APM Installation

Contents

Copyright GE Digital

Chapter

1

APM Installation

Topics:

First-time Deployment

Deploy GE Digital APM for the First Time

The following table outlines the steps that you must complete to deploy and configure GE Digital APM for the first time. After you have completed these steps, you will need to perform additional steps to configure the modules that you have purchased.

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

Step	Task	Notes
1	Ensure that your system meets the hardware and software requirements for the basic GE Digital APM system architecture.	This step is required.
2	Review how the operating systems are configured in the GE Digital APM testing environment.	This step is required.
3	Configure GE Digital APM Server roles and features.	This step is required. It is recommended that you configure your system to match the configuration used in the GE Digital APM testing environment.
4	Install the GE Digital APM Server and add-ons software on each computer that will serve as a GE Digital APM Server.	This step is required.
5	Install Redis on the GE Digital Redis server (Linux server).	This step is required. **Note:** The last supported Redis version for Windows contains Common Vulnerabilities and Exposures (CVE). Therefore, we recommend that you install Redis on a Linux server. However, if you want to install Redis on a Windows server, refer to the Install Redis on the GE Digital APM and Redis server (Windows server) topic.
6	Install Elasticsearch on a dedicated server.	This step is required. You must install Elasticsearch on a server in your environment.
7	Install ActiveMQ on a dedicated server.	This step is required. You must install ActiveMQ on a server in your environment.
8	Deploy the GE Digital APM Database Server, which includes creating and configuring your GE Digital APM database.	This step is required.
9	Create an Initial Data Source on page 35	This step is required.
10	Deploy the GE Digital APM SQL Server Report Server.	This step is required.
11	Configure GE Digital APM to Use SQL Server Report Server on page 48	This step is required.

Step	Task	Notes
12	Create security user records for individuals who will need to log in to GE Digital APM applications.	This step is required.
13	Activate Licensed Modules and Products on page 48	This step is required.
14	Configure the GE Digital APM Server for Running the Scheduled Jobs on page 49	This step is required only if you have deployed the GE Digital APM in a clustered environment and you want to dedicate a virtual machine to run all the scheduled jobs.
15	Install the GE Digital APM Mobile Application on page 49 on your mobile device based on one of the following operating systems: • Android • iOS • Windows	This step is required only if you want to install the GE Digital APM mobile application on mobile devices.
16	Enable single sign-on for an-site or off-site authentication.	This step is required only if you are enabling single sign-on.
17	Configure IIS on page 50	This step is required only if you want to redirect HTTP client requests to Meridium.
18	About GE Digital APM Module Deployment on page 54	This step is required.
19	Install Advanced Visualization	This step is required only if you want to install Advanced Visualization module.

Testing Environment Configuration

About the Operating System in the GE Digital APM Test Environment

The GE Digital APM test environment uses the 64-bit version of Windows Server 2016 and Windows Server 2019 for all instances of the GE Digital APM Server (both dedicated and supporting). The operating system is not distributed by GE Digital APM and must be obtained from another vendor. Providing instructions on installing the operating system exceeds the scope of this documentation, but this documentation provides guidelines on how to configure the operating system in the GE Digital APM test environment. We recommend that you configure your system to match the configuration used in the GE Digital APM test environment.

To configure your system to match the GE Digital APM test environment, on the computer that will function as the GE Digital APM Server, configure GE Digital APM Server roles and features.

Note: WebDAV must be disabled prior to installing the GE Digital APM Server software.

What To Do Next

• GE Digital APM Server Roles and Features for Windows Server 2016 and Windows Server 2019 on page 4

Server Roles and Features

GE Digital APM Server Roles and Features for Windows Server 2016 and Windows Server 2019

The following server roles and features are installed in all instances of the GE Digital APM Server in the GE Digital APM test environment for Windows Server 2016 and Windows Server 2019.

Tip: Roles and features can be installed via the **Add Roles and Features Wizard** on a Windows Server. To install roles and features, in **Server Manager**, in the **Manage** menu, select **Add Roles and Features** to access the wizard. Select **Role-based or feature-based installation**, select the GE Digital APM Server from the **Server Pool**, and then select **Next >**.

Server Roles

In the **Server Roles** section:

- Web Server (IIS)

  ◦ Web Server

    ◦ Common HTTP Features

      ◦ Default Document
      ◦ Directory Browsing
      ◦ HTTP Errors
      ◦ Static Content
      ◦ HTTP Redirection
      ◦ WebDAV Publishing (clear the **WebDAV Publishing** check box)

    ◦ Health and Diagnostics

      ◦ HTTP Logging
      ◦ Custom Logging (clear the **Custom Logging** check box)
      ◦ Logging Tools
      ◦ ODBC Logging
      ◦ Request Monitor
      ◦ Tracing

    ◦ Performance

      ◦ Static Content Compression
      ◦ Dynamic Content Compression

    ◦ Security

      ◦ Request Filtering
      ◦ Basic Authentication
      ◦ Centralized SSL Certificate Support (clear the **Centralized SSL Certificate Support** check box)
      ◦ Client Certificate Mapping Authentication
      ◦ Digest Authentication
      ◦ IIS Client Certificate Mapping Authentication
      ◦ IP and Domain Restrictions
      ◦ URL Authorization

- ◦ Windows Authentication
- ◦ Application Development

  - ◦ .NET Extensibility 3.5 (clear the **.NET Extensibility 3.5** check box)
  - ◦ .NET Extensibility 4.6
  - ◦ Application Initialization
  - ◦ ASP
  - ◦ ASP .NET 3.5 (clear the **ASP .NET 3.5** check box)
  - ◦ ASP.NET 4.6
  - ◦ CGI (clear the **CGI** check box)
  - ◦ ISAPI Extensions
  - ◦ ISAPI Filters
  - ◦ Server Side Includes (clear the **Server Side Includes** check box)
  - ◦ WebSocket Protocol
- ◦ Management Tools

  - ◦ IIS Management Console
  - ◦ IIS 6 Management Compatibility
  - ◦ IIS Management Scripts and Tools

Features

In the **Features** section:

- .NET Framework 4.6 Features

  Note: All the .NET Framework features are required.
- Remote Server Administration Tools (As needed, select or clear the check boxes next to the Remote Server Administration Tools)
- Windows Internal Database
- Windows PowerShell (clear the **Windows PowerShell 2.0 Engine**, **Windows PowerShell Desired State Configuration Service**, and **Windows PowerShell Web Access** check boxes)

  - ◦ Windows PowerShell 5.1
  - ◦ Windows PowerShell ISE
- Windows Process Activation Service (clear the **.NET Environment 3.5** check box)

  - ◦ Process Model
  - ◦ Configuration APIs
- WoW64 Support

What To Do Next

-

APM Server Installation

Install the GE Digital APM Server Components

Before You Begin

- Ensure that your computer meets the hardware and software requirements for the GE Digital APM Server.

- Ensure that you are an administrator with full access to the computer that will serve as the GE Digital APM Server.

Note: Before the installation begins, the installer resets IIS.

Note:

- If you want to run the GE Digital APM Server installer in silent mode from the command line, you must first ensure that Microsoft .NET Framework 4.7.2 is installed on the GE Digital APM Server. If it is not installed, an error will occur during installation. You can download this program from the official Microsoft website.
- If the GE Digital APM Server installer is run according to the procedure in this topic, and if Microsoft .NET Framework 4.7.2 has not yet been installed on the GE Digital APM Server, it will be installed automatically during the installation.

Important: Before installing the GE Digital APM Server via IIS Manager, the WebDAV Publishing service needs to be deactivated. To verify that it is deactivated, in the Server Manager, in the **Roles and Features** section of the **Local Server** workspace, ensure that **WebDAV Publishing** is not present in the list.

Procedure

1. On the GE Digital APM Server, access the GE Digital APM distribution package, and then go to the folder `Setup\Meridium APM Server and Add-ons`.
2. Open the file `setup.exe`.

   A message appears, asking if you want to allow the installer to make changes to your computer.

   Important: If the required software are not installed, a window appears, displaying a list of missing software that you must install. Select **Install**. The installer installs the software, and then the server is restarted.
3. Select **Yes**.

   The Meridium APM Server installer page appears.
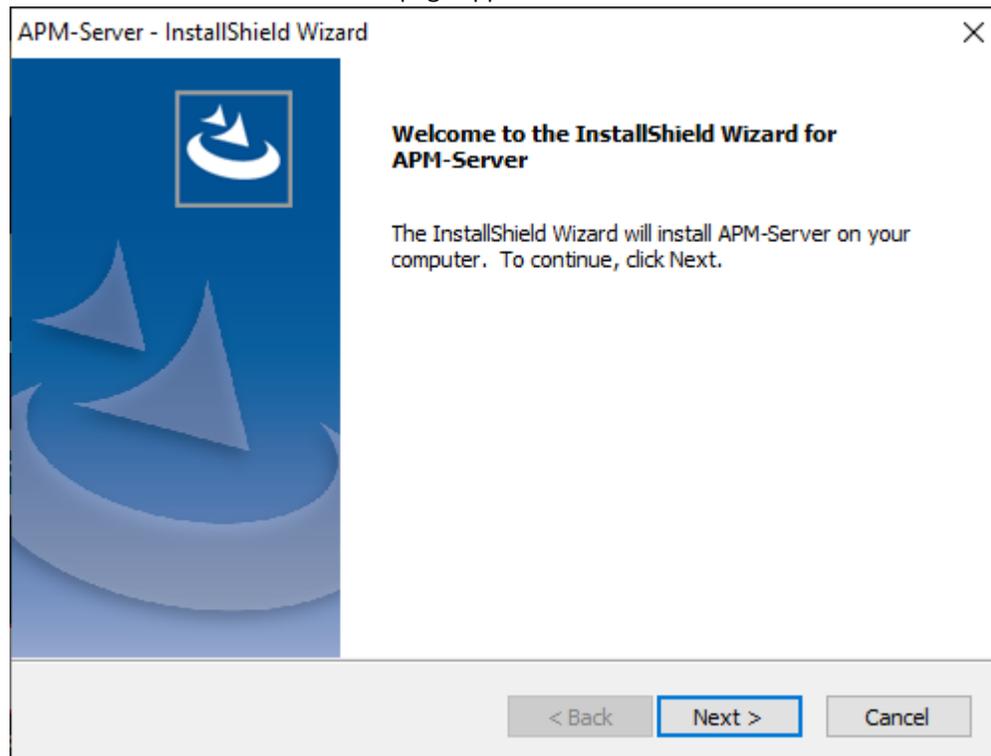
Note: If a list of required programs appears in the installer, select **Install**. The installer will install the programs, and then the server will restart.

4. Select **Next**.

The **License Agreement** page appears.
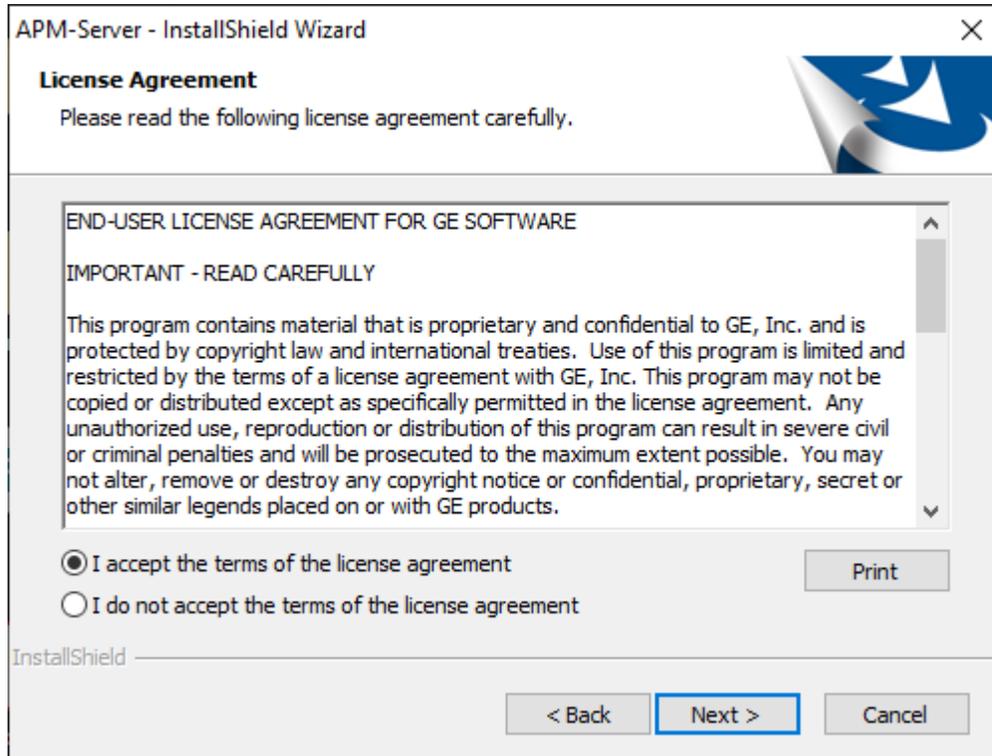
5. Read the license agreement, and if you agree to the terms, select **I accept the terms of the license agreement**, and then select **Next**.

The **Select Installation Location** page appears.
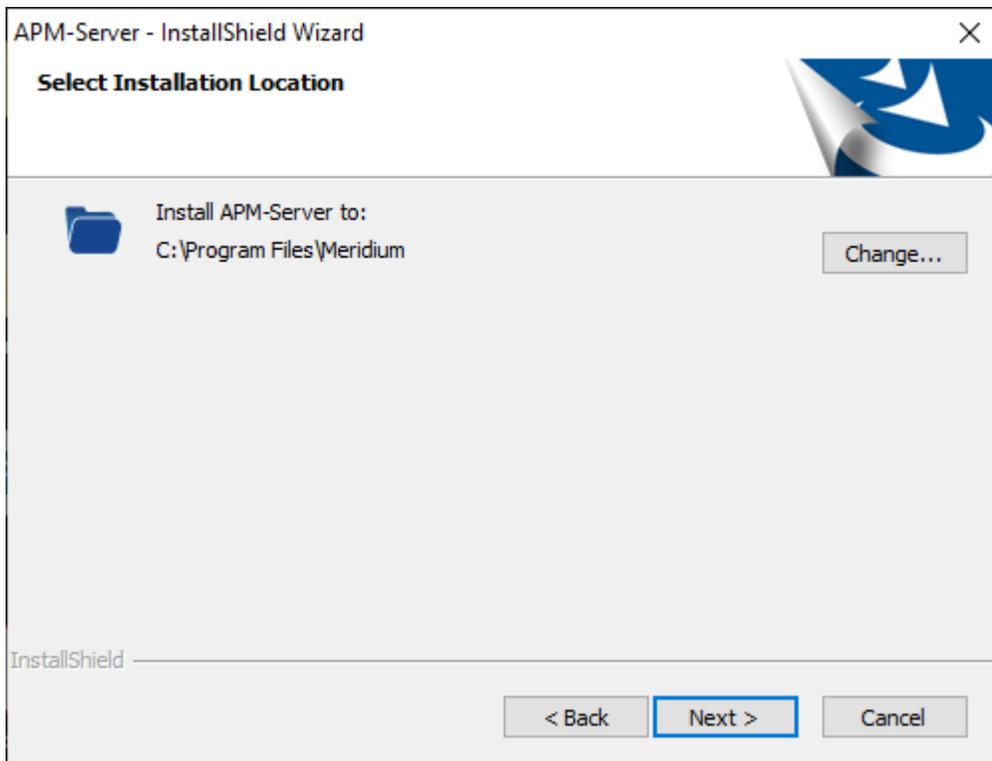
Note: By default, the Meridium APM Server software will be saved to `C:\Program Files \Meridium`. If you want to change the location, select **Change**, and then go to the location where you want to install the software.

6. Select **Next**.

   The **Select the features you want to install** page appears.
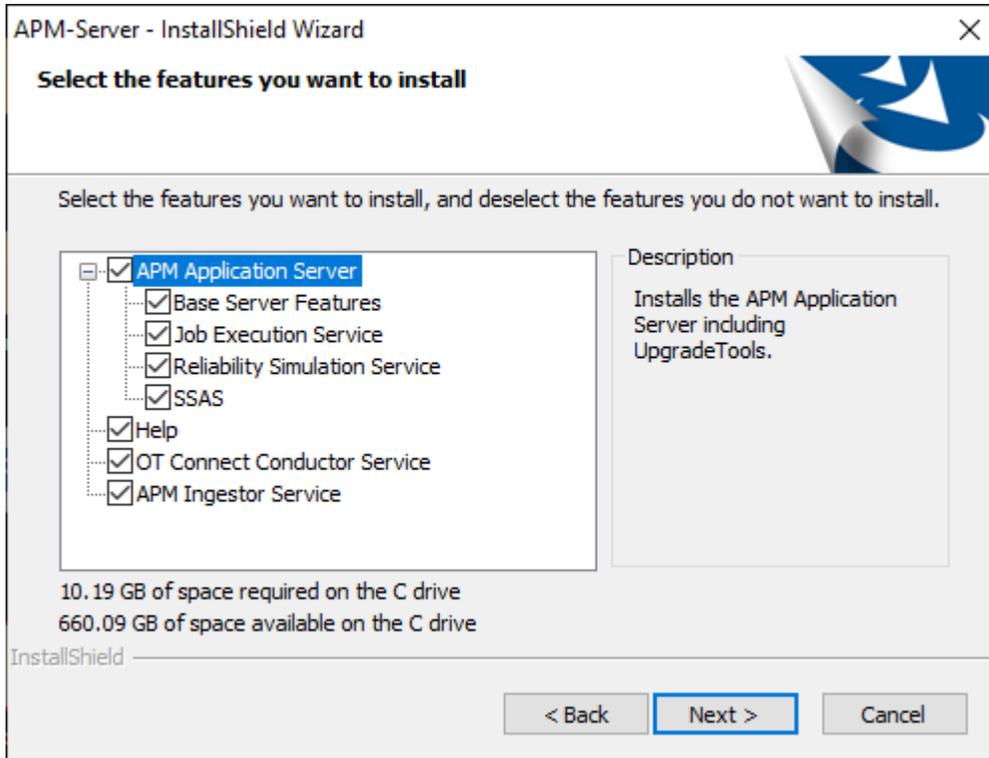
Important: You can specify which features you want to install on the GE Digital APM Server. This procedure assumes that you want to deploy only the GE Digital APM Server software and Help files.

Note: Deploying the help files will create a locally stored copy of the files on your GE Digital APM Server. By default, GE Digital APM is configured to point to this copy when Help is accessed; however, the setting is configurable.

7. Ensure that the **APM Application Server, Base Server Features,** and **Help** check boxes are selected.
8. Select **Next**.

Important: If the minimum hardware and software requirements for installing GE Digital APM are not met, the **Meridium Installer** page appears, displaying a list of missing software. As needed, install the software, and then select **Next**.

The **Select ZIP File Location** page appears.
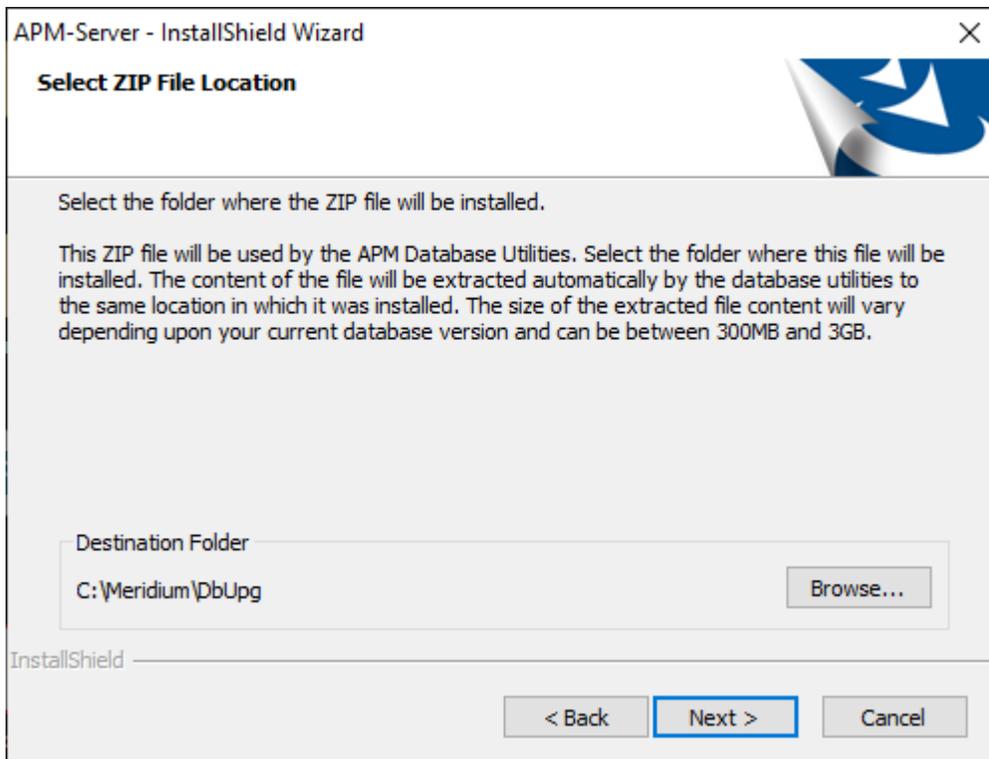
9. Change the default destination folder if needed, and then select **Next**.

   The **Websites** page appears.
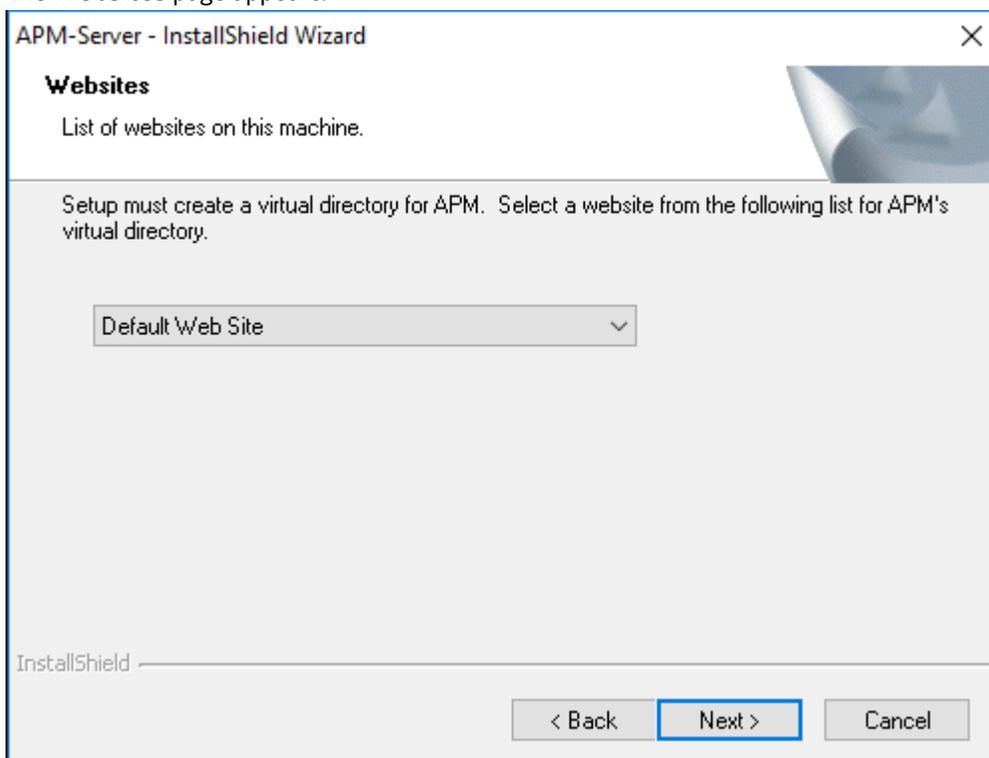
10. If needed, change the website for the Meridium virtual directory, and then select **Next**.

    The **Complete the Installation** page appears.
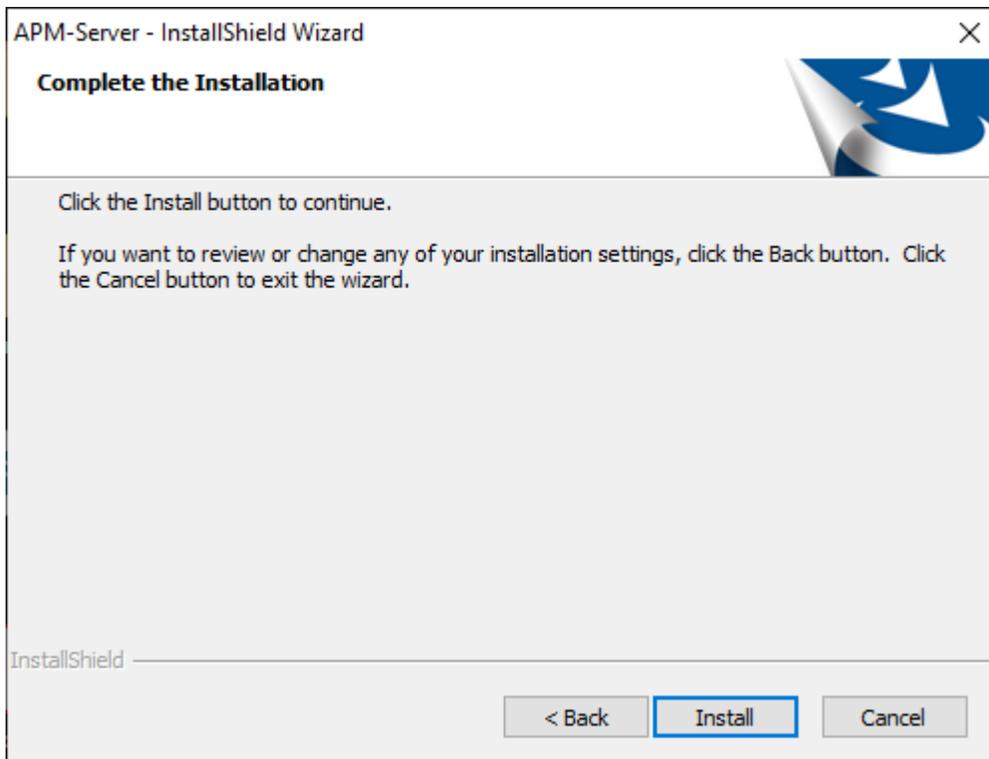
11. Select **Install**.

The **Setup Status** page appears, displaying a progress bar. When the installation is complete, the **Installation is Complete** page appears.
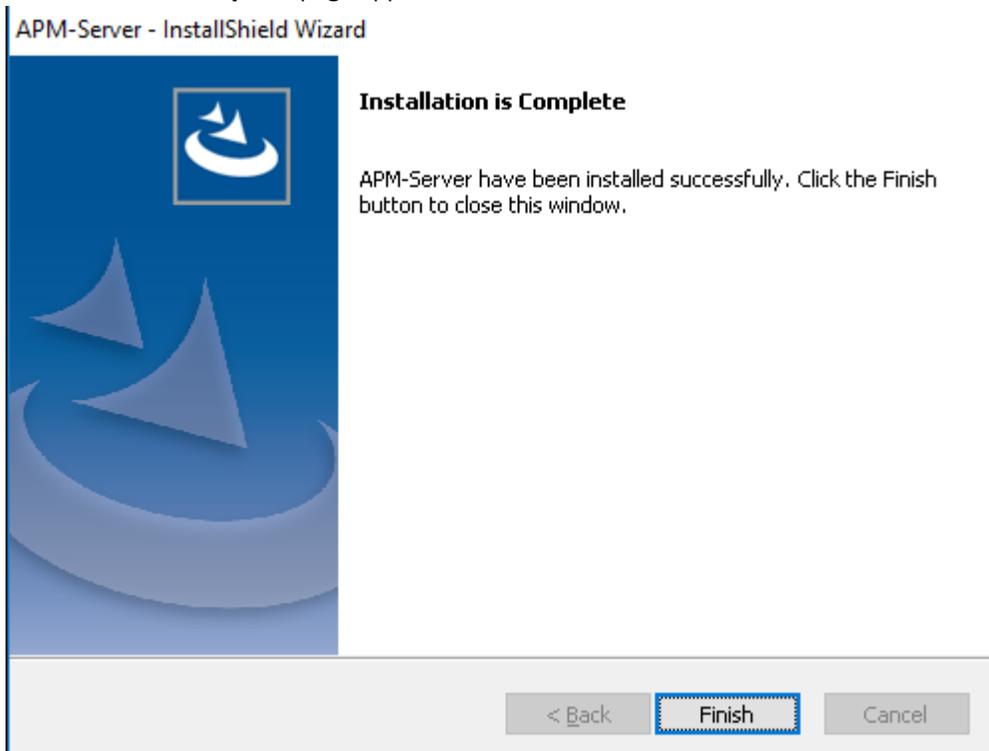
12. Select **Finish**.

Note: If prompted to restart your computer, select **Yes, I want to restart my computer now**, and then select **Finish**.

The APM Server installer closes.

Next Steps

-

Uninstall GE Digital APM Server Components After the Initial Installation

About This Task

If you need to uninstall GE Digital APM Server on a machine after the initial installation is complete, you can run the GE Digital APM Server installer again to uninstall the software.

Note: IIS will be reset automatically by the installer before the installation process begins.

Procedure

1. On the GE Digital APM Server machine, via the Control Panel, access the **Programs and Features** window.
2. In the grid, select the **APM Server** item, and then select **Uninstall**.

   The APM-Server installer appears, displaying the **Preparing Setup** screen, which contains a progress bar. After completion, a message appears, asking if you want to remove the selected application and all of its features.

