EcoStruxure™

Power Monitoring Expert 2021

IT Guide

7EN02-0449-01

01/2022

Schneider Electric

Legal Information

Safety Information

Important Information

Read these instructions carefully and look at the equipment to become familiar with the device before trying to install, operate, service or maintain it. The following special messages may appear throughout this bulletin or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of either symbol to a "Danger" or "Warning" safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result in** minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please Note

Electrical equipment should be installed, operated, serviced and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction, installation, and operation of electrical equipment and has received safety training to recognize and avoid the hazards involved.

Contents

Safety Precautions

During installation or use of this software, pay attention to all safety messages that occur in the software and that are included in the documentation. The following safety messages apply to this software in its entirety.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Do not use the software or devices for critical control or protection applications where human or equipment safety relies on the operation of the control action.
- Do not use the software to control time-critical functions.
- Do not use the software to control remote equipment without proper access control and status feedback.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

⚠ WARNING

INACCURATE DATA RESULTS

- Do not incorrectly configure the software or the devices.
- Do not base your maintenance or service actions solely on messages and information displayed by the software.
- Do not rely solely on software messages and reports to determine if the system is functioning correctly or meeting all applicable standards and requirements.
- Consider the implications of unanticipated transmission delays or failures of communications links.

Failure to follow these instructions can result in death, serious injury, equipment damage, or permanent loss of data.

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Use cybersecurity best practices to help prevent unauthorized access to the software.

Failure to follow these instructions can result in death, serious injury, equipment damage, or permanent loss of data.

Work with facility IT System Administrators to ensure that the system adheres to the site-specific cybersecurity policies.

Introduction

Power Monitoring Expert (PME) is a client-server, on-premise software application that collects power monitoring data through a network of connected devices. The power monitoring data is processed and stored using Microsoft SQL Server and can be accessed by users in a variety of formats through different user interfaces.

This document is intended for IT professionals who support the PME system installation. It provides information on possible deployment architectures, supported operating environments, required access permissions, IT and device network considerations, cybersecurity, the PME installer, as well as general dependencies and prerequisites.

Resources

The Resources page is a central reference for any resources that are referred to in this guide but that are not included in the guide.

Download Center

NOTE: The EcoStruxure™ Power Monitoring Expert System Guide includes the content of the following guides: What's New Guide, IT Guide, Web Applications Guide, and the Insulation Monitoring User Guide.

The following EcoStruxure™ Power Monitoring Expert 2021 documents are available on the Schneider Electric Download Center:

- System Guide (English) – Document number 7EN02-04445
- What's New Guide (English) – Document number 7EN12-0335
- Insulation Monitoring User Guide (English) – Document number 7EN02-0449
- Web Applications Guide (Multilingual) – (English) Document number 7EN02-0446

Exchange (requires login)

NOTE: On the Exchange you can find discussion forums, key content, service providers, and knowledge base articles. You can also sign-up to become a service provider. To gain access to the Exchange and its content, register at https://exchange.se.com/.

- Schneider Electric Exchange - EcoStruxure Power Monitoring Expert (Portal)
- Power Monitoring Expert Promote & Sell
  - PME End User License Agreement
- Power Monitoring Expert Design and Quote:
  - Tools (Commissioning Time Calculator, Daisy Chain Calculator, Database Growth Calculator, Secondary Server Calculator)
  - Documents (IT Guide (English), PME System Guide)
  - EWS Specification
  - Standard Scope of Work Packages
  - Device Support Matrix
  - Part Numbers list
- Power Monitoring Expert Install and Maintain:
  - Information on PME software updates
  - Application Notes
  - Drivers
  - Help Files
  - Upgrade Map

  - Tools (Configuration Manager, ETL Guides)
  - Documents (PME System Guide, PME/EBO Integration Solution Guide, Insulation Monitoring User Guide)
  - Standard Scope of Work Packages
  - PME Scripts
- EcoStruxure Building Operation documents on Exchange:
  - Architectural Guidelines - EcoStruxure Building Operation
  - IT System Planning Guide - EcoStruxure Building Management
  - EcoStruxure Building Operation - System Reference Guide
  - EcoStruxure Building Operation - Technical Reference Guide
  - EcoStruxure Building Operation - IT Reference Guide
- Other documents and files on Exchange:
  - PO System Guide
  - EcoStruxure Power Digital Applications for Large Buildings & Critical Facilities - Design Guide for North America
  - How Do I Extend the DDD Indicators Application to Support More Than 30 Devices

Exchange Community (requires login)

- PME Exchange Community (Online support and collaboration)
  - Software updates (see Announcements and Downloads)
- PME ETL download
- Billing Module Toolkit
- Device Drivers
  - PME Device Driver Summary Spreadsheet (shows native and downloadable drivers; includes links to downloadable drivers)
  - PME Device Driver downloads (SE, LE- Enter the device name in the search box to find the driver)
  - PME Device Driver downloads (CE)

Other

- Schneider Electric Cybersecurity Support Portal
- Schneider Electric Knowledge Base
- PME Sales Portal
- Schneider Data Privacy and Cookie Policy
- PME 7.2 Service Pack 2

Technical Support

- Schneider Electric Support (Support)
- mySchneider app
  - 24/7 support. Mobile catalog. Access to expert help.
- Offline Licensing Support
  - Offline license activation, return, and refresh

External Resources

The following are resources that are referenced in different sections of this guide; they provide additional information and downloadable components.

Microsoft® technical documentation:

- Microsoft® SQL Server® Data-Tier Application Framework Installer Download (DacFramework.msi)
- How to choose antivirus software to run on computers that are running SQL Server
- How to determine which versions and service pack levels of the Microsoft .NET Framework are installed

Overview

This section provides an overview of the PME system.

Use the links below to find the content you are looking for:

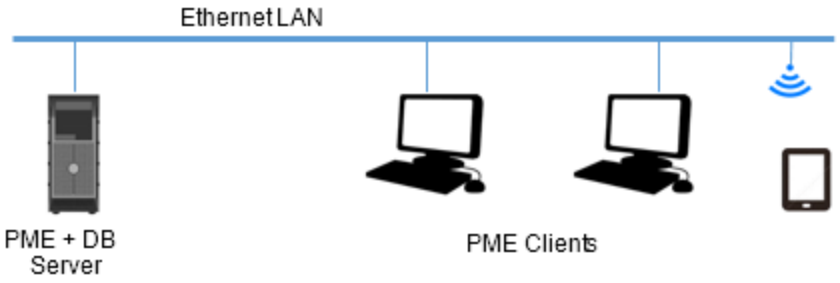
System architecture

PME is a client-server, on-premise software application that collects power monitoring data through a network of connected devices. The power monitoring data is processed and stored using Microsoft SQL Server and can be accessed by users in a variety of formats through different user interfaces.

PME is deployed in one of two basic architectures: Standalone or Distributed Database.

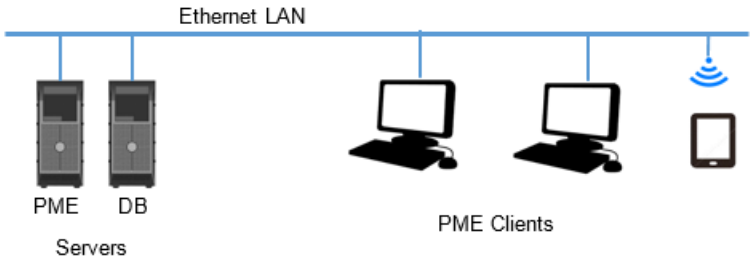
Standalone architecture

In a Standalone architecture, all PME system files, the SQL Server database, and any other tools or utilities are installed on the same computer. You access the power monitoring data through clients.

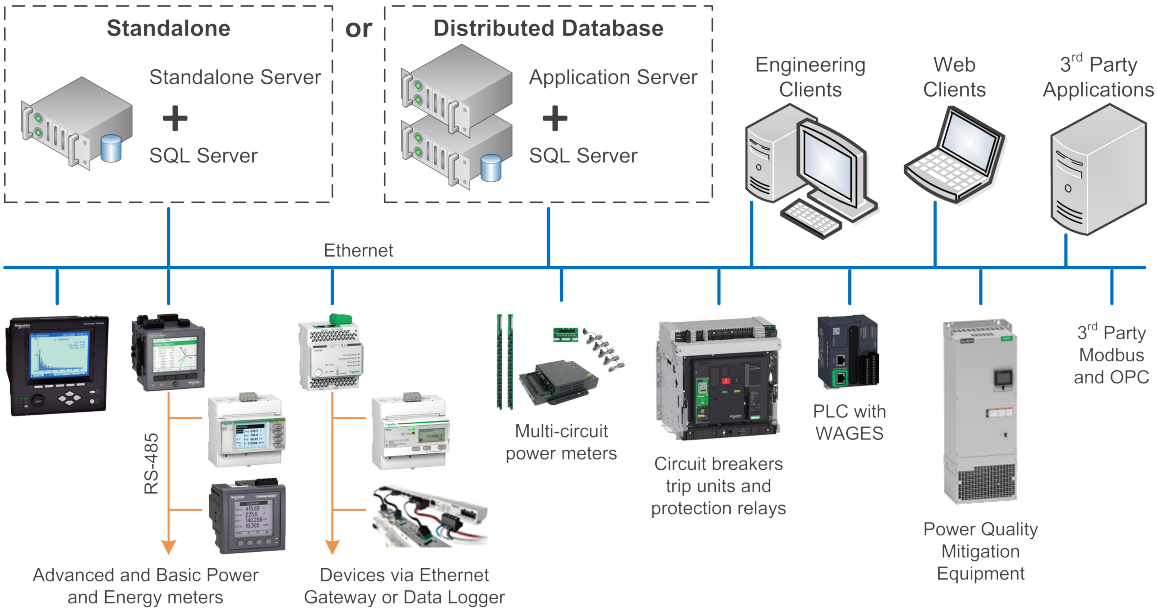


Distributed Database architecture

In a Distributed Database architecture, all PME system files, tools, and utilities are installed on one computer. The database server is installed on a second computer. There are no PME system files installed on the database server except for the historical database files. You access the power monitoring data through clients.



The following example diagram shows both architectures in the context of the overall system, including the monitoring devices:



Which architecture you should choose

We recommend you use the Standalone architecture. It is easier and more cost effective to deploy, and there are no performance advantages in using a Distributed Database architecture.

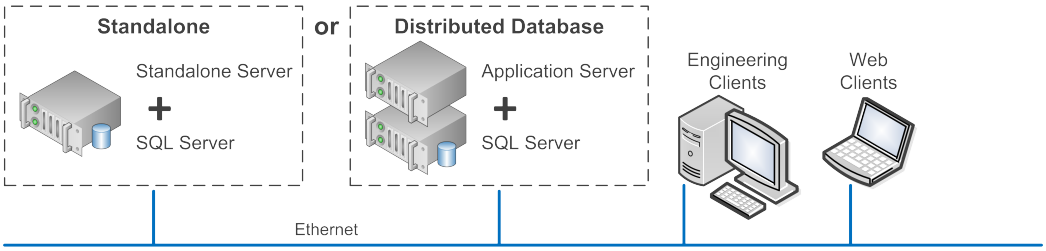
However, in some cases it might be necessary to use the Distributed Database architecture, such as:

- Your customer wants to use an existing SQL server.
- Your customer IT requirements do not allow a Microsoft SQL Server to be installed with another application on the same server.
- The application requires Microsoft SQL Server redundancy with SQL Clustering or other third-party tools.
- The application requires specific rules for database management, for example SQL jobs, back-ups, data security, and so on.

Client types

In PME you use clients to access the configuration tools and the applications for viewing data. There are two different types of clients:

- Engineering Clients configure and administer the system.
- Web Clients view power monitoring information.



Engineering Client

An Engineering Client is an administrative interface in PME that is used to configure and administer the system. Engineering Clients include tools such as the Management Console, Vista, and Designer.

One Engineering Client is installed, by default, on the PME server. Additional Engineering Clients can be installed on other computers, for example on a portable notebook computer, that are more accessible than the server. Engineering Clients require a Base Access license.

Web Client

A Web Client is used to view power monitoring information such as real-time data, historical information, and alarms which are used in day-to-day power management tasks.

Web Clients access the data on the server through a Web browser. No installation is required. Web Clients can run on any computer on the network. Web Clients require a Client Access license.

Web Clients can access the Web Applications (Dashboards, Diagrams, Trends, Alarms, and Reports) in PME.

To set up a Web Client, enter the fully qualified domain name of the PME server or its IP address, followed by `/Web` into your browser.

Examples:

- `http://10.160.42.1/Web`
- `http://PMEServer.MyCompany.com/Web`

NOTE: `Web` is the default root directory. The root directory is configurable and can be changed during installation.

By default, the first application on the navigation bar in Web Applications opens in the browser. To specify which application should open first, add one of the following application parameters to the Web address: (Note that the parameters are case-sensitive.)

```
#Dashboards, #Diagrams, #Trends, #Alarms, #Reports
```

For example, `http://PMEServer.MyCompany.com/Web/#Alarms` opens the Alarms application in the browser.

NOTE: For cybersecurity and performance reasons, we recommend that you do not use a Web Client on the PME server computer.

Licensing

PME is a proprietary software that uses licensing to control its use and distribution. The licensing is enforced through mechanisms that disable certain software functions if no valid license has been activated.

To use PME, you must purchase software licenses and activate them in the system. The licenses give you the right to use the software according to the terms and conditions described in the software End User License Agreement (EULA). The licenses generally do not expire, unless stated otherwise in the software EULA. PME licenses are per system. If you have multiple systems, you must purchase separate licenses for each. Multi-system, or enterprise licenses are not available.

PME uses a modular licensing structure where different licenses enable different functions in the software. Some of these functions are optional, others are required. The licenses are cumulative, meaning that you can add additional licenses to a system, to enable additional functionality.

See Resources for information on where to find a copy of the PME EULA.

License activation

Purchased licenses must be activated either through online or offline methods. An Internet connection for the PME server is required for online activation. Offline activation must be done from an alternate Internet-connected computer or smart-phone with web access.

Licenses are tied to the host computer (physical or virtual). If PME needs to be moved to a new computer, the licenses must first be returned and then reactivated on the new computer.

License types

PME licenses bundle together one or more PME features. For example, a Base license includes two Client Access license.

The following table shows the different licenses that are available for PME:

Type	Description
Trial license	New system installations include a time limited Trial license. The Trial license: • enables all of the PME features (except Connected Services) • includes an unlimited Device license • includes an unlimited Client Access license • may be extended on demand • cannot be reinstalled • remains active for 90 days until a purchased license is activated • expires after 90 days

Type	Description
Base license	This is a required license. It enables the PME server functions and the basic system functions. Without the Base license the system is not functional. The same Base license can be used for Standalone or Distributed Database systems. The Base license also includes two Client Access licenses. With Base license, engineering client can be accessed.

<table>
<tr><th>Type</th><th>Description</th></tr>
<tr><td>Express Base license</td><td>The Express Base license is similar to the Base license but with reduced functionality. It is intended for small starter or entry-level systems. The following shows the differences between Base and Express Base licenses:
<table>
<tr><th colspan="2">Feature</th><th>Express Base</th><th>Base</th></tr>
<tr><td colspan="2">Included device licenses</td><td>10</td><td>None</td></tr>
<tr><td colspan="2">PQ Reports</td><td>No</td><td>Yes</td></tr>
<tr><td rowspan="4">Expansion (optional):</td><td>Device Licenses (DL)</td><td>Max of 10 additional</td><td>Yes</td></tr>
<tr><td>Client Licenses (CL)</td><td>Max of 2 additional</td><td>Yes</td></tr>
<tr><td>Unlimited DL</td><td>No</td><td>Yes</td></tr>
<tr><td>Unlimited CL</td><td>No</td><td>Yes</td></tr>
<tr><td rowspan="8">SW Modules (optional)</td><td>Data Exchange Module</td><td>No</td><td>Yes</td></tr>
<tr><td>Energy Billing</td><td>No</td><td>Yes</td></tr>
<tr><td>Energy Analysis Reports</td><td>Yes</td><td>Yes</td></tr>
<tr><td>Energy Analysis Dashboards</td><td>Yes</td><td>Yes</td></tr>
<tr><td>Capacity Management</td><td>No</td><td>Yes</td></tr>
<tr><td>Insulation Monitoring</td><td>No</td><td>Yes</td></tr>
<tr><td>PQ Performance</td><td>No</td><td>Yes</td></tr>
<tr><td>Breaker Performance</td><td>No</td><td>Yes</td></tr>
<tr><td>Backup Power</td><td>No</td><td>Yes</td></tr>
<tr><td>Event Notification</td><td>No</td><td>Yes</td></tr>
<tr><td colspan="2">Edition Upgrade</td><td>To Standard Edition</td><td>n/a</td></tr>
</table>
</td></tr>
</table>

Type	Description
Device license	This is a required license. It enables the use of monitoring devices in PME. Depending on the locale, device licenses are sold as: • Bundles of 5, 25, 50, 100, 200, unlimited - for the US, Canada, and India. • Individual licenses, with 3 different license types - for countries other than the US, Canada, and India: – **E** for entry-range device types – **M** for mid-range device types – **S** for high-end device types **NOTE**: Unlimited individual device licenses are available. **NOTE**: At least one device license must be activated in the system for PME to be able to communicate with a device.
Client Access license	This is a required license. It allow access to Web Applications. • Client Access licenses are assigned to users. • Each user needs their own Client Access license. • A Client Access license is assigned and bound to a new user when they first log into the PME web applications. • The **supervisor** account also needs a Client Access license. • To free up an assigned Client Access license, the user must be deleted in PME. **NOTE**: An unlimited Client Access license is available that includes unlimited web application use. **NOTE**: Management Console does not require a license.

Type	Description
Software Module license	This is an optional license. It enables the use of a Software Module. Each Software Module requires its own specific license. The following Software Modules exist in PME: • Backup Power Module • Breaker Performance Module • Capacity Management Module • Energy Analysis Dashboard Module • Energy Analysis Reports Module • Energy Billing Module • Event Notification Module • Insulation Monitoring Module • Power Quality Performance Module
Data Exchange Module license	This is an optional license. It enables the use of the following features and functions in PME: • OPC DA Server • Measurement Aggregation Export Report • Measurement Statistics Export Report • VIP Modbus Slave functionality • COMTRADE export with ETL **NOTE**: OPC DA Server licenses on older PME systems will automatically be converted to Data Exchange Module licenses on upgrade.
Developer/Demo license	This is a special license. Contact Schneider Electric for details.

Basic administration tasks

Install Windows updates

Apply critical and routine Windows and SQL Server updates to the PME servers and clients; no prior approval by Schneider Electric is required.

Check the scheduled database maintenance tasks

NOTICE
LOSS OF DATA • Back up the database at regular intervals. • Back up the database before upgrading or migrating the system. • Back up the database before trimming it. • Back up the database before making manual database edits. • Verify correct database behavior after making database or system changes. **Failure to follow these instructions can result in permanent loss of data.**

In Standalone PME systems, the database maintenance tasks for backup, archive, maintenance, and trim are pre-configured and scheduled to run automatically by default. For Distributed Database PME systems, we recommend that these scheduled tasks are set up manually.

