | View | View |
| Has Task Execution | View, Insert | View, Insert | View | View |
| Has Task Revision | View, Insert | View, Insert | View | View |

Deploy Modules and Features

| Family | MI Thickness Monitoring Administrator | MI Thickness Monitoring Inspector | MI Thickness Monitoring User | MI Thickness Monitoring Viewer |
|-----------------|---------------------------------------|-----------------------------------|------------------------------|--------------------------------|
| Has Tasks | View, Insert | View, Insert | View, Insert | View |
| Has TML Group | View, Update, Insert, Delete | View, Update, Insert, Delete | View | View |
| Is a User | View | View | View | View |
| User Assignment | View | View | View | View |