   APM-Server - InstallShield Wizard   ✕

   Do you want to completely remove the selected application and all of its features?

   [Yes]   [No]
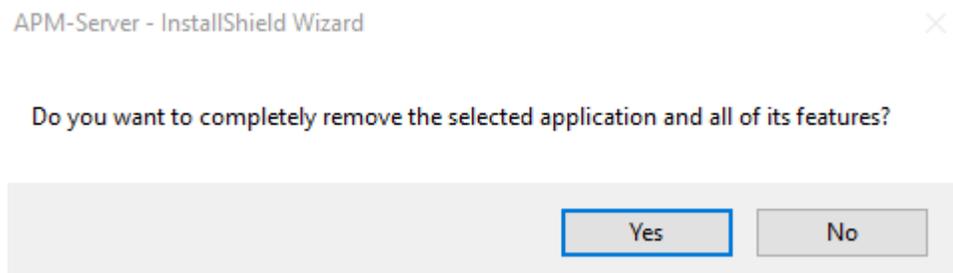
3. Select **Yes**

   The **Setup Status** screen appears, displaying a progress bar. After the application and all of its features are removed, the **Uninstall Complete** screen appears.
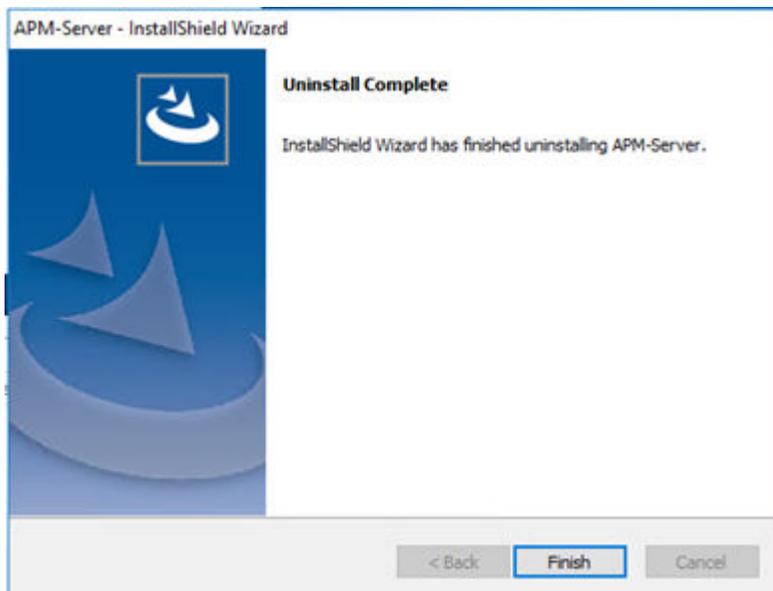
4. Select **Finish**

The APM Server installer closes.

Redis on Linux Installation

About Redis

Redis is a high-performance, NoSQL key-value database typically used for caching data to scale high-traffic websites. It is an open source software component licensed under the Three Clause BSD License. GE Digital APM uses Redis for caching purposes and to ensure a consistent shared cache among the various servers and services that make up a GE Digital APM installation.

More Details

Redis provides a basic Pub-Sub messaging infrastructure that allows the server to notify subscribed clients of changes or various events that occur on the server. GE Digital APM uses this feature to notify servers/services when cached data has changed, caches expire, or caches are removed.

The GE Digital APM Servers are set up using one of the following configurations:

- Single server cache configuration
- High availability configuration

If GE Digital APM Servers are set up in a load-balanced configuration, you can configure Redis clusters for Automatic Fail-Over monitoring. Redis uses a primary/replica topology with monitoring capabilities to provide high availability.

Install Redis on the GE Digital Redis Servers

Before You Begin

- Make sure that you have sudo privileges on Linux.

About This Task

This topic describes how to install Redis on the Linux-based GE Digital Redis servers.

Note: The last supported Redis version for Windows contains Common Vulnerabilities and Exposures (CVE). Therefore, we recommend that you install Redis on a Linux server.

Procedure

1. Log in to the GE Digital Redis server.
2. Access the **Terminal** window, and then run the following commands:

   a. ```
   sudo apt-get update
   ```

   b. ```
   sudo apt-get install redis-server
   ```

   Redis and its dependencies are downloaded and installed on the Redis server.
3. Navigate to the directory `/etc/redis/redis.conf`, and then access the `redis.conf` file.
4. Open the `redis.conf` file using a text editor (for example, Nano), and then modify the configuration settings as described in the following table:

Configuration Option	Description
`notify-keyspace-events`	Specify `EA` against the configuration option.
`bind`	Specify the IP address of the Redis server on which you installed Redis.
`requirepass`	Specify the password for the Redis connections. **Note:** You must set a complex password string that contains random characters to ensure that the connections are secured. In a high-availability configuration setup, you must use the same password for all the servers.
`masterauth`	Specify the same password that you specified for the `requirepass` configuration option. **Note:** In a high-availability configuration setup, the password is used to authenticate the Redis nodes with the primary Redis server, and then the nodes and the primary Redis server are connected.
`slaveof`	In a high-availability configuration setup, if the Redis server is defined as a replica of the primary Redis server, replace the following placeholder text with appropriate values: • *\<masterip\>*: Replace with the IP address of the primary Redis server. • *\<masterport\>*: Replace with the port (that is, 6379) of the primary Redis server.
`slave-priority`	Specify the priority as `1` for the replica server. **Note:** The priority is specified as 100 by default. If there are multiple replica servers, specify the priorities for all the replica servers in an incremental order. For example, configure the first server and specify the priority as `1`, then specify the priority for the second server as `2`, and so on.

   Note: For more information on the configuration options available in the `redis.conf` file, refer to the Redis documentation.
5. Run the following command to restart Redis:

   ```
   sudo systemctl restart redis
   ```

6. Run the following command to ensure that the Redis service is running on the Redis server:

```
systemctl status redis
```

Configuring and Securing the Redis Server

Basic Configuration

To configure the Redis server, use the conf file that you have specified while installing Redis. By default, this file is located at `C:\Program Files\Redis\redis.windows-service.conf`. After you modify the file, restart the Redis service to apply the changes.

You can also use the CONFIG GET and CONFIG SET commands from a Redis client to view or alter the server configuration.

Note: Ensure that the value for configuration option `notify-keyspace-events` in the conf file is specified as `EA`.

Server and Ports Configuration

By default, the Redis server runs on TCP Port 6379. Ensure that port 6379 is accessible between the Redis client and the Redis server. Any firewalls between the systems must be configured to support traffic over this port. You can set the default port in the conf file.

Secure Access Configuration

It is recommended to always use Redis in an environment in which the network and the Redis server are secured.

You can secure the access to Redis using any of the following methods:

- **Configure Redis to use a password:**
  By default, Redis is configured without a password. When using a password on the Redis server, you must configure the connection string to include the password.
  To set the password:

  1. On the GE Digital APM Server, access the folder `C:\ProgramData\Meridium`, and then, open the file `MeridiumAppSettings.xml`.
  2. Within the <cacheServiceUrl> setting, change the default value localhost to `localhost,password=<Redis Server password>`.

  Note: You can encrypt the password in the XML file by running `MeridiumCachePasswordUtility.exe` at a command prompt, and passing in `C:\ProgramData\Meridium\MeridiumAppSettings.xml` as a command line parameter.
- **Set up a firewall on the Redis server:** This will allow only connections from the GE Digital APM servers.

Note: If the network transmissions are across an unsecured/open network, we recommend that you use third-party software (for example, Stunnel) to enable SSL communication between systems.

Standard Deployment Architecture

The following image illustrates the standard deployment architecture of the Redis system:
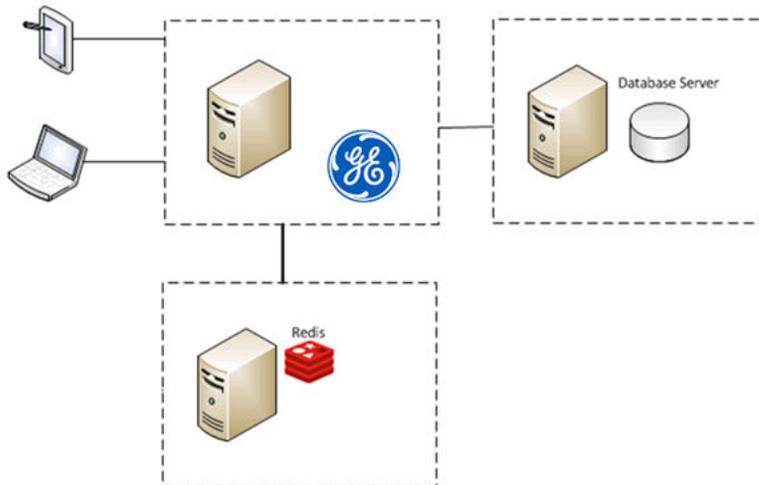
Set Up the GE Digital APM Server - Single Server Cache Configuration

About This Task

This task describes how to configure GE Digital APM servers using single server cache configuration.

Procedure

1. On the GE Digital APM Server machine, navigate to the folder `C:\ProgramData\Meridium`.
2. Open the file `appsettings.Global.json` in an application that you can use to modify JSON.
3. As needed, modify the following values:

```
// Connection settings for Redis, Timeouts in milliseconds
    "cacheOptions": {
        "host": "localhost",
        "port": 6379,
        "syncTimeout": 25000,
        "password": "my redis password"
        // Uncomment to add failover hosts.

        // "failoverHosts": [{"host": "host", "port": 6379}]
    },
```

Note: The password in the XML file can be encrypted by running `MeridiumCachePasswordUtility.exe` from a command prompt and passing in `C:\ProgramData\Meridium\MeridiumAppSettings.xml` as a command line parameter.

Configure Redis - High Availability Configuration

About This Task

The following image illustrates how the Redis servers are connected in a high-availability configuration setup using the primary/replica configuration:
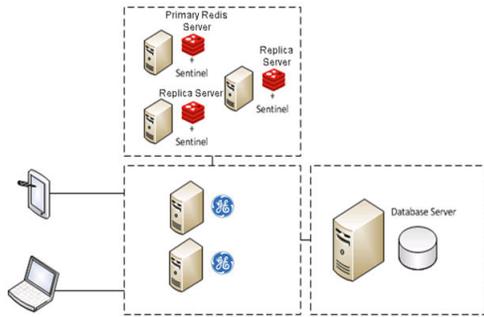
Sentinel: Automatic Fail-Over Monitoring and Configuration

About This Task

This setup will automatically replicate any data changes from the primary Redis server to the replica server. Sentinel will then automatically detect a failure and reconfigure the replica server to be the primary server in the event of failure.

Note: It is recommended that you configure Redis in a primary/replica setup with Sentinel. You must perform the steps on each Redis and Sentinel server.

Procedure

1. Create the following service file for the Sentinel server:

   `/etc/systemd/system/sentinel.service`

2. Open the service file using a text editor (for example, Nano), and then add the following text to the file:

   ```
   [Unit]
   Description=Sentinel for Redis
   After=network.target

   [Service]
   LimitNOFILE=64000
   User=redis
   Group=redis
   ExecStart=/usr/bin/redis-server /etc/redis/sentinel.conf --daemonize
   no --sentinel

   [Install]
   WantedBy=multi-user.target
   ```

3. Save the service file.

4. Create the following Sentinel configuration file:

   `/etc/redis/sentinel.conf`

5. Open the configuration file using a text editor (for example, Nano), and then add the following text to the file:

   ```
   sentinel monitor <primary-server-group-name> <primary-server IP>
   6379 2
   sentinel auth-pass <primary-server-group-name> <primary-server
   password>
   logfile /var/log/redis/sentinel-server.log
   bind <server ip> 127.0.0.1
   ```

Important: If a password is configured in the `/etc/redis/redis.conf` file, add the following configuration directive to `/etc/redis/sentinel.conf`:

```
masterauth <redis password>
```

6. Save the configuration file.
7. Run the following commands to make Redis the owner of the `/etc/redis/sentinel.conf` file:

   a. ```
   sudo chown redis:redis /etc/redis/sentinel.conf
   ```

   b. ```
   sudo chmod 600 /etc/redis/sentinel.conf
   ```

8. Run the following command to start Sentinel:

   ```
   sudo systemctl start sentinel
   ```

   Note: By default, the Sentinel server runs on TCP Port 6379. If you are connected to an unsecure network, you must block the port from any external access. However, the port must be accessible from all Sentinel and Redis servers.

9. To use GE Digital APM, Redis, and Sentinel in a High Availability Configuration:

   a) On the GE Digital APM Server machine, navigate to the folder `C:\ProgramData\Meridium`.
   b) Open the file `appsettings.Global.json` using a text editor (for example, Notepad).
   c) As needed, modify the following values. Ensure that the `Host` is set as the main host, and any additional hosts are listed as `FailoverHost`.

   ```
   // Connection settings for Redis, Timeouts in milliseconds
       "cacheOptions": {
           "host": "localhost",
           "port": 6379,
           "syncTimeout": 25000
           // Uncomment to add failover hosts.
           "failoverHosts": [{"host": "otherhost", "port": 6379}]
       },
   ```

   d) For each GE Digital APM Server in the high-availability configuration, repeat steps a through c.

Next Steps

-

Elasticsearch Installation

Install Elasticsearch on a Dedicated Server

Procedure

1. On the server on which you want to install Elasticsearch, install one of the following:

   - OpenJDK V11

     a. Download OpenJDK 11 (LTS) from the AdoptOpenJDK website.
        The OpenJDK 11 installer is downloaded to your local drive.
     b. Run the OpenJDK 11 installer and follow the instructions in the wizard.
     c. In the **Custom Setup** page, select the **Set JAVA_HOME variable** menu, and then select **Will be installed on local hard drive**.

    d. When the installation is complete, close the OpenJDK 11 installer.
- Oracle JDK V11

    a. Download and install Oracle JDK V11.

    b. Configure the JAVA_HOME environment variable to point Elasticsearch to the Java installation directory, and then add Java to the Path system variable.

      Note: For more information on how to configure the JAVA_HOME environment variable, refer to the Oracle documentation.

2. Download the ZIP file for Windows, `elasticsearch-7.9.3.zip`, from the official Elasticsearch 7.9.3 Downloads page.

3. Extract the contents of the zip file to `C:\ElasticSearch`.

4. Go to `C:\ElasticSearch\elasticsearch-7.9.3\config`, and then access the `elasticsearch.yml` file.

5. In the .yml file, uncomment the following properties, and then modify the values to match those shown here:

```
cluster.name: apm-cluster
node.name: ${COMPUTERNAME}
path.data: /ProgramData/Meridium/ElasticSearch
path.logs: /ProgramData/Meridium/Logs
bootstrap.memory_lock: true
network.host: 0.0.0.0
http.port: 9200
action.destructive_requires_name: true
```

6. Save and close the .yml file.

7. Select the **Start** button on Windows, right-click **Command Prompt**, and then select **Run as administrator**.
   The **Command Prompt** window appears.

8. At the command prompt, enter `cd C:\ElasticSearch\elasticsearch-7.9.3\bin`, and then press Enter.

9. At the command prompt, enter `elasticsearch-service install`, and then press Enter.
   Elasticsearch is installed.

10. Access the Microsoft Management Console (services.msc) and perform the following operations for the Elasticsearch service:

- Verify that the service runs as Local System.
- Modify the startup to be Automatic.
- Start the service to verify installation and configuration.

11. On the server on which Elasticsearch is installed, go to `http://localhost:9200/` in a web browser, and ensure that Elasticsearch runs successfully.
    A response that is similar to the following sample appears.

```
{
"name" : "apm-node",
"cluster_name" : "apm-cluster",
"cluster_uuid" : "58cS6NyzQJOLZ8Xr1e3vkg",
"version" : {
"number" : "7.9.3",
"build_hash" : "3adb13b",
"build_date" : "2017-03-23T03:31:50.652Z",
"build_snapshot" : false,
"lucene_version" : "6.4.1"
},
```

12. On the server on which Elasticsearch is installed, go to `http://[elastic-search-server]:9200/` in a web browser, and ensure that Elasticsearch runs successfully.
A response that is similar to the sample provided in the previous step appears.

13. On the GE Digital APM server, go to `C:\ProgramData\Meridium\appsettings.Global.json`.

14. As needed, modify the following value.

```
"elasticSearch": {
        "url": "http://localhost:9200"
    },
```

15. After all third-party services are configured, reset IIS and services on all GE Digital APM App Servers.

Next Steps

- Add User Authentication for Elasticsearch on page 20

Add User Authentication for Elasticsearch

To enhance security, you can implement user authentication for Elasticsearch using the X-Pack security.

Procedure

1. From the Elasticsearch installation folder, navigate to the config folder, and then access the file `elasticsearch.yml`.

2. In the `.yml` file, add the following line of code:

   `xpack.security.enabled: true`

3. Based on your Elasticsearch cluster type, complete one of the following steps:

   - For a single node cluster, add the following line of code in the `elasticsearch.yml` file:
     `discovery.type: single-node`
     Save and close the `elasticsearch.yml` file.
   - For a multi-node cluster, Elasticsearch requires TLS communication between the nodes. For instructions, refer to https://www.elastic.co/guide/en/elasticsearch/reference/7.9/configuring-tls.html#node-certificates.

4. From the Elasticsearch installation folder, set the bootstrap password. To do so:

   a) Run the command prompt as an administrator.
   b) Change the directory to the Elasticsearch installation folder.
   c) Run the following command: `bin/elasticsearch-keystore add "bootstrap.password"`
   d) Enter the password.

5. On the GE Digital APM server, navigate to `C:\ProgramData\Meridium`, and then modify the `appsettings.Global.json` file to update the Elasticsearch settings with the password:

```
"elasticSearch": {
        "url": "http://localhost:9200",
        "password": "<value>"
    },
```

6. Restart Elasticsearch, Search, and IIS.

Next Steps

Install ActiveMQ on a Dedicated Server on page 21

ActiveMQ Installation

Install ActiveMQ on a Dedicated Server

Procedure

1. On the server on which you want to install ActiveMQ, install one of the following:

   - OpenJDK V11

     a. Download OpenJDK 11 (LTS) from the AdoptOpenJDK website.
        The OpenJDK 11 installer is downloaded to your local drive.
     b. Run the OpenJDK 11 installer and follow the instructions in the wizard.
     c. In the **Custom Setup** page, select the **Set JAVA_HOME variable** menu, and then select **Will be installed on local hard drive**.
     d. When the installation is complete, close the OpenJDK 11 installer.

   - Oracle JDK V11

     a. Download and install Oracle JDK V11.
     b. Configure the JAVA_HOME environment variable to point Elasticsearch to the Java installation directory, and then add Java to the Path system variable.

        Note: For more information on how to configure the JAVA_HOME environment variable, refer to the Oracle documentation.

2. Download the zip file for Windows, `apache-activemq-5.xxx.zip`, (where xxx is the latest minor version of ActiveMQ 5), from the official ActiveMQ https://activemq.apache.org/components/classic/download/ page.
3. Extract the contents of the zip file to `C:\Program Files\ActiveMQ`.
4. Go to `C:\Program Files\ActiveMQ\apache-activemq-5.15.11\conf`, and then access the `activemq.xml` file.
5. In the `activemq.xml` file, perform the following actions:

   a) Locate the `<broker>` tag, and then add the attribute `schedulerSupport="true"` and `schedulePeriodForDestinationPurge="10000"` to the tag.
   b) Locate the `<transportConnectors>` tag and comment out the ones with names amqp, stomp, mqtt, and ws.
   c) Locate the `<policyEntries>` tag.

      - If a `<policyEntry>` tag exists with the attribute `queue=">"`, modify the tag to match the following: `<policyEntry queue=">" gcInactiveDestinations="true" inactiveTimoutBeforeGC="30000"> <deadLetterStrategy> <sharedDeadLetterStrategy processExpired="false" /> </deadLetterStrategy> </policyEntry>`.
      - If the `<policyEntry>` tag does not exist, add the following: `<policyEntry queue=">" gcInactiveDestinations="true" inactiveTimoutBeforeGC="30000"> <deadLetterStrategy> <sharedDeadLetterStrategy processExpired="false" /> </deadLetterStrategy> </policyEntry>`.

6. Save and close the .xml file.
7. Access the `jetty-realm.properties` file.
8. In the properties file, change the admin password:admin: <password>, admin
9. Comment out the other account.

10. Save and close the properties file.

11. In the `wrapper.conf` file, perform the following actions.

   a) Locate the text - wrapper.java.maxmemory=1024

   b) Change the value 1024 to the minimum value of `4000`. You can increase the value if you perform heavy data loads.

12. Save and close the `wrapper.conf` file.

13. Select the **Start** button on Windows, right-click Command Prompt, and then select **Run as administrator**.
   The Command Prompt window appears.

14. Enter `cd C:\Program Files\ActiveMQ\apache-activemq-5.15.11\bin\win64`, and then press **Enter**.

15. Enter `InstallService.bat`, and then press **Enter**.
   ActiveMQ is installed.

16. Access the Microsoft Management Console (services.msc) and perform the following operations for the ActiveMQ service:

   • Verify that the service runs as Local System.

   • Modify the startup to be Automatic.

   • Start the service to verify installation and configuration.

17. On the server on which ActiveMQ is installed, go to http://localhost:8161/ in a web browser, and ensure that **ActiveMQ** runs successfully.

18. On the GE Digital APM server, go to `C:\ProgramData\Meridium\appSettings.Global.json`.

19. As needed, modify the following values. If ActiveMQ is configured to be a cluster, add the additional host under "failoverHosts":

```
// Connection settings for ActiveMQ
    "queueOptions": {
        "activeMqHost": "localhost",
        "activeMqPort": 6161,
        "failoverHosts": [
            "localhost"
        ],
```

```
            "username": "admin",
            "password": "admin
```

20. After all third-party services are configured, reset IIS and services on all GE Digital APM App Servers.

Important: Verify that the hostnames and ports are configured correctly. If the hostname is not set correctly, then the third-party library that GE Digital APM uses to connect to ActiveMQ starts logging errors in a log file. The size of the log files can reach up to 400GB in 24 hours. It is recommended to check the log files folder after starting GE Digital APM for the first time.

Next Steps

Database Server Installation

Deploy the GE Digital APM Database Server for the First Time

The installation and configuration steps differ depending on whether you are connecting to an Oracle or SQL Server Database. Use the checklist appropriate to the type of database that you are using.

Use the checklist appropriate to the type of database that you are using.

Oracle Checklist

The following checklist should be used to install and configure an Oracle Database Server, create the GE Digital APM schema, and configure the GE Digital APM Server for use with Oracle.

You should complete these steps in relatively the same order in which they are listed in the table.

Step	Task	Notes
1	Ensure that the GE Digital APM Database Server machine meets the system requirements.	This step is required.
2	On the GE Digital APM Database Server, install the Oracle Server software.	This step is required.
3	On the GE Digital APM Database Server, create the Oracle database.	This step is required.
4	On the GE Digital APM Database Server, configure the Oracle database.	This step is required.
5	On the GE Digital APM Database Server, create the GE Digital APM Oracle schema.	This step is required.
6	On the GE Digital APM Database machine, Create the Oracle Scheduler Database on page 26.	This step is required.
7	On the GE Digital APM Database machine, Create the Oracle Scheduler Schema on page 27.	This step is required.
8	On the GE Digital APM Database machine, Create the Localization Oracle Database on page 28.	This step is required.

Step	Task	Notes
9	On the GE Digital APM Database machine, Create the Localization Oracle Schema on page 28.	This step is required.
10	On the GE Digital APM Server, create an initial data source.	This step is required.
11	In GE Digital APM, build the search index.	This step is required.

Install the Oracle Server Software

About This Task

Note: You need to complete this step only if you plan to use an Oracle Database Server to host the GE Digital APM schema.

The first step in setting up the database server for the GE Digital APM schema is to install the Oracle Server software on the database server machine. Instructions for installing the Oracle Server software exceed the scope of this documentation. For information on performing the installation, refer to the Oracle installation documentation that is specific to your database server platform. If you plan to create a database via the Oracle Universal installer, then, before proceeding, you should review the section in this documentation on Creating and configuring the Oracle database.

Next Steps

- Create the Oracle Database

Create the Oracle Database

Before you create the Oracle schema that will contain the GE Digital APM repository, you must install the Database Server software on the GE Digital APM Database Server machine. The creation of the Oracle database exceeds the scope of this documentation. For details on creating an Oracle database, consult the Oracle documentation that is specific to your database platform.

When the database is created, the database character set must be specified. If you are creating a Unicode database, use the character set AL32UTF8. This is the most recent and recommended Unicode database character set.

What To Do Next

-

Configure the Oracle Database

After you have created the Oracle database, you will need to configure it. Details on configuring the Oracle database exceed the scope of this documentation. For details on configuring an Oracle database, consult the Oracle documentation that is specific to your database platform. Note, however, that the Oracle database must meet the following requirements:

The following database parameter values are recommended and must persist from one database startup to the next.

Database parameter value	Notes
dml_locks=5000	The dml_locks parameters should be set to a large value to avoid the possibility of waiting for a lock.
open_cursors=500	It is not uncommon for one GE Digital APM user to have multiple cursors open simultaneously. For this reason, you should set this value accordingly.
parallel_max_servers=0	The GE Digital APM schema is not configured for parallel query. Therefore, we recommend that you disable this feature. Enabling parallel query when the database and schema are not properly configured can severely degrade system performance.
parallel_min_servers=0	The GE Digital APM schema is not configured for parallel query. Therefore, we recommend that you disable this feature. Enabling parallel query when the database and schema are not properly configured can severely degrade system performance.
processes=500	None
query_rewrite_enabled=true	None
timed_statistics=true	Setting timed_statistics allows for minimum maintenance and enables reporting on internal wait events, which can be used to reconfigure your database.
Memory_target= 4G	Suggested minimum

Default values for database parameters that are not mentioned in the above list meet or exceed recommendations for a GE Digital APM database configuration. GE Digital APM recommends that you monitor the database so that changes can be made as necessary to accommodate the needs of your specific installations. For more information on these and other database parameters, consult the Oracle documentation.

What To Do Next

- Create the GE Digital APM Oracle Schema

Create the GE Digital APM Oracle Schema on the GE Digital APM Database Server

About This Task

The following instructions provide details on creating the GE Digital APM Oracle schema. After you have created the Oracle schema using these instructions, the schema will be referred to as the GE Digital APM database throughout this documentation.

To perform these steps, you will need Oracle DBA privileges on the GE Digital APM Database Server machine. These instructions assume that:

- You are logged in to your GE Digital APM Database Server machine with DBA privileges and have a connection to Oracle.
- You are familiar with running SQL scripts and the associated terminology.

Procedure

1. On the GE Digital APM Server machine, in the GE Digital APM distribution package, navigate to the `Database` folder.
2. Open the file `MI_DB_MASTER_<version>.zip`, and then extract the contents of the file `<version>.zip` to a folder on the C: drive.
3. Open the file `<version>.zip`, and then open the subfolder `_Setup\NewInstall\Oracle`.

This folder contains the extracted files that will need to be run by the database administrator (via the remaining steps). The database administrator will need the following three files, as well as access to the remaining instructions in this topic:

- `CRT_MI_CONNECT_ROLE.SQL`
- `CRT_MI_USER.SQL`
- `MI_V4030070.DMP.ZIP`

a) Locate and run the script `CRT_MI_CONNECT_ROLE.SQL`.

This script creates the GE Digital APM role (MI_CONNECT_ROLE), which contains several of the Oracle privileges that are necessary to run the GE Digital APM applications. This script does not require any parameters. You will need to run this script one time per database.

b) Locate and run the script `CRT_MI_USER.SQL`.

This script creates the Oracle user, and then grants to the user the role MI_CONNECT_ROLE that you created in the preceding step.

The schema is created. For example, if you were to define the parameters through the command `SQL> @CRT_MI_USER MERIDIUM_PROD MERIDIUM_PROD 1000M Meridium_DATA`, it would automatically:

- Create a user named MERIDIUM_PROD.
- Set the password for the user to MERIDIUM_PROD.
- Set the default tablespace for the user to MERIDIUM_DATA.
- Grant 1GB of quota on the default tablespace.

Note: This example assumes that the MERIDIUM_DATA tablespace already exists.

4. Import the Oracle schema that you created in the preceding steps. To do so:

a) On the GE Digital APM Database Server machine, locate the file `MI_V4030070.DMP.ZIP`, and then extract and import the contents.

b) Update the schema statistics.

5. Log in to SQL*Plus (or equivalent) as the schema owner, and then run the following command: `SQL> EXEC MI_DDL.CRT_SIDX_SI_MI_GEOD_GD`
The spatial/geo index for the database is imported.

Next Steps

-

Create the Oracle Scheduler Database

Before you create the Oracle schema that will contain the GE Digital APM repository, you must install the Database Server software on the GE Digital APM Database Server machine.

Create an Oracle database that will be used by the GE Digital APM Scheduler. You may set the database name as `apm_scheduler`. The creation of the Oracle database exceeds the scope of this documentation. For details on creating an Oracle database, consult the documentation that is specific to your database platform.

When the database is created, the database character set must be specified. If you are creating a Unicode database, use the character set AL32UTF8. This is the most recent and recommended Unicode database character set.

What To Do Next

-

Create the Oracle Scheduler Schema

About This Task

The following instructions provide details on creating the Scheduler Oracle schema.

To perform these steps, you will need Oracle DBA privileges on the GE Digital APM Database Server machine. These instructions assume that:

- You are logged in to your GE Digital APM Database Server machine with DBA privileges and have a connection to Oracle.
- You are familiar with running SQL scripts and the associated terminology.