Check the task outputs regularly and confirm that backups are created as expected. Review and adjust the schedules to meet your application needs, if required.

NOTE: You can perform additional, manual backups using standard SQL Server backup procedures.

Monitor the database size for systems with SQL Server Express databases

NOTICE
LOSS OF DATA • Back up or archive the database before trimming it. • Trim the SQL Server Express database before it reaches the size limit. **Failure to follow these instructions can result in permanent loss of data.**

SQL Server Express has a maximum database size limit of 10 GB. The database stops logging data when this size limit is reached. The scheduled default database maintenance tasks include a database size notification task. When the size threshold is reached, the task logs a system log event message and triggers a Critical alarm in PME every time the task runs.

Check the PME system log and Alarms on a regular basis for database size notification messages. Check the database size on a regular basis and take action before reaching the database size limit.

Cybersecurity

This section includes information on how to help secure your system.

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Use cybersecurity best practices to help prevent unauthorized access to the software.

Failure to follow these instructions can result in death, serious injury, equipment damage, or permanent loss of data.

Work with facility IT System Administrators to ensure that the system adheres to the site-specific cybersecurity policies.

Cybersecurity awareness

Knowledge is first step to prevent cyber intrusions. Review the following resources to increase your cybersecurity awareness:

- Securing Power Monitoring and Control Systems (Schneider Electric White Paper)
- Social engineering (security)

To find out about the latest cybersecurity news, sign up for security notifications, or to report a vulnerability, visit the Schneider Electric Cybersecurity Support Portal. See Resources for link information.

RECOMMENDATION: Sign-up for security notification emails on the Schneider Electric Cybersecurity Support Portal.

Cybersecurity features

PME includes features that help to secure your system, including:

- Data encryption using SHA-512 and AES-256 cryptography (At Rest) and TLS 1.2 / HTTPS (In Transit)
- Compatibility with antivirus and whitelisting software
- User account management, optionally using Windows Active Directory integration
- Session timeout of inactive user sessions

For more information on these and other features, see Recommended actions.

NOTE: PME 2021 complies with the requirements of the security relevant standards for Security Level 1 (SL 1) according to IEC 62443-4-1 and IEC 62443-4-2.

Recommended actions

PME is designed for a defense in depth security strategy, in compliance with IEC 62443, the global standard for industrial automation control system security. A defense in depth strategy is a multi-layered approach to cybersecurity with intentional redundancies to increase the security of a system as a whole.

The different defense in depth layers can be described as:

- Data Layer (includes access control and encryption of data)
- Application Layer (includes antivirus software and application hardening)
- Host Layer (includes patch implementation, user authentication)
- Network Layer (includes IPsec, intrusion detection system)
- Perimeter Layer (includes firewalls, VPN)
- Physical Layer (includes guards, switches, locks, ports, physical access)
- Policies

To help secure your system, you must take specific actions for the different layers and at every stage of the project life-cycle. The following shows the actions we recommend to help secure your system, organized by life-cycle stage:

NOTE: The list of recommended actions below is not a complete list of possible cybersecurity measures. It is meant to be a starting point to improve the security of your system. Consult with cybersecurity experts to plan, install, configure, administer, and decommission your system based on your needs.

Life-cycle Stage	Layer	Recommended Action
Planning	Data Layer	Obtain security certificates.
	Application Layer	Obtain antivirus and application whitelisting software.
	Host Layer	Plan user access.
	Network Layer	Plan your network security.
	Perimeter Layer	Plan to install PME in an intranet environment. Plan IP port use.
	Physical Layer	Plan your site security.
	Policies	Plan for the implementation of cybersecurity standards.
Installing, Upgrading	Application Layer	Install antivirus and application whitelisting software. Verify install file integrity and authenticity. Protect the System Key. Apply PME updates.
	Host Layer	Install latest updates for OS and SQL Server. Check computer for cybersecurity issues.
	Network Layer	Install your network security measures.
Configuring	Data Layer	Install security certificate. Set up encrypted database communication for Distributed Database architectures
	Application Layer	Configure application whitelisting software. Configure antivirus software on your SQL Server.
	Host Layer	Configure PME users and user groups. Customize user account privileges. Restrict Windows login permissions for the PME server. Change the SQL Server Express sa account password. Configure session timeout settings. Do not install or use a web browser on the server computer.
	Network Layer	Set up your network security.
	Perimeter Layer	Disable unused IP ports.
	Physical Layer	Disable unused hardware ports.

Life-cycle Stage	Layer	Recommended Action
Administering	Data Layer	Renew security certificate. Securely store the system key.
	Application Layer	Apply PME updates. Verify update file integrity and authenticity.
	Host Layer	Apply OS and SQL Server updates. Review user accounts on a regular basis.
	Network Layer	Keep network security up-to-date.
	Physical Layer	Keep computer hardware secure.
	Policies	Perform security audits
Decommissioning	Host Layer	Decommission your system at the end of its life.

For more information on cybersecurity related PME features, functions and configurations, see the *Power Monitoring Expert System Guide*.

Planning

This section provides information to help you plan your system security.

Obtain security certificates

PME uses Transport Layer Security (TLS) 1.2 for an encrypted, authenticated connection using HTTPS between the server and its web clients. Both self-signed and authority issued certificates are supported. PME is installed with a self-signed certificate and a self-signed certificate is configured automatically. We recommend that you replace this with a security certificates from a Certificate Authority (CA).

You also need a certificate for the database server computer to use an encrypted connection between PME and the SQL database server in a Distributed Database architecture installation. See Set up encrypted database communication for Distributed Database architectures for more information on this topic and for links to Microsoft articles with certificate requirements for SQL server computers.

See Data encryption for information on data encryption, at rest and in transit, in PME.

Obtain antivirus and application whitelisting software

PME can be used with antivirus (AV) software.

PME can be used with application whitelisting software products such as McAfee Application Control software. See Configure application whitelisting software for more information.

NOTE: AV software can have a significant impact on system performance if not set up correctly. In particular, SQL Server performance can be affected if data and log files are not excluded from on-access scans. See Configure antivirus software on your SQL Server for more information.

Plan user access

Define a list of user accounts, access levels, and access permissions for your PME system. See PME accounts, Network shares, and Session timeout for more information.

Plan your network security

Determine the network security measures for your IT and device networks to provide your desired level of security.

This can include:

- use of industrial firewalls
- use of intrusion detection and prevention systems (IDS, IPS)
- application of ISO27001 (Information Security Management System Standard [=policies and procedures])
- managing wireless access and remote access
- device security
- deep packet inspection firewalls
- physically securing device access

Determine what level of expertise will be required to deploy and maintain the network architectures and security measures. Plan to have this expertise available for the system deployment and maintenance.

Plan to install PME in an intranet environment

PME is designed for an intranet environment within a secured network infrastructure. PME is NOT designed for direct Internet connection.

Plan IP port use

Determine which IP ports are required and which ones can be disabled. See IP Ports for details on PME port requirements.

Plan your site security

Determine the hardware locking measures required to provide your desired level of security.

This can include:

- personnel access restrictions to server locations
- physical locking of the computer, for example with a cable
- cementing the USB drive
- removing the CD-ROM drive
- tools such as McAfee® Enterprise Policy Orchestrator (ePO) suite of products
- industrial, security hardened PCs such as the Magelis Box

Define workarounds and alternatives for cybersecurity-imposed restrictions, for example, for USB and CD-ROM drive access.

Plan for the implementation of cybersecurity standards

Consider implementing cybersecurity standards such as:

- IEC62443, the global standard for industrial automation control system security.
- ISO27001, a specification for an information security management system.

Installing and Upgrading

This section provides information on how to help secure your system during the Installing and Upgrading phase.

Install antivirus and application whitelisting software

Install the antivirus and application whitelisting software.

NOTE: Application whitelisting software can prevent a legitimate application from executing, if not configured correctly. See Configure application whitelisting software for more information.

Verify install file integrity and authenticity

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Use cybersecurity best practices to help prevent unauthorized access to the software.

Failure to follow these instructions can result in death, serious injury, equipment damage, or permanent loss of data.

Work with facility IT System Administrators to ensure that the system adheres to the site-specific cybersecurity policies.

Verify the file integrity and authenticity for software updates and other components before installing them in the system. Do not install files for which the integrity and authenticity cannot be confirmed.

For details on how to verify file integrity and authenticity, see Verifying file integrity and authenticity.

Protect the System Key

During the installation of PME, a system key is generated and a copy of this key is exported as a `.key` file. This system key is the encryption key used by the software to encrypt user and system credentials. A PME server retains the original key in the registry. The exported copy is needed for the installation of Engineering clients and Secondary servers. It is also needed in case of a future side-by-side system upgrade or migration.

As long as the PME server has the original key stored in the registry, it is possible to use the installer to export a copy at any time. However, if the original key is deleted from the server, it cannot be recreated or exported. In that case, you can use the exported copy to restore the system key in the registry. Without the system key, PME user accounts can no longer be accessed.

NOTE: Protect the exported system key in a location accessible only to authorized users. An unauthorized user might be able to use the system key to gain access to your power monitoring software and devices.

Install latest updates for OS and SQL Server

Install the latest updates for the operating system and the SQL Server.

Check computer for cybersecurity issues

Check the pre-existing computer hardware and software for malware and other potential cybersecurity issues.

For example,

- Scan the system with up-to-date antivirus/antimalware tool
- Check the Windows user accounts and access permissions
- Verify firewall settings to ensure least-access
- Verify computer hardware integrity

Install your network security measures

Install the network security hardware and software measures for your IT and device networks.

Configuring

This section provides information on how to help secure your system during the Configuring phase.

Install security certificate

PME is installed with a self-signed certificate and a self-signed certificate is configured automatically. We recommend that you replace this with a security certificate from a Certificate Authority (CA).

See Data encryption for information on data encryption, at rest and in transit, in PME.

Set up encrypted database communication for Distributed Database architectures

We recommend that the connections between PME and the SQL database server, in Distributed Database architecture installations, are encrypted using at least Transport Layer Security (TLS) 1.2. This requires a certificate from a public certification authority for the SQL Server computer and the configuration of both servers to use encrypted connections.

NOTE: Only the communication between the PME application server and the database server will be encrypted, not the data in the database.

NOTE: The use of self-signed certificates is supported but we recommend that you use a certificate from a certification authority.

High level configuration steps:

1. Install a Server Authentication certificate from a public certification authority on the SQL Server computer.
2. Take PME out of service by informing system users of the outage and disabling any automated system control or third-party interactions.
3. Stop all PME services.
4. Configure the SQL server to force encrypted connections.
5. Configure PME to use encryption on database connections. See Configure database connection encryption for more information.
6. Confirm that the PME application server computer can verify the ownership of the certificate used by the SQL Server computer.
7. Restart PME, verify the correct operation of the system, and put the system back into service.

Detailed configuration information:

- See Enable Encrypted Connections to the Database Engine, a Microsoft document, for information on certificate requirements, as well as detailed installation and configuration instructions.
- See TLS 1.2 support for Microsoft SQL Server, a Microsoft document, for information on TLS 1.2 support in different versions of SQL Server.

Configure application whitelisting software

Application whitelisting software, such as McAfee Application Control, is used to prevent unauthorized applications from running on your system.

When you deploy whitelisting software to help protect a system, it scans the system and creates a whitelist of all executable binaries and scripts present on the system. The whitelist also includes hidden files and folders.

The whitelist includes all authorized files and determines trusted or known files. In Enabled mode, only files that are present in the whitelist can execute. All files in the whitelist are protected and cannot be changed or deleted. An executable binary or script that is not in the whitelist is said to be unauthorized and is prevented from running.

Consider the following when using whitelisting software with PME:

- Complete the system configuration before setting up and enabling the whitelisting software.
- Any program or script that should be able to update the system will need to be configured as an updater.
- After solidification, no updates or extensions, such as add-on device drivers, may be installed.
- Disable the whitelisting software when making changes to the PME system. Enable it again after the change.
- Follow the instructions of the software vendor for installing, configuring, and operating the whitelisting software.

NOTE: Verify the correct operation of your PME system after you enable the whitelisting software.

Configure antivirus software on your SQL Server

We recommend that you run anti virus software on your SQL server. Follow the recommendations described in Microsoft Support article (ID: 309422).

NOTE: Antivirus software can have a significant impact on system performance if it is not set up correctly. Consider the following:

- SQL Server performance can be affected if data and log files are not excluded from on-access scans.
- Special configuration of the antivirus software might be required.
- Follow the instructions of the software vendor for installing, configuring, and operating the antivirus and whitelisting software.

Configure PME users and user groups

There are no pre-configured user accounts or user groups in a newly installed system. One supervisor account is created, with a user defined password, during the installation of the software. Create additional user accounts and groups after installation. PME supports Windows users and groups for integration with Windows and Active Directory.

RECOMMENDATION: Use Windows users instead of standard users in your PME system to improve cybersecurity. Windows offers advanced user management functions, such as enforcing password strength and limiting the number of invalid login attempts. These functions are required for IEC 62443 compliance, the global standard for industrial automation control system security.

For information on creating users and user groups, and on setting user access levels, see *User Manager help*.

Customize user account privileges

You can configure user account privileges in **Web Applications** > **Settings** > **Users** > **System Users** > **User Manager**.

Restrict Windows login permissions for the PME server

We recommend that you restrict the Windows login permissions for the PME server computer to PME system administrators only. Preventing non-administrator users from logging into the server reduces the risk of unauthorized system changes and increases the cybersecurity of your system.

Change the SQL Server Express sa account password

If SQL Server Express is installed, with SQL Server authentication, through the PME installer, change the sa account password after the installation is complete.

Configure session timeout settings

You can configure session timeout settings in **Web Applications** > **Settings** > **Security** > **Session Timeout**. See Session timeout for information on this feature.

Configure system integration security settings

You can configure system integration settings in **Web Applications** > **Settings** > **Security** > **Integrations**. See System integration security for information on this feature.

Do not install or use a web browser on the server computer

Using a web browser on a server computer increases the vulnerability of the server and the network. Access PME web clients on client computers only, not on the server.

RECOMMENDATION: Remove the PME Web Applications shortcuts from the server.

Set up your network security

Set up the network security measures for your IT and device networks.

Disable unused IP ports

Disable or block IP ports that are not required for the operation of your system. See IP Ports for details on PME port requirements.

Disable unused hardware ports

Computer ports and inputs, such as USB ports or DVD drives are not required for PME to function correctly. These inputs can be permanently disabled if necessary. The same applies to the AutoRun and AutoPlay functionality which can also be disabled without affecting the operation of

the software.

Administering

This section provides information on how to help secure your system during the Administering phase.

Renew security certificate

Renew the security certificate before it expires.

Securely store the system key

See Protect the System Key for details.

Apply PME updates

Install software updates that apply to your system when they become available. Check the PME Exchange Community (requires login) or the Schneider Electric Exchange - EcoStruxure Power Monitoring Expert (Portal) for available updates, or contact your service provider.

Verify update file integrity and authenticity

See Verify install file integrity and authenticity for details.

Apply OS and SQL Server updates

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Apply the latest updates and hotfixes to your Operating System and software.

Failure to follow these instructions can result in death, serious injury, equipment damage, or permanent loss of data.

Critical and routine Windows and SQL Server updates can be applied to the operating systems hosting the PME server and clients without prior approval by Schneider Electric.

Consider implementing best practices, such as:

- Establish a reliable process for finding and applying the latest security updates.
- Use systematic procedures governed by corporate policy.
- Use automated scanners for detecting missing patches, misconfigurations, use of default accounts, and so on.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Before installing the update, verify that the system is not performing critical control actions that may affect human or equipment safety.
- Verify correct system operation after the update.

Failure to follow these instructions can result in death or serious injury.

⚠ WARNING

INACCURATE DATA RESULTS

- Before installing the update, verify that the system data results are not used for critical decision making that may affect human or equipment safety.
- Verify correct system data results after the update.

Failure to follow these instructions can result in death, serious injury, equipment damage, or permanent loss of data.

Review user accounts on a regular basis

Review PME user accounts on a regular basis. Update passwords and user permissions, and remove unused accounts as required.

RECOMMENDATION: Use Windows users instead of standard users in your PME system to improve cybersecurity. Windows offers advanced user management functions, such as enforcing password strength and limiting the number of invalid login attempts. These functions are required for IEC 62443 compliance, the global standard for industrial automation control system security.

NOTE: To only use Windows users, replace any existing standard users in the system with Windows users. Disallow logins for standard users in Web Applications, this disables the **supervisor** user.

Keep network security up-to-date

Keep security related networking tools and equipment up-to-date and working as expected.

NOTE: Network security equipment, such as firewalls, are complex devices and must be maintained by trained individuals.

Keep computer hardware secure

See Plan your site security for more information.

Perform security audits

Perform comprehensive system security audits on a regular basis. Regularly scan and verify security.

Consider implementing best practices, such as:

- Check the OS and PME system logs.
- Check performance monitor profiles

Decommission

Decommissioning removes PME files to prevent potential disclosure of sensitive, confidential and proprietary data and software from your system. You risk disclosing your power system data, system configuration, user information, and other sensitive information if you don't decommission. We strongly recommend you decommission your system at the end of its life.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

Before decommissioning, verify that the system is not performing critical control actions that may affect human or equipment safety.

Failure to follow these instructions can result in death or serious injury.

⚠ WARNING

INACCURATE DATA RESULTS

Before decommissioning, verify that the system data results are not used for critical decision making that may affect human or equipment safety.

Failure to follow these instructions can result in death, serious injury, equipment damage, or permanent loss of data.

To decommission PME you have two choices, **Destroy** or **Overwrite.**

Destroy: Choose this if you do not need to use your hard drives for any other software.

Overwrite: Choose this if you still need to use your hard drives for other software. This method uses a commercial tool to put random data in place of PME files on your hard drives.

See Decommissioning Reference for detailed instructions.

IT Requirements

This section provides information on specifications and requirements related to information technology (IT) components, such as computer hardware, operating environment, and networking.

Use the links in the following table to find the content you are looking for:

Topic	Content
Computer Hardware	Computer types, CPU, RAM, and HDDs.
Operating Environment	OS, DB server, Web browser, and other compatible software.
Network connectivity	Required network shares, Windows domain compatibility, IPv6 compatibility, and IP port requirements.
Other IT considerations	Computer name limitations, display resolution.

Computer Hardware

The performance of a computer is determined by the following factors:

- Computer type (desktop, workstation, or server)
- Central processing unit (CPU)
- Random-access memory (RAM)
- Data storage, for example Hard Disk Drive (HDD)

When choosing the computer hardware for your PME system, you need to consider the following:

- Number of devices in the system
- Number of concurrent users
- System performance expectations
- Data exchange with other systems
- Historical data logging needs
- System availability and recovery needs

NOTE: Undersized computer hardware is a common source of performance issues with PME systems.

Choosing Computer Type, CPU, and RAM

The computer type, CPU, and RAM determine the overall performance and reliability of the system. CPU is important for device communications and RAM affects SQL Server performance.

As a starting point for the selection of these components, we are defining two different system categories, **Basic Systems** and **Advanced Systems**. Decide which category best describes your system needs and then use the information provided in the tables below to define your computer hardware specifications.

Basic Systems

A *basic system* is defined by any of the following characteristics:

- Factory default measurement logging (logging frequency ≥ 15 minutes)
- No custom applications
- No Power Quality Performance monitoring
- Only a small number of branch circuit monitor devices in the system
- A mix of device type with approximately:
  - 70% entry level devices (for example iEM3xxx)
  - 20% intermediate level devices (for example PM55xx)
  - 10% advanced level devices (for example ION9000)

Minimum recommended computer hardware for servers in Basic Systems:

System Size	Devices	Users	Computer Hardware
Small	≤ 100	≤ 5	Desktop Intel Core i5 (4 core)* 8 GB (RAM)
Medium	≤ 250	≤ 10	Workstation Intel Xeon Bronze (6 core)* 16 GB (RAM)
	≤ 600	≤ 10	Server Intel Xeon Bronze (8 core)* 24 GB (RAM)
Large	≤ 2500	≤ 10	Server Intel Xeon Silver (10 core)* 32 GB (RAM)

*Equivalent or higher processor

Advanced Systems

An *advanced system* is defined by any of the following characteristics:

- Custom measurement logging with <15-minute intervals
- Custom applications using the VIP module
- Power Quality Performance monitoring
- Large number of concurrent users
- High percentage of advanced level devices in the system
- Large number of branch circuit monitor devices in the system
- Large scale data exchange with third party systems (for example through OPC, ETL, or EWS)
- Other resource intensive software systems installed on the same computer
- Distributed Database architecture

Minimum recommended computer hardware for servers in Advanced Systems:

System Size	Devices	Users	OPC Tags	Computer Hardware	RAM		
					Standalone architecture	Distributed Database architecture - Application Server	Distributed Database architecture - Database Server
Small	≤ 100	≤ 15	5000	Workstation Intel Xeon W-21xx (4 Core)*	16 GB	16 GB	16 GB
Medium	≤ 250	≤ 20	10000	Server Intel Xeon Bronze (8 core)*	24 GB	16 GB	24 GB
	≤ 600	≤ 35	30000	Server Intel Xeon Silver (10 core)*	32 GB	24 GB	32 GB
Large	≤ 2500	≤ 50	50000	Server Intel Xeon Silver (12 core)*	64 GB	32 GB	64 GB

*Equivalent or higher processor

Client Computers

Since all the data processing is done on the server, the client computer hardware recommendations are the same for Basic Systems and Advanced Systems.

Minimum recommended computer hardware for clients:

- Engineering Client
  - Intel Core i3 (2 core or better)
  - 4 GB of RAM
- Web Client
  - 2 GHz, Dual Core processor
  - 4 GB of RAM
  - Monitor resolution of 1280 x 960 pixels

NOTE: To improve the information display, we recommend a minimum monitor resolution of 1440 x 1080.

Choosing Data Storage

The type of data storage determines the historical data access performance and the amount of historical data that can be stored in the system. Data storage configurations are also important for system availability and recovery.

Storage Size

The data storage must have enough space for the different programs and applications that are running on the computer. This includes space for the historical data that is recorded by the system and some free space as a buffer.

The following table shows the estimated storage space that is required, without the historical data logs. The estimates are rounded up and allow for updates and system maintenance.

Component	Storage Space
Windows Operating System software	100 GB
Microsoft SQL Server software	2 GB
PME software	5 GB
PME system databases	5 GB
PME historical database	**(see below)**
Free space	30% of the storage size

PME historical database

The storage space that is required for the historical database (ION_Data), is equal to five times the size of the main database file (ION_data.mdf):

```
Storage Space for ION_Data (GB) = 5x .mdf (GB)
```

It can be broken down into the following components, where ION_data.mdf size is the estimated maximum size when PME is in steady-state:

Component	Storage Space
Main database file (.mdf)	(1x) ION_data.mdf size
Transaction log file (.ldf)	(1x) ION_data.mdf size
Last two full backups	(2x) ION_data.mdf size
Free Space for Backups or tempDB	(1x) ION_data.mdf size
Total	**(5x) ION_data.mdf size**

Optionally, the component can include storage of archive database when data archive and / or trim strategy is performed. For **medium to large systems** (250-2,500 devices), we recommend you to perform data archive and / or trim strategy to support healthy database. See Archive and Trim strategy for more information.

NOTE: Use the Database Growth Calculator tool to estimate the database size for 'n' years of archive data. The tool is available through the Exchange Community. See Resources for link information.

The estimates above are based on the following assumptions:

- The .ldf file is typically just 10% of the .mdf size, but occasionally expands to 100% during normal operation.
- The system default is to keep two database backups.
- 100% of the .mdf size is required for free space. The tempDB will occasionally expand to 100% of the total .mdf size, but not at the same time as a backup. If the backups and tempDB are on different hard drive groups, each of them require x1 .mdf in hard drive space.

Main Database File Size (ION_data.mdf)

Unlike the system software, the historical database size is continuously growing. Its size and growth can be estimated based on the amount of:

- Factory default measurement logging
- Custom measurement logging
- Power quality event logging

Also, the database is configured to automatically grow by 10% when required to create room for additional measurements. This growth operation can occur at any time and you need to consider it in the database size calculations.

NOTE: Use the Database Growth Calculator tool to estimate the database growth for your system. The tool is available through the Exchange Community. See Resources for link information.

For optimum performance, minimize database auto-growth by configuring the database container to the estimated maximum size after growth. During commissioning, use the Database Growth Calculator tool to estimate the maximum ION_Data database size based on your data retention policy, and configure the database container to the estimated maximum value. For example, if the ION_data database file is estimated for 2 TB and above in container size then split the database in to multiple files. For more details on how to set database container size and / or to add new files to be database, see Increase the Size of a Database. You can view the size of the ION_Data database using the Database Manager tool.

Storage Performance and Availability

Storage Type

The two main storage solutions that are available are Hard Disk Drives (HDD) and Solid-State Drives (SSD). HDDs are good at providing cheap, bulk storage for non-performance critical data. SSDs are good at providing strategic storage for high performance data. We recommend that you use SSDs for the Microsoft Message Queuing (MSMQ) storage in medium, large, and extra large PME systems.

Storage Configuration

Storage drives can be configured as single drives or a number of separate drives. For a small Basic Systems, a single drive is sufficient. For all other systems, we recommend that you divide the data storage into different drives.

For **medium to large systems** (250-2,500 devices):

Drive Type	Components
SSD	Software: OS, PME, SQL Databases: ApplicationModules, ION_Network, ION_SystemLog MSMQ
HDD or SSD	SQL tempdb
HDD or SSD	ION_Data
HDD or SSD	ION_Data.ldf
HDD or SSD	ION_Data archive database, database backups

RAID Systems

In addition to separating the software components into different drive groups, redundant arrays (RAID) can be used to improve performance and add simple redundancy. In a RAID 1 configuration, one drive is a complete copy of a second drive. If either of the two drives stops operating, the other takes over without any data loss. The faulty drive can then be replaced to restore the RAID configuration.

Recommended RAID 1 configurations:

2x Drive

Component	Group 0 Drive 1+2
OS	✓
tempDB	✓
MDF	✓
LDF	✓
Backups and archive	✓

4x Drive

Component	Group 0 Drive 1+2	Group 1 Drive 3+4
OS	✓	
tempDB		✓
MDF	✓	
LDF		✓
Backups and archive		✓

6x Drive

Component	Group 0 Drive 1+2	Group 1 Drive 3+4	Group 2 Drive 5+6
OS	✓		
tempDB	✓		
MDF		✓	
LDF			✓
Backups and archive			✓

8x Drive

Component	Group 0 Drive 1+2	Group 1 Drive 3+4	Group 2 Drive 5+6	Group 3 Drive 7+8
OS	✓			
tempDB		✓		
MDF			✓	
LDF				✓
Backups and archive				✓

NOTE: Plan for system growth by having a computer with space for additional drives. This makes it easy to add additional storage as the system grows.

NOTE: It is possible to use other RAID configurations, such as RAID 0 or RAID 5. These configurations are not discussed in this document.

Operating Environment

PME supports the following environments and software:

NOTE: The operating system and SQL Server combination you choose must be supported by Microsoft. This applies to edition, version, and 32-/64-bit.

Software	Supported Versions
Operating system	Windows 10 Professional/Enterprise Windows Server 2012 Standard Windows Server 2012 R2 Standard/Enterprise Windows Server 2016 Standard Windows Server 2019 Standard
Database system**	SQL Server 2012 Express SQL Server 2014 Express SQL Server 2016 Express SQL Server 2017 Express SQL Server 2019 Express (included with PME 2021) SQL Server 2012 Standard/Enterprise/Business Intelligence SQL Server 2014 Standard/Enterprise/Business Intelligence SQL Server 2016 Standard/Enterprise/Business Intelligence SQL Server 2017 Standard/Enterprise/Business Intelligence SQL Server 2019 Standard/Enterprise/Business Intelligence
Virtual environment***	VMWare Workstation 10 VMWare ESX1 6.0 Oracle Virtual Box 5.0.4 Microsoft Hyper-V from Windows 8.1, Windows Server 2012 Citrix XenServer 6.2 Parallels Desktop 10 QEMU-KVM
Microsoft Excel	Microsoft Excel 2013, 2016, 365
Desktop Web browser	Google Chrome version 42 and later Mozilla Firefox version 35 and later Apple Safari versions 7 or 8 and later Microsoft Edge
Mobile Web browser	Safari on iOS8.3+ operating systems, Chrome on Android systems
.NET Framework	.NET 4.6 or higher

** PME includes a free version of SQL Server Express. You have the option to install this Express version during the installation of PME, if you don't want to use a different SQL Server.

*** You must configure virtual environments with a supported Windows operating system and SQL Server edition. It is possible to mix virtual and non-virtual environments for PME server and clients.

Windows Updates

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Apply the latest updates and hotfixes to your Operating System and software.

Failure to follow these instructions can result in death, serious injury, equipment damage, or permanent loss of data.

Critical and routine Windows Updates can be applied to the operating systems hosting the PME server and clients without prior approval by Schneider Electric.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Before installing the update, verify that the system is not performing critical control actions that may affect human or equipment safety.
- Verify correct system operation after the update.

Failure to follow these instructions can result in death or serious injury.

⚠ WARNING

INACCURATE DATA RESULTS

- Before installing the update, verify that the system data results are not used for critical decision making that may affect human or equipment safety.
- Verify correct system data results after the update.

Failure to follow these instructions can result in death, serious injury, equipment damage, or permanent loss of data.

Localization

PME supports the following languages:

English, Chinese (Traditional and Simplified), Czech, French, German, Italian, Japanese, Korean, Norwegian (Bokmål), Polish, Portuguese, Russian, Spanish, Swedish, and Turkish.

A non-English version of PME only supports an operating system and SQL Server of the same locale. For example, a Spanish version of the product must be used with a Spanish version of SQL Server and an operating system with a regional setting of Spanish.

The English version of PME can be used with a supported language, non-English operating system and SQL Server as long as both have the same locale. For example, an English version of the product can be used with a German version of SQL Server and an operating system with a regional setting of German.

Operating System considerations

Windows or Windows Server?

PME supports both Windows and Windows Server operating systems. However, we recommend you use the Windows Server for the following reasons:

- Windows Server can use server-class computer hardware. It can access more CPUs and more RAM than Windows. For example, Windows 10 is limited to two physical CPUs.
- Windows Server offers better performance for running PME services.

32-bit or 64-bit systems?

PME supports 64-bit operating systems only.

SQL Server considerations

Express Version or Full version?

Microsoft SQL Server is available as a free, scaled down Express version, and as a priced, full server version. You can use both versions with PME. However, the Express version has the following built in limitations:

- Maximum database size of 10 GB.
- No SQL Server Agent service.
- Limited to lesser of 1 socket or 4 cores.
- Limited to use a maximum of 1 GB of the total system RAM.

In addition, PME has the following limitations when used with SQL Server Express:

- Only supported for Standalone systems, not for Distributed Database systems.
- Not supported for systems with Power Quality Performance module.

NOTE: PME includes a free version of SQL Server Express. You have the option to install this Express version during the installation of PME, if you do not want to use a different SQL Server.

Existing or new SQL Server?

You can use PME with an existing SQL Server, or you can install a new one. The following table lists the installation requirements for new and existing SQL Server types:

Type	Description
New SQL Server Standard	PME requires a certain configuration of the SQL Server.
New SQL Server Express	PME includes a free version of SQL Server Express. You have the option to install this Express version during the installation of PME.
Existing SQL Server Standard	To use an existing instance of SQL Server Standard , the SQL Server setup wizard must be rerun to configure the software correctly for use with PME.
Existing SQL Server Express	The PME installer can add a new instance to an existing SQL Server Express for use with PME.

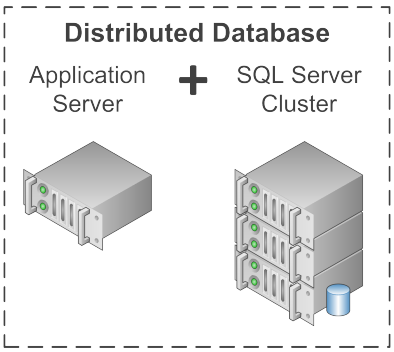
NOTE: The operating system and SQL Server combination you choose must be supported by Microsoft. This applies to edition, version, and 32-/64-bit.

SQL Server clustering

Clustering refers to a group of two or more SQL Servers that work together and appear as a single server to the outside. When a client connects to an SQL Server cluster, it appears that there is only a single SQL Server. In case of a server failure, the remaining servers take over without an interruption. Using clustering increases system availability.

PME can be used in a clustered environment when deployed in a Distributed Database architecture.

- The **Application Server** is deployed in a non-clustered environment.
- The **SQL Server** component is deployed in the clustered environment.



NOTE: SQL Server clustering is only supported for Distributed Database systems, not for Standalone systems.

SQL Server compute capacity

When using SQL Server in virtualized environment, there is a defined compute capacity limit on the sockets and cores of CPU as per the SQL Server edition. The performance of the SQL server depends on this compute capacity limit. See Compute capacity limits by edition of SQL Server for more information. Plan your SQL server virtualized environment deployment as per the compute capacity limit to achieve better performance.

Network connectivity

Network communication

The PME server, database server, and clients must be able to communicate with each other over the network using TCP/IP protocol. The licensing component of PME requires that PME clients and server can resolve each other's address by name (not just fully qualified domain name or IP address). If a proxy server is used on the network, then a local address bypass must be configured on the PME server.

An Internet connection is not required for PME to function correctly.

Network shares

Engineering Clients require that the **Power Monitoring Expert** folder on the PME server is shared with full read and write permissions. File and Printer Sharing must be enabled.

Windows Domain compatibility

Domain membership is not required for PME to function.

- PME can be installed on servers in a domain environment, however it cannot be installed on domain controllers. If PME is installed on a server that is subsequently changed to a domain controller, the software ceases to function correctly.
- For Distributed Database installations of PME, the Database Manager tool can only be used if the database server and the PME application server are in the same domain. The Database Manager cannot be used, in a distributed database installation, if the database server and the PME application server are in workgroups.
- A domain account is required for Side-by-Side upgrades of distributed systems using the Configuration Manager Tool. This domain account must be:
  - A member of the Administrators group on the PME server
  - Added as a Login in SQL Server with sysadmin role in the database instance.
- PME supports Windows Active Directory services for user account sharing.

IPv6 compatibility

PME supports IPv6 (and IPv4) for communications with metering devices. The software components of PME require IPv4. That means PME can be used on computers with single stack IPv4 or dual stack IPv4/IPv6 network adapters.

IP Port Requirements

PME uses certain ports for the communication between its components and the connected devices. Which ports are required for a specific installation depends on the system configuration and the monitoring devices used. See IP Ports for a list of relevant ports.

Other IT considerations

Internet Information Services (IIS) .NET Trust Level

The .NET Trust Level for PME web applications and Default Web Site must be set to **Full (internal)**, in IIS Manager. See IIS Application Pools for a list of PME web (ASP.NET) applications.

PME Server name limitations

The computer name for the PME server must have 15 characters or less, and use only letters, numbers or hyphens.

NOTE: The computer name must not be changed after the PME software is installed. If the computer name is changed after the install, the software ceases to function correctly. If that occurs, contact Technical Support for assistance.

Display resolution

The minimum display resolution for PME user interfaces is 1280 x 960 pixels.

Device Networks

This section provides information on the communication links between the software and the monitoring devices.

Use the links in the following table to find the content you are looking for:

Topic	Content
Device networks overview	Device network basics and the supported protocols and device types.
Network types	Ethernet and serial communication networks.
Network performance	Ways to improve the device communication performance.
Time synchronization	Time synchronization on the monitoring device network.
Tools	The Daisy Chain Calculator tool.

Device networks overview

PME is a software application that processes, stores, analyzes, and displays power system data and information. PME collects the source data from devices that are installed in the electrical system that is being monitored. Each device must be connected to a communication network through which the software initiates the data retrieval.

Examples of monitoring devices include:

- Power and energy monitoring devices
- Contactors and protection relays
- Circuit breaker trip units
- Smart panels
- Power quality mitigation equipment
- Programmable Logic Controllers (PLCs)

PME supports the following communication protocols:

- Modbus™ TCP
- Modbus™ RTU
- ION™
- OPC DA

For a device to be compatible with PME, it must support one of these communication protocols.

Network types

The two basic types of communication networks for PME are Ethernet and serial.

Ethernet (TCP) networks

Ethernet (TCP) device networks can be integrated into regular corporate LANs or they can be separate, independent networks, providing a higher level of security and availability.

Devices are configured in PME by providing fixed IP addresses (IPv4 or IPv6) and ports, or based on host names. Host names must be used for devices with dynamic address assignment, for example using the DHCP protocol. When host names are used in PME, then a host name resolution mechanism is required by the external IT network.

Device communications are based on encapsulated Modbus or ION protocol and are not encrypted. Bandwidth requirements per device are typically low, but depend heavily on the amount and type of data requested from the device by PME.

Ethernet (TCP) networks are in many ways superior to serial networks and we recommend that you use Ethernet (TCP) networks whenever possible.

Serial device networks

Serial communication is the traditional way of connecting devices to PME. Serial communications require an intermediate converter or gateway, for example a Link150, to establish a network connection. The performance of a serial communication network can become the limiting factor for the overall system performance.

NOTE: If you use an ION meter as a gateway, with Ethergate protocol, you lose the ability to multi-master the serial devices.