Procedure

1. On the GE Digital APM Server machine, in the GE Digital APM distribution package, navigate to the `Database` folder.
2. Open the file `MI_DB_MASTER_<version>.zip`, and then extract the contents of the file `<version>.zip` to a folder on the C: drive.
3. Open the file `<version>.zip`, and then open the subfolder `_Setup\NewInstall\Oracle`.

   This folder contains the extracted files that will need to be run by the database administrator (via the remaining steps). The database administrator will need the following two files, as well as access to the remaining instructions in this topic:

   - `CRT_MI_CONNECT_ROLE.SQL`
   - `CRT_MI_USER.SQL`
   - `SCHEDULER.SQL`

   a) Locate and run the script `CRT_MI_CONNECT_ROLE.SQL`.

   This script creates the GE Digital APM role (MI_CONNECT_ROLE), which contains several of the Oracle privileges that are necessary to run the GE Digital APM applications. This script does not require any parameters. You will need to run this script one time per database.

   b) Locate and run the script `CRT_MI_USER.SQL`.

   This script creates the Oracle user, and then grants to the user the role MI_CONNECT_ROLE that you created in the preceding step.

   The schema is created. For example, if you were to define the parameters through the command `SQL> @CRT_MI_USER SCHEDULER_PROD SCHEDULER_PROD 1000M SCHEDULER_DATA`, it would automatically:

   - Create a user named SCHEDULER_PROD.
   - Set the password for the user to SCHEDULER_PROD.
   - Set the default tablespace for the user to SCHEDULER_DATA.
   - Grant 1GB of quota on the default tablespace.

   Note: This example assumes that the SCHEDULER_DATA tablespace already exists.

   c) Connect as the user, created in the previous step. And then, locate and run the script `SCHEDULER.SQL`. This script will set up the schema and create the initial data for the scheduler.

4. On the GE Digital APM server, navigate to `C:\ProgramData\Meridium`.
5. Open the `appsettings.Global.json` file using a text editor.
6. Modify the following values:

a) `DatabaseProvider`: Set the scheduler service database provider as `Oracle`.

```
"scheduler": {
        // Scheduler service API URL
        "serviceUrl": "http://localhost/meridium/scheduler/",
        // Scheduler service database provider. Valid values are
PostgreSQL, SqlServer, Oracle
        "databaseProvider": "Oracle"
    },
```

b) `connectionStrings`: To connect to the Oracle database, enter the connection string. For more details on the `connectionString` format, refer to the Oracle documentation. The following lines of code show a sample `connectingString` for the Oracle database.

```
"connectionStrings": {
        // Scheduler service connection string for the above
configured DatabaseProvider
        "SchedulerDatabase": "Data
Source=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST={0})(PORT={1}))
(CONNECT_DATA=(SERVICE_NAME={0})));User Id={0};Password={0};",
```

Next Steps

- Create an Initial Data Source

Create the Localization Oracle Database

Before you create the Oracle schema that will contain the GE Digital APM repository, you must install the Database Server software on the GE Digital APM Database Server machine.

Create an Oracle database that will be used by the GE Digital APM Localization. You may set the database name as `apm_localization`. The creation of the Oracle database exceeds the scope of this documentation. For details on creating an Oracle database, consult the documentation that is specific to your database platform.

When the database is created, the database character set must be specified. If you are creating a Unicode database, use the character set AL32UTF8. This is the most recent and recommended Unicode database character set.

What To Do Next

-

Create the Localization Oracle Schema

About This Task

The following instructions provide details on creating the Localization Oracle schema.

To perform these steps, you will need Oracle DBA privileges on the GE Digital APM Database Server machine. These instructions assume that:

- You are logged in to your GE Digital APM Database Server machine with DBA privileges and have a connection to Oracle.
- You are familiar with running SQL scripts and the associated terminology.

Procedure

1. On the GE Digital APM Server machine, in the GE Digital APM distribution package, navigate to the `Database` folder.
2. Open the file `MI_DB_MASTER_<version>.zip`, and then extract the contents of the file `<version>.zip` to a folder on the C: drive.
3. Open the file `<version>.zip`, and then open the subfolder `_Setup\NewInstall\Oracle`.

   This folder contains the extracted files that will need to be run by the database administrator (via the remaining steps). The database administrator will need the following two files, as well as access to the remaining instructions in this topic:

   - `CRT_MI_CONNECT_ROLE.SQL`
   - `CRT_MI_USER.SQL`

   a) Locate and run the script `CRT_MI_CONNECT_ROLE.SQL`.

   This script creates the GE Digital APM role (MI_CONNECT_ROLE), which contains several of the Oracle privileges that are necessary to run the GE Digital APM applications. This script does not require any parameters. You will need to run this script one time per database.

   b) Locate and run the script `CRT_MI_USER.SQL`.

   This script creates the Oracle user, and then grants to the user the role MI_CONNECT_ROLE that you created in the preceding step.

   The schema is created. For example, if you were to define the parameters through the command `SQL> @CRT_MI_USER LOCALIZER_PROD LOCALIZER_PROD 1000M LOCALIZER_DATA`, it would automatically:

   - Create a user named LOCALIZER_PROD.
   - Set the password for the user to LOCALIZER_PROD.
   - Set the default tablespace for the user to LOCALIZER_DATA.
   - Grant 1GB of quota on the default tablespace.

   Note: This example assumes that the LOCALIZER_DATA tablespace already exists.
4. Import the Oracle schema that you created in the preceding steps. To do so:

   a) On the GE Digital APM Server machine, in the GE Digital APM distribution package, navigate to the `C:\Meridium\DbUpg\DBBackupFiles\Oracle` folder.

   b) Locate the dump files `EXPDP_LOCALIZER_PROD`*NUMBER*`.DMP`, and then extract and import the contents.

   c) Update the schema statistics.
5. On the GE Digital APM server, navigate to `C:\ProgramData\Meridium`.
6. Open the `appsettings.Global.json` file using a text editor.
7. Modify the following values:

   a) DatabaseProvider: Set the Localization database provider as `Oracle`.

   ```
   "LocalizerDatabase": {
           // Localizer service database provider. Valid values are
   PostgreSQL, SqlServer, Oracle
           "databaseProvider": "Oracle"}
   ```

   b) `connectionStrings`: To connect to the Oracle database, enter the connection string. For more details on the `connectionString` format, refer to the Oracle documentation. The following lines of code show a sample `connectingString` for the Oracle database.

   ```
   "connectionStrings: {
               // Localizer service connection string for the above
   ```

```
configured DatabaseProvider
          "LocalizerDatabase": "Data
Source=(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST={0})(PORT={1}))
(CONNECT_DATA=(SERVICE_NAME={0})));User Id={0};Password={0};"}
```

Next Steps

- Create an Initial Data Source

SQL Server Checklist

The following checklist should be used to install and configure a SQL Server Database Server, create the GE Digital APM database, and configure the GE Digital APM Server for use with the SQL Server.

You should complete these steps in relatively the same order in which they are listed in the table.

Step	Task	Notes
1	Ensure that the GE Digital APM Database Server machine meets the system requirements.	This step is required.
2	On the GE Digital APM Database Server, install the SQL Server software.	This step is required.
3	On the GE Digital APM Database Server, create the SQL Server database.	This step is required.
4	On the GE Digital APM Database Server, configure the SQL Server database.	This step is required.
5	On the GE Digital APM Database server machine, Create the SQL Server Scheduler Database on page 33.	This step is required.
6	On the GE Digital APM Database server machine, Configure the SQL Server Database on page 32.	This step is required.
7	On the GE Digital APM Database server machine, Create the SQL Server Localization Database on page 34.	This step is required.
8	On the GE Digital APM Database server machine, Configure the SQL Server Localization Database on page 34.	This step is required.
9	On the GE Digital APM Server, create an initial data source.	This step is required.
10	In GE Digital APM, build the search index.	This step is required.

Install the SQL Server Software

About This Task

If you will connect to a SQL Server database, the first step is to install the SQL Server software on the Database Server machine. This documentation assumes that your system meets Database Server system requirements. The installation of the SQL Server software exceeds the scope of this documentation. For information on performing the installation, refer to the SQL Server documentation that is specific to your database server platform.

When you prepare to install SQL Server on the Database Server, you should consider the following notes:

Procedure

1. GE Digital APM requires mixed-mode authentication for SQL Server installations. The documentation and scripts supplied by GE Digital assume that the SQL Server instance allows mixed-mode authentication.
2. The GE Digital APM database must be owned by the SQL Server login referenced in the GE Digital APM data source. Being a member of the SQL Server db_owner role is not sufficient. GE Digital provides a script to properly configure the SQL Server database for use with GE Digital APM.
3. The database supplied by GE Digital (via a .bak file) was created with the SQL Server collation Latin1_General_CI_AS.

Next Steps

- About Creating and Configuring the SQL Server Database on page 31

About Creating and Configuring the SQL Server Database

After you have installed the SQL Server software on the Database Server machine, you can create the GE Digital APM database by restoring a database backup file that is provided by GE Digital. For example, the restore database option in SQL Server Management Studio could be used to create the database. Specific instructions for creating the GE Digital APM database are not included in this documentation.

After you have created the database, you will need to configure it. To create and configure the GE Digital APM database, you must have access to:

- Microsoft SQL Server Management Studio.
- A privileged SQL Server account with sysadmin rights in the target instance.
- Two files from the GE Digital APM distribution package that will be extracted on the GE Digital APM Server:

  ◦ `GE Digital APM`, which is included in the file **GE Digital APM** in the GE Digital APM distribution package.
  -and-
  ◦ `MI_SQL_DB_Configure.sql`, which was extracted from the GE Digital APM distribution package.

These instructions assume that you are familiar with SQL Server Management Studio or another third-party tool for running SQL scripts.

Note: If you do not have sufficient privileges to restore or configure the database, ask the person responsible for creating the database to create the database and complete the configuration steps. That person will need a copy of these instructions, the BAK file, and the `MI_SQL_DB_Configure.sql` script.

What To Do Next

- Create the SQL Server Database on page 31

Create the SQL Server Database

The following instructions provide details on locating the files that are needed for creating and configuring the SQL Server database. To create the database, you will restore a backup file that is included in your GE Digital APM distribution package. For example, the restore database option in SQL Server Management Studio could be used to create the database. Specific instructions on creating the SQL Server database are not included in this documentation.

Steps

1. On the GE Digital APM Server, access the GE Digital APM distribution package, and then navigate to the `Database` folder.
2. Open the `MI_DB_MASTER_<version>.zip` file, and then extract the contents of the file to a folder on the C: drive.

   Important: The name of the folder to which you extract the files must not contain any spaces.
3. Open `_Setup\NewInstall\SQLServer`, and then locate the `MI_<version>.BAK` file.
4. Place the `MI_<version>.BAK` file in a location where it can be referenced by the SQL Server service, and then restore the file.
   The GE Digital APM database is created.

What To Do Next

- Configure the SQL Server Database

Configure the SQL Server Database

About This Task

The following instructions explain how to configure a SQL Server database for use by GE Digital APM. These instructions assume that the SQL Server database has already been created by restoring a backup file using SQL Server Management Studio or another third-party tool.

These instructions provide details on configuring the GE Digital APM SQL Server database using the script `MI_SQL_DB_Configure.sql`, which is included in your GE Digital APM distribution package. This script ensures that the database will be properly configured for use with GE Digital APM.

When you run the script `MI_SQL_DB_Configure.sql`, the following database settings will be configured automatically:

- The database will be set to read/write mode.
- The database will be configured to allow multiple users.
- The database will be set to Full recovery mode.
- A SQL Server login will be created, and this login will own the database.
- The SQL Server database name, SQL Server login name, and password will all match.

Procedure

1. Open a SQL Server Management Studio query window that is connected via a privileged login.
2. Open the file `MI_SQL_DB_Configure.sql`, and then copy its contents into the SQL Server Management Studio query window.
3. Set the @dbname variable to the name of the GE Digital APM SQL Server database that you created.
4. Execute the edited script.
5. As needed, use SQL Server Management Studio to modify the password. These are the same login credentials that will be used when you create the GE Digital APM data source that will connect to this database.
6. Create the custom server-level error messages, which are required by the GE Digital APM system. These error messages must be created at the instance level. Creating them requires a privileged login assigned to either the System Administrator (sysadmin) or Server Administrator (serveradmin) fixed server roles. To create the GE Digital APM error messages:

   a) Make sure that you are connected to the Database Server with SQL Server Management Studio as a System Administrator or Server Administrator user

b) Execute the stored procedure MI_ERRORS_CRT_ALL_MSGS. This procedure was supplied with the GE Digital APM database and can be executed by using the command `exec <databasename>..MI_ERRORS_CRT_ALL_MSGS`, where `<databasename>` is the name of the database you created in the preceding steps.

Next Steps

- Create an Initial Data Source on page 35

Create the SQL Server Scheduler Database

Create SQL Server database that will be used by the GE Digital APM Scheduler. You may set the database name as `apm_scheduler`. The creation of the SQL Server database exceeds the scope of this documentation. For details on creating an SQL Server database, consult the documentation that is specific to your database platform.

What To Do Next

- Configure the SQL Server Database

Configure the SQL Server Scheduler Database

About This Task

The following instructions explain how to configure a SQL Server database for use by GE Digital APM Scheduler. These instructions assume that the SQL Server database has already been created by restoring a backup file using SQL Server Management Studio or another third-party tool.

Procedure

1. Create an empty database with username. You may set the database name as `apm_scheduler`.
2. Run MI_SQL_DB_Configure.sql to configure the database (password).
3. Open a SQL Server Management Studio query window that is connected via a privileged login.
4. Open the GE Digital APM distribution package and navigate to the `Database` folder.
5. Open the file `MI_DB_MASTER_<version>.zip`, and then extract the contents of the file `<version>.zip` to a folder on the C: drive.
6. Open the file `<version>.zip`, and then open the subfolder `_Setup\NewInstall\SQLServer`.
7. Execute the `Scheduler.sql` script. This script will create the required objects for APM Scheduler.
8. On the GE Digital APM server, navigate to `C:\ProgramData\Meridium`.
9. Open the `appsettings.Global.json` file using a text editor.
10. Modify the following values:

    a) DatabaseProvider: Set the scheduler service database provider as `SqlServer`.

    ```
    "scheduler": {
            // Scheduler service API URL
            "serviceUrl": "http://localhost/meridium/scheduler/",
            // Scheduler service database provider. Valid values are
    PostgreSQL, SqlServer, Oracle
            "databaseProvider": "SqlServer"
        },
    ```

b) `connectionStrings`: To connect to the SQL Server database, enter the connection string. For more details on the `connectionString` format, refer to the SQL Server documentation. The following lines of code show a sample `connectingString` for the SQL Server database.

```
"connectionStrings": {
        // Scheduler service connection string for the above
configured DatabaseProvider
        "schedulerDatabase":
"DATABASE={2};SERVER={3};UID={0};PASSWORD={1};MultipleActiveResultS
ets=true;Max Pool Size=1000;Encrypt=false;",
```

Create the SQL Server Localization Database

Create SQL Server database that will be used by the GE Digital APM Scheduler. Name the database as apm_localization. The creation of the SQL Server database exceeds the scope of this documentation. For details on creating an SQL Server database, consult the documentation that is specific to your database platform.

What To Do Next

- Configure the SQL Server Database

Configure the SQL Server Localization Database

About This Task

The following instructions explain how to configure a SQL Server database for use by GE Digital APM Localization. These instructions assume that the SQL Server database has already been created by restoring a backup file using SQL Server Management Studio or another third-party tool.

Procedure

1. Open a SQL Server Management Studio query window that is connected via a privileged login.
2. Open the GE Digital APM distribution package and navigate to the `C:\Meridium\DbUpg \DBBackupFiles` folder.
3. Open the subfolder `\SQL`.
4. Restore database using the backup file `apm_localization.bak`. This database includes the required objects for GE Digital APM localization.
5. Run `MI_SQL_DB_Configure.sql` to configure the database (password).
6. On the GE Digital APM server, navigate to `C:\ProgramData\Meridium`.
7. Open the `appsettings.Global.json` file using a text editor.
8. Modify the following values:

   a) DatabaseProvider: Set the Localization database provider as `SqlServer`.

   ```
   "localizer": {
           // Localizer service database provider. Valid values are
   PostgreSQL, SqlServer, Oracle
           "databaseProvider": "SqlServer"}
   ```

   b) `connectionStrings`: To connect to the SQL Server database, enter the connection string. For more details on the `connectionString` format, refer to the SQL Server documentation. The following lines of code show a sample `connectingString` for the SQL Server database.

   ```
   "connectionStrings": {
               // Localizer service connection string for the above
   ```

```
configured DatabaseProvider
          "LocalizerDatabase":
"DATABASE={2};SERVER={3};UID={0};PASSWORD={1};MultipleActiveResultS
ets=true;Max Pool Size=1000;",}
```

Initial Data Source Creation

Create an Initial Data Source

Before You Begin

Note: This procedure cannot be completed until you set up the GE Digital APM Database Server. If you have not yet done so, return to the GE Digital APM deployment workflow.

Procedure

1. Access the GE Digital APM log in page.

   Tip: You can access the GE Digital APM log in page via the Apps interface on the GE Digital APM Server. To access the log in page, select the Windows start button, and then select the arrow icon in the lower-left corner of the screen. Then, under **Meridium APM Applications**, select **APM**.

2. Select **Add Datasource**.

   The **Create Datasource** window appears.

Create Datasource

Data Source ID

Database Server

Data Source Description

Database Name

Database Type
▼

Alias

Database User Name

Host

Password

Port

Service

Save   Cancel

3. In the **Data Source ID** box, enter a name for the Data Source. This is required and must be unique for the GE Digital APM Server. It cannot contain spaces or special characters aside from underscores.

   Important: You cannot modify the ID after you save the Data Source.

4. In the **Data Source Description** box, enter a description of the Data Source.

   Note: The description of the Data Source will be displayed on the GE Digital APM **Welcome** page, in the list of available Data Sources.

5. In the **Database Type** list, select either **Oracle** or **SQL Server**. Note that Postgres option also appears in the list, however it is not supported in the current version.

   If you selected **Oracle**, the following boxes are enabled:

   • **Database Alias**
   • **Oracle Host**
   • **Oracle Port**
   • **Oracle Service**

   If you selected **SQL Server**, the following boxes are enabled:

   • **Database Server**
   • **Database Name**

6. If you selected **Oracle** in step 5 on page 37, then either enter a value in the **Database Alias** box, or enter values in the **Oracle Host**, **Oracle Port**, and **Oracle Service** boxes. Note that a database alias, contained within a `tnsnames.ora` file, contains the Oracle host, port, and service information related to the database, and may have been set up by a database administrator to simplify access. To determine whether a database alias has been created, and to determine the appropriate values for the

Database Alias box or **Oracle Host**, **Oracle Port**, and **Oracle Service** boxes, contact your database administrator.

Note:

If you selected **Oracle** in step 5 on page 37, then you do not need to enter values in the **Database Server** and **Database Name** boxes.

7. If you selected **SQL Server** in step 5 on page 37, then enter values in the **Database Server** and **Database Name** boxes. Note that, if you selected SQL Server in step 5 on page 37, you do not need to enter values in the **Database Alias**, **Oracle Host**, **Oracle Port**, and **Oracle Service** boxes.

8. In the **Database User Name** box, enter the user name or schema name for the database that you are defining.

9. In the **Password** box, enter the password for the associated database user name. The password must meet the criteria specified by the password policy.

10. Select **Save**.
The GE Digital APM log in page appears, displaying the data source.

Note: When initially logging in to GE Digital APM, both the user name and password are MIADMIN. These values are case-sensitive.

Note: When logging in to GE Digital APM, a notification may appear, asking if you want to allow your machine to be used for additional local storage. This local storage is used to store log in information and preferences. Allowing this local storage is optional.

Note: If you receive the error message `Datasource Not Found`, review the log files `Meridium_WebApi_timestamp.txt` available at `\ProgramData\Meridium\Logs` for more details.

Next Steps

- Deploy the SQL Server Report Server for the First Time

SQL Server Report Server Installation

Deploy the SQL Server Report Server for the First Time

Microsoft SQL Server Reporting Services is a third-party component that the GE Digital APM system uses to support its reporting functionality. After SQL Server Reporting Services has been installed, you will need to configure the Report Server and set it up to be used with GE Digital APM. Some of the configuration tasks that you must perform are standard SQL Server Reporting Services procedures that must be performed for any new installation of SQL Server Reporting Services. This documentation does not provide details on configuring standard aspects of the Report Server.

For information on setting up the Report Server, see the SQL Server Setup Help, which you can access on the Report Server via the Reporting Services Configuration Manager, which should have been installed when you installed SQL Server Reporting Services.

After the Report Server has been set up, you will need to complete various additional tasks to ensure the proper functioning of the Report Server with GE Digital APM. These tasks may be completed by multiple people in your organization. We recommend, however, that the tasks be completed in the order in which they are listed.

Step	Task	Notes
1	Ensure that the SQL Server Report Server machine meets the system requirements.	This step is required.
2	Configure the SQL Server to use an execution account.	This step is required.
3	Create a domain user and add that user to Content Manager Role on the Home Folder of the SQL Server Report Server.	This step is required.
4	Install and configure GE Digital APM SSRS.	This step is required.
5	Configure GE Digital APM to use the SQL Server Report Server.	This step is required.

Configure SQL Server Report Server

Configure the SQL Server Report Server to Use an Execution Account

About This Task

Tip: For more information on Execution Accounts, consult Microsoft's Configure the Unattended Execution Account (SSRS Configuration Manager) documentation.

Procedure

1. On the machine that will serve as the SQL Server Report Server, access the Reporting Services Configuration Manager.

   The **Reporting Services Configuration Manager** window appears.
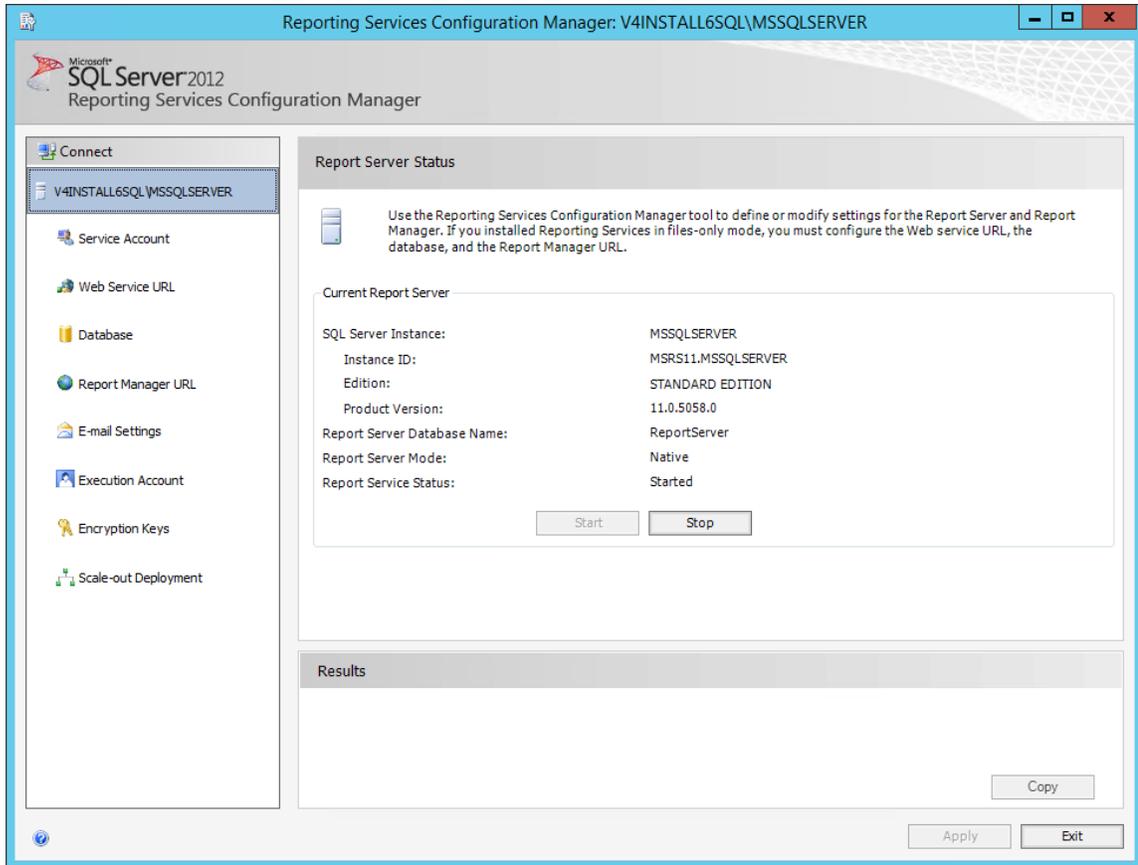
2. In the left pane, for the account that will be set as an execution account, select the **Execution Account** tab.

   The **Execution Account** section appears.
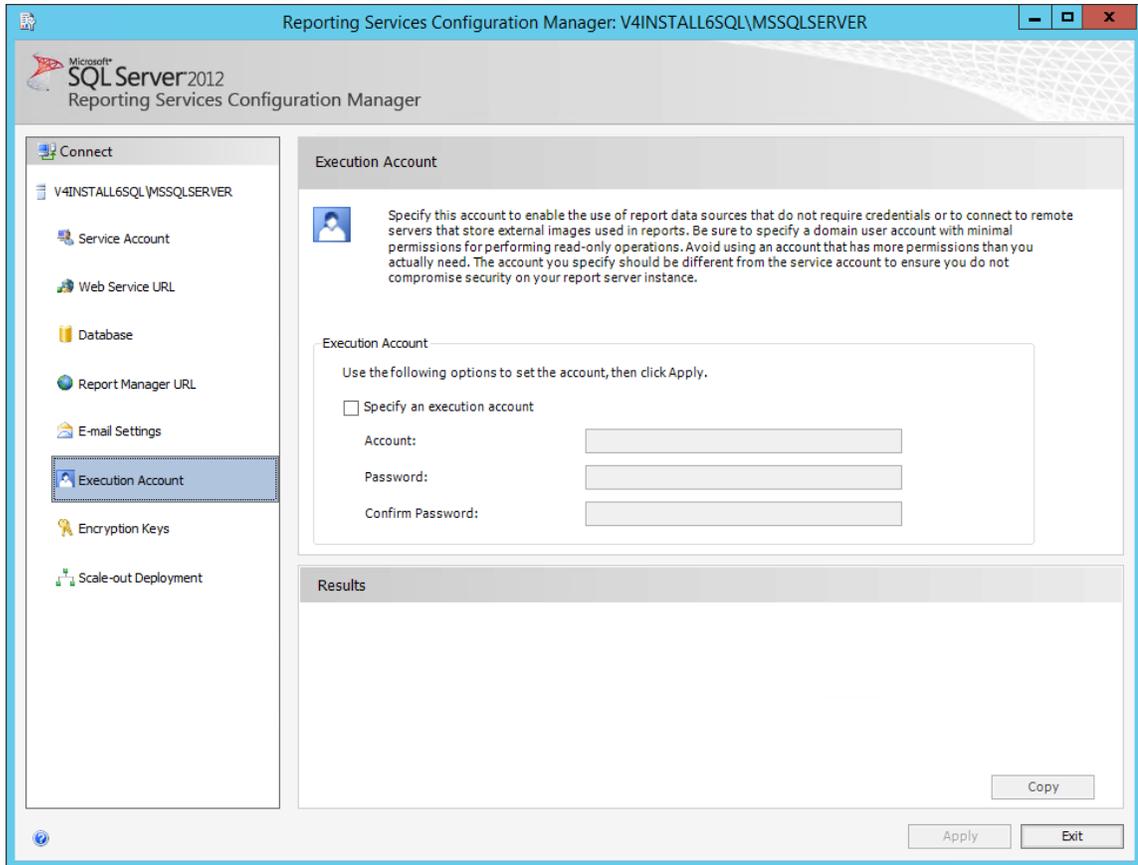
3. In the **Execution Account** section, select the **Specify as an execution account** check box, then enter values in the required fields, and then select **Apply**.

   The account is specified as an execution account.

Next Steps

Create a Domain User

About This Task

In this procedure, you will create a domain user and add that user to the Content Manager Role on the Home folder of the SQL Server Report Server.

Procedure

1. Create a Windows/domain user with minimum privileges (e.g., meridium_reports_user). The user name requires minimum privileges to connect to the GE Digital APM Server to get data for reports. It is recommended that:

   - The password for this user should never expire.
   - The user should be restricted to change password.
   - The user should be restricted to log in to other servers (e.g., meridium_reports_user).
   - The user should also be part of IIS_IUSRS group on the SQL Server Report Server machine.

2. Open Reporting Services Configuration Manager.

3. Select the **Report Manager URL** tab.
   The **Report Manager URL** section appears.
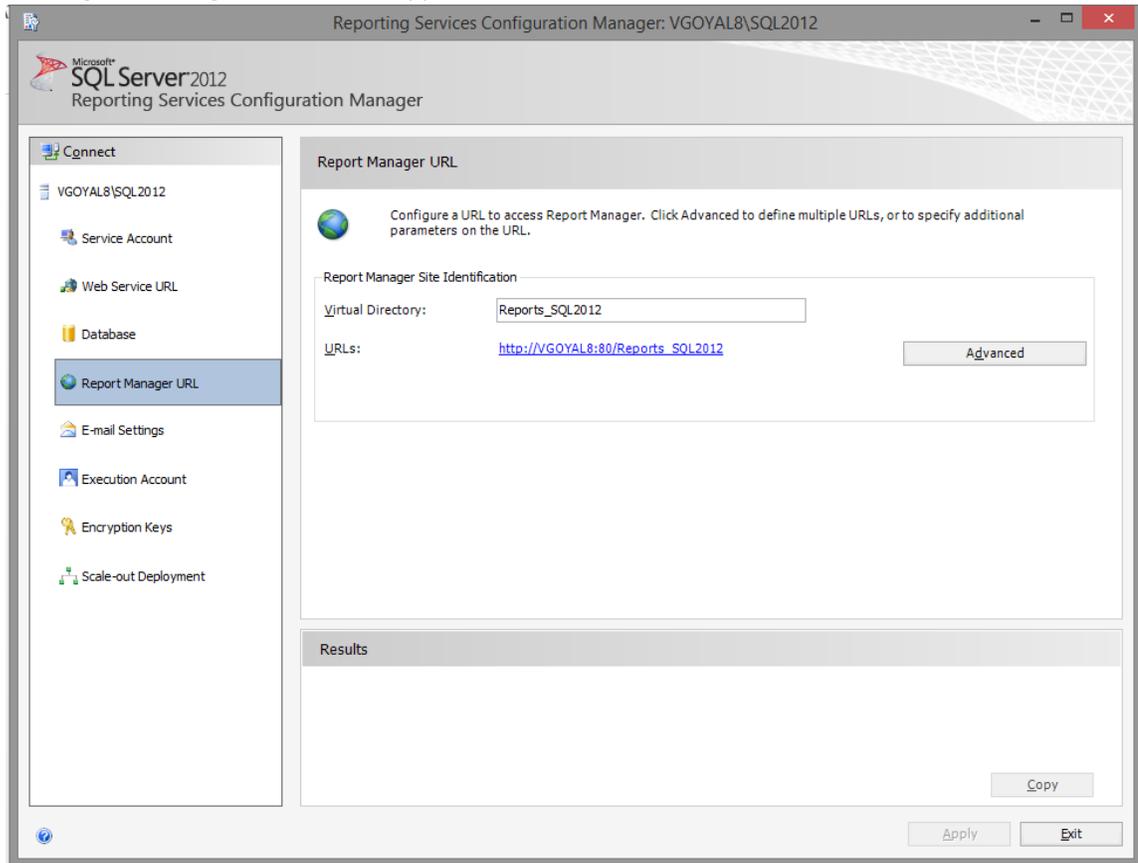
4. In the **Report Manager Site Identification** section, select the URL to open Report Manager.
   Report Manager opens in the default browser, displaying the Home folder.
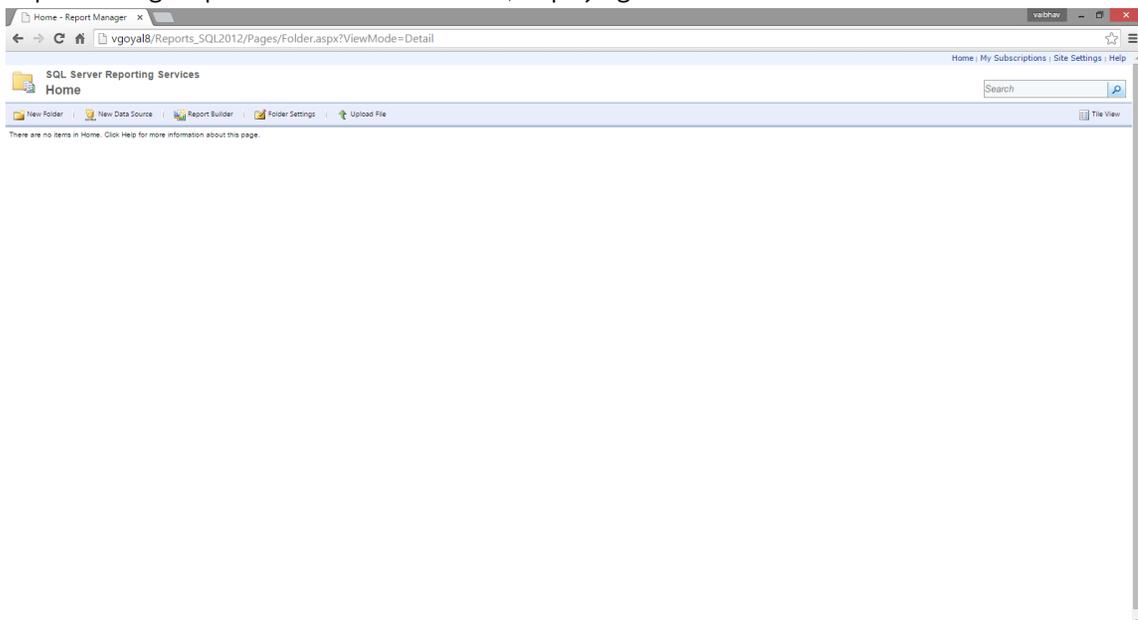
5. Select **Folder Settings**.
   A **Security** section appears.
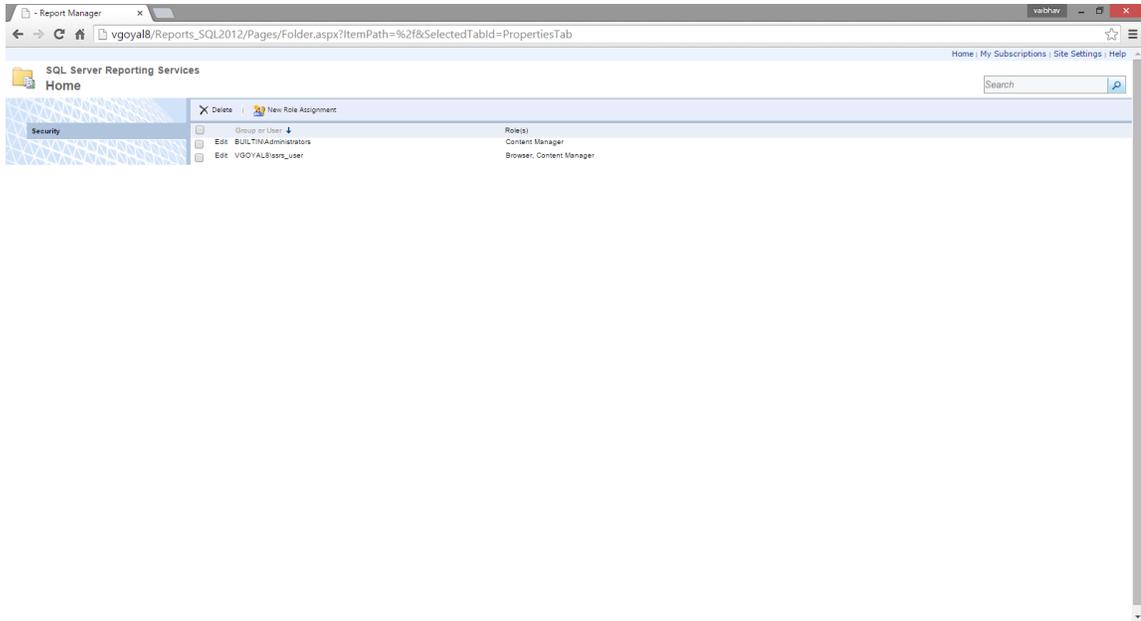
6. Select **New Role Assignment**.

   The New Role Assignment form is displayed.

7. Enter the user name of the user that you created in step 1, and then select **Content Manager**.

   The form will appear similar to the following image.
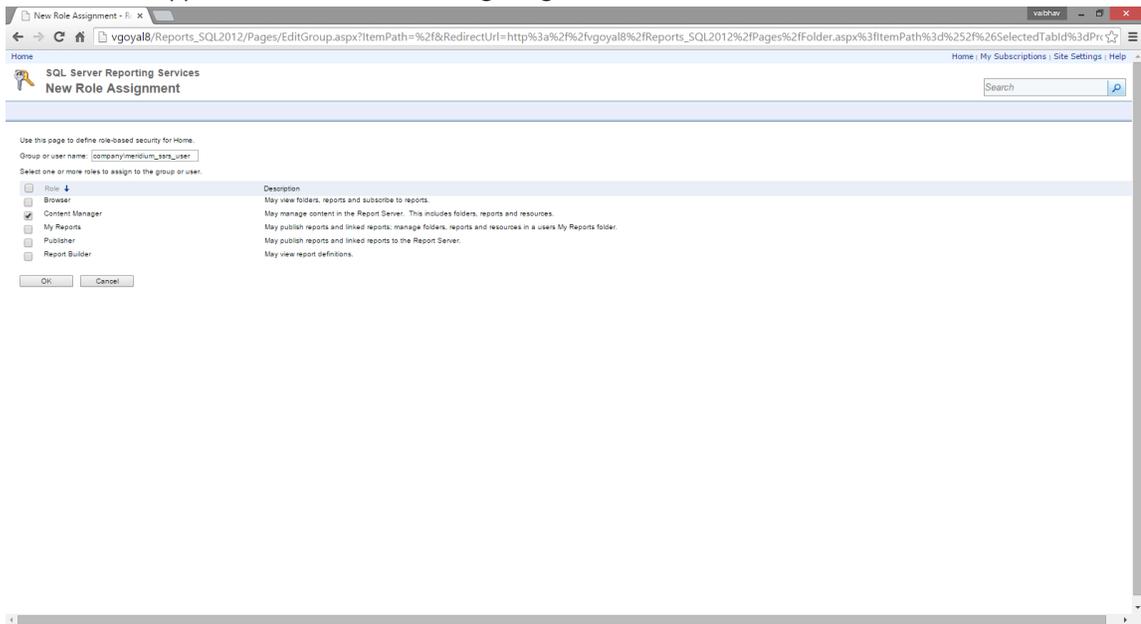
8. Select **OK**.

   The user is added to Content Manager role.

Next Steps

- Install and Configure GE Digital APM SSRS

Install and Configure GE Digital APM SSRS

About This Task

These instructions assume that the SQL Server Report Server meets the system requirements.

Procedure

1. On the machine that will serve as the SQL Server Report Server, in the GE Digital APM distribution package, navigate to the folder `Setup\SSRS`.
2. Open the file `Setup.exe`.

   A message appears, asking if you want to allow the installer to make changes to your machine.
3. Select **Yes**.
   The Meridium SSRS installer appears, displaying the welcome screen.
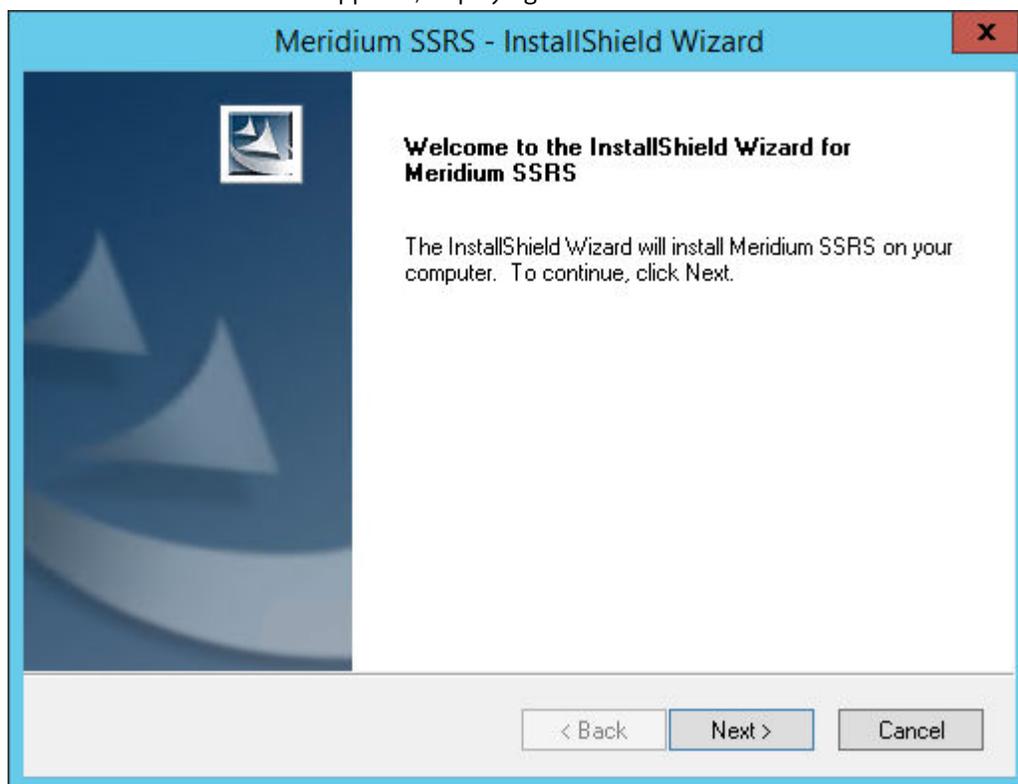
4. Select **Next**.
   The **License Agreement** screen appears.
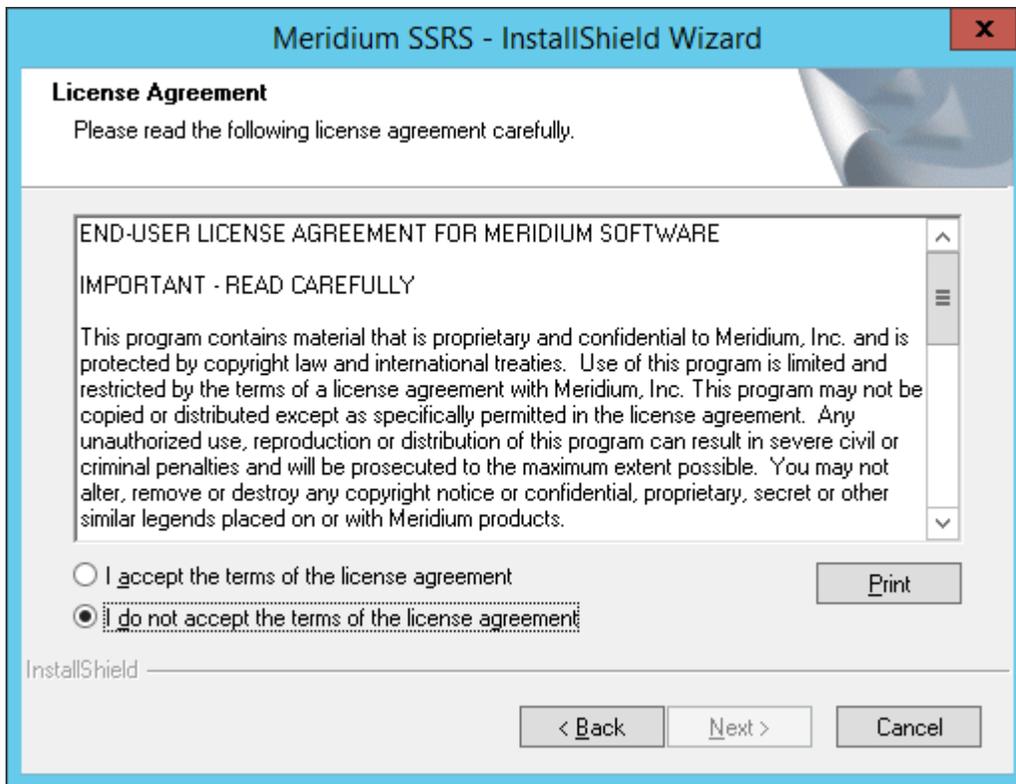
5. Read the License Agreement, and then, if you agree to the terms, select the **I accept the terms of the license agreement** check box. Then, select **Next**.
The **Select Installation Location** screen appears, prompting you to select the location where the software will be installed. By default, the software will be installed in the following folder:
`C:\Program Files\Meridium`.
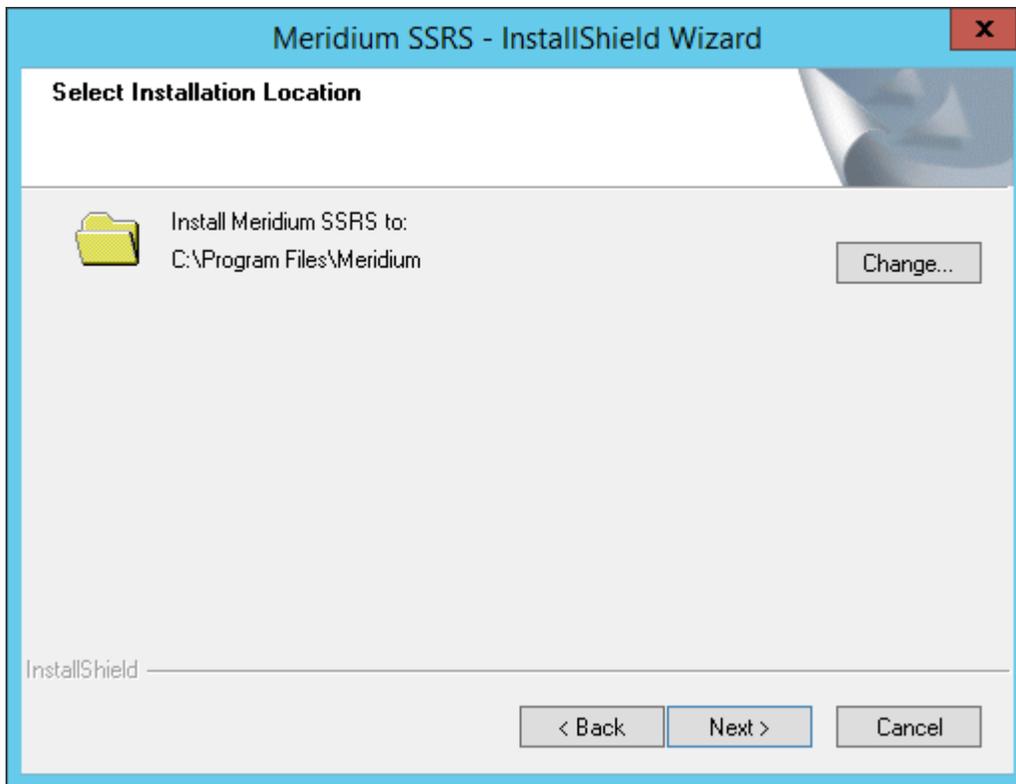
6. Do one of the following actions.

   - To install in the default location, select **Next**.
   - To change the location to install the software, select **Change**, and then navigate to the location where you want to install the software. The folder path that you select will be displayed in place of the default folder path. When you are satisfied with the installation location, select **Next**.
     The **SQL Server Reporting Server Instances** screen appears.
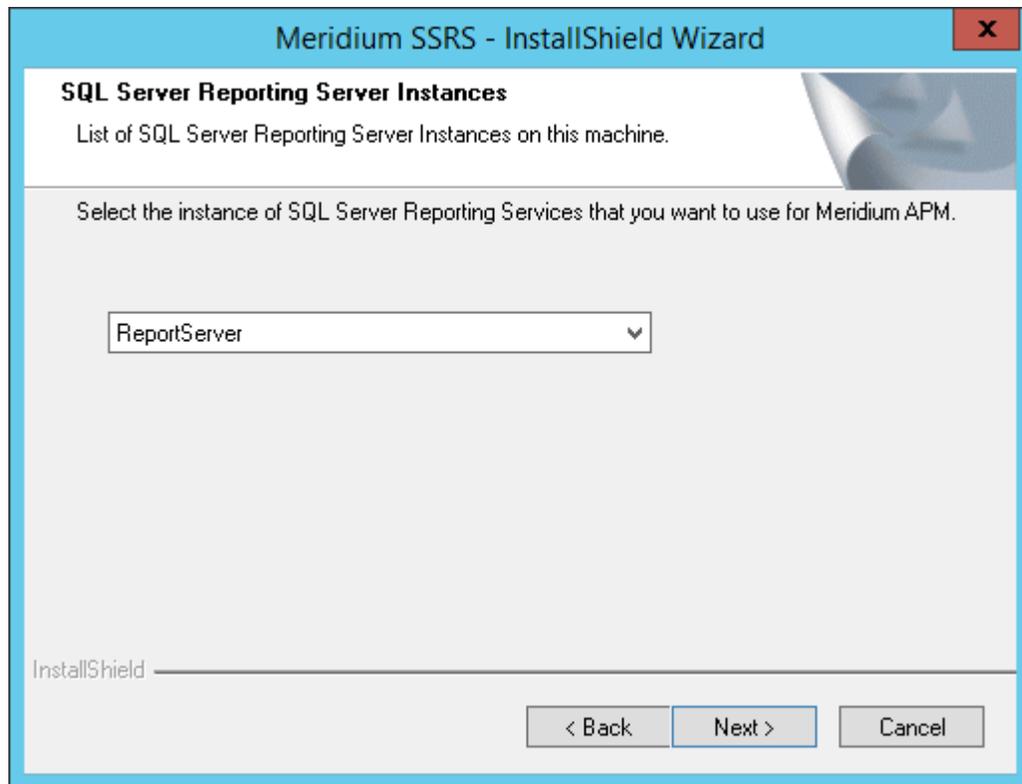
7. Select the instance of SQL Server Reporting Services that you want to use, and then select **Next**. The **Complete the Installation** screen appears.

8. Select **Install**.
   The **Setup Status** screen appears, which displays a progress bar that shows the progress of the GE Digital APM Server 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.
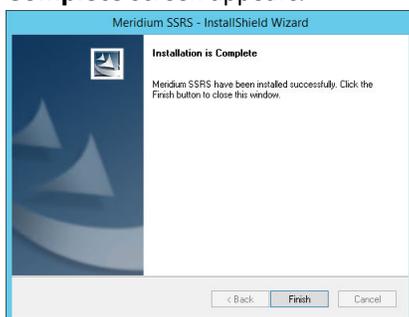
9. Select **Finish**.
   The **Meridium SSRS - InstallShield Wizard** window is closed.

10. Navigate to the folder `C:\Program Files\Microsoft SQL Server\` `{ReportServicesInstance}\Reporting Services\ReportServer`.

11. Open the `rsreportserver.config` file using a text editor (for example, Notepad).

12. Locate the following code in the configuration file, and then replace *{meridium.applicationserver}* with the name of the GE Digital APM server: `<ServerUrl>http://` `{meridium.applicationserver}/meridium/api/</ServerUrl>`

13. Save the configuration file.
    The GE Digital APM SSRS is installed and configured.

Next Steps

-

Reporting Server Configuration

Configure GE Digital APM to Use SQL Server Report Server

To configure GE Digital APM to use the SQL Server Report server, complete the steps provided in the following topic:

- Configure GE Digital APM to Use Reporting Server

What To Do Next

-

Security User Creation

Create Security User Records

Create security user records for the individuals who will need to log in to GE Digital APM applications. To create a security user, follow the steps provided in the following topics:

- Create a Security User

What To Do Next

-

License Activation

Activate Licensed Modules and Products

License activation determines which modules and products will be available in GE Digital APM. You require license activation for all the modules (i.e., they cannot be used until the associated license is activated).

You can activate licenses via one of the following methods:

- Activate a License via GE Digital APM
- Activate a License via Command Prompt

What To Do Next

-

Server Configuration for Scheduled Jobs

Configure the GE Digital APM Server for Running the Scheduled Jobs

You must configure the GE Digital APM server for all the scheduled jobs if you have deployed the GE Digital APM in a clustered environment and you want to dedicate a machine to run all the scheduled jobs.

Procedure

1. On the GE Digital APM Server machines that you want to put in standby mode, navigate to the folder `C:\Program Files\Meridium\ApplicationServer\scheduler`.
2. Access the file `appsettings.json`.
3. When the GE Digital APM is deployed on multiple servers, you can enable the background jobs in selected servers by setting this flag. See the following example of the modified line of code:

```
"scheduler": {
"turnOff": true,
```

   Note: By default, the value of the key **turnOff** is set to `false`. In your cluster environment, the value of the key **turnOff** should be set to `false` in at least one server.
4. Save the file.

   The GE Digital APM server is configured for all the scheduled jobs.

Next Steps

Mobile Application

Install the GE Digital APM Mobile Application

This steps is required only if you want to install the GE Digital APM mobile application on mobile devices.

Install the GE Digital APM mobile application on your mobile device based on one of the following operating systems:

- Android
- iOS
- Windows

What To Do Next

Single Sign On

Enable Single Sign-on

Enable single sign-on for on-site or off-site authentication. This step is required only if you are enabling single sign-on.

To enable single sign-on for on-site or off-site authentication, complete steps provided in the following topic:

- About Enabling GE Digital APM SSO

What To Do Next

-

IIS Configuration

Configure IIS

About This Task

This topic describes how to set up the HTTP redirect for the default website.

Procedure

1. On the GE Digital APM Server, via the **Server Manager**, access the **IIS Manager**.
2. In the **Connections** pane, expand the server name, expand **Sites**, and then select **Default Web Site**.
3. In the **Default Web Site Home** pane, double-click **HTTP Redirect**.
4. In the **HTTP Redirect** pane, select the **Redirect requests to this destination** check box, and then enter the redirect destination as `/Meridium`.
5. In the Redirect Behavior section, select the **Only redirect request to content in this directory (not subdirectories)** check box.
6. In the **Tasks** pane, select **Apply**.

Next Steps

-

Module Deployment

Deploy Modules for the First Time

After you have installed GE Digital APM for the first time, you must deploy your licensed modules. To do so, complete the module-specific steps provided in the following documentation:

-

Install Advanced Visualization

Install Advanced Visualization

The Advanced Visualization module enables you to create customized dashboards and portals that display APM information in the form of charts or reports.

To install Advanced Visualization, complete steps provided in the following topic:

- Deploy Advanced Visualization for the First Time

Chapter

2

Module Deployment

Topics:

Overview

About GE Digital APM Module Deployment

The APM Module Deployment document provides information on how to configure various GE Digital APM modules for the first time. These instructions assume that you have completed the steps for deploying the basic GE Digital APM system architecture. For more information, refer to the module-specific information using the left navigation.

Action Management Deployment

Deploy Recommended Actions for the First Time

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

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

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

Recommended Actions Security Groups

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

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

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

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

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

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

APM Connect Deployment

Deploy APM Connect and Adapters

For information on how to deploy, refer to the corresponding module documentation:
- APM Connect
- Maximo Adapters

- OT Connect
- SAP Adapters
-

Asset Criticality Analysis Deployment

Deploy 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 system architecture.

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

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

ACA Security Groups

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

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

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

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

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

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

Asset Health Manager Deployment

Deploy 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 system architecture.

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

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

About the Asset Health Services

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

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

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

Services Summary

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

- **Asset Health Indicator Service:** Automatically updates the following field values in a Health Indicator record when reading values related to the health indicator source record (for example, a Content Map or Measurement Location record) change:

  ◦ Alert Level
  ◦ Last Reading Date
  ◦ Last Char Reading Value (for records that accept character values)
  ◦ Last Numeric Reading Value (for records that accept numeric values)

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

- **Policy Trigger Service**: When an input to a policy (i.e., an associated record in the 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.

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

- **OT Connect:** Monitors the subscribed tags (tags that are used in policies and health indicators or tags for which readings are being stored in the 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.

> **Standard System Architecture Configuration**
>
> The following diagram illustrates the machines in the GE Digital APM system architecture when the Policy Designer, OT Connect, and Asset Health Manager (AHM) modules are used together. This image depicts the standard configuration, where the OPC Server software and OT Connect software are on the same machine.
>
> **Note:** In this example configuration, only one machine of each type is illustrated. Your specific architecture may include multiple GE Digital APM Servers, multiple OPC Servers, or multiple GE Digital APM Servers used for policy executions.
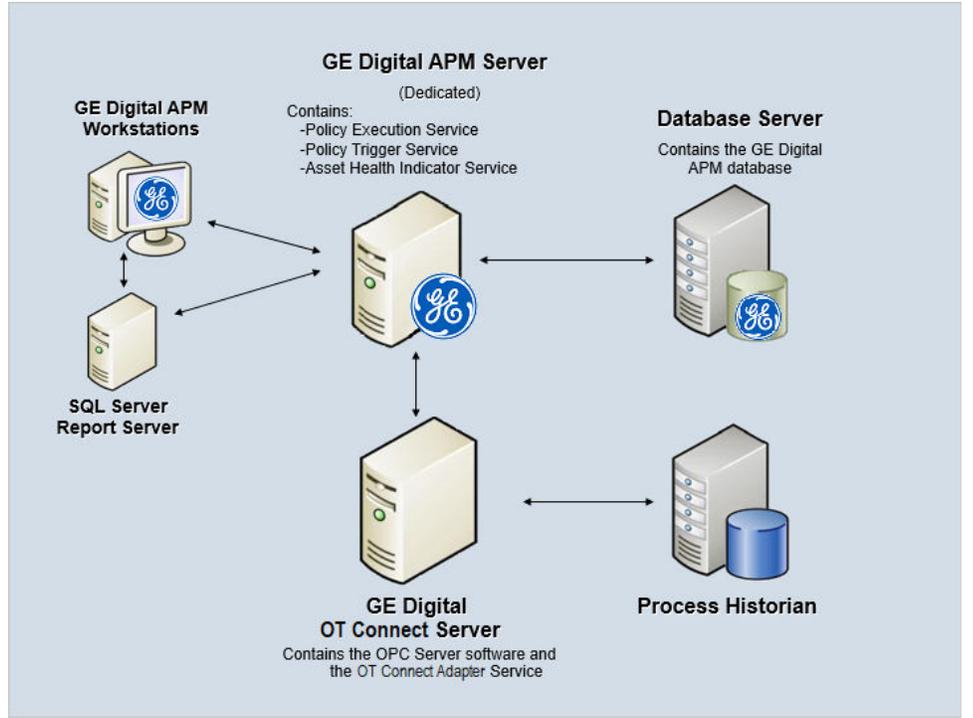
The following table summarizes the machines illustrated in this diagram and the software and services that you will install when you complete the first-time deployment steps for Asset Health Manager, OT Connect, and Policy Designer.