Serial device communications are based on Modbus RTU or ION protocol and are not encrypted. See Tools for information on how to design a serial network.

PME also supports communication through telephone modems.

Reasons for using serial networks include:

- The device type only supports serial communications.
- A serial communication network is already in place.
- The existing Ethernet (TCP) networks do not allow the connection of monitoring devices.
- Serial communications are less affected by electrical noise.

Ethernet (TCP) networks are in many ways superior to serial networks and we recommend that you use Ethernet (TCP) networks whenever possible.

Network performance

Communications between the software and the devices consist of:

- On demand, real-time data requests, for example for Diagrams or Dashboards displays.
- Periodic polling and uploading of data logs, events, and waveform records.

To optimize the on demand and background polling performance, consider the following when designing the system and the communication network:

- Real-time data polling periods should be set to meet the user needs. Do not poll with high speed when it is not needed. Real-time data clients include Vista, Diagrams, OPC, VIP, Trends, and EWS.
- Disable devices that are not presently commissioned or functional. This includes devices that are inoperable, or that have a communication error rate >5%.
- Connect high-end devices with power quality monitoring features, such as the ION9000, directly through Ethernet, not serial. These devices can generate large amounts of logged data, such as power quality data, which requires a high bandwidth connection to the monitoring software. If a direct Ethernet connection is not possible, then connect the devices through small serial loops, with one or two devices per loop.

  NOTE: Test the data upload performance when using high-end devices on serial networks. Depending on configuration and operating conditions, it is possible for devices to have a higher data generation rate than can be uploaded over a serial network.

  NOTE: The ION9000T, a high-end power monitoring device with high speed transient capture, will not upload high speed transient waveform data to the software if it is connected through a serial connection.
- Setup the devices to only log those measurements that are needed to meet the user needs.
- Schedule the log uploads to occur at times when the system usage is low, for example during night time or off hours.
- Use the Daisy Chain Calculator tool to determine the maximum number of devices in a serial loop for your system. See Tools for more information.
- In most applications, Ethernet networks will provide a better performance than serial networks.

Time synchronization

To maintain accurate time in the monitoring system, the devices must be time synchronized. Depending on the synchronization mechanism, different levels of time accuracy can be achieved. PME has the ability to synchronize devices to the PME server computer clock. This can be done over serial networks and Ethernet networks.

The time synchronization to the computer clock using the regular communications protocols can maintain a system time accuracy in the range of seconds. This is accurate enough for many applications. However, for applications such as power event analysis or protection coordination studies, that require high absolute and relative time accuracy, you need to use other time synchronization methods for the devices, such as PTP or GPS time synchronization.

NOTE: Time synchronization might be disabled by default in certain monitoring devices. Configure time synchronization for your devices and the software as part of the device or system deployment. Choose a single time synchronization source per device.

Tools

Use the Daisy Chain Calculator tool to design your serial communication networks. This tool helps you estimate the communication utilization for serial daisy chains. You can use it for new system design and for optimizing existing systems.

NOTE: The Daisy Chain Calculator is available through the Exchange Community. See Resources for link information.

System maintenance and Disaster recovery

This section provides recommendation related to system maintenance and disaster recovery.

Use the links in the following table to find the content you are looking for:

Topic	Content
System maintenance	Provides information on database maintenance and recommended actions.
Disaster recovery strategy	Provides information on disaster recovery and recommended strategy.

System maintenance

Once a PME system is installed and commissioned, it must be maintained on a regular basis. Without periodic, proactive system maintenance, system performance degrades over time and the system operates with poor performance (timeouts and sluggish response) and eventually becomes unusable.

This section provides guidelines and recommendations for creating a maintenance schedule. Proper adherence to the maintenance guide ensures a steady-state operation of a PME system.

This section does not detail troubleshooting system issues, but identifies the steps to develop a maintenance plan that should allow for a commissioned system to continuously run at optimal performance.

A maintenance plan keeps your PME system healthy. A comprehensive maintenance plan starts in the system planning stage before commissioning. The plan should include frequent monitoring and system reviews, and maintenance tasks to ensure the system is operating under healthy conditions.

The following sections provide recommendations for developing your maintenance plan:

- Designing for maintenance
- Database maintenance
- System health review

Designing for maintenance

Before installing and deploying a system, it is important to plan and design the IT architecture in support of maintenance and backup activities. Maintenance and backup activities often require additional resources (CPU, RAM and hard drive space) to perform and complete the activity. The recommendations are as follows:

- System sizing

  Size a system for the final state (for example: maximum devices, maximum logging parameters, etc) to ensure that the system runs in a healthy state for a longer time. See IT Requirements for recommended system sizing.

- Storage space allocation

  Make sure there is enough hard drive space to perform database maintenance, archive and trim operations. See Storage Performance and Availability for recommended hard drive sizing.

- Disk I/O performance

  Disk read/write operations impacts system performance. Plan to have different storage devices installed for the system files, the database files, and the Microsoft Message Queuing (MSMQ) files. See Choosing Data Storage for recommended storage information.

- Pre-size databases

  By default, ION_Data database is configured with a 10% auto-growth parameter. This growth operation can lead to a fragmented database and hard drive and can impact database performance over time. To minimize the use of the auto-growth feature, pre-allocate hard

drive space for the ION_Data database during system commissioning, including systems running SQL Server Express. See Database growth topic of System Guide for recommendation on database growth.

- Database auto growth

  For systems expected to have large ION_Data databases (> 100 GB), change the default auto-growth setting to a fixed size rather than by percentage (Default is 10%). In this case, the database auto-grows when the database exceeds the preset container size. This ensures better control of database growth. Auto-growth events are expensive operations that slow down the performance of your database. Take the following preventive steps to ensure your auto-growth is in control:

  - Minimize future auto-growth events by monitoring the growth of your databases, and re-establishing auto-growth settings when a database growth profile changes.
  - Monitor auto-growth events so you can be alerted when your databases grow.
  - Consider defragmenting your database file system.

  See SQL Server Database Growth and Autogrowth Settings for more information.

Database maintenance

PME uses databases to store information such as system configuration, data logs, and system event log messages. These databases must be maintained to preserve performance, manage disk space usage, and guard against data loss in case of database failure. Maintenance is the key to a healthy system that supports system longevity and future scalability. You must not ignore maintenance. Non-maintenance may lead to system downtime and you might need to rebuild the system from scratch.

NOTICE
LOSS OF DATA • Back up the database at regular intervals. • Back up the database before upgrading or migrating the system. • Back up the database before trimming it. • Back up the database before making manual database edits. • Verify correct database behavior after making database or system changes. **Failure to follow these instructions can result in permanent loss of data.**

Database maintenance for PME includes the following key activities:

- Performance maintenance
- Accurate and up-to-date query statistics
- Minimize index fragmentation
- Data archive and trim
- Database integrity check

Based on the key activities, see Consolidated recommendation for database maintenance.

Performance maintenance

For performance maintenance, enable and schedule the following daily maintenance tasks for all PME systems of any configuration:

Database	Type of Data	Maintenance Tasks*		
		Maintenance (update statistics and index defragmentation)	Trim**	Size Notification
ApplicationModules	Web Applications related configuration data and system event log entries.	✓	✓	–
ION_Data	Historical power system data such as interval data logs, waveforms and alarms.	✓	✓	✓ **NOTE**: For systems with SQL Server Express, enable SQL Express Database Size Notification.
ION_Network	Device network and other system configuration data.	✓	–	–
ION_SystemLog	Non-Web Applications related system event log entries.	✓	✓	–

* See Default maintenance task settings for basic task definitions.
** Keep the last 30 days of data.

In Standalone PME systems, the database maintenance tasks are pre-configured and scheduled to run automatically by default. For Distributed Database PME systems, you need to configure the tasks and set up the schedules manually.

For more information, see the Database maintenance section in the Configuring chapter of this guide.

Accurate and up-to-date query statistics

SQL Server uses statistics to create query plans that improve query performance. As the database increases and holds more data, the statistics becomes less relevant over the time. Updating statistics ensures that queries run with relevant statistics.

For all systems, it is recommend to update database statistics daily. The following table shows the default database maintenance task schedules for standalone systems:

Database	Task*	Trigger Time
ApplicationModules	Maintenance	Daily at 03:30
ION_Data	Maintenance	Daily at 02:00
ION_Network	Maintenance	Daily at 07:30
ION_SystemLog	Maintenance	Daily at 07:05

* See Default maintenance task settings for basic task definitions.

In distributed systems, the database maintenance tasks are not pre-configured. You need to set up these tasks manually.

These scheduled tasks trigger the **DatabaseMaintenance.ps1** Windows PowerShell script. This script executes the local [Maintenance].[UpdateStatisticsAll] stored procedure in each database.

Check the PME system logs and SQL Server logs to confirm that the scheduled tasks are completed successfully. The log might report errors if an issue arises. As the database grows, these jobs will take longer time to complete.

See Microsoft's SQL Server documentation on SQL Server Query Statistics for more information about query statistics.

For more information, see the Database maintenance section in the Configuring chapter of this guide.

Minimize index fragmentation

Database index maintenance is important to ensure optimal performance. When data is written to the databases, fragmentation occurs. Heavy fragmented indexes can degrade query performance and reduce PME's response time.

To minimize index fragmentation, monitor the fragmentation regularly and perform re-indexing.

For small to medium size systems:

It is recommend to re-index daily. The following table shows the default database maintenance task schedules for standalone systems:

Database	Task*	Trigger Time
ApplicationModules	Maintenance	Daily at 03:30
ION_Data	Maintenance	Daily at 02:00
ION_Network	Maintenance	Daily at 07:30
ION_SystemLog	Maintenance	Daily at 07:05

* See Default maintenance task settings for basic task definitions.

In distributed systems, the database maintenance tasks are not pre-configured. You need to set up these tasks manually.

These scheduled tasks trigger the **DatabaseMaintenance.ps1** Windows PowerShell script. This script executes the local [Maintenance].[DefragIndexAll] stored procedure in each database.

Check the PME system logs and SQL Server logs to confirm that the scheduled tasks are completed successfully. The log might report errors if an issue arises. As the database grows, these jobs will take longer to complete.

For large systems:

For large systems with ION_Data growing over 100 GB in size, it is important to review the frequency of the [ION_Data] database maintenance scheduled task and switch to running them manually.

Index fragmentation in ION_Data is unavoidable for large systems because of the amount of data written to the system and queried on a regular basis. Index fragmentation is also common when database reads exceeds database writes, that is, when PME is configured with added components to move data from PME to another non-PME system.

For large systems, you need to monitor the index fragmentation daily. To monitor, run the following SQL commands against the database:

- DBCC SHOWCONTIG
- sys.dm_db_index_physical_stats

Both the commands generate a report on index fragmentation. The time it takes to complete these statements depend on the amount of data in the table and the level of fragmentation. The more fragmented the index, the longer the query will run. You should expect the query to return results within 1 to 20 minutes.

DBCC SHOWCONTIG

DBCC SHOWCONTIG displays fragmentation information for the data and indexes for specified tables.

NOTE: This command applies to SQL Server 2008 to 2019 and is expected to be deprecated in a future version of SQL Server.

For ION_Data, run the following commands:

```
USE ION_Data

GO

DBCC SHOWCONTIG WITH TABLERESULTS, ALL_INDEXES
```

Review the output from DBCC SHOWCONTIG for the following three statistics:

Average Page Density:

Shows the accurate indication of how full your pages are. A high percentage means the pages are almost full, and a low percentage indicates much free space. This value should be compared to the fill factor setting specified when the index was created to decide whether or not the index is internally fragmented. The fill factor is the percentage of space on each leaf-level page that should be filled with data, and it is applied only when the index is created, rebuilt or reorganized. If the Average Page Density and Fill Factor are close in value, then it would suggest that there is little index fragmentation.

Scan Density:

Shows the ratio between the Best Count of extents that should be necessary to read when scanning all the pages of the index, and the Actual Count of extents that was read. This percentage should be as close to 100% as possible. Defining an acceptable level is difficult, but anything under 75% definitely indicates external fragmentation.

Logical Scan Fragmentation:

Shows the ratio of pages that are out of logical order. The value should be as close to 0% as possible and anything over 10% indicates external fragmentation.

See DBCC SHOWCONTIG (Transact-SQL) for more information on DBCC SHOWCONTIG command.

sys.dm_db_index_physical_stats

sys.dm_db_index_physical_stats also returns size and fragmentation information for the data and indexes of the specified table or view in SQL Server. This command is available in SQL Server 2005 or later.

For ION_Data, run the following commands to show fragmentation details for tables with more than 100,000 rows and a fragmentation level of greater than 50%. Comment out the WHERE clause to show results for all table indices. The output is sorted by fragmentation level from highest to lowest.

```
USE ION_Data
GO
SELECT
      DB_NAME(db_id()) AS DatabaseName,
      OBJECT_NAME(object_id) AS TableName,
      object_id,
      index_id,
      index_type_desc,
      avg_fragmentation_in_percent,
      fragment_count,
      page_count,
      avg_page_space_used_in_percent,
      record_count
FROM
      sys.dm_db_index_physical_stats(db_id(),DEFAULT, DEFAULT,
DEFAULT, 'SAMPLED')
WHERE
      (record_count > 100000) AND (avg_fragmentation_in_percent > 50)
```

```
ORDER BY
      avg_fragmentation_in_percent DESC;
```

When reviewing the output from sys.dm_db_index_physical_stats, review the values in the avg_fragmentation_in_percent column. You should defragement the indexes, if the fragementation is 10% and above.

See sys.dm_db_index_physical_stats (Transact-SQL) for more information on sys.dm_db_index_physical_stats command.

Correcting index fragmentation

Any index with over 10% fragmentation should be corrected.

There are different corrective statements depending on the level of fragmentation. For PME, select the statements as follows:

Fragmentation Percentage	Corrective Statement	Remarks
10 to 30%	ALTER INDEX REORGANIZE	Reorganizing an index uses minimal system resources and is an online operation, which means PME can remain online during this operation.
> 30%	ALTER INDEX REBUILD WITH (ONLINE = OFF)	Rebuilding an index drops and re-creates the index. Depending on the type of index and Database Engine version, a rebuild operation can be done online or offline. For large indexes, it is recommended to perform this operation offline.

See Resolve index fragmentation by reorganizing or rebuilding indexes for more information on correcting index fragmentation.

Data archive and trim

The archive strategy supports data retention and compliance, while the trim strategy supports disaster recovery goals.

Archive and Trim shortens the backup process by keeping only business critical data in the live database and also reduces the resource demands in the disaster recovery efforts by shrinking the database to backup and restore.

Archiving is not recommended since it fractures the data into multiple databases. PME is unable to query multiple databases at the same time to make comparisons in the data. It is possible to run reports against an archived database, but it can only be done on one database at a time.

However, the ION_Data database may need to be reduced in size for two reasons:

- SQL Server Express is used as the database engine, which has a limit of 10 GB for the .mdf file.

- SQL Server (Standard or Enterprise edition) is used as the database engine and the ION_Data database has become so large that query performance (in Vista for example) is not acceptable to the PME system users. It is also important to ensure that the ION_Data database is trimmed well within the hard drive size, as it can affect the operation of PME.

For PME systems with considerable database growth (medium to very large systems), it is important to consider frequent removal of older and lesser used data from ION_Data. PME includes an ION_Data data archive maintenance task by default. The database archive task is pre-configured and disabled for standalone systems, while it must be manually added for distributed systems.

To determine if data archiving is needed, you must:

- Understand the importance of archive and trim
- Determine the data retention needs
- Develop the archive and trim strategy

Understand the importance of archive and trim

The purpose of the archive is to remove data from the live ION_Data database to reduce its overall size. An archive is a copy of a subset of data from the live ION_Data database based on a date range and the type of data (Data Records, Waveforms and Events).

When an ION_Data archive is created, it is attached to the SQL Server database engine so that its data is still accessible to Vista and Diagrams. However, the data is not available to other applications in the Web Applications component.

NOTE: Data archival in PME is different from the normal terminology of archiving. PME's archive task does not remove data from the database, it only copies data to the archive. Once the data is archived in PME, it cannot be re-imported back.

We recommend to manually trim the database of historical data after each archive task.

Determine the data retention needs

The live system only needs to hold as much data as needed for business. Consider the following questions along with the business use cases to determine the data retention needs:

- What is the oldest date of data that is needed for trends and alarms?
- Is it sufficient to review older data trends only through web reports or diagrams?
- What date range of data is needed for historical reporting – start and end dates?
- How often should data be archived?

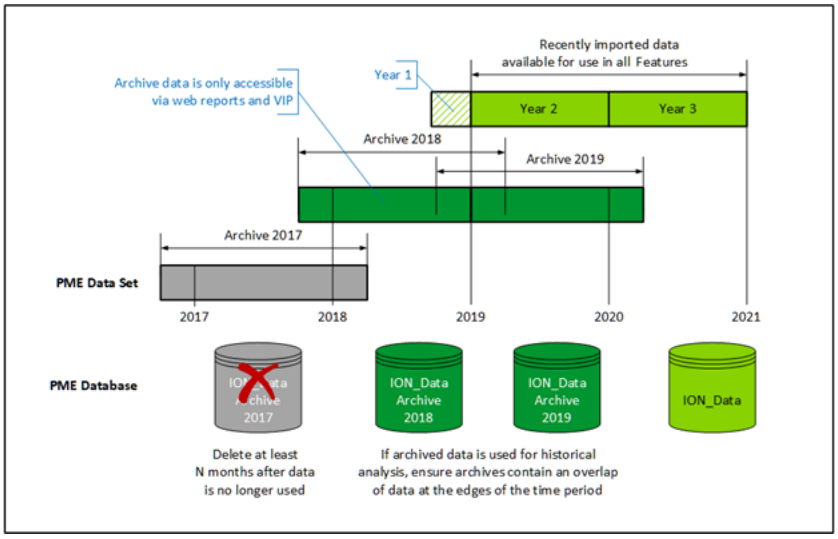
Develop the archive and trim strategy

These questions determine key aspects of the archive and trim strategy, in particular:

- When to archive data from the live database?
- When to trim data from the live database?
- When to delete historical archives?

Example: Archive and Trim Strategy

The following diagram illustrates an example ION_Data archive and trim strategy for a small to medium system that started data collection in Q4 2016 and the strategy planned till 2021.



Based on the business needs, the data retention requirements are:

- Perform analysis with at least two calendar years of data in the main PME system
- Reporting on the last 3 calendar years of data
- Data older than 3 calendar years can be deleted

The example strategy is as follows:

- Keep two calendar years of data in the main ION_Data database.
- Start archive activity at the end of Q1 of the third year.

  NOTE: There should be 2 years and 3 months of data in ION_Data.

  In this example, archive data from start of Q4 Year 1 to end of Q1 Year 3 into the database called ION_Data Archive Year 1. This results in a new archive database named ION_Data_Archive_2017 containing data from 01 September 2016 to 01 April 2018.
- Backup the newly created archive database.
- Schedule the archive activity once per year starting at the end of Q1 of the current year.

  NOTE: Archive the older year of data with an additional 3 months on each side of the year of interest.
- After each successful archive, backup the newly created archive database.
- Schedule the trim activity to trim data in the last 3 months of the dataset from the main ION_Data database.
- Schedule the trim to run every 3 months.
- When an archive database contains data older than 3 years, mark the archive database for deletion.
- Delete the marked archive database after 12 months of non-use.

NOTE: This strategy creates an overlap of data for every year.

Recommendation for archive and trim

- Archive and trim the ION_Data database often and in small batches. Together these two tasks reduce the size of ION_Data and its backup files.
- Archive historical data often even when disk space is not an issue or when not using SQL express.
- Trim historical data in small batches and often.
- Always perform a database trim after verifying a new archive.

Recommended consolidated archive and trim plan for systems

The recommended consolidated archive plan of ION_Data database for the different purpose of PME system are as follows:

Archive strategy parameter	Purpose of PME system		
	Analysis & decision making (Capacity management, Energy usage analysis, Power Quality compliance)	Real-time monitoring & troubleshooting (Electric distribution monitoring & alarming, Insulation monitoring, Backup power testing)	Critical large advanced distributed system (with mix of real-time and analysis based applications)
Maximum data retention (ION_Data and Archive databases)	4 years	1 year	4 years
Live data in ION_Data	3 years	1 year	2 years
ION_Data archives	Start after end of year 3	Not applicable	Start after end of year 2
Archive frequency	Annually	Not applicable	Every 3 months
Number of archives to store on server	1	Not applicable	8
Additional IT resources needed for archive databases*	Use database growth calculator to estimate size archive database	Not applicable	Use database growth calculator to estimate size archive database

*See Database growth topic of System Guide for recommendation on database growth.

The recommended consolidated trim plan of ION_Data database for the different purpose of PME system are as follows:

Trim strategy parameter	Purpose of PME system		
	Analysis & decision making (Capacity management, Energy usage analysis, Power Quality compliance)	Real-time monitoring & troubleshooting (Electric distribution monitoring & alarming, Insulation monitoring, Backup power testing)	Critical large advanced distributed system (with mix of real-time and analysis based applications)
Trim	Data with timestamps older than 3 years from today	Data with timestamps older than 1 year from today	Data with timestamps older than 2 years from today
Trim frequency	Monthly	Monthly	Monthly

Database integrity check

Database corruption is a rare event that is usually caused by inoperative hardware on the server. A database integrity check reviews the allocation and structural integrity of all objects in each database to ensure it is not corrupt.

Run DBCC CHECKDB in SQL Server Management Studio on all PME related databases once per month or quarter.

Check for errors reported in the output of DBCC CHECKDB. A database with integrity displays the following at the end of the output.

```
CHECKDB found 0 allocation errors and 0 consistency errors in database
'ION_Data'.
```

```
DBCC execution completed. If DBCC printed error messages, contact your
system administrator.
```

See DBCC CHECKDB (Transact-SQL) for more information on database integrity.

Consolidated recommendation for database maintenance

Based on the key activities discussed, the following is the consolidated recommendation for database maintenance as per the systems:

For all systems (Small, Medium, and Large):

- Schedule the ApplicationModules database trim task to run daily.
- Schedule the ION_SystemLog database trim task to run daily.
- If the number of connected devices have increased over time, review hardware and hard drive space requirements at least once per year to ensure server specifications meets growing demand.
- Review the frequency of the ION_Data database maintenance task as the system grows. Reduce the frequency from daily to weekly to monthly as the database grows and the maintenance tasks (Update statistics and re-indexing) take longer to complete.
- Never shrink the database container; it causes fragmentation.
- Archive and trim the ION_Data database regularly and in batches, such as 3 to 12 month data sets. Refer to Historical Data Archive and Trim Strategy for more information.

- Commission PME's default ION_Data archive Windows scheduled task.
- Develop a process and schedule for:
  - Verifying the newly created archive database
  - Backing up the newly created archive database
  - Deleting the archive database when necessary

For large ION_Data databases (> 100 GB):

Large ION_Data databases require additional effort to maintain because all the maintenance task might not run completely.

- Disable the ION_Data database maintenance task
  - With large systems, index fragmentation occurs quickly and is unavoidable.
  - Defragmentation takes lot of time and the performance gained because of defragmentation is comparatively less.
  - If you plan to rebuild indexes, ensure that you have an equivalent amount of free space as the database size.
- If ION_Data database increases over 100 GB unexpectedly, it can be due to following reasons:
  - Database fragmentation can occur when there are more database read than database write actions.
  - Power quality and / or waveform logging is enabled accidentally, then power quality data increases.
  - More data points are logged than usual and frequent logging is performed.
- Defragmenting indexes may require a lot of free hard drive space to allow reindexing to succeed. Review hard drive space requirements.

System health review

You can adjust the system for optimal performance by monitoring the state of a system.

Frequent review of system health is to ensure optimal system health over the long term. This task involves identifying and resolving potential issues. It is recommended to perform system health checks at least once per month or quarter depending on the amount of data flowing into the system and how often the system is used.

It is recommended to use the following approach to set up regular system health checks:

1. Determine which system health checks are appropriate. The following is a list of system health checks appropriate for most of the PME system. Customized PME systems might include additional checks or have some removed, however all system health checks listed should be considered:

List of checks	Application Server	Database Server
Anti-malware	✓	✓

List of checks	Application Server	Database Server
Services running	✓	-
Message queues	✓	-
Device communication	✓	-
Processor usage	✓	✓
Memory usage	✓	✓
Disk usage	✓	✓
File system growth	✓	✓
File system fragmentation	✓	✓
Log files	✓	✓
Windows scheduled task history and status	✓	✓
Database growth	-	✓
Database fragmentation	-	✓
Database integrity	-	✓
Database backup	-	✓
Software licensing	✓	✓
Software updates	✓	✓

2. Identify and document how the above information can be collected for the system health review. Note the following tools:
   - PME Diagnostic Tool - Install and deploy this tool to obtain a snapshot of the current state of the system.
   - PME Diagnostics Viewer. See Diagnostics Viewer topic in System Guide for more information.
3. Create a template system health report. This report should contain at least the following information:
   - Report date
   - Contact information
   - A list of each system health check with the following information for each line item:
     - Status – Passed, Caution, or Failed
     - Description of contributing factor to the given status
     - Recommended action
4. Determine a storage location for system health reports. Reports should be stored in a consistent location and they should be accessible by administrators and support users.
5. Create an initial system health report.
6. In the location created in step 4, save the template report and the initial system health report.

The following table provides the information on list of system checks on why the check is required and what you need to check:

List of checks	Why	What to check
Anti-Malware	If the PME server has an internet connection, it is at risk for viruses and malware. The anti-malware software should be monitoring for threats in real-time and running full scans once per month.	• Check for warnings and threats. • If threats were found, were the infected files quarantined? • Check that the latest anti-malware definitions are installed.
Services running	These services are core of PME and must always be running.	• Use Windows Services, Windows Event Logs and Diagnostics Viewer – Service Diagnostics to ensure all ION, SQL Server and IIS services are running. • If they are stopped, investigate logs for root cause. See Diagnostics Viewer topic in System Guide for more information.
Message queues	• Log Inserter writes log data into a message queue instead of writing it to SQL Server directly. Another process (the Log Subsystem Router Service) reads the messages from the queue and writes the data to SQL Server. • The message queues should be at or near zero the majority of the time. One indicator of poor system health is when PME is operating in steady-state and the message queue size stays above zero for any queue for an extended period of time.	Use Diagnostics Viewer – Log Pipeline Service to check status of PME MSMQs. See Diagnostics Viewer topic in System Guide for more information.

List of checks	Why	What to check
Device communication	Networking issues can lead to communication loss with devices. For devices without onboard logging, communication loss means data loss. Monitor device communications often to ensure the expected devices are communicating.	• Use Diagnostics Viewer – Communication Diagnostics to check for communication issues, such as Timeouts or Log Inserter issues. • Repeated and frequent timeouts are common for long daisy chains – this is a sign that the loop performance needs to be assessed. • The LogInserter service diagnostic will reveal which devices cannot log data at the device level, and which DataRecorders have issues (reference LogHandle column). See Diagnostics Viewer topic in System Guide for more information.
Processor usage	CPU usage over time should be less than 80%.	• Is CPU trend showing at least 20% free? • Are processes using and releasing CPU resources? In Windows Resource Monitor, track the following object counters: • Processor: % Privileged Time • Processor: %User Time • System: Processor Queue Length See Monitor CPU Usage for more information.
Memory usage	Prevent low memory problems by applying the appropriate server resources (RAM, CPU) as the system grows. Take into consideration future extensions of the system and upgrades, which could be performed in-place if the server is prepared ahead. Monitor memory usage to confirm that it is within range.	Use Windows Resource Monitor to track the following object counters over time to determine normal usage and identify issues: • Memory: Available Bytes • Memory: Pages/sec See Monitor Memory Usage for more information.

List of checks	Why	What to check
Disk usage	There is a risk of disk I/O issues particularly in PME systems with large ION_Data databases.	Use Windows Resource Monitor to track the following object counters for each disk: Primary • PhysicalDisk: Avg. Disk sec/Write • PhysicalDisk: Avg. Disk sec/Read Secondary • PhysicalDisk: Avg. Disk Queue Length • PhysicalDisk: Disk Bytes/sec • PhysicalDisk: Disk Transfers/sec Track these counters over time to determine normal usage and identify issues. See Monitoring Disk Usage for more information.
File system growth	If a disk completely fills up, data loss occurs. You must ensure the all disks have adequate disk space for all maintenance tasks (defragmentation, backups, database reindexing). There should be at least 20 - 30% free disk space at all times for optimum performance. Possible causes of file system growth include database file growth, log file growth, data archives, and space used by 3rd party software. The best preventive measure is to track of the disk space usage and assess the growth over time. If the used space for a disk has consistently increased for several months and the percent free disk space is below 30% then action is required. Investigate the root cause of the growth, and develop a plan to either prevent more disk space from being used or for more disk space to be added.	• Ensure file system fragmentation job is running regularly • Check for unsustainable file system growth. If found, take preventive action to reduce the risk of a full disk, that is, add more disk space or adjust system configuration to reduce disk space usage.

List of checks	Why	What to check
File system fragmentation	If file system (or disk) fragmentation is greater than 40% on the database drive, SQL server experiences a thrashing/page faulting condition when manipulating a large volume of rows. For PME, file system fragmentation usually results in database auto-growth. It is most common in small and medium databases because of the SQL express database size limit.	• Pre-allocate hard drive space for the ION_Data database. See Diagnostics Viewer topic in System Guide for more information. • Check file system fragmentation on all drives used by PME at least once per month • Schedule time and perform file system defragmentation if necessary. For standalone systems, ensure SQL Server services are stopped before defragmentation.
Log files	There are many logs that contain critical error information, non-critical error information, warnings, and informational messages. Logs can be a good source of information for how well a system is performing as well as gathering data for troubleshooting specific issues. IIS logs should be trimmed regularly.	Check: • ION_SystemLog • IIS Logs • Windows Event Logs • SQL Server Logs • Check for unexpected errors in the log files • Check for errors related to PME components • Check log size to ensure total size is not excessively large (> 1 GB) • Archive historical logs if folder has too many log files. Sometimes certain irrelevant errors or warnings can be ignored. Any anomalous messages in these logs should be recorded and investigated.
Windows scheduled task history and status	PME's default database maintenance tasks are configured as Windows Scheduled tasks. Ensure scheduled tasks are successfully launched at the scheduled time and completing.	• Check Windows Scheduled Task Logs, if any. • Check PME System Logs for errors related to these tasks.

List of checks	Why	What to check
Database growth	Unexpected database growth can lead to poor performance. Usually significant database growth is a trigger. Unexpected database growth suggests possible excessive data logging due to device misconfiguration. For example, unexpected high-frequency logging (1 second logging intervals) or waveform logging when waveform data is not necessary.	Check database growth since the last system health check. Does the growth align with expectations?
Database fragmentation	Database fragmentation, if not addressed, is a common cause of poor system performance.	Check for index fragmentation over 10%
Database integrity	Database corruption is a rare event that is usually caused by inoperative hardware on the server. A database integrity check reviews the allocation and structural integrity of all objects in each database to ensure it is not corrupt.	• Run DBCC CHECKDB on all PME related databases. • Check for errors reported in the output of DBCC CHECKDB.
Database backup	Confirm that the backup scheduled tasks are completing successfully.	• Review SQL Server Logs for errors related to each job. • Confirm that the expected database backup files exist, and that copies of the backups have been made to another media and off-site.
Software licensing	To ensure all PME and SQL Server features are functional.	Check that the license is still valid.
Software updates	The latest updates ensure the system has the latest cybersecurity protection, and known software bugs are fixed.	Check to see if software is out-dated and identify when is the correct time for an upgrade.

Disaster recovery strategy

Disaster recovery requires planning and assessment to develop a strategy that meets both the business requirement and PME system configuration. The disaster recovery strategy is the result of two objectives:

- Data retention - The amount of data required in the active system.
- System recovery - The minimal state of the system that should be recovered after a disaster and the acceptable limit of data and time loss.

Disasters can occur at any time and, if unprepared, such events can lead to data loss and service disruptions. Factors leading to system disasters include:

- Inoperative hardware
- Sudden power interruption / outage
- External threats such as malware, virus attacks, hacking
- Human errors such as accidental data deletion
- Implementation or upgrade issues
- Database corruption, such as a database exceeding the maximum expected size or allowable hard drive space
- Natural disasters (For example, earthquakes, fire, flood, storms, and so on)

Some SQL Server disasters cannot be prevented, so it is important to prepare a complete disaster recovery plan (DRP) to ensure minimal impact on service and data availability.

An effective disaster recovery plan should comprise:

- Identify disaster recovery objectives
- IT architecture and resources plan
- Backup plan
- Recovery plan

Developing the plan requires collaboration with the IT team, application champions (administrators, power users) and recovery experts.

NOTE: If you have limited time and resource to define the strategy, you can consider third-party products and services for assistance.

Identify disaster recovery objectives

The plan starts with identifying disaster recovery objectives. This includes the business aspect of the system. You might want to consider the value of the PME system and the data it contains:

- What is the business cost of one day of downtime, both explicit and implied?
- What would be the result if an hour’s, day's or month's worth of analysis, reporting, alarming and data were lost?
- What would be the result of a complete loss of the PME system?

If your system is not critical, you may decide the best strategy is a simple one where a new PME system is redeployed in the event of a disaster and device data is re-imported and you experience potentially irrelevant historical data loss. If your system is critical, you may develop a plan for a quick recovery with minimal data loss.

You must set a written expectation of what constitutes an acceptable loss. Consider the following questions:

- What is an acceptable level of data loss in your PME systems?

  The answer to this question determines the **Recovery Point Objective (RPO)** objective. It is the maximum amount of recent data the business can lose when a disaster strikes. It helps to measure how much time can occur between your last data backup and the disaster without causing serious damage to your business. RPO is used to determine how often to perform data backups.

  For example, your backup schedule is set to daily at midnight and a disaster occurs at 8 AM. At the point of the disaster, you would have lost 8 hours' worth of data. If your RPO is one day of data then the loss of the last 8 hours of data is not an issue. However, if your RPO is one hour of data, then you must revise your backup schedule to at least one backup per hour.

- What is an acceptable recovery time?

  The answer to this question determines the **Recovery Time Objective (RTO)** objective. It is the amount of time the business can survive without the system after a disaster and before operations are restored to normal. It determines how quickly you need to recover the PME system after a disaster.

  For example, if your RTO is 24 hours, you can wait up to 24 hours before the system must be available to users. If data and infrastructure are not recovered within 24 hours, the business might be impacted.

- What level of disaster should we be prepared for?

  Identify the possible disasters that could affect your PME system and the level of impact of each disaster. For example: If your PME system is an on-premise solution, you should prepare for disasters such as power loss, fire, flood, etc. If your PME system is hosted on off-site servers in a data center, prepare for natural disasters but with low priority compared to cybersecurity risks.

IT architecture and resources plan

It is important to design the IT architecture so you can allocate the necessary hardware and networking resources in support of optimal performance and disaster recovery. Maintenance and backup activities often require additional resources (CPU, RAM and hard drive space) to perform and complete the activity. You can also prevent disasters using additional hardware. The recommended best practices are as follows:

- Hard drive space allocation

  Ensure there is enough hard drive space to perform backup operations and take at least two backup files. The spare hard drives can ensure minimal rebuild time. RAID arrays (commonly used on all PME systems) can protect against disk damages. See Storage Performance and Availability for recommended hard drive sizing.

- Backup power

  UPS systems and redundant power supplies to servers can prevent server power interruption.

- Connection redundancy

  If available, redundant data links can protect critical data transmission when the communication cannot be established in the network.

- Standby servers

  With supporting infrastructure and cost, standby servers can provide another set of hardware that can replace the PME system hardware in the event of an inoperative server. This approach is valuable when PME is a critical system.

Backup plan

Creating backups are a key part of every PME deployment. A backup solution unique to the PME deployment can be created based on the recovery objectives, the PME system, and available IT resources. The backup plan should comprise:

- Components backup
- Backup frequency
- Storage and retention of backup
- Test the backup

Once you have a strategy with details, document the details and supporting processes. Whenever a system or process change occurs, review and update this document. Store the document outside of the PME server.

Components backup

The following table contains the components of a standard PME system that must be considered for backup:

Component	Name	Description
PME Database	ION_Network	Sometimes called the NOM (Network Object Model), the ION_Network database stores device information, such as, device name, device type and connection address (for example, IP address and TCP/IP port or device/Modbus ID). It also contains information about the optional Application Module settings, other ION Servers, Sites, Dial Out Modems, and Connection Schedules. There is only one ION_Network per system

Component	Name	Description
PMEDatabase	Application Module	The Application_Modules database contains configuration settings (for example, layouts, colors, application events, and so on) and cached historical data for some of the Web Applications (for example, Dashboards and Trends).
PME Database	ION_Data	The ION_Data database contains the historical data, events and waveforms from devices connected to the system. This includes: onboard logging configured on devices; and, PC-based logging configured in the device translators and the Virtual Processors.
PME Database	ION_Data archive	The ION_Data archive databases contain historical data that have been sectioned off from the main ION_Data database.
System Database	master	The master database is the core system database for a SQL Server installation. It contains information such as SQL Server credentials and system configuration settings.
System Database	model	The model database is used as a template for all databases created on the SQL Server instance.
System Database	msdb	The msdb database is used by SQL Server Agent for scheduling alerts and jobs. msdb also contains history tables such as the backup and restore history tables.
PME Files	PME	The application folder is where all the program and configuration files for PME are stored. By default this is “%Program Files%\Schneider Electric\Power Monitoring Expert”
System Files	SQL Server	The SQL Server folder is where all the program and configuration files for SQL Server, SQL Server Reporting Services, and SQL Server Agent are stored. By default, this is “%Program Files%\Microsoft SQL Server”.
System Files	Windows registry	Contains configuration information for the entire server

Component	Name	Description
System and PME Files	Full Server Backup	It is advised to take an image of the entire PME application and database servers (excluding the actual database files – MDF, NDF, and LDF files). This backs up other important configuration information such as service credentials, security policies, and IIS setup. It can be important when simplifying and reducing the time taken for a system recovery.