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

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

AHM Security Groups

The following table lists the baseline Security Groups available for users within this module, the baseline Roles to which those Security Groups are assigned, and the OT Connect groups that are assigned to the Health Roles to support the Health and OT Connect integration.

Note: For more information on the privileges related to OT Connect families and the workflows that Health users must have access to, refer to the OT Connect documentation.

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
MI OT Connect Administrator MI OT Connect User	MI Health Admin
MI OT Connect Viewer MI Content Template Viewer	MI Health Power MI Health User

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

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

Family	MI AHI Administrator	MI AHI User	MI AHI Viewer
Measurement Location	View	View	View
Measurement Location Template	View	View	View
OPC Reading **Note:** This family is obsolete from V4.4.0.0.0.	View	View	View
OPC System **Note:** This family is obsolete from V4.4.0.0.0.	View	View	View
OPC Tag **Note:** This family is obsolete from V4.4.0.0.0.	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 **Note:** This family is obsolete from V4.4.0.0.0.	View	View	View
Has OPC Tag **Note:** This family is obsolete from V4.4.0.0.0.	View	View	View
Has Readings	View	View	View
Has Recommendations	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Timestamped Value	View, Update, Insert, Delete	View	View

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

Asset Strategy Implementation Deployment

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 system architecture.

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

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

Asset Strategy Implementation (ASI) Security Groups and Roles

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

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

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

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

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

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
Maintenance Item	None	View, Update, Insert, Delete	View
Maintenance Package	None	View, Update, Insert, Delete	View
Maintenance Plan	None	View, Update, Insert, Delete	View
Material	None	View, Update, Insert, Delete	View
Measurement Location	None	View, Update, Insert, Delete	View
Measurement Location Group	None	View, Update, Insert, Delete	View
Measurement Location Template	View, Update, Insert, Delete	View, Update, Insert	View
Notification	None	View, Update, Insert, Delete	View
Object List Item	None	View, Update, Insert, Delete	View
Operation	None	View, Update, Insert, Delete	View
Operator Rounds Allowable Values	None	View	View
Probability	None	View	View
Proposed Strategy	None	View	View
Protection Level	None	View	View
PRT	None	View, Update, Insert, Delete	View
PRT Template	View, Update, Insert, Delete	View	View
RCM FMEA Asset	None	View	View
RCM FMEA Recommendation	None	View	View
Risk	None	View	View
Risk Assessment	None	View	View
Risk Category	None	View	View
Risk Matrix	None	View	View
Risk Rank	None	View	View
Risk Threshold	None	View	View
SAP System	View, Update, Insert, Delete	View	View
Site Reference	View	View	View
System Strategy	None	View	View
Task List	None	View, Update, Insert, Delete	View
Task Types	None	View	View

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
Thickness Monitoring Task	None	View, Update, Insert, Delete	View
Unit Strategy	None	View	View
Work Management Item Child Definition	View, Update, Insert, Delete	View	View
Work Management Item Definition	View, Update, Insert, Delete	View	View
Work Management Item Definition Configuration	View, Update, Insert, Delete	View	View
Relationship Families			
Authorized to Implement	View, Update, Insert, Delete	View	View
Documents Action	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Actions	None	View	View
Has Action Mapping	View, Update, Insert, Delete	View	View
Has Action Revisions	None	View	View
Has Active Strategy	None	View	View
Has Asset Strategy	None	View	View
Has Associated Recommendation	None	View	View
Has Checkpoint	None	View, Insert	View
Has Child Hierarchy Item	None	View	View
Has Child Work Management Item	View, Update, Insert, Delete	View	View
Has Cycles	None	View, Update, Insert, Delete	View
Has Driving Recommendation	None	View	View
Has Execution Mapping	View, Update, Insert, Delete	View	View
Has Health Indicators	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has KPI Measurement	None	View	View
Has Maintenance Item	None	View, Update, Insert, Delete	View
Has Maintenance Package	None	View, Update, Insert, Delete	View
Has Material	None	View, Update, Insert, Delete	View
Has Measurement Location Group	None	View, Update, Insert, Delete	View

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

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

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

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

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
Maintenance Item	None	View, Update, Insert, Delete	View
Maintenance Package	None	View, Update, Insert, Delete	View
Maintenance Plan	None	View, Update, Insert, Delete	View
Material	None	View, Update, Insert, Delete	View
Measurement Location	None	View, Update, Insert, Delete	View
Measurement Location Group	None	View, Update, Insert, Delete	View
Measurement Location Template	View, Update, Insert, Delete	View, Update, Insert	View
Notification	None	View, Update, Insert, Delete	View
Object List Item	None	View, Update, Insert, Delete	View
Operation	None	View, Update, Insert, Delete	View
Operator Rounds Allowable Values	None	View	View
Probability	None	View	View
Proposed Strategy	None	View	View
Protection Level	None	View	View
PRT	None	View, Update, Insert, Delete	View
PRT Template	View, Update, Insert, Delete	View	View
RCM FMEA Asset	None	View	View
RCM FMEA Recommendation	None	View	View
Risk	None	View	View
Risk Assessment	None	View	View
Risk Category	None	View	View
Risk Matrix	None	View	View
Risk Rank	None	View	View
Risk Threshold	None	View	View
SAP System	View, Update, Insert, Delete	View	View
Site Reference	View	View	View
System Strategy	None	View	View
Task List	None	View, Update, Insert, Delete	View
Task Types	None	View	View

Family	MI ASI Administrator	MI ASI User	MI ASI Viewer
Thickness Monitoring Task	None	View, Update, Insert, Delete	View
Unit Strategy	None	View	View
Work Management Item Child Definition	View, Update, Insert, Delete	View	View
Work Management Item Definition	View, Update, Insert, Delete	View	View
Work Management Item Definition Configuration	View, Update, Insert, Delete	View	View
Relationship Families			
Authorized to Implement	View, Update, Insert, Delete	View	View
Documents Action	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Actions	None	View	View
Has Action Mapping	View, Update, Insert, Delete	View	View
Has Action Revisions	None	View	View
Has Active Strategy	None	View	View
Has Asset Strategy	None	View	View
Has Associated Recommendation	None	View	View
Has Checkpoint	None	View, Insert	View
Has Child Hierarchy Item	None	View	View
Has Child Work Management Item	View, Update, Insert, Delete	View	View
Has Cycles	None	View, Update, Insert, Delete	View
Has Driving Recommendation	None	View	View
Has Execution Mapping	View, Update, Insert, Delete	View	View
Has Health Indicators	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has KPI Measurement	None	View	View
Has Maintenance Item	None	View, Update, Insert, Delete	View
Has Maintenance Package	None	View, Update, Insert, Delete	View
Has Material	None	View, Update, Insert, Delete	View
Has Measurement Location Group	None	View, Update, Insert, Delete	View

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

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

Before You Begin

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

Procedure

1. On a machine from which you can access the SAP Server, access your ASI ABAP installation package.
2. Determine how to proceed based on your ABAP release and level and type of SAP system.

   - For ECC6, if your currently installed ABAP release is 400_600 or 420_600 and the level is 0000 or 0032, proceed to step 17 on page 75. Otherwise, proceed to the next step.
   - For S/4 Hana, if your currently installed ABAP release is 4XX_750 and the level is 0000, proceed to step 17 on page 75. Otherwise, proceed to the next step.
3. Navigate to the folder `\\SAP ASI ABAP Add-On\Service Pack Files\ECC6` or `\\SAP ASI ABAP Add-On\Service Pack Files\S/4 Hana`, and then select one of the following folders:

   - **Exchange Upgrade**: To upgrade the ASI ABAP Add-on when upgrading to a new SAP version.
   - **Installation**: To install the ASI ABAP Add-on for the first time.
   - **Upgrade**: To upgrade the ASI ABAP Add-on.
4. Copy the .pat file(s). The file names begin with either D07 or H4S.
5. On the SAP Server, paste the copied file(s) into the folder **usr\sap\trans\eps\in**.
6. Log in to the SAP system as a user with:

   - SCTSIMPSGL and S_CTS_ADMIN authorizations.

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

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

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

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

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

   In the **Message Text** column, on the row corresponding the uploaded .pat file, the message Uploaded successfully is displayed.
10. At the top of the screen, select .

    The **Add-On Installation Tool** screen appears again.
11. Select **Start**.

    A new grid appears. MIAPM appears in the list of add-on packages that can be installed.
12. Select the row containing the text MIAPM in the first column, and then select **Continue**.

    The **Support Package selection** tab appears.

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

    Note:

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

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

    At the bottom of the screen, an indicator appears, displaying the progress of the installation.
14. When the indicator disappears, a message appears, indicating that the add-on package will be installed.
15. Select .

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

    The MIAPM add-on package appears in the list of installed add-on packages on the Add-On Installation Tool screen.
17. In the installation package, navigate to the folder `\\SAP ASI ABAP Add-On\Support Package \`.

    Depending on your SAP system, navigate to either the `ECC6` folder or navigate to the `S/4 Hana` folder.
18. If your APBP release was 420_600 and level was 0000, navigate to the folder **\V4.2.0**.

    -or-

    If your ABAP release was any other version, navigate to the folder **\V4.0.0**.
19. Copy the .pat file(s).
20. On the SAP Server, paste the copied file(s) into the folder `\\usr\sap\trans\eps\in`.
21. Log in to the SAP system.
22. Run the following transaction: SPAM.

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

    A message appears, asking if you want to upload the package.
24. Select **Yes**.

    A summary screen appears, indicating that the package was uploaded successfully.
25. Select **Back**.
26. Select **Display/define**.

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

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

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

32. Select .
33. Select Menu, then select **Support Package**, and then select

    The installation is complete.

Next Steps

- Configure SAP for External Numbering

Verify ASI ABAP Add-On

Procedure

1. In SAP, select **Menu**, then select **System**, and then select **Status…**.
   The System: Status window appears.

2. In the SAP System data subsection, select .
   The System: Component information window appears.

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

   - **Release:**
     - ECC6: 700_600 depending on the version of SAP that you have installed.
     - S/4 Hana: 4XX_750
   - **Level:**
     - ECC6: 0003
     - S/4 Hana: 0003

   Note: If the level does not match, go back to step 17 on page 75 of Install or Upgrade the ASI ABAP
   Add-On on the SAP System and rerun the installation steps.

Next Steps

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

Uninstall the ASI ABAP Base Service Pack Add-On

Before You Begin

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

Procedure

1. Log in to the SAP server as a user with either SCTSIMPSGL and S_CTS_ADMIN authorizations or
   SAP_ALL authorization.
2. Enter SAINT.
   The **Add-On Installation Tool** screen appears.
3. Select the **Uninstallable components** tab.
   MIAPM appears in the list of add-on packages that can be uninstalled.
4. Select **MIAPM**, and then select **Continue**.
   The **Start options** dialog box appears.
5. Select **Default options**.
6. Select .

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

7. Select **Finish**.

Results

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

Configure SAP for External Numbering

About This Task

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

Procedure

Define the following External Number Ranges using the SAP documentation:

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

Next Steps

Configure SAP Permissions

Configure SAP Permissions

Before You Begin

Complete the steps described in Create APM Connect User Profile.

Procedure

Configure the following security permissions:

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

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

Asset Strategy Management Deployment

Deploy 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 system architecture.

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

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

ASM Security Groups

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

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

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

Security Group	Roles
MI ASM Reviewer	MI Strategy Admin
	MI Strategy Power
	MI Strategy User
MI ASM Viewer	MI APM Viewer
	MI Strategy Admin
	MI Strategy Power
	MI Strategy User

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

Family	MI ASM Analyst	MI ASM Administrator	MI ASM Reviewer	MI ASM Viewer
Entity Families				
Action	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Action Mapping	View	None	None	None
Active Strategy	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Analysis Link	View	View	View	View
Asset Criticality Analysis	View	View	View	View
Asset Criticality Analysis System	View	View	View	View
Asset Strategy	View, Update, Insert, Delete	View	View, Update	View
Calibration Task	View	None	View	None
Checkpoint Task	View, Update, Insert	View, Update, Insert	View, Update, Insert	View
Consequence	View	View, Update, Insert, Delete	View	View
Distribution	View, Update, Insert, Delete	View	View	View
Execution Mapping	View	None	None	None
Growth Model	View	View	View	View
Health Indicator	View, Update, Insert, Delete	None	View, Update	View

Family	MI ASM Analyst	MI ASM Administrator	MI ASM Reviewer	MI ASM Viewer
Health Indicator Mapping	View	View, Update, Insert, Delete	View	View
Hierarchy Item Child Definition	View	View, Update, Insert, Delete	View	View
Hierarchy Item Definition	View	View, Update, Insert, Delete	View	View
Implementation Package	View, Insert	None	None	None
Inspection Task	View	None	View	View
KPI	View	View	View	View
KPI Measurement	View	View	View	View
Measurement Location	View	View	View	View
Measurement Location Group	View, Update, Insert	None	None	None
Measurement Location Template	View	View	View	View
Operator Rounds Allowable Values	View	View	View	View
Probability	View	View, Update, Insert, Delete	View	View
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

Family	MI ASM Analyst	MI ASM Administrator	MI ASM Reviewer	MI ASM Viewer
Risk Matrix	View	View, Update, Insert, Delete	View	View
Risk Rank	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View
Risk Threshold	View	Insert, View, Update, Delete	View	View
Site Reference	View	View	View	View
System Action	View, Update, Insert, Delete	View	View	View
System Action Mapping	View	View, Update, Insert, Delete	View	View
System Action Optimization	View, Update, Insert, Delete	View	View	View
System Action Result	View, Update, Insert, Delete	View	View	View
System Analysis	View, Update, Insert, Delete	View	View	View
System Element	View, Update, Insert, Delete	View	View	View
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

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
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

Family	MI ASM Analyst	MI ASM Administrator	MI ASM Reviewer	MI ASM Viewer
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
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

Family	MI ASM Analyst	MI ASM Administrator	MI ASM Reviewer	MI ASM Viewer
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
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

Family	MI ASM Analyst	MI ASM Administrator	MI ASM Reviewer	MI ASM Viewer
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 software have facilities at multiple sites or locations around the world. Each site contains unique locations and equipment.

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

Asset Strategy Optimization Deployment

Deploy 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 system architecture.

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

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

ASO Security Groups

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

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

Calibration Management Deployment

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 system architecture.

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

Step	Task	Notes
1	Review the Calibration Management data model to determine which relationship definitions you will need to modify to include your custom families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to one or more of the Calibration Management Security Groups and Roles.	This step is required.
3	Configure the Has Standard Gas relationship family to include the desired Instrument families as predecessors to the Standard Gas Cylinder family in Configuration Manager.	This step is required only if you will use one or more standard gas cylinders to calibrate an asset.
4	Define alternate search queries.	This step is required only if you do not want to use the baseline search queries.
5	Configure default values for Calibration Template and Calibration Event Records by accessing the Calibration Setup Defaults family in Application Settings.	This step is required.
6	Install the Meridium Device Service on page 86 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.

Install the Meridium Device Service

About This Task

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

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

Procedure

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

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

   The **Calibration Tools** section appears, displaying a list of test equipment and standard gas cylinders.
3. In the upper-right corner of the page, select **Calibrator Settings**.
   The **Calibrator Settings** window appears.
4. In the **Select Device** box, select the required device.
5. If you selected the CMX Calibration Management software, enter values in the following fields:

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

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

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

     Important: 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.

Compliance Management Deployment

Deploy Compliance Management

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

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

Deploy Compliance Management for the First Time

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

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

Step	Task	Notes
1	Review the Compliance Management data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign users to the MI Inspection Security Group to provide privileges to the Compliance Management families.	This step is required.
3	Assign Security Users to one or more of the Security Roles used in Compliance Management.	This step is required. Security Users will need permissions to the Compliance Management families before they can use the Compliance Management features.
4	Create Inspection Strategy records using Record Manager.	This step is required. You should create Compliance Strategy records that adhere to the compliance standards of a regulatory body that requires inspections.
5	Design a policy to use for a Compliance Strategy Template.	This step is required. You can create this policy using the Policy Designer.
6	Create a query that will return the assets that you want to link to the Compliance Strategy Template.	This step is optional. You can also add assets to the Compliance Strategy Template by individual asset.
7	Create a Compliance Strategy Template using the administrative features of Compliance Management.	This step is required.
8	Link assets to the Compliance Strategy Template.	This step is required.
9	Map the Policy to the Compliance Strategy Template that you created.	This step is required.

10	Configure Inspection Management ActiveMQ settings for MIExecution Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
11	Ensure that the Meridium MIExecution Service is installed and running.	If the basic GE Digital APM system architecture is already installed, the Meridium MIExecution Service is automatically installed, and the service runs automatically.

Compliance Management Security Groups and Roles

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

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

Security Groups

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

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

Security Group	Permissions
MI Inspection	- View - Insert - Update - Delete
MI Inspection Viewer	View
MI RBI Administrator	View
MI RBI Analyst	View
MI RBI Viewer	View

Security Group	Permissions
MI Thickness Monitoring Administrator	View
MI Thickness Monitoring Inspector	View
MI Thickness Monitoring User	View
MI Thickness Monitoring Viewer	View

Security Roles

Compliance Management security roles can perform the following tasks:

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

The following security roles are available in Compliance Management:

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

Configure Inspection Management ActiveMQ settings for MIExecution Service

The MIExecution Service, on each GE Digital APM Server serves RBI, Inspection and Thickness Monitoring module queues. This service is configured to use a single shared ActiveMQ queue service across APM. Available queue configuration options include retries and concurrency limit.

Procedure

1. On the GE Digital APM Server, access the folder that contains the MIExecution Service files.

   Note: If you have installed GE Digital APM in the default location, you can locate the folder in `C:\Program Files\Meridium\ApplicationServer\mi-execution`

2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).
3. In the file, locate the following text:

```
"Queue_Config": {
        "Queues": [
          {
            "Name": "MI_IM_Queue",
            "ConcurrencyLimit": 8,
            "Retries": 5
          }
        ]
          }
```

   Note: `ConcurrencyLimit` indicates the maximum number of messages that will be consumed concurrently. `Retries` indicates the number of times it retries to send the messages to ActiveMQ if it fails.

4. Update the key values as desired.
5. Save and close the file.
   The updated settings will be applied when the MIExecution Service is stopped and restarted.

elog Deployment

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 system architecture.

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

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

Failure Modes and Effects Analysis Deployment

Deploy 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 system architecture.

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

Step	Task	Notes
1	Assign Security Users to one or more of the 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.

Generation Availability Analysis Deployment

Deploy 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 system architecture.

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

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

Step	Task	Notes
6	Add a GAA Unit.	This step is required. You must define the GAA Unit to represent the functional location that you want to use in GAA. You must add a GAA Unit at the level next to GAA Plant in the functional location.

You must define a GAA Unit after defining a GAA Company and a GAA Plant. GAA Unit is stored in a GAA Unit record.

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

Generation Availability Analysis Wind Deployment

Deploy GAA Wind for the First Time

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

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

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

Step	Task	Notes
3	Specify additional system code tables for the GAA Wind families.	By default, GE Digital APM provides a set of system code tables for the GAA Wind families. You can modify these default system code tables or add new system code tables.
4	Configure the GAA Wind Report Configuration records.	This step is required.
5	Using the GAA Wind Asset Hierarchy Data Loader, create the following records in the GAA Wind Asset Hierarchy: • GAA Company • GAA Wind Plant • GAA Wind Group • GAA Wind Sub Group • GAA Wind Unit	This step is required.
6	Using the GAA Wind Sub Group Capacity Data Loader, create the GAA Wind Sub Group Capacity record.	This step is required.

Hazards Analysis Deployment

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 system architecture.

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

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

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

Update the Query Parameter Type

About This Task

After the database for GE Digital APM is upgraded, if the entity key fields are of the type string, you must modify the catalog query parameters to use the correct type by performing the following steps:

Procedure

1. Access the **Query** page.
2. Select **Browse**.
   The **Select a query from the catalog** window appears.
3. Navigate to the folder containing the query that you want to update, and select the link for the query.
   The **Results** workspace appears.
4. Select the **SQL** tab.
   The **SQL** workspace appears, where you can modify the SQL code.
5. Modify all the entity key numeric parameters to :k.

   For example, (? :n) must be updated to (? :k).
6. Select **Save**.
   The modified query is saved.

Revert the Hazard Analysis Queries to Baseline

This action is required only if you have modified the Hazard Analysis queries.

About This Task

If you have modified the Hazard Analysis queries, perform the following steps to revert the query to baseline.

Procedure

1. Access the Catalog page.
2. Navigate to the Public folder for the query that you want to revert.

   For Hazard Analysis, the public queries are stored in the following folder:

   `Public\Meridium\Modules\Hazards Analysis\Queries`

3. Select the check box next to the query that you want to revert, and then select 🗑.
   The **Confirm Delete** window appears, prompting you to confirm if you want to delete the selected query.
4. Select **OK**.
   The selected query is deleted.
5. Navigate to the Baseline folder for queries.

   For Hazard Analysis, the baseline queries are stored in the following folder:

   `Baseline/Meridium/Modules/Hazards Analysis/Queries`

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

Layers of Protection Analysis Deployment

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 system architecture.

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

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

Update the Query Parameter Type

About This Task

After the database for GE Digital APM is upgraded, if the entity key fields are of the type string, you must modify the catalog query parameters to use the correct type by performing the following steps:

Procedure

1. Access the **Query** page.
2. Select **Browse**.
   The **Select a query from the catalog** window appears.
3. Navigate to the folder containing the query that you want to update, and select the link for the query.
   The **Results** workspace appears.
4. Select the **SQL** tab.
   The **SQL** workspace appears, where you can modify the SQL code.
5. Modify all the entity key numeric parameters to :k.

   For example, (? :n) must be updated to (? :k).
6. Select **Save**.
   The modified query is saved.

Life Cycle Cost Analysis Deployment

Deploy 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 system architecture.

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

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

LCC Security Groups

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

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

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

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

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

Inspection Management Deployment

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 system architecture.

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

Step	Task	Notes
1	Review the Inspection Management data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Configure GE Digital APM to create Task Revision records.	This step is required only if you want Task Revision records to be created every time you create or update a task. These records are used to track historical data related to a task.
3	Assign Security Users to one or more of the Security Roles used in IM.	This step is required. Security Users will need permissions to the Inspection Management families before they can use the Inspection Management features.
4	Assign Resource Roles to users.	This step is required to define the users who can perform Inspection workflows as Inspectors, supervisors, administrators, contract inspectors, and risk analysts in Inspection Management.
5	Modify baseline Application Configuration settings.	This step is required only if you want to modify Application Configurations. The following Application Configurations are defined in the baseline database: Asset Query Path; Associated Relationship Family; Published Query Path; Summary Query Path; Alerts Query Path; Asset Is Successor; Profile Configuration; Method Configuration; Strategy Rule Configuration.

Step	Task	Notes
6	Define the Inspection Profile for each piece of equipment that you will inspect.	This step is required only if you plan to create Inspection records in baseline families other than the Checklists subfamilies.
7	Modify the baseline Asset query.	This step is required only if you want Inspection records to be linked to records in a family other than the Equipment family.
8	Define Event Configurations for any new Inspection families that you have created.	This step is required only if you have created custom Inspection families that you want to use within Inspection Management.
9	for custom inspections.	This step is optional.
10	Define Taxonomy Configurations for Inspection Families and Checklist Configurations.	This step is required only if you want to link Inspection Families and Checklist Configurations to assets using equipment taxonomy.
11	Assign certifications to users.	This step is optional.
12	Group inspection work into Work Packs.	This step is optional.
13	Configure Inspection Management ActiveMQ settings for MIExecution Service on page 104Configure Inspection Management ActiveMQ settings for MIExecution Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
14	Ensure that the Meridium MIExecution Service is installed and running.	If the basic GE Digital APM system architecture is already installed, the Meridium MIExecution Service is automatically installed, and the service runs automatically.
15	Modify the Inspection Event preferences.	This step is required to avoid creating redundant related records while creating inspection record.

Configure GE Digital APM to Create Task Revisions

About This Task

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

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

- Task Revision
- Inspection Task Revision

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

Procedure

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

Results

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

Configure Inspection Management ActiveMQ settings for MIExecution Service

The MIExecution Service,on each GE Digital APM Server serves RBI, Inspection and Thickness Monitoring module queues. This service is configured to use a single shared ActiveMQ queue service across APM. Available queue configuration options include retries and concurrency limit.

Procedure

1. On the GE Digital APM Server, access the folder that contains the MIExecution Service files.

   Note: If you have installed GE Digital APM in the default location, you can locate the folder in `C:\Program Files\Meridium\ApplicationServer\mi-execution`
2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).
3. In the file, locate the following text:

```
"Queue_Config": {
        "Queues": [
          {
            "Name": "MI_IM_Queue",
            "ConcurrencyLimit": 100,
            "Retries": 5,
              "LimitPerTenantRequired": true
          }
        ]
            }
```

   Note: `ConcurrencyLimit` indicates the maximum number of messages that will be consumed concurrently. `Retries` indicates the number of times it retries to send the messages to ActiveMQ if it fails. `LimitPerTenantRequired` indicates whether Maximum Concurrency limit per Tenant is specified in scheduler service for the queue.
4. Update the key values as desired.
5. Save and close the file.
   The updated settings will be applied when the MIExecution Service is stopped and restarted.

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 following roles can be assigned to a group or user:

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

These roles are used in State Management.

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

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

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

Note that:

- The family-level privileges granted to the following families are also spread to all of their subfamilies:
  - Event
  - Taxonomy References
- The Has Task History relationship family is inactive in the baseline 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.

Modify the Inspection Event Preferences

Procedure

1. Access the **Inspection Configuration** workspace.
2. Select the **Event Configurations** tab.
   The **Event Configurations** section appears, displaying a list of the Event Configurations currently applied to the Inspection Configuration.
3. In the upper-right corner of the workspace, select ✏.
   The grid in the **Event Configurations** section can now be modified.
4. In the **Event Configurations** section, select the **Related Families** links corresponding to the Inspection families as listed in the following table:
   The **Related Families** window appears.

Relationship	Family	Inspection families
• **HAS FINDINGS** • **HAS SUB-INSPECTION** • **HAS SUB-INSPECTION**	• **GENERAL FINDING** • **BUNDLE SUB-INSPECTION** • **PRESSURE TEST SUB-INSPECTION**	• **API 510 External Checklist** • **API 510 Internal Checklist** • **API 510 Internal Exchanger Checklist** • **API 570 External Checklist** • **API 653 External Checklist** • **API 653 Internal Checklist** • **Checklist Inspection Template** • **External PRD Checklist** • **ILI Checklist** • **PRD Pop Test Checklist** • **Third Party Damage Checklist**

5. Select the check boxescorresponding to **Relationship** and **Family** as mentioned in the above table.
6. In the upper-right corner of the workspace, select 🗑.
   A message appears, confirming that you want to delete the family preferences.
7. Select **Yes**.
   The selected family preferences are deleted.
8. For each Inspection family that has **General Finding** as an available related family, deselect the **Link** and **Unlink** check boxes.
9. Select **Done**.
   One or more related families are modified.
10. For each Inspection family that has **Asset Corrosion Analysis** as an available related family, deselect the **Delete** check box.
11. Select **Done**.
   One or more related families are modified.

12. In the upper-right corner of the workspace, select ⊟.
    The Related Family preferences are modified.

Management of Change Deployment

Deploy MoC for the First Time

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

Manage Translations Deployment

Deploy Manage Translations for the First Time

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

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

Step	Task	Note
1	Based on your database provider, select one of the following: • Oracle 1. Create the Localization Oracle Database on page 28 2. Create the Localization Oracle Schema on page 28 • SQL 1. Create the SQL Server Localization Database on page 34 2. Configure the SQL Server Localization Database on page 34	This step is required.

Metrics and Scorecards Deployment

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 system architecture.

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

Step	Task	Notes

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

2	Verify that your event and asset criticality data meet the standard classification requirements, and modify the Event or Asset Criticality Data for the Work History cube as needed.	This step is required.
3	Localize the event and asset criticality values in the application.	This step is optional.
4	Schedule cubes for processing on the SQL Server Analysis Server.	This step is required.

Step	Task	Notes
5	Assign Security Users to one or more of the Metrics and Scorecards Security Groups and Roles.	This step is required.
6	Create Analysis Services Cube records for each cube that has been defined in SQL Server Analysis Services. Since 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.	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.

About Configuring a Cube for Usage Metrics Tracking

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

The MI_SEC_LOG_EVENTS table records the following events:

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

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

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

Note: Usage metrics are recorded only for activities performed via 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_SEC_LOG_EVENTS table. After you create the cube, you must join the MI_SEC_LOG_EVENTS and the MIV_MI_IS_A_USER tables. You must also join the MIV_MI_IS_A_USER and MIV_MI_HUMAN_RESOURCE tables.

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

About Scheduling Cubes for Processing

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

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

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

Install SQL Server Analysis Services on the Server

SQL Server Analysis Services is the foundation for the 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 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 APM 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.