All PME databases should be backed up frequently and a full server backup should be taken upon system configuration changes (for example, Vista diagrams, updating device drivers, registry settings, VIP framework changes, and so on). Use Configuration Manager for performing the backup. See Configuration Manager topic in System Guide for more information.

Database recovery model

When backing up databases it is important to choose an appropriate recovery model. The recovery model is a database property that controls how transactions are logged, whether the transaction log requires (and allows) backing up, and what types of restore operations are available.

PME databases use one of two recovery models:

- Simple recovery model

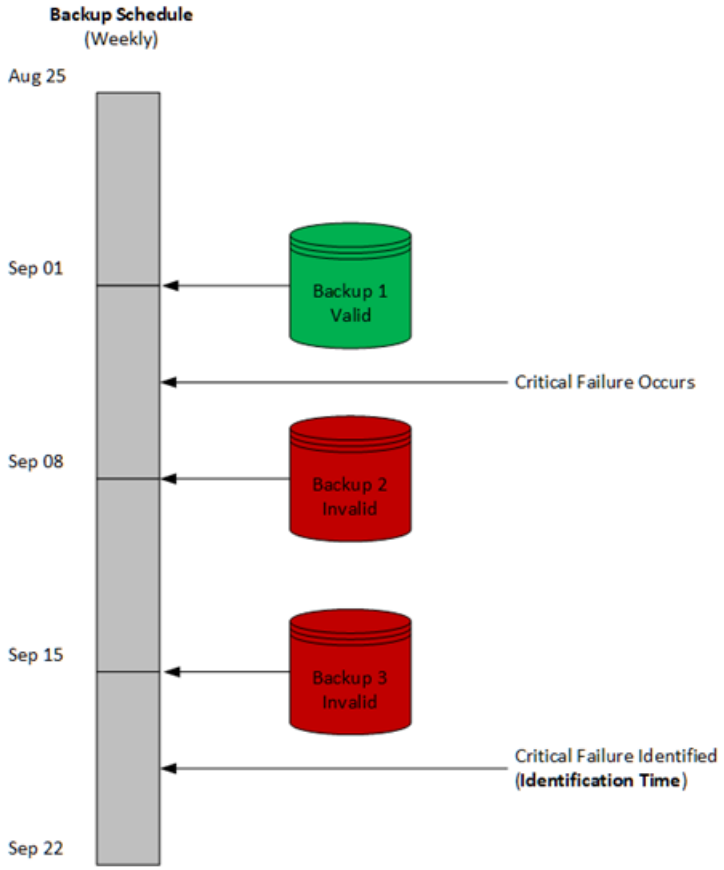
  Complete database backup is taken and a restore can only be done up to the point when the backup was taken.

- Full recovery model

  Provides backup options such as differential, incremental, and transaction log. The restore can be done using different options.

All PME databases are configured with the simple recovery model by default. The ION_Data database recovery model should be updated to reflect your backup plan.

The recovery model is determined by comparing the disaster identification time with the backup schedule. For example, as per the following diagram:



A system that is configured to have a single backup cannot be recovered. System is not accessed by users over the weekend, and becomes inoperative such that the automated backup jobs are still able to run. In this case, the backup would not be valid and there would be loss of the complete PME system.

You can prevent this situation by setting the ION_Data database recovery model to Full, thus allowing more refined backup options.

In the case of critical PME systems, consider:

- Being aware of your disaster identification time and adjust your backup schedule appropriately
- Using a full recovery model with several differential backups (advanced configuration)
- Keeping multiple backup copies on a rotational basis

The key benefit of the full recovery model is that it can restore a database exactly to any point in time since the last full backup was taken, including potentially to the point the disaster occurred, resulting in no data loss. It should only be used if simple recovery is not sufficient to meet the recovery needs as it incurs cost of performance and storage space.

Backup frequency

By default, PME is configured to backup the ApplicationModules and ION_Network databases on a daily basis, while the ION_Data database is backed up once per week. This default configuration assumes that meters installed throughout the network have onboard memory and

onboard logging enabled with a log of at least 14 days of data. This weekly frequency balances the need for performance in steady state and disaster recovery preparation. Frequent transaction log backups can lead to an unnecessarily bloated LDF file, which can cause performance issues.

If your PME system is critical, it is important to ensure you have a frequent backup strategy to support quick recovery. In this case, the recommended practices are:

- Set the ION_Data database recovery model to Full
- Schedule daily full backups
- Schedule hourly transaction log backups
- Continue to keep the last 2 full backup files on the server
- Increase hard drive storage space by the 2 x size of a ION_Data.MDF file for the additional transaction log backup files
- Keep the last 24 transaction log backup files on the server

The recommended backup configuration and frequency for PME and system database are as follows:

Component	Name	Description	Recovery Model	Backup Frequency
PME Database	ION_Network	All	Simple	Daily
PME Database	Application Module	All	Simple	Daily
PME Database	ION_Data	For systems with meters that have at least 14 days of onboard logging	Simple	Weekly
PME Database *	ION_Data	For systems without onboard logging or for critical systems **NOTE**: Perform hourly transaction logs backup. Review data storage requirements for the additional transaction log backup files	Full	Daily
PME Database	ION_Data archive	All	Simple	Upon creation
System Database	master	All	Simple	Daily
System Database	model	All	Full	As required
System Database	msdb	All	Simple	Daily

Additionally, all the components should be manually backed up after an update.

The recommended backup configuration and frequency for PME and system files are as follows:

Component	Name	Backup frequency
PME Files	PME	• Backup upon significant system change • Use Configuration Manager to backup and archive PME files. Be sure to deselect the database options. See Configuration Manager topic in System Guide for more information.
System Files	SQL Server	• Backup upon significant system change • Backup “%PROGRAMFILES% Microsoft SQL Server” folder upon major system changes (hotfixes and upgrades)
System Files	Windows registry	Monthly and after a significant system change
System and PME Files	Full Server Backup	• Annually or upon significant system change • Backup the entire PME application and database servers (excluding MDF, NDF, and LDF database files) once a year and after each significant system change (upgrade)

Storage and retention of backup

In the PME Planning stage, we recommend to have enough additional hard drive space to support at least three times the expected size of the main ION_Data (MDF) database. This estimation assumes that two backup files are stored on the production server.

We recommend the following storage and retention strategy:

- Follow the 3-2-1 Rule
  - Store backups locally on a RAID protected drive for the shortest amount of recovery time.
  - Store a copy of backups on a centralized set of disks so you can recover the backups on another server if the production SQL Server encounters a critical issue.
  - Store a copy of the backups off-site on external drives or in the cloud in case a site disaster occurs.
- Set up automated processes to backup and move files to separate locations.
- Maintain a reasonable set of backups off site and outside of the PME servers. We recommend the following backup retention strategy. Check with your legal team on keeping certain amount of critical data in the event of a disaster.
  - 10 daily backups
  - 5 weekly backups
  - 6 monthly backups
  - 3 on-demand or annual backups
- Historical backup files should be stored off-site.
- Delete the old backup files on a regular basis in order to manage the storage cost.

Test the backup

A critical aspect to the backup strategy is to ensure that you can recover files from the backups. Prepare a test procedure to verify that the backup files contain the expected data and that the backups can actually be restored, that is, the backup files are not corrupt.

When practicing the restore procedure, ensure that you restore to a different server and at a different location.

This practice ensures that the recovery team:

- Knows the steps to follow when recovering from a data loss or disaster.
- Has existing infrastructure to support a recovery.
- Can stay calm and act efficiently in a real disaster situation.

Recovery plan

Backup files are worthless if they cannot be restored, so you must have a recovery plan with the goal of getting a recovered PME system functional with minimum downtime and data loss. The disaster recovery objectives and backup and archive strategies help create a recovery strategy.

The most important point to remember when creating a recovery plan is that it is not valid until it is actually tested, and your recovery position is good as your last recovery test. Once you have a recovery plan, allocate some time to test your disaster recovery strategy. Be aware of who is executing the recovery as well. Do not assume that a specific person is available to restore the PME system.

We recommend the following approach to developing a recovery strategy:

1. Set a time expectation for recovery (Recovery Time Objective).
2. Identify the necessary hardware, software, backup and archive files and types (full, differential, and log).

   Ensure resources – physical (servers, software, network) and personnel – are allocated and assigned, so they are readily available if a disaster strikes.
3. Document the entire recovery procedure.

   If you have a large recovery time window, such as 1 week, you may have enough time to contact PME support team to assist in a recovery procedure. If you have a smaller time window then any PME administrator (factoring in employee turnover) should be capable of performing a restore, so this procedure should be well documented. At a minimum, all backup and archive locations should be documented and accessible to any PME administrator. Store the documentation outside of the PME production servers.

   NOTE: Training PME administrators and / or support staff on PME disaster recovery may be important to ensure you have redundant personnel available.
4. Schedule system downtime and test the restore procedure. This is a necessary step to ensure the disaster recovery strategy is valid. Track the time the recovery procedure takes to verify your time expectation for recovery is valid. Take corrective action for any areas missed in your recovery documentation, backup, or archive strategies.

5. Progressively update recovery documentation after any major system changes are made that changes the restore procedure.

NOTE: See SQL Server Limitations on Restoring System Databases in cases where a full SQL server recovery is needed.

Recommended consolidated disaster recovery strategy plan

The recommended consolidated disaster recovery strategy plan of ION_Data database for the different purpose of PME system are as follows:

	Purpose of PME system		
Disaster recovery strategy parameter	**Analysis & decision making (Capacity management, Energy usage analysis, Power Quality compliance)**	**Real-time monitoring & troubleshooting (Electric distribution monitoring & alarming, Insulation monitoring, Backup power testing)**	**Critical large advanced distributed system (with mix of real-time and analysis based applications)**
Device memory	On board logging (14 to 30 days)	None	None
Recovery point objective	Up to 1 week	Yesterday	As close to the point of disaster as possible
Recovery time objective	24 hours	36 hours	24 hours
Database recovery model	Simple	Simple	Full
Full backup with frequency	Full with weekly	Full with weekly	Full with daily
Additional backup with frequency	Not applicable	Differential with daily	Transaction logs with hourly
Number of full backup files to store on server	2	2	2
Number of additional backup files to store on server	Not applicable	2 to 6	Depends on how often the transaction log backup files are validated
Additional IT resources needed for additional backup files*	Standard	Additional storage required for differential backup	Additional storage required for transaction log backup

*See IT Requirements for recommended system sizing.

Reference

Use the links below to find the content you are looking for:

Cybersecurity Reference

This section contains reference information related to cybersecurity.

Data encryption

At Rest

PME encrypts the passwords of its user accounts, as well as the Windows and SQL Server accounts using SHA-512 and AES-256 cryptography. PME uses a unique encryption key for each installation. The key is generated during the installation of PME. The PME installer offers functionality for exporting/importing encryption keys for the installation of PME clients or system upgrades.

The power monitoring data that is collected by PME, and system configuration data are not encrypted.

In Transit

PME uses Transport Layer Security (TLS) 1.2 for an encrypted, authenticated connection using HTTPS between the server and the web clients. Both self-signed and authority issued certificates are supported. PME is installed with a self-signed certificate and a self-signed certificate is configured automatically. We recommend that you replace this with a security certificates from a Certificate Authority (CA).

The communication between PME and connected monitoring devices is not encrypted.

PME accounts

The following types of accounts are required for a PME system:

PME Users

A user account in PME provides access to the system. There are 3 different types of users - standard users, Windows users, and Windows groups. Each user has an access level, which determines the actions the user is allowed to perform in PME. There are no pre-configured user accounts or user groups in the system. One supervisor account is created with a user defined password during the installation of the software. Additional user accounts and groups must be created manually after installation. PME supports Windows Active Directory integration for Windows users and groups.

TIP: Use Windows users and groups to take advantage of Windows account security features such as maximum login attempts or minimum password requirements.

Windows accounts used by PME

PME uses Windows accounts for report subscriptions and database maintenance. The accounts are created automatically during the installation of the software. The accounts share the same password, which is set at install time and can be changed at any time through the installer.

If PME is configured to use Windows Integrated Authentication, then an additional Windows account is required for database access. This Windows account is also used to run the PME services and the IIS Application Pools. This account must be created manually and account details must be provided during the installation of the software.

See Windows accounts for more information.

SQL Database server accounts

If PME is configured to use SQL Server Authentication, then SQL server accounts are required for database access. The accounts are created automatically during the installation of the software. The accounts share the same password, which is set at install time and can be changed at any time through the installer.

If SQL Server Express is installed with SQL Server Authentication, through the PME installer, a sa account with a unique, default password is created automatically during install. The password can be changed at any time through SQL Server Management Studio.

See SQL Server accounts for more information.

EcoStruxure Web Services account

If EcoStruxure™ Web Services (EWS) are used, data exchange credentials must be defined. The credentials consist of a single username and password. The EWS credentials are set manually in the **Web Applications** > **SETTINGS** > **Security** > **EWS Login** area of the software.

PME Services

PME uses a number of services to perform the background server tasks. The services use the Local Service and NT AUTHORITY\System accounts, or the Windows account used for Windows Integrated Authentication, if that is configured.

See PME Windows services for more information.

Network shares

PME Engineering Clients and Secondary servers require that the **Power Monitoring Expert** folder on the PME server is shared with change and read permissions. This file share must be manually set up before installing Engineering clients or Secondary servers.

Session timeout

PME automatically times out inactive client sessions. Web Applications clients are logged out and Windows application clients (Vista, Designer, Management Console) are locked after a period of inactivity. The timeout period is configurable, it is set to 20 minutes by default.

To restart or unlock the session you must enter the login credentials. A session is considered inactive, if none of the following actions are detected:

- Mouse movement
- Mouse click
- Keyboard activity
- Touch screen activity

NOTE: If custom content links are added to the Web Applications framework, then the custom content must either implement the idle detection, or activity on that content is not registered and the web client session can time out unexpectedly. See Adding idle detection to custom Web Application links for details.

System integration security

Specify which third-party web resources are allowed to either embed (frame) the PME web applications, or to which the PME web applications can redirect requests. This is configurable in the PME Web Applications settings.

Specify which web applications of PME needed to integrate with third-party systems based on the generated links. The generated links are authenticated. This is configurable in the PME Web Applications settings.

Verifying file integrity and authenticity

Verify the file integrity and authenticity for software updates and other components before installing them in the system. Do not install files for which the integrity and authenticity cannot be confirmed.

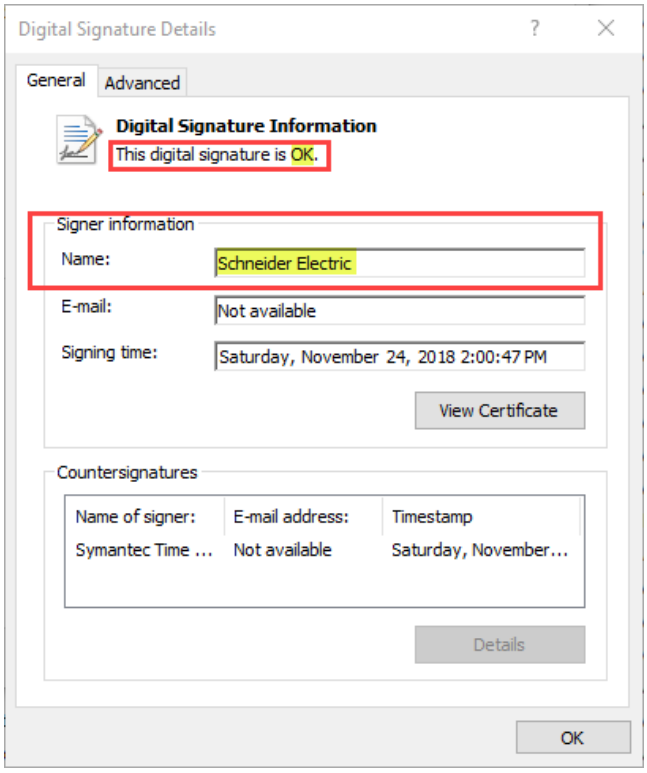
To verify the file integrity and authenticity:

1. Right-click the file and select **Properties**. This opens the Properties dialog.
2. In the Properties dialog, select the **Digital Signatures** tab.
3. In the Signature list, highlight the Name of signer. Click **Details**.

   NOTE: Only Schneider Electric should be shown in the Signature list.

4. Verify that the digital signature is OK and that the signer name shows **Schneider Electric**.

   Example:



5. Close the properties dialog.

Accounts and services

Windows accounts

The following tables provide information on the Windows accounts used by Power Monitoring Expert (PME):

User Account	Role/Group/Permissions	Notes
IONUser (account)	- No group membership. - Has List/Read/Write/Execute permissions on the PME share folder.	- Automatically created during the installation of PME. - Used to run report subscriptions. - Needs access to the folder where subscriptions are saved.
IONMaintenance (account)*	Member of Users group	- Automatically created during the installation of PME. - Used to run database maintenance jobs in Windows Task Scheduler.
Login used to run the PME installer	Needs to be a member of local Administrators group	- Manually created by the user. - Used to log into Windows to run the PME installer - If possible, the local Administrator account should be used.
Login used to access PME applications	Needs to be a member of Users group	- Manually created by the user. - Used to log into Windows to run the PME Web Applications or Engineering Client applications.
Login to run application engineering tools	Needs to be a member of local Administrators group	- Manually created by the user. - Used to log into Windows to run PME application engineering tools. An example is the Configuration Manager Tool, used for system upgrades.
Login to run the Database Manager tool	Needs sysadmin permissions on SQL database instance.	- Manually created by the user. - Used to log into Windows to run the PME Database Manager tool. - This Windows account needs to be added to the SQL server database.
SQL Server Database Engine service	NT AUTHORITY\SYSTEM	Must have access to the database folder(s) and the Temp folder of the installer user during installation. Permissions can be lowered after PME is installed.

* This account is only created on standalone servers where the SQL Server software and PME are installed on the same computer.

NOTE: For information on which accounts are used to run the PME Windows services, see PME Windows services and IIS Application Pools.

For installations using Windows Integrated Authentication, the following additional accounts and permissions are required:

User Account	Role/Group/Permissions	Notes
Account used for Windows Integrated Authentication	- Needs to be a member of local Administrators group - Needs 'Log on as a service' privilege on application server	- Manually created by the user. - Used by PME to access the SQL server databases.
Login used to access PME Engineering Client applications	Needs sysadmin server role for the PME databases.	This is not an additional user account. It is just an added requirement for the Logins used to access the Engineering Client applications (Vista, Designer, Management Console, Management Console tools). The PME databases are: ApplicationModules, ION_Data, ION_Network, ION_Systemlog.