Deploy the Work History Cube

Procedure

1. Copy the `Cubes` folder from the Release CD to the SQL Server Analysis Services server.

2. On the SQL Server Analysis Services server, in the `Cubes` folder, select the `Work History` folder.

   The following files and folders appear:

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

3. Run the Analysis Services Deployment Wizard program.
   The **Welcome** page appears.

4. Select **Next**.

5. When the wizard prompts you to choose the database file, navigate to the `Work History` folder, and then select the `Work History.asdatabase` file.

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

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

Modify the Event or Asset Criticality Data for Work History Cube

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

Modify the Non-Standard Event Type Data Using the View

Before You Begin

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

Procedure

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

   SELECT distinct MI_EVENT_TYP_CHR from MI_EVENT

2. Verify if the results match the standard event type IDs defined by the Work History cube.

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

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

```
  WHEN 'Repair' THEN 'Repair'

  WHEN 'Inspection' THEN 'PM/PdM'

  ELSE 'Unknown'

END AS EventType
```

Modify the Non-Standard Event Priority Data Using the View

Before You Begin

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

Procedure

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

   SELECT distinct MI_EVWKHIST_ORDR_PRTY_C from MI_EVWKHIST

   SELECT distinct MI_EVWKHIST_RQST_PRTY_C from MI_EVWKHIST

2. Verify if the results match the standard event priority IDs defined by the Work History cube.

3. If the results do not match, then modify the case statement CASE ISNULL(MI_EVWKHIST_ORDR_PRTY_C, MI_EVWKHIST_RQST_PRTY_C) in the view to display the standard event priority IDs.

   Example

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

   ```
   CASE ISNULL(MI_EVWKHIST_ORDR_PRTY_C,
   MI_EVWKHIST_RQST_PRTY_C)

   WHEN 'Very Low' THEN '1'

   WHEN 'Low' THEN '2'

   WHEN 'Medium' THEN '3'

   WHEN 'High' THEN '4'

   WHEN 'Emergency' THEN '5'

   WHEN '1' THEN '1'

   WHEN '2' THEN '2'

   WHEN '3' THEN '3'

   WHEN '4' THEN '4'

   WHEN '5' THEN '5'
   ```

```
WHEN 'M' THEN '3'

ELSE 'Unknown'

END AS Priority
```

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

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

Procedure

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

   SELECT distinct MI_EVWKHIST_DETCT_MTHD_CD_C from MI_EVWKHIST

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

   Example

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

   ```
   CASE MI_EVWKHIST_DETCT_MTHD_CD_C

   WHEN 'Continous Condition Monitoring' THEN '0001'

   WHEN 'Corrective Maintenance' THEN '0002'

   WHEN 'Formal Inspection' THEN '0003'

   WHEN 'Operator Routine Observation' THEN '0004'

   WHEN 'Periodic Condition Monitoring' THEN '0005'

   WHEN 'Preventive Maintenance' THEN '0006'

   WHEN 'Production Interference' THEN '0007'

   WHEN 'Radar operator Observation' THEN '0008'

   WHEN '0001' THEN '0001'

   WHEN '0002' THEN '0002'

   WHEN '0003' THEN '0003'

   WHEN '0004' THEN '0004'

   WHEN '0005' THEN '0005'
   ```

```
WHEN '0006' THEN '0006'

WHEN '0007' THEN '0007'

WHEN '0008' THEN '0008'

WHEN '0009' THEN '0001'

ELSE 'Unknown'

END AS DetectionMethod
```

Modify the Non-Standard Event Breakdown Data Using the View

Before You Begin

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

Procedure

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

   SELECT distinct MI_EVWKHIST_BRKDN_IND_F from MI_EVWKHIST

2. Verify if the results match the standard event breakdown IDs defined by the Work History cube.

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

   Example

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

   ```
   CASE MI_EVWKHIST_BRKDN_IND_F

     WHEN 'Y' THEN 'Y'

     WHEN 'N' THEN 'N'

     WHEN 'No' THEN 'N'

     ELSE 'Unknown'

   END AS Breakdown
   ```

Modify the Non-Standard Equipment Criticality Data Using the View

Before You Begin

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

Procedure

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

   SELECT distinct MI_EQUIP000_CRITI_MTHD_IND_C from MI_EQUIP000

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

> **Example**
>
> Suppose distinct Equipment Criticality returned by the query in Step 1 is *A*, *B*, *C*, and *H* and if *H* in your data is actually *A* equipment criticality ID, then you should modify the CASE statement in the View as:
>
> ```
> CASE MI_EQUIP000_CRITI_IND_C
>
> WHEN 'HIGH' THEN 'A'
>
> WHEN 'Medium' THEN 'B'
>
> WHEN 'Low' THEN 'C'
>
> WHEN 'A' THEN 'A'
>
> WHEN 'B' THEN 'B'
>
> WHEN 'C' THEN 'C'
>
> WHEN 'H' THEN 'A'
>
> ELSE 'Unknown'
>
> END AS EquipmentCriticality
> ```

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

Before You Begin

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

Procedure

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

   SELECT distinct MI_FNCLOC00_CRTCAL_IND_C from MI_FNCLOC00

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

Example

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

```
CASE A.MI_FNCLOC00_CRTCAL_IND_C

WHEN 'HIGH' THEN 'A'

WHEN 'Medium' THEN 'B'

WHEN 'Low' THEN 'C'

WHEN 'A' THEN 'A'

WHEN 'B' THEN 'B'

WHEN 'C' THEN 'C'

WHEN 'M' THEN 'B'

ELSE 'Unknown'

END AS FunctionalLocationCriticality
```

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

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

Procedure

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

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

```
UPDATE [MI_DIM_EVENT_TYPE] SET [MI_DIM_EVENT_TYPE].[EventTypeCaption]
= '<New Data>' WHERE [MI_DIM_EVENT_TYPE].[EventTypeCaption] =
'<Standard Data Caption>'
```

Note: In this query:

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

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

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

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

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

Map an Event Type to a Standard Event Type ID

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

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

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

- INSPECTION
- PM/PdM
- Reading
- Repair

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

- Run the query `UPDATE [MI_DIM_EVENT_TYPE] SET [MI_DIM_EVENT_TYPE].[EventTypeCaption] = 'INSPECTION' WHERE [MI_DIM_EVENT_TYPE].[EventTypeCaption] = 'Miscellaneous'`.
  The event type INSPECTION is mapped to the standard event type ID Miscellaneous.

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

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

Procedure

1. In the **Applications** menu, navigate to the **TOOLS** section, and then select **Queries**..
   The **Query** page appears.
2. Select **Create New**.
   The **Select a Family or Query** window appears.
3. Search for the Event Priority Dimension family, and then select **Add**.
   The **Design** workspace appears.
4. Select the **SQL** tab.
   The **SQL** workspace appears.
5. Run the query `SELECT [MI_DIM_EVENT_PRIORITY].[Priority] "Priority", [MI_DIM_EVENT_PRIORITY].[PriorityCaption] "PriorityCaption" FROM [MI_DIM_EVENT_PRIORITY].`
   The standard event priority data available in GE Digital APM appears in the query results.
6. Run the following queries:

   - `SELECT distinct MI_EVWKHIST_BRKDN_IND_F from MI_EVWKHIST`
   - `SELECT distinct MI_EVWKHIST_RQST_PRTY_C from MI_EVWKHIST`

   The event priority data available in your database appears in the query results.
7. Verify if the event priority data returned by the query in Step 6 matches the standard event priority IDs returned by the query in Step 5.
8. If the results do not match, perform the following steps to map the event priority data available in your database with the standard event priority ID available in GE Digital APM:

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

   Note: In this query:

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

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

   > **Map Event Priority Data to a Standard Event Priority ID**
   >
   > The following standard event priority data is returned by the query run in Step 5.

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

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

- 1
- 2
- 3
- 4

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

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

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

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

Procedure

1. In the **Applications** menu, navigate to the **TOOLS** section, and then select **Queries**.
   The **Query** page appears.
2. Select **Create New**.
   The **Select a Family or Query** window appears.
3. Search for the Event Detection Method Dimension family, and then select **Add**.
   The **Design** workspace appears.
4. Select the **SQL** tab.
   The **SQL** workspace appears.
5. Run the query `SELECT [MI_DIM_EVENT_DETECTION].[DetectionMethod] "DetectionMethod", [MI_DIM_EVENT_DETECTION].[DetectionMethodCaption] "DetectionMethodCaption" FROM [MI_DIM_EVENT_DETECTION]`.
   The standard event detection methods available in GE Digital APM appears in the query results.
6. Run the query `SELECT distinct MI_EVWKHIST_DETCT_MTHD_CD_C from MI_EVWKHIST`.
   The event detection methods available in your database appears in the query results.
7. Verify if the event detection methods returned by the query in Step 6 match the standard event detection method IDs returned by the query in Step 5.
8. If the results do not match, perform the following steps to map the event detection methods available in your database with the standard event detection method ID available in GE Digital APM:

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

```
UPDATE [MI_DIM_EVENT_DETECTION] SET [MI_DIM_EVENT_DETECTION].
[DetectionMethod] = '<New Data>' WHERE [MI_DIM_EVENT_DETECTION].
[DetectionMethod] = '<Standard Data Caption>'
```

Note: In this query:

- <New Data> denotes the event detection method that you want to map to the standard event detection method ID available in GE Digital APM.
- <Standard Data Caption> denotes the captions corresponding to the standard event detection method available in GE Digital APM.

b) Replace <New Data> with a value that you want to map with the standard event detection method available in GE Digital APM.

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

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

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

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

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

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

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

- Inspection
- Observation
- Preventive Maintenance
- Production Interference

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

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

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

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

Procedure

1. In the **Applications** menu, navigate to the **TOOLS** section, and then select **Queries**.
   The **Query** page appears.
2. Select **Create New**.
   The **Select a Family or Query** window appears.
3. Search for the Event Breakdown Dimension family, and then select **Add**.
   The **Design** workspace appears.
4. Select the **SQL** tab.
   The **SQL** workspace appears.
5. Run the query `SELECT [MI_DIM_EVENT_BREAKDOWN].[Breakdown] "Breakdown", [MI_DIM_EVENT_BREAKDOWN].[BreakdownCaption] "BreakdownCaption" FROM [MI_DIM_EVENT_BREAKDOWN].`
   The standard event breakdown data available in GE Digital APM appears in the query results.
6. Run the query `SELECT distinct MI_EVWKHIST_BRKDN_IND_F from MI_EVWKHIST.`
   The event breakdown data available in your database appears in the query results.
7. Verify if the event breakdown data returned by the query in Step 6 matches the standard event breakdown IDs returned by the query in Step 5.
8. If the results do not match, perform the following steps to map the event breakdown data available in your database with the standard event breakdown ID available in GE Digital APM:

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

   `UPDATE [MI_DIM_EVENT_BREAKDOWN] SET [MI_DIM_EVENT_BREAKDOWN].[BreakdownCaption] = '<New Data>' WHERE [MI_DIM_EVENT_BREAKDOWN].[BreakdownCaption] = '<Standard Data Caption>'`

   Note: In this query:

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

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

   > **Map an Event Breakdown Indicator to a Standard Event Breakdown ID**
   >
   > The following standard event breakdown data is returned by the query run in Step 5.

Breakdown	BreakdownCaption
N	N
Unknown	Unknown
Y	Y

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

- No
- Yes
- Unknown

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

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

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

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

Procedure

1. In the **Applications** menu, navigate to the **TOOLS** section, and then select **Queries**.
   The **Query** page appears.
2. Select **Create New**.
   The **Select a Family or Query** window appears.
3. Search for the Asset Criticality Dimension family, and then select **Add**.
   The **Design** workspace appears.
4. Select the **SQL** tab.
   The **SQL** workspace appears.
5. Run the query `SELECT [MI_DIM_ASSET_CRITICALITY].[Criticality] "Criticality", [MI_DIM_ASSET_CRITICALITY].[CriticalityCaption] "CriticalityCaption" FROM [MI_DIM_ASSET_CRITICALITY].`
   The standard asset criticality data available in GE Digital APM appears in the query results.
6. Run the following queries:

   - For equipment criticality data, run the query `SELECT distinct MI_EQUIP000_CRITI_MTHD_IND_C from MI_EQUIP000.`
     The equipment criticality data available in your database appears in the query results.
   - For functional location criticality data, run the query `SELECT distinct MI_FNCLOC00_CRTCAL_IND_C from MI_FNCLOC00.`
     The functional location criticality data available in your database appears in the query results.

7. Verify if the asset criticality data returned by the query in Step 6 matches the standard asset criticality IDs returned by the query in Step 5.
8. If the results do not match, perform the following steps to map the asset criticality data available in your database with the standard asset criticality ID available in GE Digital APM:

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

```
UPDATE [MI_DIM_ASSET_CRITICALITY] SET [MI_DIM_ASSET_CRITICALITY].
[CriticalityCaption] = '<New Data>' WHERE [MI_DIM_ASSET_CRITICALITY].
[CriticalityCaption] = '<Standard Data Caption>'
```

Note: In this query:

- <New Data> denotes the asset criticality data that you want to map to the standard asset criticality ID available in GE Digital APM.
- <Standard Data Caption> denotes the captions corresponding to the standard asset criticality data available in GE Digital APM.

b) Replace <New Data> with a value that you want to map with the standard asset criticality data available in GE Digital APM.

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

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

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

Map Asset Criticality Data to a Standard Asset Criticality ID

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

Criticality	CriticalityCaption
A	High
B	Medium
C	Low
Unknown	Unknown

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

- X
- Y
- Z
- H

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

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

Localize the Event or Asset Criticality Values

By default, the Meridium Work History cube displays the event and asset criticality data in English. However, you can modify the event or asset criticality values to other languages supported by 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

Procedure

1. In the **Tables**, select the table MI_DIM_EVENT_TYPE.
   The table values appear, displaying the event type ID and the event caption.
2. In the **EventTypeCaption** column, select the cell for the event type that you want to localize, and then manually modify the caption.
3. Save the modification, and then process the cube.
4. Log in to 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 breakdown values appears in the language to which you have modified.

Example: Localize the Event Breakdown Values

Procedure

1. In the **Tables**, select the table MI_DIM_EVENT_BREAKDOWN.
   The table values appear, displaying the breakdown ID and the breakdown caption.
2. In the **BreakdownCaption** column, select the cell for the breakdown that you want to localize, and then manually modify the caption.
3. Save the modification, and then process the cube.
4. Log in to 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 **Breakdown**.
   The caption for the event type values appears in the language to which you have modified.

Example: Localize the Event Priority Values

Procedure

1. In the **Tables**, select the table MI_DIM_EVENT_PRIORITY.
   The table values appear, displaying the Priority ID and the Priority caption.
2. In the **PriorityCaption** column, select the cell for the priority caption that you want to localize, and then manually modify the caption.
3. Save the modification, and then process the cube.
4. Log in to 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 Priority**, select **Priority**, and then select **Priority**.
   The caption for the priorities appears in the language to which you have modified.

Example: Localize Event Detection Method Values

Procedure

1. In the **Tables**, select the table MI_DIM_EVENT_DETECTION_METHOD.
   The table values appear, displaying the event type ID and the event caption.
2. In the **DetectionMethodCaption** column, select the cell for the detection method that you want to localize, and then manually modify the caption.
3. Save the modification, and then process the cube.
4. Log in to 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 Detection**, select **Detection**, and then select **Detection Method**.
   The caption of the Detection Method values appear in the language to which it was modified.

Example: Localize Equipment Criticality Values

Procedure

1. In the **Tables**, select the table MI_DIM_ASSET_CRITICALITY.
   The table values appear, displaying the Criticality ID and the Criticality caption.
2. In the **CriticalityCaption** column, select the cell for the caption that you want to localize, and then manually modify the caption.
3. Save the modification, and then process the cube.
4. Log in to 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 **Equipment**, select **Criticality**, and then select **Criticality**.
   The caption of the criticality values appear in the language to which it was modified.

Example: Localize Functional Location Criticality Values

Procedure

1. In the **Tables**, select the table MI_DIM_ASSET_CRITICALITY.
   The table values appear, displaying the criticality ID and the criticality caption.
2. In the **CriticalityCaption** column, select the cell for the caption that you want to localize, and then manually modify the caption.
3. Save the modification, and then process the cube.
4. Log in to 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 **Functional Location**, select **Criticality**, and then select **Criticality**.
   The caption of the functional location criticality values appear in the language to which it was modified.

Policy Designer Deployment

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 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.

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

Note: The following settings also apply to Family Policies:

- MaxSubPolicyDepth
- MathNodeExecutionTimeout

Table 1: Procedure

Step	Task	Notes
1	Assign Security Users to one or more of the Policy Designer Security Groups and Roles.	This step is required.
2	Review the Policy Designer data model to determine which relationship definitions you will need to modify to include your custom equipment and location families, and as needed, modify the relationship definitions using Configuration Manager.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
3	Configure Queue Settings for Policy Execution Service on page 133.	This step is optional. You can perform this step if you want to modify the default retries, concurrency, or duplicate trigger timeout settings.
4	Configure the Time Limit for Policy Execution on page 134.	This step is optional. You can perform this step if you want to modify the policy execution time limit for the Policy Execution Service. By default, the policy execution time limit is 15 minutes per policy instance.

Step	Task	Notes
5	Configure Execution Time Out Value for Math Node on page 135.	This step is optional. You can perform this step if you want to modify the Math node execution time limit for the Policy Execution Service. By default, the Math node execution time limit is 5 minutes.
6	Configure the SubPolicy Node for Policy Execution on page 137	This step is optional. You can perform this step if you want to modify the maximum depth of nesting for sub policies.
7	Configure the Default Historical Readings Time Range for the OT Connect Tag node on page 136.	This step is optional. You can perform this step to modify the default time range of retrieving Historical Readings for the OT Connect Tag node if a specific time range cannot be determined. By default, the OT Connect tag node will retrieve two years of HDA data.
8	On the GE Digital APM Server, stop and restart the Meridium 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 that you want to use for policy execution. @@@This is a broken paragraph@@@
9	Configure Queue Settings for Policy Trigger Service on page 133.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
10	On the GE Digital APM Server, stop and restart the Meridium Policy Trigger service.	This step is required. @@@This is a broken paragraph@@@ @@@This is a broken paragraph@@@
11	On the GE Digital APM Server, reset IIS.	This step is required only if you have modified the time out value for the Math node execution or Policy Execution, modified the default historical readings time range for the OT Connect node, or modified the maximum depth for nested sub policies in the `appSettings. json` configuration file.

Step	Task	Notes
12	Configure Policy Reference Clean Up Batch Size on page 138	This step is optional. When you delete a record, the related policy instances and execution history gets deleted in the background. You can perform this step to modify and set the default batch size and sleep interval that runs in the background.
13	Configure Alternative Query for Policy Overview	This step is optional. The alternative query provides additional information on the most recent execution of each policy but may impact performance.

About the Asset Health Services

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

Services Summary

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

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

  This service also facilitates the automatic creation of Health Indicator records for configured sources.
- Policy Trigger Service: When an input to a policy (that is, an associated record in the GE Digital APM database or reading value in the process historian) changes, when a policy schedule is due, or a user submits an Execute Now request, a message is added to the policy trigger queue. The Policy Trigger Service monitors the trigger queue. When it receives a message, it determines which policy instances should be executed for the message, and then it sends corresponding messages to the policy execution queue. Even if your GE Digital APM system is configured with multiple Policy Execution servers, only one policy execution queue is used.
- Policy Execution Service: The Policy Execution Service handles the execution of policies. Specifically, the Policy Execution Service monitors the policy execution queue and executes the policy instances that are added to it. If the GE Digital APM system is configured with multiple Policy Execution servers, when each Policy Execution Service completes the execution of a policy instance, it will execute the next instance from the shared policy execution queue. In this way, the policy execution load is automatically balanced across all available Policy Execution Services.
- OT Connect Service: Monitors the subscribed tags (that is, tags that are used in policies and health indicators) and when data changes occur on these tags adds messages to the appropriate queues. This service also facilitates the automatic import and synchronization of tags from a configured OT Source. For more information, refer to the OT Connect section of the documentation.

Standard System Architecture Configuration

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

Note: In this example configuration, only one machine of each type is illustrated. Your specific architecture may include multiple GE Digital APM Servers, multiple OPC Servers, or multiple GE Digital APM Servers used for policy executions.
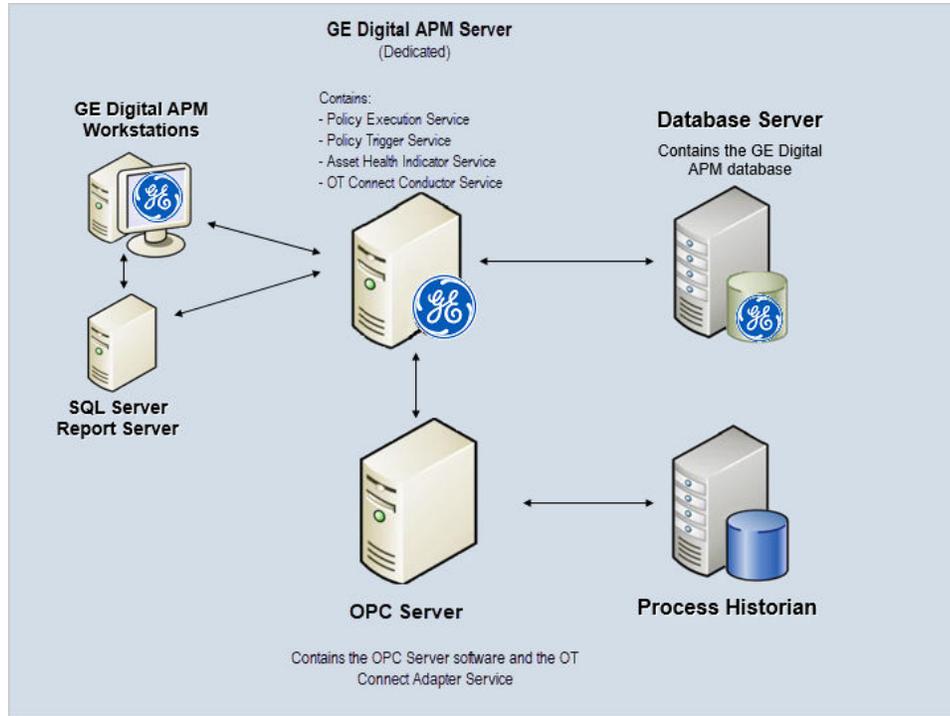
The following table summarizes the machines illustrated in this diagram and the software and services that you will install when you complete the first-time deployment steps for Asset Health Manager, OT Connect, and Policy Designer.

Machine	Software Installed	Service Installed with APM Software
GE Digital APM Server	GE Digital APM Server software	Asset Health Indicator Service
		Policy Trigger Service
		Policy Execution Service
		OT Connect Conductor Service

Machine	Software Installed	Service Installed with APM Software
OPC Server	GE Digital OT Connect Adapter software	OT Connect Adapter Service
	OPC Server software	N/A
Process Historian	Process historian software	N/A

About Policy Execution

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

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

Automatic Execution

When any record or reading value is updated by the GE Digital APM Server, or when a reading value for a tag associated with one or more policies is updated on the process historian, a message is added to the policy trigger queue. The Policy Trigger Service monitors the trigger queue. When it receives a message, it determines which policy instances should be executed for the message, if any. Only active policy instances associated with the record or reading update will be executed. The Policy Trigger Service then sends corresponding messages to the policy execution queue for each relevant policy instance. Finally, a Policy Execution Service executes each policy instance that was added to the policy execution queue in turn.

Scheduled Execution

When a scheduled policy is due, a scheduled job adds a message to the policy trigger queue. The Policy Trigger Service monitors the trigger queue and sends messages to the policy execution queue for each active instance of the policy. Finally, a Policy Execution Service executes each active instance that was added to the policy execution queue in turn.

On Demand Execution

When you request a policy or policy instance execution from the Policy Designer user interface, or select a hyperlink configured to execute a policy or policy instance, a message is added to the policy trigger queue. The Policy Trigger Service monitors the trigger queue and sends messages to the policy execution queue for each active instance of the policy. Finally, a Policy Execution Service executes each active instance that was added to the policy execution queue in turn.

Configure Queue Settings for Policy Execution Service

About This Task

The Policy Execution Service processes messages from queues, which are managed by ActiveMQ. The Policy Execution Service provides the following queue configuration options:

- Retries
- Redelivery attempts and interval
- Concurrency limit

Increasing the concurrency limit allows the policy execution service to process more messages in parallel, resulting in higher throughput of policy executions, provided that the system has available resources. Reducing the concurrency limit reduces the policy execution throughput and the system resources used by policy execution. GE Digital APM recommends that the concurrency limit be less than or equal to the number of logical processors on the GE Digital APM Server used for policy executions.

Procedure

1. On the GE Digital APM Server, access the folder that contains the Policy Execution Service files.

   Note: If you have installed GE Digital APM in the default location, you can locate the folder in `C:\Program Files\Meridium\ApplicationServer\policy-execution`.

2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).

3. In the file, locate the following text:

```
"triggerMessageSettings": {
    "concurrencyLimit": 8,
        "retries": 5,
        "redeliveryAttempts": 3,
        "redeliveryMinInterval": 1,
        "redeliveryMaxInterval": 2440,
        "redeliveryDelta": 5
    },
    "executionMessageSettings": {
      "concurrencyLimit": 8,
      "retries": 5,
      "redeliveryAttempts": 3,
      "redeliveryMinInterval": 1,
      "redeliveryMaxInterval": 2440,
      "redeliveryDelta": 5
    }
```

4. Update the key values as desired.
5. Save and close the file.
   The updated settings will be applied when the Meridium Policy Execution service is stopped and restarted.

Configure Queue Settings for Policy Trigger Service

About This Task

The Policy Trigger Service processes messages from queues, which are managed by ActiveMQ. The Policy Execution Service provides the following queue configuration options:

- Retries
- Redelivery attempts and interval
- Concurrency limit
- Duplicate Measurement Location reading trigger elimination timeout

Procedure

1. On the GE Digital APM Server, access the folder that contains the Policy Trigger Service files.

   Note: If you have installed GE Digital APM in the default location, you can locate the folder in `C:\Program Files\Meridium\ApplicationServer\policy-trigger`.
2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).
3. In the file, locate the following text:

   ```
   "DuplicateTriggerTimeout": 5000,

   "notificationMessageSettings": {
       "concurrencyLimit": 16,
       "retries": 10,
       "redeliveryAttempts": 3,
       "redeliveryMinInterval": 1,
       "redeliveryMaxInterval": 2440,
       "redeliveryDelta": 5
     }
   ```
4. Update the key values as desired.
5. Save and close the file.
   The updated settings will be applied when the Meridium Policy Trigger service is stopped and restarted.

Configure the Time Limit for Policy Execution

About This Task

The Policy Execution Service limits the amount of time allocated to execute each policy instance. This ensures that the Policy Execution Service queue is not backlogged when a poorly designed policy takes too long to execute. If a policy execution is canceled as a result of the time limit, an error message appears in the policy execution history indicating that the time limit was exceeded. By default, the policy execution time limit is set to 15 minutes per policy instance. The minimum time limit is 1 minute, and the maximum time limit is 1 hour. This topic describes how to modify the Policy Execution Service configuration to change the time limit for policy execution.

Procedure

1. On the GE Digital APM Server, access the folder that contains the Policy Execution Service files.

   Note: If you have installed GE Digital APM in the default location, you can locate the folder in the following directory:

   `C:\Program Files\Meridium\ApplicationServer\policy-execution`
2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).
3. In the file, locate the following text:

   ```
   "PolicyExecutionTimeoutMs": 900000
   ```

4. Replace `900000` with the time limit value in milliseconds, that you want to apply to policy executions.

   Note: The value you enter should be between the minimum time limit of 60000 milliseconds (that is, 1 minute) and the maximum time limit of 3600000 milliseconds (that is, 1 hour).

5. Save and close the file.
   The modified settings are applied when the Policy Execution Service is restarted. If the execution time of a policy instance exceeds the time limit that you have specified, the execution is canceled, and an error message is added to the policy execution history.

6. On the GE Digital APM Server, access the folder that contains the Meridium configuration files.

   Note: If you have installed GE Digital APM in the default location, you can locate the folder in the following directory:

   `C:\Program Files\Meridium`

7. Go to `C:\Program Files\Meridium\ApplicationServer\api`.

8. Access the `appsettings` file in an application that can be used to modify JSON files (for example, Notepad++).

9. Repeat steps 3 through 5.
   The modified settings are applied when Meridium Policy Execution service is stopped and restarted on each policy execution server and IIS is reset on the GE Digital APM Server.

Configure Execution Time Out Value for Math Node

About This Task

If the execution of a Math node in a policy takes a very long time, the execution times out after a pre-defined duration. By default, the execution times out after 1 minute. However, you can configure the interval after which the execution must time out for the Math node.

Procedure

1. On the Policy Execution Server, go to `C:\Program Files\Meridium\ApplicationServer\policy-execution`.

2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).

3. In the file, locate the following text:

   ```
   "MathNodeExecutionTimeout": 60000
   ```

4. Replace `60000` with the interval value in milliseconds at which the execution of the Math node must time out.

5. Save and close the file.

6. On the GE Digital APM Server, go to `C:\Program Files\Meridium\ApplicationServer\api`.

7. Access the `appsettings` file in an application that can be used to modify JSON files (for example, Notepad++).

8. Repeat steps 3 through 5.
   The updated settings will be applied when the Policy Execution Service is stopped and restarted on the Policy Execution Server and IIS is reset on the GE Digital APM Server.

Configure the Default Historical Readings Time Range for the OT Connect Tag node

About This Task

During policy execution, if a specific time range to retrieve the historical data for the OT Connect Tag node cannot be determined. For example, if there is no collection filter applied to the Historical Readings output from the node, by default, two years of data will be added. However, you can change the default time range by modifying the settings on the Policy Execution Server and GE Digital APM Server.