NOTE: When PME is installed with Windows Integrated Authentication, the Windows account that is used to access the database is also used to run the PME services and the IIS Application Pools.

SQL Server accounts

The database server hosts several databases for Power Monitoring Expert (PME). The following tables lists the SQL Server logins and permissions created for PME:

For installations with SQL Server Authentication:

Login	Authentication	Server Role	Database	Membership
AMUser	SQL	Public	ApplicationModules	AMApplicationRole
ION	SQL	Public	ApplicationModules	db_owner
			ION_Data	db_owner
			ION_Network	db_owner
			ION_SystemLog	db_owner
ionedsd	SQL	Public	ION_Data	ION_DSD_Reader
			ION_Network	NOM_DSD_Reader
IONMaintenance*	Windows	Public	ApplicationModules	db_backupoperator, db_ddladmin, Maintenance
			ION_Data	db_backupoperator, db_ddladmin, Maintenance
			ION_Network	db_backupoperator, db_ddladmin, Maintenance
			ION_SystemLog	db_backupoperator, db_ddladmin, Maintenance

* This account is only created on standalone servers where the SQL Server software and PME are installed on the same computer.

For installations with Windows Integrated Authentication:

Login	Authentication	Server Role	Database	Membership
Account used for Windows Integrated Authentication	Windows	Public	ApplicationModules	db_owner
			ION_Data	db_owner
			ION_Network	db_owner
			ION_SystemLog	db_owner

IONMaintenance *	Windows	Public	ApplicationModules	db_ backupoperator, db_ddladmin, Maintenance
			ION_Data	db_ backupoperator, db_ddladmin, Maintenance
			ION_Networks	db_ backupoperator, db_ddladmin, Maintenance
			ION_SystemLog	db_ backupoperator, db_ddladmin, Maintenance

* This account is only created on standalone servers where the SQL Server software and PME are installed on the same computer.

NOTE: When PME is installed with Windows Integrated Authentication, the Windows account that is used to access the database is also used to run the PME services and the IIS Application Pools.

Other

PME must have access to the master and tempdb System Databases.

The PME Database Manager tool requires that the Windows account that is used to run it has sysadmin permissions on the PME SQL Server instance. The Database Manager is an optional tool, used for managing the PME databases.

PME Windows services

All PME applications without a user interface run as Windows services. The following table lists all PME services:

Service Name	Startup Type	Log On Account	Description
ION Application Modules Alarm Services Host	Manual	NT AUTHORITY\System *	Allows the Event Notification Module (ENM) to read alarms directly from the ION_Data database. Starts on demand from other services (for example, from the Event Notification Module).
ION Application Modules Core Services Host	Automatic	NT AUTHORITY\System *	Hosts common web services used by the Web Applications component.
ION Application Modules Data Services Host	Automatic	NT AUTHORITY\System *	Hosts web services that provide low-level access to system data (that is, real-time, historical, alarming, and authentication) for the Web Applications component.
ION Application Modules Provider Engine Host	Automatic	NT AUTHORITY\System *	Hosts web services that provide data processing for the Web Applications component.
ION Cloud Agent Service	Automatic	NT AUTHORITY\System *	Manages interaction with cloud services.
ION Component Identifier Service	Manual	Local Service *	Locates local and remote product components. Starts shortly after startup by request of ION Connection Management Service.

Service Name	Startup Type	Log On Account	Description
ION Connection Management Service	Manual	NT AUTHORITY\System *	Determines the connection status of sites and devices in the system, and handles allocation of resources such as modems. This service manages the state of site and device connectivity for the system. In order to establish the most appropriate state for the system, each connection and disconnection request is evaluated against the overall state of the system and availability of communications channels. Starts shortly after startup by request of ION Network Router Service.
ION Diagnostics and Usage Service	Automatic	Local Service *	Collects basic, non-identifying information from the Power Monitoring Expert system and uploads it to a secure location on the cloud for data mining by Schneider Electric. Customers can opt-in or opt-out at any time.
ION Event Watcher Service	Automatic	Local Service *	Monitors system events for conditions specified in Event Watcher Manager.
ION Log Inserter Service	Automatic	NT AUTHORITY\System *	Provides historical data collection for the power monitoring system (that is, devices and Virtual Processor), and stores it in the ION_Data database.
ION Log Subsystem Router Service	Automatic (Delayed Start)	NT AUTHORITY\System *	Transfers data received from power monitoring devices to storage and processing.
ION Managed Circuit Service	Automatic	Local Service *	This service is used to create individual real-time and historical data sources for multi-circuit meters.

Service Name	Startup Type	Log On Account	Description
ION Network Router Service	Automatic	NT AUTHORITY\System *	Routes all ION requests between the software components, such as client workstations, the Real Time Data Service, Log Inserter, and the Query Server. The service dynamically detects changes to the network configuration, including the addition of new servers. It can also recognize new software nodes, such as Vista, that are added to an existing server.
ION OPC Data Access Server	Manual	NT AUTHORITY\System *	Serves real-time OPC data (OPC DA) to OPC client applications. Starts on an OPC client request for data, if the Data Exchange Module license has been activated.
ION PQDIF Exporter Service	Manual	Local Service *	Translates power quality data from the ION_Data database into PQDIF file format and manages scheduled PQDIF exports.
ION Query Service	Automatic	NT AUTHORITY\System *	Provides historical data retrieval from the ION_Data database for client applications (for example, Vista and Diagrams).
ION Real Time Data Service	Automatic	Local Service *	Manages and provides access to real-time data for all client applications (Vista, Diagrams, Trends, and so on).
ION Report Subscription Service	Automatic (Delayed Start)	Local Service *	Runs Reports subscriptions according to user-defined schedules. Starts several minutes after the server starts.

Service Name	Startup Type	Log On Account	Description
ION Site Service	Automatic	NT AUTHORITY\System *	Manages communication links to and from the product. ION Site Service is responsible for handling packet communications to system devices and controlling direct device communications. The service reacts to changes in network configuration: for example, changes to certain channels, configuration parameters, ports, or device parameters can often interrupt a connection.
ION Software Data Processing Service	Automatic (Delayed Start)	Local Service *	Performs evaluations based on real time data from the power monitoring system.
ION Software Modbus Gateway Service	Manual	Local Service *	Enables software data services via ModbusTCP/IP, and is treated like a device in the system. For example, the Circuit Breaker Aging Service uses this service.
ION Virtual Processor Service - NVIP.DEFAULT	Automatic	Local Service *	Provides aggregation, control, and mathematical analysis of power monitoring system data.
ION Virtual Processor Service – NVIP.PQADVISOR	Automatic	Local Service *	Serves up data for the Power Quality Performance diagrams. Functions only when the Power Quality Performance module is licensed and configured.
ION Virtual Processor Service – NVIP.DDD	Automatic	Local Service *	Serves up data for the Disturbance Direction Indicators application. Functions only when the Disturbance Direction Indicators application is configured.

Service Name	Startup Type	Log On Account	Description
ION XML Subscription Service	Automatic	Local Service *	Manages subscriptions to XML data for Vista user diagrams. This service is used only by the Diagrams application. When you open a Vista user diagram in a web browser, the ION XML Subscription Service creates a subscription and delivers the real-time data in XML format.
ION XML Subscription Store Service	Automatic	Local Service *	Stores XML data subscriptions for the power monitoring devices on the network. This service is used only by the Diagrams application.
ImadminSchneider	Automatic	Local Service	This service runs the FlexNet Publisher License Server Manager.
SQL Server (ION)	Automatic	Local System	Provides storage, processing and controlled access of data, and rapid transaction processing for the ION_Data, ION_Network, ION_SystemLog, and the ApplicationModules databases.

* When PME is installed with Windows Integrated Authentication, the Windows account that is used to access the database is also used to run the PME services.

** This service only exists on systems with SQL Server, not SQL Server Express.

IIS Application Pools

The Power Monitoring Expert installer enables and configures IIS to host the different Web applications. The following table lists the application pools and applications:

Application Pool	Identity	Application
Application Modules App Pool	NetworkService *	Dashboards EWS (EcoStruxure Web Services) Slideshow System Data Service Web
ION App Pool	NetworkService *	ION ION Report Data Service Web Services
Web Reporter App Pool	NetworkService *	ModelingConfig reporter

* When PME is installed with Windows Integrated Authentication, then the Windows account that is used to access the database, is also used to run the IIS Application Pools, instead of the **Local System** account.

NOTE: The .NET Trust Level for PME web applications and Default Web Site must be set to **Full (internal)**, in IIS Manager.

Databases

PME Databases

Power Monitoring Expert uses four databases to store device communication parameters, system configuration settings, and logged historical data.

ION_Network database

Sometimes called the NOM (Network Object Model), the ION_Network database stores device information, such as, device name, device type and connection address (for example, IP address and TCP/IP port or device/Modbus ID). It also contains information about the optional Application Module settings, other ION Servers, Sites, Dial Out Modems, and Connection Schedules. There is only one ION_Network per system.

ION_Data database

The ION_Data database contains the historical data, events and waveforms from devices connected to the system. This includes: onboard logging configured on devices; and, PC-based logging configured in the device translators and the Virtual Processors.

Application Modules database

The Application_Modules database contains configuration settings (for example, layouts, colors, application events, and so on) and cached historical data for some of the Web Applications (for example, Dashboards and Trends).

ION_System log database

The ION_SystemLog database holds system events and their timestamps, which is accessible to view in Management Console. Event priorities can range from 0-255 and are grouped into Diagnostic (0 - 5), Information (6 - 20), Warning (21 - 63), Error (64 - 191), and Critical (192 - 255) categories. System events can include:

- ION Service stopped or is starting or user connection to an ION Service is lost.
- Device has been declared offline / online.
- ION Site Service connected, disconnected or failed to connect to a Site.
- ION User logs on / off Vista or Designer.
- ION User saves a Vista or Designer node diagram.
- Plus many other Warnings and Errors relating to PME system functions.

Database maintenance task definitions

The following are high level definitions of PME relevant database maintenance tasks.

Archive

Database archiving copies older data from the operational database into a separate, new database. The goal of archiving is to keep data safe for future reference. Data is typically archived based on calendar time intervals, for example by month or by year.

The PME archive task creates a new archive database each time the task is run. Each new archive database is attached to SQL server and is available to be accessed by PME.

NOTE: The PME archive task does not trim data from the operational database; it only makes a copy of the archived data, leaving the original data in the operational database. See Considerations for trimming archived data from ION_Data for important information on this topic.

Backup

Backing up a database creates a copy of the operational database. The goal of a backup is to have an identical duplicate of the operational database that can be used to restore the system in case the operational database becomes nonfunctional. Database backups should be created on a regular basis, for example daily or weekly.

Maintenance

The PME database Maintenance task defragments the database and updates the database statistics. The goal of these activities is to maintain database performance. Maintenance tasks should be run on a regular basis, for example daily.

Size Notification

The size notification task is used to monitor the size of the database and to notify users when a certain size threshold is reached. When the size threshold is reached, the task logs a system log event message and triggers a Critical alarm in PME every time the task runs.

NOTE: The Size Notification task is only configured for systems using SQL Server Express, which has a maximum database size limitation of 10 GB.

Trim

Trimming a database deletes data from the database. The goal of trimming is to prevent the database from growing to a size that could affect system performance. Databases should be trimmed on a regular basis, for example daily or weekly. For PME only the system log databases are trimmed.

Considerations for trimming archived data from ION_Data

When archiving and then trimming data from the ION_Data database, you are moving this data from the operational database into an archive store for long-term retention. This data is then no longer available in the ION_Data database for analysis in PME. PME has very limited access to archived data.

We recommend that you only trim archived data from the ION_Data operational database, when:

- It approaches its size limit, for example 10 GB for a SQL Server Express database.
- It reaches a size that impacts query performance.
- The database drive is low on available free space and you cannot switch to a larger drive.

When you trim data from an SQL database, the database file size remains unchanged. After the trim, the database will first fill the new free space before growing the database file size again. To reduce the database file size after trimming, Shrink the database, using standard SQL Server tools.

NOTE: The PME archive task does not trim the database; it only copies data to the archive.

Archive data access in PME:

Application	Archive Data Access
Vista	Yes
Reports	Can access either data from the operational database or from an archive database but not both at the same time.
Dashboards	No
Diagrams	Yes
Trends	No
Alarms	No

Database maintenance account requirements

PME uses Task Scheduler in Windows for the scheduling and execution of database maintenance tasks. Task Scheduler requires a Windows account to run the tasks. In Standalone PME systems, an account, **IONMaintenance**, is created by the installer and automatically assigned to the Task Manager tasks. In Distributed PME systems you need to create an account manually. This account must meet the following minimum requirements:

In Windows on the computer where the database server is installed, the account:

- must be a member of the Users group.
- must have the following Windows policy settings: **Log on as a batch**; **Deny log on locally**.

In SQL Server, the account:

- must have a **public** server role
- (for archive task only) must have a **sysadmin** server role
- must have the following role memberships for the PME databases (ION_Data, ION_Network, ION_SystemLog, ApplicationModules):
  - db_backupoperator
  - db_ddladmin
  - Maintenance
  - public

NOTE: You will need the password for this account during the initial task setup, and later if you want to edit the tasks in Task Manager in the future.

Database maintenance

PME uses databases to store information such as system configuration, data logs, and system event log messages. These databases must be maintained to preserve performance, manage disk space use, and guard against data loss in case of database failure.

NOTICE

LOSS OF DATA

- Back up the database at regular intervals.
- Back up the database before upgrading or migrating the system.
- Back up the database before trimming it.
- Back up the database before making manual database edits.
- Verify correct database behavior after making database or system changes.

Failure to follow these instructions can result in permanent loss of data.

The following table shows the PME databases and the recommended database maintenance tasks for each:

Database	Type of Data	Maintenance Tasks*
ApplicationModules	Web Applications related configuration data and system event log entries.	Backup, Maintenance, Trim
ION_Data	Historical power system data such as interval data logs, waveforms and alarms.	Archive, Backup, Maintenance, Size Notification**
ION_Network	Device network and other system configuration data	Backup, Maintenance
ION_SystemLog	Non-Web Applications related system event log entries.	Maintenance, Trim

* See Database maintenance task definitions for basic task definitions.
** Size Notification is only used for systems with SQL Server Express, which has a maximum database size limit of 10 GB.

In Standalone PME systems, the database maintenance tasks are pre-configured and scheduled to run automatically by default. For Distributed Database PME systems, you need to configure the tasks and set up the schedules manually.

NOTE: It is best to automate the maintenance tasks, but you can run them manually on demand using Database Manager and Microsoft SQL Server Management Studio.

The following table shows the default database maintenance task schedules for Standalone PME systems:

Database	Task	Enabled	Trigger Time
ApplicationModules	Backup	Yes	Daily at 01:30
ApplicationModules	Maintenance	Yes	Daily at 03:30
ApplicationModules	Trim	Yes	Daily at 02:30
ION_Data	Archive*	**No****	Annually, on Jan 3 at 01:00

Database	Task	Enabled	Trigger Time
ION_Data	Backup	Yes	Weekly, Fridays at 00:00
ION_Data	Maintenance	Yes	Daily at 02:00
ION_Data	Size Notification***	Yes	Daily at 03:00
ION_Network	Backup	Yes	Daily at 01:00
ION_Network	Maintenance	Yes	Daily at 07:30
ION_SystemLog	Maintenance	Yes	Daily at 07:05
ION_SystemLog	Trim	Yes	Daily at 04:00

* The PME archive task does not trim the database, it only copies data to the archive.
** You need to edit the Windows user account settings before enabling the archive task. See the Note on the ION_Data archive task for more details.
*** Size Notification is only used for systems with SQL Server Express, which has a maximum database size limit of 10 GB.

For more information on the default task settings see Default maintenance task settings.

Managing database maintenance tasks for Standalone PME systems

In Standalone systems, the database maintenance tasks are pre-configured and scheduled to run automatically by default. The scheduling and execution of the tasks is done with Task Scheduler in Windows. The database interaction specific steps of the tasks are defined as Windows PowerShell scripts.

Note on the ION_Data archive task:

NOTE: The archive task for the ION_Data database is disabled by default. The Windows user account that is used to run this task must have a sysadmin server role in the SQL Server database server. The Windows user account that is used by default, IONMaintenance, does not have a sysadmin server role. To enable and run the scheduled archive task successfully, you need to add the sysadmin role to IONMaintenance, or change the user account that is used to run this task to an account with sysadmin role. See Database maintenance account requirements for more information on account requirements.

To edit the task schedule settings (enable or disable tasks, set trigger times):

NOTE: The database maintenance tasks in Task Scheduler are configured to run using the **IONMaintenance** Windows user account. To save any changes to the task settings in Task Scheduler, you need to enter the password for the **IONMaintenance** account. See Using IONMaintenance for database maintenance tasks for information on where to find the password.

1. On the PME application server, open Task Scheduler in Windows.
2. In the Task Scheduler Library, open the **Schneider Electric** > **Power Monitoring Expert** folder to see the configured database maintenance tasks.

3. Edit the tasks as required:
   a. To enable or disable a task, select it and use the **Actions** pane in Task Scheduler.
   b. To edit task settings, double-click a task and make the desired changes in the **Job Properties** dialog box.
4. (Optional) Select **Enable All Tasks History** in the **Actions** pane in Task Scheduler. This turns on event recording for the scheduled tasks, which is useful for auditing and troubleshooting.
5. Close Task Scheduler.

To edit the task script settings (change backup and archive location, set the data to keep on trim, size notification threshold):

1. On the PME application server, open the `...\Power Monitoring Expert\config\cfg\DbScheduledTasks\Support\Configuration.ps1` script file in a text editor.
2. Change the values of the variables in the script file for the settings you want to change. The following settings can be customized:

   NOTE: Follow the instructions in the script file on formatting and syntax.

Setting	Variable	Default Value	Comments
Backup folder location	$locationForBackupFiles	...\Power Monitoring Expert \Database\Backup	Sets the folder to which the database backups are saved. The backup script will create the following subfolders in this location: ...\Data for ION_Data ...\Network for ION_Network ...\SystemLog for ION_SystemLog ...\Applications for ApplicationModules NOTE: IONMaintenance needs Read and Write permissions on this folder.
Archive folder location	$locationForArchiveDBFiles	...\Power Monitoring Expert \Database\Archive	Sets the folder to which the database archives are saved. NOTE: IONMaintenance needs Read and Write permissions on this folder.
Data to keep when trimming	$diagnosticsDaysToKeep	30	Sets how many days' worth of data is left in the database after trimming.
Database size (max)	$maximumDatabaseSizeIn Gigabytes	9	Sets the maximum database size. This value is used by the size notification task to assess what percentage of database space has been used. The maximum size for a SQL Express database is 10GB. The maximum size in the script is set to 9GB to allow for a 1GB warning buffer before the database stops logging data.
Database size notification limit	$databaseSizeNotification ThresholdPercentage	85	Sets the threshold for when a database size notification will be issued.