Procedure

1. On the Policy Execution Server, go to `C:\Program Files\Meridium\ApplicationServer\policy-execution`.
2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example; Notepad++).
3. In the file, locate the following text:

   ```
   "DefaultHdaTimeRangeYrs": 2
   ```

4. Replace `2` with the number of years for which you want to retrieve the historical data of the OT Connect Tag node.
5. On the GE Digital APM Server, go to `C:\Program Files\Meridium\ApplicationServer\api`.
6. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).
7. Repeat steps 3 through 5.
   The updated settings will be applied when the Policy Execution Service is restarted on the Policy Execution Server and IIS is reset on the GE Digital APM Server.

Configure Alternative Query for the Policy Designer Overview Page

About This Task

To optimize the performance of the **Policy Designer Overview** page in the systems with a large volume of policy execution history records, the Policies tab displays a simplified view which does not display the latest policy execution results. If you want to see the latest results in the Policies list, you can configure the **Policy Designer Overview** page to use the alternative query (Policy Overview – Policies Alternate Query) that is provided in the GE Digital APM Catalog.

Note: When you configure an alternative query for **Policy Designer Overview** page, you might face some performance issues.

Procedure

1. Access GE Digital APM using the super user account.
2. Access the **Catalog** page.
3. In the **Catalog** section, select **Public** > **Meridium** > **Modules** > **Policy Manager** > **Queries**.
   The **Queries** workspace appears, displaying the catalog items of the Queries folder in a table.
4. Select the check box corresponding to the Policy Overview – Policies query.
5. In the same row, select ⚙.
   The **Catalog Item Properties** window appears, displaying the properties of the Policy Overview – Policies query.

6. In the **Name** box, modify the value to rename the query.

7. Select **Done**.
   The Policy Overview – Policies query is renamed.

8. Select the check box corresponding to the alternative query (Policy Overview – Policies Alternate Query).

9. In the same row, select ⚙.
   The **Catalog Item Properties** window appears, displaying the properties of the alternative query.

10. In the **Name** box, delete the existing value, and then enter `Policy Overview – Policies`.

11. Select **Done**.
    The alternative query is configured for the **Policy Designer Overview** page.

Configure the SubPolicy Node for Policy Execution

About This Task

If the policies contain recursive sub policies in them, the policy does not execute. If the sub policy nesting is more than 10 levels, the policy does not get executed. This topic describes how to modify the Policy Execution Service configuration to change the recursion limit for policy execution.

.

Procedure

1. On the GE Digital APM Server, access the folder that contains the Policy Execution Service files.

   Note: If you have installed GE Digital APM in the default location, you can locate the folder in the following directory:

   `C:\Program Files\Meridium\ApplicationServer\policy-execution`

2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).

3. In the file, locate the following text:

   ```
   "MaxSubPolicyDepth": 10
   ```

4. Replace `10` with the MaxSubPolicyDepth that you want to apply to policy executions.

5. Save and close the file.
   The modified settings are applied when the Policy Execution Service is restarted. If the execution of a sub policy instance exceeds 10, the execution is canceled, and an error message is added to the execution log and execution history.

6. On the GE Digital APM Server, access the folder that contains the Meridium configuration files.

   Note: If you have installed GE Digital APM in the default location, you can locate the folder in the following directory:

   `C:\Program Files\Meridium`

7. Go to `C:\Program Files\Meridium\ApplicationServer\api`.

8. Access the `appsettings` file in an application that can be used to modify JSON files (for example, Notepad++).

9. Repeat steps 3 through 5.
   The modified settings are applied when Meridium Policy Execution service is stopped and restarted on each policy execution server and IIS is reset on the GE Digital APM Server.

Configure Policy Reference Clean Up Batch Size

About This Task

When policies and policy instances are inserted, modified or deleted, this may result in changes to very large numbers of related records. In order to optimize the performance for the end user, the related record clean-up is completed in batches by a background task. You can configure the batch size and the frequency for this task. The batch size must be less than 1000 in order to avoid database table locks.

Procedure

1. On the GE Digital APM Server, access the folder that contains the Policy Execution Service files.

   Note: If you have installed GE Digital APM in the default location, you can locate the folder in `C:\Program Files\Meridium\ApplicationServer\policy-execution`.
2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).
3. In the file, locate the following text:

   ```
   "PolicyRefCleanupBatchSize": 500,
   "PolicyRefCleanUpFreqSeconds": 15,
   ```

4. Update the key values as desired.
5. Save and close the file.
   The updated settings will be applied when the Meridium Policy Execution service is stopped and restarted.

Production Loss Analysis Deployment

Deploy 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 system architecture.

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

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

Step	Task	Notes
3	Change the default currency symbol.	This step is optional. By default, the currency symbol is set to $ and appears in the following places: • Default Margin field on the Production Profile datasheet. • **Production Summary** workspace.
4	Define all products.	This step is required. You must define all products whose production you plan to track using PLA. Each product is stored in a Product record.
5	Define Production Units.	This step is required. You must identify the Production Units that produce the products you defined in the previous task. A single product can be produced by more than one Production Unit. A single Production Unit can also produce more than one product. Each Production Unit is stored in a Production Unit record, which can be linked to an existing Functional Location record that contains detailed information about the Production Unit.
6	Define Production Profiles.	This step is required. For each Production Unit that you defined in the previous step, you must identify all the products that it produces and information about those products, such as the maximum demonstrated rate of production and the amount of profit one of those products yields. The combination of data about a product and the corresponding Production Unit is the Production Profile for that Production Unit. A Production Unit will have one Production Profile for each product it produces. Each Production Profile is stored in a Production Profile record, which is linked to the corresponding Product record and Production Unit record.

Step	Task	Notes
7	Define Production Event Codes.	The baseline GE Digital APM database contains Production Event Code records that define a set of basic production event codes. Therefore, this step is required only if you do not want to use the baseline production event codes or if you want to use codes in addition to those that are provided.
		You must use Production Event Codes to categorize the types of events that can cause you to produce less than the maximum sustained capacity amount. Production Event Codes define the cause of lost production and answer the question: Why are we losing production? You can also group the types of events by structuring them in a hierarchy. For example, you might group event types into planned and unplanned, where planned events are events such as maintenance down days or employee holidays, and unplanned events are events such as equipment failures or natural disasters (e.g., floods or hurricanes).
		Each production event code will be stored in a separate Production Event Code record.
8	Define Impact Codes.	The baseline GE Digital APM database contains Impact Code records that define a set of basic Impact Codes. Therefore, this step is required only if you do not want to use the baseline Impact Codes or if you want to use codes in addition to those that are provided.
9	Define OEE Codes.	The baseline GE Digital APM database contains OEE Code records that define a set of basic OEE Codes. Therefore, this step is required only if you do not want to use the baseline OEE Codes or if you want to use codes in addition to those that are provided. For non-baseline codes to be included in the OEE Metric View, however, they must be children of the baseline parent codes.

Step	Task	Notes
10	Configure PLA for OT Connect integration: 1. Deploy OT Connect. **Note:** Deploying OT Connect requires the OT Connect license. 2. Configure the PLA Service policy. 3. Link Production Profile records to Policy Instance ID records.	This step is required if you want to use the integration between PLA and the OT Connect feature where Production Data records are created automatically using the baseline PLA Service policy in Policy Designer.
11	Replace the Top 10 Bad Actors query for the **PLA Overview** page.	This step is optional. The Top 10 Bad Actors query is used by GE Digital APM to populate the **Top 10 Bad Actors** graph on the **PLA Overview** page. In some databases, when viewing this graph, you may receive an error that prevents the graph from populating correctly. If this error occurs, replace the Top 10 Bad Actors query.

Reliability Analytics Deployment

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 system architecture.

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

Step	Task	Notes
1	Review the following data models to determine which relationship definitions you will need to modify to include your custom equipment and location families: • Probability Distribution Analysis Data Model • Production Analysis Data Model • Reliability Automation Rule Data Model • Reliability Distribution Analysis Data Model • Reliability Growth Analysis Data Model • Spares Analysis Data Model • System Reliability Analysis Data Model Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to one or more Reliability Analytics Security Groups and Roles.	This step is required.
3	Ensure that the Meridium Simulation Service is installed and running.	If the basic GE Digital APM system architecture is already installed, the Meridium Simulation Service is automatically installed and run. **Note:** Reliability Simulation service is required to execute the tasks that take a long time. APM Client (browser) will keep polling the APM Server to check the progress of the such tasks and report the progress to the end user in the background.
4	Configure ActiveMQ Settings for the Simulation Service on page 142.	This step is optional. Default values exist for the concurrency limit, number of retries, number of threads, and the time limit of the Simulation Service. You can change these values as needed.

Configure ActiveMQ Settings for the Simulation Service

Before You Begin

Ensure that the Simulation Service is running. If the basic GE Digital APM system architecture is already installed, the Simulation Service is automatically installed and run.

About This Task

The Simulation Service processes simulation requests. It is required to execute the tasks that take a long time. GE Digital APM Client (browser) will keep polling the GE Digital APM Server to check the progress of the such tasks and report the progress to the end user in the background.

This topic describes how to chance the concurrency limit, number of retries, number of threads, and the time limit of the Simulation Service.

Procedure

1. On the GE Digital APM server, access the folder that contains the Simulation Service files. If you have installed GE Digital APM in the default location, the files are located in `C:\Program Files\Meridium\ApplicationServer\SimulationService`.
2. Access the `appsettings.json` file.
3. As needed, modify values of the following parameters.

Parameter	Description	Notes
ConcurrencyLimit	The maximum number of messages to be consumed concurrently.	The default value is 3. You can enter a number between 1 and 3.
Retries	The number of times to retry sending messages to ActiveMQ in case of a failure.	The default value is 1.
NumberOfThreadsPerSimulation	The number of threads to run per simulation.	The default value is 1.
TimeLimitInMinutes	The time limit, in minutes, after which the simulation ends.	The default value is 240. You can enter a value up to 240.

```
"ReliabilitySimulation":{
    "ConcurrencyLimit": 2,
    "Retries": 10
    "NumberOfThreadsPerSimulation": 1,
     "TimeLimitInMinutes": 240
}
```

4. Save and close the file.
5. Restart the Simulation Service.
   The Simulation Service is configured.

Reliability Centered Maintenance Deployment

Deploy 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 system architecture.

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

Step	Task	Notes
1	Assign Security Users to one or more of the 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.

Reports Deployment

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 system architecture.

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

Step	Task	Notes
1	Install the APM Reports Designer on page 144.	This step is required.
2	Set Up the APM Report Designer on page 145.	This step is required.

Install the APM Reports Designer

Before You Begin

• Install one of the following versions of Microsoft Visual Studio and the corresponding version of Microsoft SQL Server Data Tools (SSDT):

Visual Studio Version	SSDT Version
Microsoft Visual Studio 2017	Microsoft SQL Server Data Tools (SSDT) - Business Intelligence for Microsoft Visual Studio 2017 (15.8.0)
Microsoft Visual Studio 2019	Microsoft SQL Server Data Tools (SSDT) - Business Intelligence for Microsoft Visual Studio 2019

◦ If you install SSDT for Microsoft Visual Studio 2019, install Microsoft Reporting Service Projects (VSIX 2.6.2). For more information on how to install Microsoft Reporting Services Projects (VSIX 2.6.2), refer to the Microsoft SSDT documentation.

Note: The following versions of SSDT are supported with Microsoft SQL Server 2016:

◦ 2017 (15.8.0)
◦ 2019

Procedure

1. On the machine that will serve as the APM Reports Designer, access the GE Digital APM Distribution package, and then navigate to the `Admin` folder.
2. Run `Setup.exe`.
   The **Meridium Admin - InstallShield Wizard** window appears.
3. Select **Next**.
   The **License Agreement** window appears.
4. Read the License Agreement and, if you agree, select the **I accept the terms of the license agreement** check box, and then select **Next**.
   The **Select Installation Location** window appears.
5. Select **Next** to accept the default location.
   The **Select the features you want to install** window appears.
6. Select **SSRS Data Processing extension for Visual Studio**, and then select **Next**.
   The **Complete the Installation** window appears.
7. Select **Install**.
   The **Setup Status** window appears, displaying a progress bar that shows the progress of the installation process.

   When the SSRS Data Processing extension for Visual Studio is installed, a message appears, indicating that the installation is complete.
8. Select **Finish**.
   The **Meridium Admin - InstallShield Wizard** window is closed.
9. As described in the following table, navigate to the paths corresponding to the Microsoft Visual Studio version installed in your system.

Visual Studio Version	Path
Microsoft Visual Studio 2017	`C:\Program Files (x86)\Microsoft Visual Studio\2017\Professional \Common7\IDE\CommonExtensions \Microsoft\SSRS`
Microsoft Visual Studio 2019	`C:\Program Files (x86)\Microsoft Visual Studio\2019\Professional \Common7\IDE\CommonExtensions \Microsoft\SSRS`

10. Open the `RSReportDesigner.config` file using a text editor (for example, Notepad).
11. Locate the following code in the configuration file, and then replace *{meridiumserver}* with the name of the GE Digital APM server: `<ServerUrl>http://{meridiumserver}/meridium/api/</ServerUrl>`
12. Save the configuration file.

Results

The APM Report Designer is installed.

Set Up the APM Report Designer

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

Before You Begin

Procedure

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/v1
   ```

   The APM Report Designer setup is complete.

Risk Based Inspection 580 Deployment

Deploy 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 system architecture.

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

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

Step	Task	Notes
3	On the GE Digital APM Server, using Configuration Manager, import the following files • 101_MI_STMPCNFG.xml • 102_MI_STRMAPP.xml These files are located in the following folder: `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks`. You must extract the `4030000` archive from the `MI_DB_MASTER_4300000` archive.	This step is required only if you are deploying Risk Based Inspection on an existing GE Digital APM database. These data mapping records are used in RBI 581 and Risk Based Inspection. This will overwrite the existing Strategy Mapping Composite Entities. If you have customized your Strategy Mapping Content, you should instead follow the instructions in Article 000029119.
4	Assign the following types of RBI users to at least one TM Security Group: • Users who are responsible for completing the steps necessary to use TM Analysis values to calculate RBI 580 corrosion rates. • Users who should be able to navigate to TM via RBI 580.	This step is required only if you are using the integration between the RBI and Thickness Monitoring modules.
5	Modify the MI_DEGRADATION_MECHANISM_TYPES System Code Table.	This step is required only if you want to create your own Potential Degradation Mechanisms records.
6	Select the **Recommendation Creation Enabled** check box in the **Global Preferences** workspace.	This step is required only if you do not want to create Recommendations in RBI, but want to use the Asset Strategy Management (ASM) module to recommend actions and manage mitigated risk. This check box is selected by default.
7	Select the **Enable Recommendations to be Generated at Created State** check box in the **Global Preferences** workspace.	This step is required only if you want to create RBI Recommendation records while RBI Analysis records are in the Created state. This check box is cleared by default.
8	Select the **Allow Override of Calculated Unmitigated Risk Values** check box in the **Global Preferences** workspace.	This step is required only if you want to override the calculated values of unmitigated risk because you use a custom calculator. This check box is cleared by default.
9	Select the **Consider Half-Life when Determining Inspection Task Interval** check box in the **Global Preferences** workspace.	This step is required only if you want additional values such as half-life to determine the inspection task interval. This check box is cleared by default.

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.
15	Configure Risk Based Inspection ActiveMQ settings for MIExecution Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
16	Ensure that the Meridium MIExecution Service is installed and running.	If the basic GE Digital APM system architecture is already installed, the Meridium MIExecution Service is automatically installed, and the service runs automatically.
17	Add RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you want to use additional RBI Component type records that are not provided in the baseline GE Digital APM database.

Configure Risk Based Inspection ActiveMQ settings for MIExecution Service

The MIExecution Service,on each GE Digital APM Server serves RBI, Inspection and Thickness Monitoring module queues. This service is configured to use a single shared ActiveMQ queue service across APM. Available queue configuration options include retries and concurrency limit.

Procedure

1. On the GE Digital APM Server, access the folder that contains the MIExecution Service files.

   Note: If you have installed GE Digital APM in the default location, you can locate the folder in `C:\Program Files\Meridium\ApplicationServer\mi-execution`

2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).
3. In the file, locate the following text:

```
"Queue_Config": {
        "Queues": [
            {
              "Name": "MI_RBI_Queue",
              "ConcurrencyLimit": 100,
              "Retries": 5,
                  "LimitPerTenantRequired": true
            }
        ]
            }
```

Note: `ConcurrencyLimit` indicates the maximum number of messages that will be consumed concurrently. `Retries` indicates the number of times it retries to send the messages to ActiveMQ if it fails. `LimitPerTenantRequired` indicates whether Maximum Concurrency limit per Tenant is specified in scheduler service for the queue.

4. Update the key values as desired.
5. Save and close the file.
   The updated settings will be applied when the MIExecution Service is stopped and restarted.

Add RBI Component Types

Procedure

1. Log in to GE Digital APM as an administrator.
2. Go to **Admin > Configuration Manager > System Codes and Tables**.
3. Search for MI RBI COMPONENT TYPES.
4. In the System Code section, select ＋.
   The **Create System Code** window appears.
5. Add the RBI Component Types to the system code table.
6. Select **Save**.
7. Log out of GE Digital APM and log in.
8. To add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table, perform the following steps:

   a) Select , and enter EquipmentTypes.
      A blank EquipmentTypes datasheet appears.
   b) In the **CriticalityItemType** box, select the existing RBI Component Type that you have added.
   c) Enter values in the required boxes, and then select to save the record.

Risk Based Inspection 581 Deployment

Deploy 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 system architecture.

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

Step	Task	Notes
1	Review and complete the steps required for deploying R Scripts.	This step is required. This will install R Scripts and other third-party software that is used by the RBI 581 module.
2	Review the RBI data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
3	Assign Security Users to one or more of the Security Roles used in RBI.	This step is required.
4	Add the following types of RBI 581 users to at least one TM Security Group: • Users who are responsible for completing the steps necessary to use TM Analysis values to calculate RBI 581 corrosion rates. • Users who should be able to navigate to TM via RBI 581.	This step is required only if you are using the integration between the RBI 581 and Thickness Monitoring modules
5	Select the **Is a Unit?** check box in Functional Location records that represent units in your facility.	This step is required, and marks Functional Location records as Process Units.
6	Using the Belongs to a Unit relationship, link Equipment records to Functional Location records representing units to which that equipment belongs (i.e., the **Is a Unit?** check box is selected).	This step is optional.
7	Add the **RBI-581** tab to the datasheet of the following families: • Criticality RBI Component - Cylindrical Shell • Criticality RBI Component - Exchanger Bundle • Criticality RBI Component - Exchanger Header • Criticality RBI Component - Exchanger Tube • Criticality RBI Component - Piping • Criticality RBI Component - Tank Bottom	This step is required only for families for which you have customized the datasheet.

Step	Task	Notes
8	Using Configuration Management, import the following files located in the `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks` folder: • `06_MI_DATA_GRP.xml` • `07_MI_MPPG_QRY.xml` • `08_MI_CLMND_PR.xml`	This step is required only if you are deploying RBI 581 on an existing database. This will create data mappings between families in RBI 581. **Important:** These data mapping records are used in RBI 581 and Risk Based Inspection. After you complete this step, all existing changes to data mapping in the RBI 581 and Risk Based Inspection will be reverted to baseline. All customization for data mappings will be lost. Do not perform this step unless your organization will be satisfied with the baseline data mappings, or you are prepared to customize the records again following the execution of the script.
9	Using Configuration Manager, import the following files located in the `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\20_IEU\50_Other\2_RecordsLinks` folder: • `101_MI_STMPCNFG.xml` • `102_MI_STRMAPP.xml`	This step is required. This will update the RBI Strategy Mapping Composite entities, overwriting the existing ones.
10	Update Risk Matrix Mappings and Policies to account for overridden financial consequence for RBI 581 Risk Analyses.	The Operations Category on the Risk Matrix does not account for overridden financial consequence for RBI 581 Risk Analyses. If you are using this feature, you are required to update your Risk Matrix Mappings and Policies by following Article 000035710.

Step	Task	Notes
11	Using Configuration Manager, import the `MI_REPFLUID_581.xml` file located in the `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\_IEU_ManualImports` folder.	This step is required to import the Representative Fluids that are used in RBI 581. If you want to use only RBI 581 (i.e., you do not want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 representative fluids. If you want to verify that the file has been imported successfully, run the following query: ``` SELECT Count([MI_REPFLUID]. [MI_REPFLUID_FLUID_C]) "Fluid" FROM [MI_REPFLUID] ``` This will return a list of 30 records. If you want to use both RBI 580 and RBI 581, import these files without deleting the existing content. In this case, the aforementioned query returns a list of 111 records.
12	Using Configuration Manager, import the `MI_CMT_FLE0.xml` file located in the `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\_IEU_ManualImports` folder.	This step is required to import the Component Damage Flammable records. If you want to use only RBI 581 (i.e., you do not want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Component Damage Flammable records. This will ensure that the content in this table is as per API 3rd Edition table 4.8. If you want to verify that the file has been imported successfully, run the following query: ``` SELECT Count([MI_CMT_FLE0]. [MI_CMT_FLE0_FLUID_C]) "Fluid" FROM [MI_CMT_FLE0] ``` This will return a list of 64 records. If you want to use both RBI 580 and RBI 581, import these files without deleting the existing content.

Step	Task	Notes
13	Add RBI Component Types to the MI RBI COMPONENT TYPES system code table.	This step is required only if you want to use additional RBI Component type records that are not provided in the baseline GE Digital APM database.
14	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.	This step is required to import the Fluid Viscosity records. If you want to use only RBI 581 (i.e., you do not want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Fluid Viscosity tables. This will ensure that the content in this table is as per API 3rd Edition table 6.1. If you want to verify that the file has been imported successfully, run the following query: ```SELECT Count([MI_FLD_VSCY].[MI_FLD_VSCY_FLUID_C]) "Fluid" FROM [MI_FLD_VSCY]``` This will return a list of 5 records. If you want to use both RBI 580 and RBI 581, import these files without deleting the existing content. In this case, the aforementioned query returns a list of 10 records.

Step	Task	Notes
15	Using Configuration Manager, import the `MI_PRL_CNS0.xml` file located in the `C:\Meridium\DbUpg\MI_DB_MASTER_4030000\4030000\_IEU_ManualImports` folder.	This step is required to import the Personal Injury Flammable CE Constants records. If you want to use only RBI 581 (i.e., you do not want to use RBI 580), you must delete the existing content, and then import this file. This will remove all the information related to the RBI 580 Fluid Viscosity records. This will ensure that the content in this table is as per API 3rd Edition table 4.9. If you want to verify that the file has been imported successfully, run the following query: ```SELECT Count([MI_PRL_CNS0].[MI_PRL_CNS0_FLUID_C]) "Fluid" FROM [MI_PRL_CNS0]``` This will return a list of 62 records. If you want to use both RBI 580 and RBI 581, import these files without deleting the existing content. In this case, the aforementioned query returns a list of 62 records.
16	On the GE Digital APM Server, restart Redis.	This step is required, and has to be performed after you complete all the previous steps.
17	On the GE Digital APM Server, reset IIS.	This step is required, and has to be performed after you complete all the previous steps.
18	Configure Risk Based Inspection ActiveMQ settings for MIExecution Service.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
19	Ensure that the Meridium MIExecution Service is installed and running.	If the basic GE Digital APM system architecture is already installed, the Meridium MIExecution Service is automatically installed, and the service runs automatically.

Add the RBI-581 Tab to Criticality RBI Component Datasheets

Before You Begin

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

154

If you have customized the datasheet for one or more of the Criticality RBI Components, after activating the RBI 581 license, you must perform the following procedure to add the **RBI-581** section to those customized datasheets. The following table indicates the fields that must appear on each datasheet.

Caption	Field ID	Criticality RBI Component - Cylindrical Shell	Criticality RBI Component - Exchanger Bundle	Criticality RBI Component - Exchanger Header	Criticality RBI Component - Exchanger Tube	Criticality RBI Component - Piping	Criticality RBI Component - Tank Bottom
Base Material	Base MaterialMI_CCRBICOM_BASE_MATER_C	✓	✓	✓	✓	✓	✓
Cladding Material	MI_CCRBICOM_CLADDING_MATERIL_C	✓	✓	✓	✓	✓	✓
Cladding Present	MI_CCRBICOM_CLADDING_PRESENT_L	✓	✓	✓	✓	✓	✓
CM Corrosion Rate	MI_CCRBICOM_CM_COR_RT_C	✓	✓	✓	✓	✓	✓
Coefficient Y Material	MI_CCRBICOM_COEFFICNT_Y_MTRL_C	✗	✗	✗	✗	✓	✗
Corrosion Allow	MI_RBICOMPO_CORRO_ALLOW_N	✓	✓	✓	✓	✓	✓
Detection System	MI_CCRBICOM_DETECTION_SYSTEM_C	✓	✓	✓	✓	✓	✓
Fluid Velocity	MI_CCRBICOM_FLUID_VELOCITY_N	✓	✓	✓	✓	✓	✓
Furnished Cladding Thk	MI_CCRBICOM_FRNSHD_CLDDG_THK_N	✓	✓	✓	✓	✓	✓
Geometry Type	MI_CCRBICOM_GEOMETRY_TYPE_C	✓	✓	✓	✓	✓	✓
GFF Component Type	MI_CCRBICOM_GFF_COMPO_TYPE_CHR	✓	✓	✓	✓	✓	✓
Has Release Prevention Barrier?	MI_CCRBICTB_HAS_RELEA_PREVE_F	✗	✗	✗	✗	✗	✓

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_RBICOMPO_IS_INTRU_CHR	✓	✓	✓	✓	✓	✓
Isolation System	MI_CCRBICOM_ISOLA_SYSTE_CHR	✓	✓	✓	✓	✓	✓
Liner Present	MI_CCRBICOM_LINER_PRESE_CHR	✓	✓	✓	✓	✓	✓
Liner Type	MI_CCRBICOM_LINER_TP_C	✓	✓	✓	✓	✓	✓
Minimum Structural Thickness	MI_CCRBICOM_MNMM_STRCTRL_THS_N	✓	✓	✓	✓	✓	✓
Mitigation System	MI_CCRBICOM_MITIGATION_SYSTM_C	✓	✓	✓	✓	✓	✓
Percent Liquid Volume	MI_RBICOMPO_PER_LIQ_VOL_N	✓	✓	✓	✓	✓	✓
pH of Water	MI_CCRBICOM_PH_OF_WATER_N	✓	✓	✓	✓	✓	✓
Specified Tmin	MI_CCRBICOM_SPECIFIED_TMIN_N	✓	✓	✓	✓	✓	✓
Total Acid Number	MI_CCRBICOM_TOTAL_ACID_NUMBR_N	✓	✓	✓	✓	✓	✓

Procedure

1. Access the Family Management page.
2. In the left section, select the Criticality RBI Component whose datasheet you want to modify.
   In the workspace, the corresponding Criticality RBI Component family appears, displaying the **Information** section.
3. In the workspace, select the **Datasheets** tab, and then select **Manage Datasheets**.
   The **Datasheet Builder** page appears, displaying the datasheet layout of the selected Criticality RBI Component family.
4. In the upper-right corner of the page, select
   A **new section** tab appears at the top of the workspace, displaying a blank section.

5. On the new tab, rename new section to RBI-581.

6. In the **RBI-581** section, select ▤.

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

8. In the left pane, locate a field that corresponds to the table at the beginning of this topic, and then add that field into the empty cell in the **Value(s)** column using the drag-and-drop method.
   In the cell, an input box that corresponds to the selected field appears.

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

10. In the upper-right corner of the page, select ≡+.
    In the **RBI-581** section, in the table, a new row appears.

11. Repeat steps 8 to 10 for each of the fields specified in the table at the beginning of this topic.

12. In the upper-right corner of the page, select **Save**.
    The datasheet for the Criticality RBI Component that you selected in step 2 is saved, and the **RBI-581** tab appears on the selected Criticality RBI Component datasheet.

Add RBI Component Types

Procedure

1. Log in to GE Digital APM as an administrator.

2. Go to **Admin > Configuration Manager > System Codes and Tables**.

3. Search for MI RBI COMPONENT TYPES.

4. In the System Code section, select ✛.
   The **Create System Code** window appears.

5. Add the RBI Component Types to the system code table.

6. Select **Save**.

7. Log out of GE Digital APM and log in.

8. To add existing RBI Component Types to the MI RBI COMPONENT TYPES system code table, perform the following steps:

   a) Select 🗐+, and enter EquipmentTypes.
      A blank EquipmentTypes datasheet appears.

   b) In the **CriticalityItemType** box, select the existing RBI Component Type that you have added.

   c) Enter values in the required boxes, and then select 💾 to save the record.

Configure Risk Based Inspection ActiveMQ settings for MIExecution Service

The MIExecution Service,on each GE Digital APM Server serves RBI, Inspection and Thickness Monitoring module queues. This service is configured to use a single shared ActiveMQ queue service across APM. Available queue configuration options include retries and concurrency limit.

Procedure

1. On the GE Digital APM Server, access the folder that contains the MIExecution Service files.

   Note: If you have installed GE Digital APM in the default location, you can locate the folder in
   `C:\Program Files\Meridium\ApplicationServer\mi-execution`

2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).
3. In the file, locate the following text:

```
"Queue_Config": {
        "Queues": [
            {
              "Name": "MI_RBI_Queue",
              "ConcurrencyLimit": 100,
              "Retries": 5,
                "LimitPerTenantRequired": true
            }
        ]
            }
```

Note: `ConcurrencyLimit` indicates the maximum number of messages that will be consumed concurrently. `Retries` indicates the number of times it retries to send the messages to ActiveMQ if it fails. `LimitPerTenantRequired` indicates whether Maximum Concurrency limit per Tenant is specified in scheduler service for the queue.

4. Update the key values as desired.
5. Save and close the file.
   The updated settings will be applied when the MIExecution Service is stopped and restarted.

Root Cause Analysis Deployment

Deploy 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 system architecture.

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

Step	Task	Notes
1	Review the RCA data model to determine which relationship definitions you will need to modify to include your custom equipment and location families. Modify any relationship definitions as required.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to one or more of the RCA Security Groups and Roles.	This step is required. Users will not be able to access Root Cause Analysis unless they belong to an RCA Security Group.
3	Specify the Team Charter after you create a new Root Cause Analysis record.	This step is optional. A default Team Charter exists in the baseline GE Digital APM database. You can select the default Team Charter or define your own.

Step	Task	Notes
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.
5	Configure ActiveMQ for the Reliability Execution Service on page 159.	This step is optional. Default values exist for the concurrency limit and number of retries for the Reliability Execution Service. You can change these values as needed.

Configure ActiveMQ for the Reliability Execution Service

About This Task

The Reliability Execution Service processes RCA email notification requests. The service uses a single ActiveMQ queue service across GE Digital APM.

This topic describes how to change the concurrency limit and number of retries for the Reliability Execution Service.

Procedure

1. On the GE Digital APM server, access the folder that contains the Reliability Execution Service files. If you have installed GE Digital APM in the default location, the files are located in `C:\Program Files \Meridium\ApplicationServer\ReliabilityExecution`.
2. Access the `appsettings.json` file.
3. As needed, modify values of the following parameters.

Parameter	Description	Notes
ConcurrencyLimit	The maximum number of messages to be consumed concurrently.	The default value is 2. You can enter 1 or 2.
Retries	The number of times to retry sending messages to ActiveMQ in case of a failure.	The default value is 10. You can enter a number between 1 and 10.

```
"Queue_Config":{
    "Queues": [
        {
            "Name": "RCA_Alert_Queue",
            "IsCancelAllowed": false,
            "ConcurrencyLimit": 2,
            "Retries": 10
        }
    ]
}
```

4. Save and close the file.
5. Restart the Reliability Execution Service.
   The Reliability Execution Service is configured.

Rounds Designer Deployment

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 system architecture.

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

Step	Task	Notes
1	Review the Rounds data model to determine which relationship definitions you will need to modify to include your custom asset families. Modify any relationship definitions as needed. For example, if you have created a new asset family, create a relationship definition as follows: • Relationship family: Has Checkpoint • Predecessor: The asset family • Successor: The Measurement Location family or Lubrication Requirement family • Cardinality: One to Many	This step is required only if you have asset data in families outside of the baseline Equipment and Functional Location families.
2	Assign Security Users to the following Rounds Security Groups and Roles: • MI Operator Rounds Administrator • MI Operator Rounds Mobile User	This step is required. **Note:** The MAPM Security Group that has been provided with 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.
3	Manage Measurement Location Template mappings.	This step is required only if you added fields to the Measurement Location Template family via Configuration Manager.
4	Install the GE Digital APM application on the mobile device that you plan to use for data collection.	This step is required only if you will use a mobile device for data collection.
5	Set the local time zone on the mobile device that you will use for data collection, typically the user time zone.	This step is required only if you will use a mobile device for data collection.
6	Set up the Scheduled Compliance task.	This step is required. The scheduled compliance task should be configured to start as soon as the Rounds module is deployed and set to run continuously as long as Rounds in use.

Step	Task	Notes
7	As needed, modify your server timeout settings.	This step is only required if you want to process large amounts of data in a single transaction (for example, if you collect a large number of readings for a Route or several Routes and then attempt to upload all of those readings simultaneously). If you need to modify server timeout settings, follow the instructions in Article 000032427.
8	Configure automatic synchronization of Measurement Location and Measurement Location Template Records with Allowable Values.	This step is optional.
9	Grant permissions to the Everyone group to view records that belong to the Site Reference family.	This step is required.

Manage the Measurement Location Template Mappings

About This Task

The Measurement Location Template family and the Measurement Location family are provided as part of the baseline Rounds data model. If you create a Measurement Location Template in the 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 complete the following steps.

Procedure

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

   Note: For more information on Measurement Location templates, refer the Family Management documentation.

Rounds Security Groups

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

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

Security Group	Roles
MI Operator Rounds Administrator	MI Health Admin
MI Operator Rounds Mobile User	MI Health Admin MI Health Power MI Health User
MI Lubrication Management Administrator	MI Health Admin
MI Lubrication Management User	MI Health Admin MI Health Power MI Health User
MI Rounds Designer Viewer	MI APM Viewer
MI Rounds Pro Administrator	MI Rounds-Pro Admin
MI Rounds Pro Mobile User	Mi Rounds-Pro User

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

Note:

- Users who should be able to run Rounds queries to view the Rounds data after it has been uploaded from a tablet or a mobile device will need a combination of the privileges listed in the following table, depending on the families included in the queries they want to run.
- To create work requests via Operator Rounds Recommendations, users must also have the appropriate privileges to create EAM notifications (e.g., be a member of the MI SAP Interface User Security Group).
- The privileges assigned to the members of the MAPM Security Group, which was provided in the baseline Rounds module in Meridium Enterprise APM V3.6.0, are also assigned to the members of the MI Operator Rounds Mobile User Security Group. We recommend that you use the MI Operator Rounds User Security Group instead of the MAPM Security Group.

Family	MI Operator Rounds Administrator	MI Operator Rounds Mobile User	MAPM Security Group	MI Rounds Designer Viewer	MI Lubrication Management Administrator	MI Lubrication Management User
Entity Families						
Checkpoint Condition	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Checkpoint Task	View, Update, Insert, Delete	View, Update	View, Update	View	View, Update, Insert, Delete	View, Update
Health Indicator	View	View	View	View	View	View
Health Indicator Mapping	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Hierarchy Item Child Definition (Deprecated)	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View

Family	MI Operator Rounds Administrator	MI Operator Rounds Mobile User	MAPM Security Group	MI Rounds Designer Viewer	MI Lubrication Management Administrator	MI Lubrication Management User
Hierarchy Item Definition (Deprecated)	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Lubricant	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Lubrication Component	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Lubrication Management Recommendation	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Lubricant Manufacturer	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Lubrication Method	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Lubrication Requirement	View, Update, Insert, Delete	View, Update	View, Update	View	View, Update, Insert, Delete	View
Lubrication Requirement Template	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Measurement Location	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Measurement Location Template	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
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	MAPM 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
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
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

Family	MI Operator Rounds Administrator	MI Operator Rounds Mobile User	MAPM Security Group	MI Rounds Designer Viewer	MI Lubrication Management Administrator	MI Lubrication Management User
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 Recommen dation	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View, Update, Insert, Delete	View, Update, Insert, Delete
Route Has Checkpoint	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View
Route Has Human Resource	View, Update, Insert, Delete	Insert	Insert	View	View, Update, Insert, Delete	Insert
Template Has Checkpoint	View, Update, Insert, Delete	View	View	View	View, Update, Insert, Delete	View

Rounds Pro Deployment

Deploy Rounds Pro for the First Time

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

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

Step	Task	Notes
1	Review the data model to determine which relationship definitions you will need to modify to include your custom Equipment and Functional Location families. Modify any relationship definitions as needed via Configuration Manager.	This step is required only if you have asset data in families outside of the baseline Equipment and Functional Location families.
2	Assign Security Users to the following Rounds Pro Security Groups: • MI Rounds-Pro Administrator • MI Rounds-Pro Mobile User	This step is required.

Step	Task	Notes
3	Install the Rounds Pro mobile application on the mobile device that you plan to use for data collection.	This step is required only if you will use a mobile device for data collection. For information on installation of Rounds Pro on mobile devices see the following sections: • Install the Rounds Pro Mobile App on an iOS Device • Install the Rounds Pro Mobile App on an Android Device • Install the Rounds Pro Mobile App on a Windows Device
4	Set the local time zone on the mobile device that you will use for data collection, typically the user time zone.	This step is required only if you will use a mobile device for data collection.
6	Configure ActiveMQ settings for Rounds Service on page 166	This step is required.

Configure ActiveMQ settings for Rounds Service

The Rounds Service is responsible for syncing the data between GE Digital APM Server and the Rounds Pro app, it is also responsible to handle the changes on Steps and Step Templates and works with the core scheduling service. Rounds Service should be running on all GE Digital APM Application Servers. Ensure the Rounds Service is Running on all the APM Servers. This service is configured to use a single shared ActiveMQ queue service across APM. Available queue configuration options include retries and concurrency limit. Changes to the following settings are optional.

Procedure

1. On the GE Digital APM Server, access the folder that contains the Rounds Service files.

   Note: If you have installed GE Digital APM in the default location, you can locate the folder in `C:\Program Files\Meridium\ApplicationServer\Rounds-service`.

2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).

3. In the file, locate the following text:

   ```
   "Queue_Config": {
           "Queues": [
             {
               "Name": "ROUNDSPRO_Queue",
               "IsCancelAllowed": false,
               "ConcurrencyLimit": 16,
               "Retries": 100
             }
           ]
         }
   ```

   Note: `ConcurrencyLimit` indicates the maximum number of messages that will be consumed concurrently. `Retries` indicates the number of times it retries to send the messages to ActiveMQ if it fails.

4. Update the key values as desired.

5. Save and close the file.

Results

The updated settings will be applied when the Rounds Service is restarted.

R Scripts Deployment

R Scripts System Requirements

License Requirements

This feature is available with the core GE Digital APM application; no specific license is required.

Additional Components Required

In addition to the basic GE Digital APM system architecture, your system must also contain the following additional components:

- R Server: A machine on which the R Server software is installed. The software requirements of this server are determined by the third-party distributor of the software.

The GE Digital APM testing environment uses the following:

- DeployR Open 8.0.0 with Microsoft DeployR Enterprise 8.0.0 or Microsoft Machine Learning Server 9.2.1 running on Windows servers
- Rserve 1.8-8 with R V4.1.3 running in Docker containers on Linux servers

Install R Server or Machine Learning Server

You can find more information about Microsoft R Server and Machine Learning Server, including required software dependencies and installation instructions, on https://msdn.microsoft.com/en-us/microsoft-r/rserver-install-windows.

Note: The World Wide Web Publishing service must be enabled on the R Server or Machine Learning Server in order to use R scripts in GE Digital APM. If this setting is disabled during the installation of R Server, you must enable it.

Note: Microsoft DeployR 8.0.0 and Microsoft Machine Learning Server are out of support from Microsoft. You may continue to use these R servers with GE Digital APM V5.0.0.0.0 however, GE Digital recommends migrating to open source Rserve and R. R Scripts will no longer support DeployR 8.0.0 or Machine Learning Server in GE Digital APM future releases.

Important: To ensure that the date and time values are handled as expected, the time zone of the Windows server where R Server or Machine Learning Server is installed must be set to UTC.

Install Rserve and R

About Rserve

Rserve is an open-source package that enables TCP/IP connections to R. Details about the Rserve package can be found at http://rforge.net/Rserve/.

Note: GE Digital APM supports only two forms of Rserve authentication (refer to https://github.com/s-u/Rserve/wiki/Security):

- No authentication
- Plaintext password authentication

Install Rserve and R

Rserve and R can be installed on either Windows or Linux platforms; however, Linux is recommended.

Important: To ensure that the date and time values are handled as expected, the time zone of the Docker container running Rserve must be set to UTC.

GE Digital has tested Rserve with R V4.1.3 running in a Docker container, using the images provided by the Rocker project (https://www.rocker-project.org/) as base images. The following sample Docker files can be used to build suitable containers:

SAMPLE MINIMAL DOCKERFILE:

```
FROM rocker/r-ver:4.1.3
# install Rserve
RUN install2.r --error \
    -r https://cran.rstudio.com \
    Rserve && \
    rm -rf /tmp/downloaded_packages/ /tmp/*.rds

ENTRYPOINT R -e "Rserve::run.Rserve()"
```

SAMPLE DOCKERFILE WITH SOME PACKAGES PRE-INSTALLED:

```
FROM rocker/r-ver:4.1.3
# install tidyverse
RUN /rocker_scripts/install_tidyverse.sh

# install tidymodels
RUN install2.r --error --skipinstalled tidymodels && \
    rm -rf /tmp/downloaded_packages

# install RcppArmadillo
RUN install2.r --error \
    -r https://cran.rstudio.com \
    RcppArmadillo && \
    rm -rf /tmp/downloaded_packages/ /tmp/*.rds

# install WeibullR
RUN install2.r --error \
    -r http://R-Forge.R-project.org \
    WeibullR && \
    rm -rf /tmp/downloaded_packages/ /tmp/*.rds

# install survival
RUN install2.r --error \
    -r https://cran.rstudio.com \
    survival && \
    rm -rf /tmp/downloaded_packages/ /tmp/*.rds

# install Rserve
RUN install2.r --error \
    -r https://cran.rstudio.com \
    Rserve && \
    rm -rf /tmp/downloaded_packages/ /tmp/*.rds

ENTRYPOINT R -e "Rserve::run.Rserve()"
```

Deploy R Scripts for the First Time

Before You Begin

After you have installed and configured the basic GE Digital APM system architecture, including the R server of your choice, you will need to perform some configuration steps specifically for R Scripts.

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

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

Results

Step	Task	Notes
1	Ensure that your R Server is configured according to the R Scripts system requirements. For more information, refer to the APM System Requirements documentation.	This step is required.
2	In GE Digital APM, specify the R Server credentials.	This step is required.

Specify R Server Credentials

Before You Begin

You must be a Super User or member of the MI Configuration Role security group to modify the R Server credentials.

Procedure

1. In the **Applications** menu, navigate to **ADMIN** > **Operations Manager** > **Connections**.
   The **Connections** page appears.
2. Select **R Server**.
   The **R Server** workspace appears.
3. In the **R Server Version** box, specify the version of R Server.
4. In the **Server Address** box, enter the URL of the R Server (for example, `http://MyRServer:7400/deployr`).
5. In the **User Name** and **Password** boxes, enter the user name and password that you want to use for the R Server connection.
6. Select **Save**.
   The R Server credentials are saved.
7. Select **Perform Connection Test** to confirm that the connection is valid.

Rules Deployment

Install the GE Digital APM Rules Editor

Before You Begin

- Microsoft Visual Studio 2017 or 2019 Professional must be installed on every workstation where you want to work with 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.

Procedure

1. On the machine that will serve as the GE Digital APM 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**.
10. If you have Microsoft Visual Studio 2019 Professional installed, go to the `C:\Program Files (x86)\Microsoft Visual Studio\2019\Professional\Common7\IDE` folder.
11. Access the `devenve.exe.config` file in an application that can be used to modify text files (for example, Notepad++).

12. In the file, locate the following text:

```
<assemblyIdentity name="System.Runtime.CompilerServices.Unsafe"
publicKeyToken="b03f5f7f11d50a3a" culture="neutral"/>
```

13. Below the line, within the `bindingRedirect` tag, ensure that the value of the `oldVersion` parameter is `0.0.0.0-4.0.6.0` and the value of the `newVersion` parameter is `4.0.6.0`.
14. Save and close the file.

Results

- The GE Digital APM rules editor is installed.

SIS Management Deployment

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 system architecture.

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

Step	Task	Notes
1	Define alternate search queries.	This step is required only if you do not want to use the baseline search queries.
2	Modify threshold values in the SIL Threshold family.	This step is required only if you want to modify the default boundary values specified in the SIL Threshold family. **Tip:** To prevent ambiguity in SIL values for driving risk ranks that fall on the boundary value of two SIL thresholds, avoid specifying contiguous boundary values where the lower boundary value of one threshold is the upper boundary value of the preceding SIL threshold. For example, for the SIL value of 1, if you have specified a SIL threshold of 10 through 100, then, for a SIL value of 2 you can specify the SIL threshold of 100.1 through 1000.
3	Import data from an Exida project file.	This step is required only if you want to create SIL Analyses using an Exida project file.
4	Export data from an Exida project file.	This step is optional.

Step	Task	Notes
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.
6	Assign View permissions to the Hazards Analysis family to SIS Management Security Groups in Configuration Manager. As needed, you can assign additional privileges.	This step is required only for Security Groups that will be used in the integration between the SIS Management module and Hazards Analysis.
7	Review the SIS Management data model to determine which relationship definitions you will need to modify to include your custom equipment or location families. Modify any relationship definitions as needed using the Configuration Manager.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
8	Assign Security Users to one or more of the SIS Management Security Groups and Roles.	This step is required.

Update the Query Parameter Type

About This Task

After the database for GE Digital APM is upgraded, if the entity key fields are of the type string, you must modify the catalog query parameters to use the correct type by performing the following steps:

Procedure

1. Access the **Query** page
2. Select **Browse**.
   The **Select a query from the catalog** window appears.
3. Navigate to the folder containing the query that you want to update, and select the link for the query.
   The **Results** workspace appears.
4. Select the **SQL** tab.
   The **SQL** workspace appears, where you can modify the SQL code.
5. Modify all the entity key numeric parameters to string.

   For example, (? :n) must be updated to (? :s).
6. Select **Save**.
   The modified query is saved.

Revert the SIS Management Queries to Baseline

This action is required only if you have modified the SIS Management queries.

About This Task

If you have modified the SIS Management queries, perform the following steps to revert the query to baseline.

Procedure

1. Access the Catalog page.
2. Navigate to the Public folder for the query that you want to revert.

   For SIS Management, the public queries are stored in the following folder:

   `Public\Meridium\Modules\SIS Management`

3. Select the check box next to the query that you want to revert, and then select 🗑.
   The **Confirm Delete** window appears, prompting you to confirm if you want to delete the selected query.
4. Select **OK**.
   The selected query is deleted.
5. Navigate to the Baseline folder for queries.

   For SIS Management, the baseline queries are stored in the following folder:

   `Baseline/Meridium/Modules/SIS Management`

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

Thickness Monitoring Deployment

Deploy Thickness 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 system architecture.

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

Step	Task	Notes
1	Review the TM data model to determine which relationship definitions you will need to modify to include your custom equipment families. Via Configuration Manager, modify the relationship definitions as needed.	This step is required only if you store equipment and location information in families other than the baseline Equipment and Functional Location families.
2	Assign Security Users to one or more of the 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	Assign Resource Roles to users by performing the following steps: 1. Access the Human Resource record for each user. 2. In the **Role** box, select **TM Technician**.	This step is required to allow a user (typically, a TM Inspector) to enter details in an Inspection record.
4	Configure Family Preference Application Settings.	This step is required. You must configure preferences for the families that will be used to store equipment data in Thickness Monitoring. The following relationships must be defined: • For the Equipment family, the Asset to Subcomponent Relationship field must be set to **Has TML Group**, and the Component ID field must be set to **Equipment ID**. The Subcomponent to Asset Relationship field should be left blank. • For the TML Group family, the Subcomponent to Asset Relationship field must be set to **Has TML Group**, and the Component ID field must be set to **TML Group ID**. The Asset to Subcomponent Relationship field should be left blank.
5	Configure Global Preference Application Settings.	This step is required only if you want to use custom reading preferences and Nominal T-Min preferences. Baseline reading preferences and Nominal T-Min preferences will be used if you do not define your own. You can also define additional, optional global preferences that are not defined in the baseline GE Digital APM database.
6	Configure the system to use custom TML Types.	This step is required only if you want to use custom TML Types. You can define additional TML Types to use in your Corrosion Analyses.
7	Manage Thickness Monitoring Rules Lookup records.	This step is required only if you want to view or modify Thickness Monitoring Rules Lookup records whose values are used to perform certain TM calculations.

Step	Task	Notes
8	Define additional fields that will be displayed in the header section of the TM Measurement Data Entry.	This step is required only if default Thickness Measurement fields are displayed on the headings of these pages in the baseline GE Digital APM database. You can specify that additional fields be displayed in the header section of these pages.
9	Disable the Auto Manage Tasks setting.	This step is required only if you are planning to use TM tasks.
10	Install the Meridium Device Service on all of the machines that will connect to devices that will be used with Thickness Monitoring.	This step is required only if you will use any device to collect data that you transfer to Thickness Monitoring. If you are using HTTPS to connect to GE Digital APM, follow the instructions in KBA 000055071.
11	Configure Thickness Monitoring ActiveMQ Settings for MIExecution Service on page 177.	This step is optional. You can perform this step if you want to modify the default retries or concurrency settings.
12	Ensure that the Meridium MIExecution Service is installed and running.	If the basic GE Digital APM system architecture is already installed, the Meridium MIExecution Service is automatically installed, and the service runs automatically.
13	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.

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
```

Note: For more information on customizing baseline rules, refer to the Rules section of the documentation.

Install the Meridium Device Service

About This Task

Important: You must repeat this procedure on every machine to which a datalogger will be connected.

Note: If you are using Cloud APM or the URL is secured (https), follow the instructions in https://digitalsupport.ge.com/communities/en_US/Article/HOW-TO-V4-Thickness-Monitoring-Devices-Dataloggers-and-Secure-HTTPS-Browsers-on-Windows-Machines-1553989641712 to install the Meridium Device Service.

Procedure

1. Access the **TM Dataloggers** page.

2. In the **Select TMLs** pane, select the check box next to a TML, and then select **Apply**.
3. Select **Send To Device**.

    Note: A datalogger does not need to be connected.

    The **Meridium Device Service Not Found** window appears.
4. Select the **Download** link.
    MeridiumDevices.exe is downloaded.
5. Run **MeridiumDevices.exe**, and then follow the instructions in the installer.
    The Meridium Device Service is installed.
6. In the **Meridium Device Service Not Found** window, select **Continue**.
    Dataloggers can now be used with Thickness Monitoring.

Configure the Meridium Device Service

Procedure

1. In Windows Explorer, navigate to **C:\Program Files\Meridium\Services**.
2. Using a text editor, open the **Meridium.Service.Devices.exe.config** file.
3. In the text editor, navigate to the **appSettings** section (lines 24 to 28).

    - On line 25, edit the port number used by the service.

      Note: The datalogger settings in Thickness Monitoring must be modified so that the port number matches the one defined in this step.
    - On line 26, edit the timeout value in milliseconds. By default, the value for this setting is 60000, or 1 minute.
    - On line 27, if your organization utilizes a different URL protocol for 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.

Configure Thickness Monitoring ActiveMQ Settings for MIExecution Service

The MIExecution Service,on each GE Digital APM Server serves RBI, Inspection and Thickness Monitoring module queues. This service is configured to use a single shared ActiveMQ queue service across APM. Available queue configuration options include retries and concurrency limit.

Procedure

1. On the GE Digital APM Server, access the folder that contains the MIExecution Service files.

    Note: If you have installed GE Digital APM in the default location, you can locate the folder in
    `C:\Program Files\Meridium\ApplicationServer\mi-execution`
2. Access the `appsettings.json` file in an application that can be used to modify JSON files (for example, Notepad++).
3. In the file, locate the following text:

```
"Queue_Config": {
        "Queues": [
          {
            "Name": "MI_TM_Queue",
            "ConcurrencyLimit": 100,
```

```
            "Retries": 5,
                "LimitPerTenantRequired": true
            }
        ]
            }
```

Note: `ConcurrencyLimit` indicates the maximum number of messages that will be consumed concurrently. `Retries` indicates the number of times it retries to send the messages to ActiveMQ if it fails. `LimitPerTenantRequired` indicates whether Maximum Concurrency limit per Tenant is specified in scheduler service for the queue.

4. Update the key values as desired.

5. Save and close the file.
   The updated settings will be applied when the MIExecution Service is stopped and restarted.

TM 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
Renew TMLs	No	Yes	No
Reset User Preferences	Yes	No	No

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
Renew TMLs	No	Yes	No
Reset User Preferences	Yes	No	No

TM Security Groups

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

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

Security Group	Roles
MI Thickness Monitoring Administrator	MI Mechanical Integrity Administrator
MI Thickness Monitoring Inspector	MI Mechanical Integrity Administrator MI Mechanical Integrity Power MI Mechanical Integrity User

Security Group	Roles
MI Thickness Monitoring User	MI Mechanical Integrity Administrator MI Mechanical Integrity Power MI Mechanical Integrity User
MI Thickness Monitoring Viewer	MI APM Viewer MI Mechanical Integrity Viewer

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

Family	MI Thickness Monitoring Administrator	MI Thickness Monitoring Inspector	MI Thickness Monitoring User	MI Thickness Monitoring Viewer
Entity Families				
Corrosion	View, Update, Insert	View, Update, Insert	View, Update, Insert	View
Datapoint	View, Update, Insert	View, Update, Insert	View, Update, Insert	View
Datapoint Measurement	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert	View
Equipment	View	View	View	View
Human Resource	View, Update, Insert, Delete	View	View	View
Inspection Task	View	View, Update	View	View
Inventory Group Configuration	View	View	View	View
Materials of Construction	View	View	View	View
Meridium Reference Tables	View, Update, Insert, Delete	View	View	View
RBI Inspection Auto-Selection Criteria	View	View	View	View
Resource Role	View, Update, Insert, Delete	View	View	View
Security Group	View	View	View	View
Security User	View	View	View	View
Settings	View, Update, Insert	View, Update, Insert	View	View
Task Execution	View, Insert	View, Insert	View	View
Thickness Monitoring Task	View, Update, Insert, Delete	View, Update, Insert	View, Update, Insert	View

Family	MI Thickness Monitoring Administrator	MI Thickness Monitoring Inspector	MI Thickness Monitoring User	MI Thickness Monitoring Viewer
TML Group	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View
Relationship Families				
Belongs to a Unit	View, Update, Insert, Delete	View, Update, Insert	View, Update, Insert	View
Equipment Has Equipment	View	View	View	View
Group Assignment	View	View	View	View
Has Archived Corrosion Analyses	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Archived Corrosion Analysis Settings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Archived Subcomponent Analysis Settings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Archived Subcomponent Corrosion Analyses	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Corrosion Analyses	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Corrosion Analysis Settings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Datapoints	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Inspections	None	None	None	View
Has Measurements	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Roles	View, Update, Insert, Delete	View	View	View
Has Task Execution	View, Insert	View, Insert	View	View
Has Task Revision	View, Insert	View, Insert	View	View
Has Tasks	View, Insert	View, Insert	View, Insert	View
Has TML Group	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View
Is a User	View	View	View	View
User Assignment	View	View	View	View

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

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

Security Group	Roles
MI Thickness Monitoring Administrator	MI Mechanical Integrity Administrator
MI Thickness Monitoring Inspector	MI Mechanical Integrity Administrator MI Mechanical Integrity Power MI Mechanical Integrity User
MI Thickness Monitoring User	MI Mechanical Integrity Administrator MI Mechanical Integrity Power MI Mechanical Integrity User
MI Thickness Monitoring Viewer	MI APM Viewer MI Mechanical Integrity Viewer

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

Family	MI Thickness Monitoring Administrator	MI Thickness Monitoring Inspector	MI Thickness Monitoring User	MI Thickness Monitoring Viewer
Entity Families				
Corrosion	View, Update, Insert	View, Update, Insert	View, Update, Insert	View
Datapoint	View, Update, Insert	View, Update, Insert	View, Update, Insert	View
Datapoint Measurement	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert	View
Equipment	View	View	View	View
Human Resource	View, Update, Insert, Delete	View	View	View
Inspection Task	View	View, Update	View	View
Inventory Group Configuration	View	View	View	View
Materials of Construction	View	View	View	View
Meridium Reference Tables	View, Update, Insert, Delete	View	View	View

Family	MI Thickness Monitoring Administrator	MI Thickness Monitoring Inspector	MI Thickness Monitoring User	MI Thickness Monitoring Viewer
RBI Inspection Auto-Selection Criteria	View	View	View	View
Resource Role	View, Update, Insert, Delete	View	View	View
Security Group	View	View	View	View
Security User	View	View	View	View
Settings	View, Update, Insert	View, Update, Insert	View	View
Task Execution	View, Insert	View, Insert	View	View
Thickness Monitoring Task	View, Update, Insert, Delete	View, Update, Insert	View, Update, Insert	View
TML Group	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View
Relationship Families				
Belongs to a Unit	View, Update, Insert, Delete	View, Update, Insert	View, Update, Insert	View
Equipment Has Equipment	View	View	View	View
Group Assignment	View	View	View	View
Has Archived Corrosion Analyses	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Archived Corrosion Analysis Settings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Archived Subcomponent Analysis Settings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Archived Subcomponent Corrosion Analyses	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Corrosion Analyses	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Corrosion Analysis Settings	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Datapoints	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View
Has Inspections	None	None	None	View
Has Measurements	View, Update, Insert, Delete	View, Update, Insert, Delete	View, Update, Insert, Delete	View

Family	MI Thickness Monitoring Administrator	MI Thickness Monitoring Inspector	MI Thickness Monitoring User	MI Thickness Monitoring Viewer
Has Roles	View, Update, Insert, Delete	View	View	View
Has Task Execution	View, Insert	View, Insert	View	View
Has Task Revision	View, Insert	View, Insert	View	View
Has Tasks	View, Insert	View, Insert	View, Insert	View
Has TML Group	View, Update, Insert, Delete	View, Update, Insert, Delete	View	View
Is a User	View	View	View	View
User Assignment	View	View	View	View