3. Save the script file changes and close the text editor.

Setting up database maintenance tasks for Distributed PME systems

In Distributed systems, the database maintenance tasks are not pre-configured. You need to set up these tasks manually. The scheduling and execution of the tasks is done with Task Scheduler in Windows. The database interaction specific steps of the tasks are defined as Windows PowerShell scripts. Setting up the database maintenance tasks includes the following high-level steps:

NOTE: The following sections describe how to set up the different database maintenance tasks, except for the archive task for ION_Data. See Setting up the ION_Data archive task for Distributed PME systems for instructions on how to set up this task.

Step 1: Creating a Windows user account to run the maintenance tasks. See Database maintenance account requirements for more information on the account requirements.

Step 2: Installing the Microsoft SQL Server Data-Tier Application Framework.

NOTE: This requires downloading the framework installer from Microsoft or copying it from the PME installation DVD/ISO.

Step 3: Installing and configuring the Windows PowerShell script files.

NOTE: This requires copying files from the PME application server to the database server.

Step 4: Setting up task schedules in Task Scheduler.

Step 1: Creating a Windows user account to run the maintenance tasks:

1. On the database server, create a new Windows user as a member of the Users group, for example *PMEMaintenance*.

   NOTE: You will need the password for this account during the initial task setup, and later if you want to edit the tasks in Task Manager in the future.

2. Open the Local Security Policy tool in Windows.
3. In the Local Security Policy tool, open the policy settings list in **Security Settings** > **Local Policies** > **User Rights Assignment**.
4. Add the new Windows user to the following policies: **Deny log on locally** and **Log on as a batch job**.
5. Close the Local Security Policy tool.
6. Open Microsoft SQL Server Management Studio.
7. Add the new Windows user as a database Login with the following roles and mappings:

   Server Role: **public**
   User Mapping:

Database	Role
ApplicationModules	db_backupoperator; db_ddladmin; Maintenance; public
ION_Data	db_backupoperator; db_ddladmin; Maintenance; public
ION_Network	db_backupoperator; db_ddladmin; Maintenance; public
ION_SystemLog	db_backupoperator; db_ddladmin; Maintenance; public

8. Close Microsoft SQL Server Management Studio.

NOTE: You will need the password for this account if you want to edit the tasks in Task Manager in the future, after the initial setup.

Next, install the Microsoft SQL Server Data-Tier Application Framework.

Step 2: Installing the Microsoft SQL Server Data-Tier Application Framework:

1. Check if the framework is already installed on the database server. To do this, find the following registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Microsoft SQL Server\`.
   If this key includes a `Data-Tier Application Framework` key, then the framework is installed. Continue with Step 3 - Installing and configuring the Windows PowerShell script files
   If this key does not include a Data-Tier Application Framework key, then the framework is not installed. Continue with the installation of the framework.
2. On the database server, download the framework installer (`DacFramework.msi`) from Microsoft.

   NOTE: You can also find the framework installer (`DacFramework.msi`) on the PME DVD/ISO under `Setup\SetupSupport\database`.
3. On the database server, install `DacFramework.msi`.

Next, install and configure the Windows PowerShell script files.

Step 3: Installing and configuring the Windows PowerShell script files:

1. On the database server, create a new folder. You can choose the location and folder name, for example `C:\PME_Database_Maintenance`.
2. Copy the **DbScheduledTasks** folder from `...\Power Monitoring Expert\config\cfg\`, on the PME application server, into this new folder.
3. Open the `<New Folder Path>\DbScheduledTasks\Support\DatabaseHelper.ps1` script file in a text editor.
4. Change the values of the folder path variables in the script file to the new folder path as follows:
   a. Change the value of **$customUserDirectory** (line 28 in the script) to `<New Folder Path>\dbScheduledTasks\Support`, for example `C:\PME_Database_Maintenance\dbScheduledTasks\Support`. The default value is `C:\PMEDBs\dbScheduledTasks\Support`.

b. Change the value of **$customSystemDirectory** (line 29 in the script) to `<New Folder Path>`, for example `C:\PME_Database_Maintenance`. The default value is `C:\PMEDBs`.

c. (Only if you are using Windows Integrated Authentication) Change the value of **$pmeUsingIntegratedAuth** (line 32 in the script) to `1`. The default value is `0`.

5. Save the script file changes.
6. Open the `<New Folder Path>\DbScheduledTasks\Support\Configuration.ps1` script file in a text editor.
7. Change the value of the backup and archive folder path variables in the script file to the new folder path as follows:
   a. Change the value of **$locationForBackupFiles** (line 46 in the script) to `<New Folder Path>\Backups\`, for example `C:\PME_Database_Maintenance\Backups\`. The default value is `..\Database\Backup\`.
   b. Change the value of **$locationForArchiveDBFiles** (line 54 in the script) to `<New Folder Path>\Archives\`, for example `C:\PME_Database_Maintenance\Archives\`. The default value is `..\Database\Archives\`.
8. Save the script file changes and close the text editor.

Next, set up task schedules in Task Scheduler.

Step 4: Setting up task schedules in Task Scheduler:

1. On the database server, open Task Scheduler in Windows.
2. (Optional) In the Task Scheduler Library, create a new folder for the PME database maintenance tasks, for example Task Scheduler Library > Power Monitoring Expert.
3. Create scheduled database maintenance tasks:

   NOTE: For setting up the archive task for ION_Data, see Setting up the ION_Data archive task for Distributed PME systems

   Use the following information to create the tasks. Replace the variables with the specific settings shown in the task settings table below.

   Name: *<task_name>*
   Security options: Set the Windows user account created in Step 1 to run the task.
   Security options: Select **Run whether user is logged on or not**.
   Trigger: *<trigger_time>*
   Action: Select **Start a program**.
   Action: Program/script:
   C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
   Action: Arguments: **-noninteractive -nologo -file "*<New Folder Path>*\DbScheduledTasks**<*script_name*>**" -DatabaseIdentifier** *<DB ID>*

   NOTE: The "<New Folder Path>\DbScheduledTasks\<script_name>" path must be an absolute path, not a relative path.

NOTE: Valid settings for the <*task_name*>, <*trigger_time*>, <*script_name*>, and <*DB ID*> variables are given in the Task Settings table below.

Example: ApplicationModules backup task

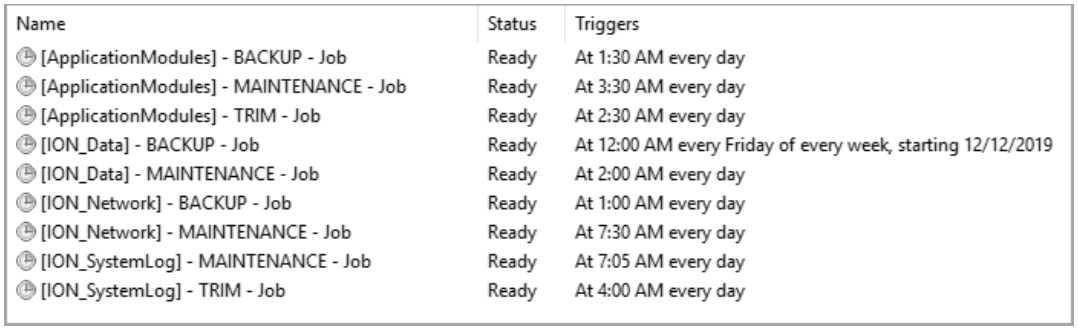
Name: [ApplicationModules] - Backup - Job
Security options: Set the Windows user account created in Step 1 to run the task.
Security options: Select Run whether user is logged on or not.
Trigger: Daily at 01:30 (1:30 AM)
Action: Select Start a program
Action: Program/script: C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
Action: Arguments: -noninteractive -nologo -file "<New Folder Path>\DbScheduledTasks\Backup.ps1" -DatabaseIdentifier APPS

Task Settings table:

NOTE: The task names and trigger times shown in the table are recommendations. You can choose different names or triggers if necessary.

Task	Settings
ApplicationModules backup	Task Name: [ApplicationModules] - Backup - Job Trigger Time: Daily at 01:30 (1:30 AM) Action: Arguments: Script Name: **Backup.ps1**, DB ID: **APPS**
ApplicationModules maintenance	Task Name: [ApplicationModules] - MAINTENANCE - Job Trigger Time: Daily at 03:30 (3:30 AM) Action: Arguments: Script Name: **DatabaseMaintenance.ps1**, DB ID: **APPS**
ApplicationModules trim	Task Name: [ApplicationModules] - TRIM - Job Trigger Time: Daily at 02:30 (2:30 AM) Action: Arguments: Script Name: **TrimDiagnostics.ps1**, DB ID: **APPS**
ION_Data backup	Task Name: [ION_Data] - BACKUP - Job Trigger Time: Weekly at 00:00 (12:00 AM) on Fridays Action: Arguments: Script Name: **Backup.ps1**, DB ID: **ION**
ION_Data maintenance	Task Name: [ION_Data] - MAINTENANCE - Job Trigger Time: Daily at 02:00 (2:00 AM) Action: Arguments: Script Name: **DatabaseMaintenance.ps1**, DB ID: **ION**
ION_Network backup	Task Name: [ION_Network] - BACKUP - Job Trigger Time: Daily at 01:00 (1:00 AM) Action: Arguments: Script Name: **Backup.ps1**, DB ID: **NOM**
ION_Network maintenance	Task Name: [ION_Network] - MAINTENANCE - Job Trigger Time: Daily at 07:30 (7:30 AM) Action: Arguments: Script Name: **DatabaseMaintenance.ps1**, DB ID: **NOM**
ION_SystemLog maintenance	Task Name: [ION_SytemLog] - MAINTENANCE - Job Trigger Time: Daily at 07:05 (7:05 AM) Action: Arguments: Script Name: **DatabaseMaintenance.ps1**, DB ID: **SYSLOG**
ION_SystemLog trim	Task Name: [ION_SytemLog] - TRIM - Job Trigger Time: Daily at 04:00 (4:00 AM) Action: Arguments: Script Name: **TrimDiagnostics.ps1**, DB ID: **SYSLOG**

The completed task list should look like this:



Name	Status	Triggers
[ApplicationModules] - BACKUP - Job	Ready	At 1:30 AM every day
[ApplicationModules] - MAINTENANCE - Job	Ready	At 3:30 AM every day
[ApplicationModules] - TRIM - Job	Ready	At 2:30 AM every day
[ION_Data] - BACKUP - Job	Ready	At 12:00 AM every Friday of every week, starting 12/12/2019
[ION_Data] - MAINTENANCE - Job	Ready	At 2:00 AM every day
[ION_Network] - BACKUP - Job	Ready	At 1:00 AM every day
[ION_Network] - MAINTENANCE - Job	Ready	At 7:30 AM every day
[ION_SystemLog] - MAINTENANCE - Job	Ready	At 7:05 AM every day
[ION_SystemLog] - TRIM - Job	Ready	At 4:00 AM every day

4. (Optional) Manually run each task to verify its correct operation.
5. Close Task Scheduler.

To edit the task script settings (for example to change the backup and archive location or to set the amount of data to keep in the database on trim), open the `Configuration.ps1` script file, as described in Step 3 and change the values of the variables.

Configurable variables in `Configuration.ps1`:

Setting	Variable	Default Value	Comments
Backup folder location	$locationForBackupFiles	As defined in the script file; see Step 3-7.	Sets the folder to which the database backups are saved. The backup script will create the following subfolders in this location: ...\Data for ION_Data ...\Network for ION_Network ...\SystemLog for ION_SystemLog ...\Applications for ApplicationModules NOTE: The Windows user account used to run the backup task needs Read and Write permissions on this folder.
Data to keep when trimming	$diagnosticsDaysToKeep	30	Sets how many days' worth of data is left in the database after trimming.

Default maintenance task settings

The default PME database maintenance tasks are defined as Windows PowerShell scripts, and scheduled and executed using Task Scheduler in Windows. The following table shows the different configuration settings for these tasks, their defaults, and where they are configured:

Setting	Location	Default Value	Comments
Windows account used to run the task	Task Scheduler	User account that is creating the task.	Use IONMaintenance for Standalone systems. Create a new, dedicated account for Distributed systems. See create a Windows user account to run the maintenance tasks for more details.
Task trigger times	Task Scheduler	See default task schedules.	The default schedules are configured automatically for Standalone systems. The schedules for Distributed systems must be configured manually.
Task enabling or disabling	Task Scheduler	See default task schedules.	n/a

Setting	Location	Default Value	Comments
Backup folder location	PowerShell script : Configuration.ps1 Variable: $locationForBackupFiles	...\Power Monitoring Expert \Database\Backup*	Sets the folder to which the database backups are saved. The backup script will create the following subfolders in this location: ...\Data for ION_Data ...\Network for ION_Network ...\SystemLog for ION_SystemLog ...\Applications for ApplicationModules
Archive folder location	PowerShell script : Configuration.ps1 Variable: $locationForArchiveDBFiles	...\Power Monitoring Expert \Database\Archive*	Sets the folder to which the database archives are saved.
Data to keep when trimming	PowerShell script : Configuration.ps1 Variable: $diagnosticsDaysToKeep	30	Sets how many days' worth of data is left in the database after trimming.
Database size (max)**	PowerShell script : Configuration.ps1 Variable: $maximumDatabaseSizeIn Gigabytes	9	Sets the maximum database size. This value is used by the size notification task to assess what percentage of database space has been used. The maximum size for a SQL Express database is 10GB. The maximum size in the script is set to 9GB to allow for a 1GB warning buffer before the database stops logging data.
Database size notification limit**	PowerShell script : Configuration.ps1 Variable: $databaseSizeNotification ThresholdPercentage	85	Sets the threshold for when a database size notification will be issued.

* Default setting for Standalone systems.

** The database size notification is only configured for systems with SQL Server Express databases.

Setting up the ION_Data archive task for Distributed PME systems

Setting up the archive task for ION_Data is similar to setting up other database maintenance tasks but requires some additional steps.

NOTE: It is best to automate the archive task, but you can also run it manually on demand using Database Manager.

To set up the scheduled archive task for ION_Data:

1. Complete Steps 1 - 3 described in Setting up database maintenance tasks for Distributed PME systems.

   NOTE: You can use the same Windows user account (created in Step 1) that is used for other scheduled PME database maintenance tasks to run the archive task. You can also create a new account that is only used for the archive task, because only this task requires sysadmin role privileges on the database server (see next step).

2. On the database server, open SQL Server Management Studio and add the **sysadmin** server role to the Windows user account created in Step 1. This account is used to run the archive task; it needs sysadmin permissions to create new archive databases.

3. On the database server, in the folder created in Step 3, create a subfolder called **etc** and inside this folder a subfolder called **Database**, for example `C:\PME_Database_Maintenance\etc\Database`.
4. Copy the **Data** folder from `...\Power Monitoring Expert\system\etc\Database\`, on the PME application server, into the new **Database** folder on the database server.
5. On the database server, open Task Scheduler in Windows.
6. (Optional) In the Task Scheduler Library, create a new folder for the PME database maintenance tasks, if it does not already exist. For example, Task Scheduler Library > Power Monitoring Expert.
7. Create the scheduled archive task for ION_Data:

   Name: **[ION_Data] - ARCHIVE - Job**
   Security options: Set the Windows user account created in Step 1 to run the task.
   Security options: Select **Run whether user is logged on or not**.
   Trigger: **Monthly at 01:00 (1:00 AM) on January 3rd**
   Action: Select **Start a program**.
   Action: Program/script:
   C:\Windows\syswow64\WindowsPowerShell\v1.0\powershell.exe
   Action: Arguments: **-noninteractive -nologo -file "<*Folder Path*>\DbScheduledTasks\ArchiveDB.ps1" -DatabaseIdentifier ION**

   NOTE: The "<Folder Path>\DbScheduledTasks\ArchiveDB.ps1" path must be an absolute path, not a relative path.

   NOTE: The task name and trigger time shown above are recommendations. You can choose a different name or trigger if necessary.
8. (Optional) Manually run the archive task to verify its correct operation.
9. Close Task Scheduler.

To change the archive location, open the `Configuration.ps1` script file, as described in Step 3 in Setting up database maintenance tasks for Distributed PME systems and change the value of the variable:

Setting	Variable	Default Value	Comments
Archive folder location	$locationForArchiveDBFiles	As defined in the script file; see Step 3-7.	Sets the folder to which the database archives are saved. NOTE: The Windows user account used to run the archive task needs Read and Write permissions on this folder.

Using IONMaintenance for database maintenance tasks

IONMaintenance is a Windows user account that is created automatically when PME is installed in a Standalone architecture. This account is used to run the pre-configured PME database maintenance tasks in Task Scheduler in Windows. To make changes to the task schedules in

Task Scheduler, you need to enter the password for the IONMaintenance account. By default, the password for the account is generated automatically by the installer and cannot be retrieved. To have access to the password, you need to set a custom password for this account.

To set a custom password for IONMaintenance, run the PME installer in maintenance mode and select **Reset Accounts** to start the account password reset procedure. Follow the installer instructions to reset the password.

NOTE: If you set a custom password for the Windows Accounts during the installation of PME, then this is the password used by IONMaintenance and you can use this password to make changes to the task schedules in Task Scheduler.

NOTE: IONMaintenance shares the same password with IONUser, another account that is generated automatically by the installer and which is used for report subscriptions.

NOTE: If you change the password for the Windows accounts, the password you are providing must comply with the password policies of the Windows server and the SQL server. The software installer cannot validate the password at the time you enter it. If the password is not valid, the password reset and reconfiguration will not be successful. In that case, complete the reconfiguration, skipping any unsuccessful steps.

Database Manager

Use Database Manager to manually perform operations on the Power Monitoring Expert databases.

NOTICE

LOSS OF DATA

- Back up the database at regular intervals.
- Back up the database before upgrading or migrating the system.
- Back up the database before trimming it.
- Back up the database before making manual database edits.
- Verify correct database behavior after making database or system changes.

Failure to follow these instructions can result in permanent loss of data.

NOTE: Database Manager does not include manual database operations on the Application Modules database (ApplicationModules). In a disaster recovery situation or when directed by Technical Support, the Application Modules database can be restored by using the Restore database function in the SQL Server Management Studio. See Restoring a database for further information about this operation. ION databases can be restored using the same process.

For information on database maintenance tasks in PME, see Database maintenance.

Prerequisites

The following user prerequisites need to be met to work with Database Manager and database functions through SQL Server Management Studio:

- For Database Manager: Since Windows authentication is used to access the SQL Server databases, the user needs to be a member of the sysadmin SQL Server role, which is set in SQL Server Management Studio.
- For most database functions available in SQL Server Management Studio: The user needs to be a member of the sysadmin SQL Server role.

NOTE: If the Windows user that you used to log into the system is not a member of the sysadmin role, and you want to run Database Manager, you can do so without logging out by completing the following steps:

1. Navigate to the system\bin folder in the product's install location.
2. Locate DatabaseManager.exe.
3. Click the EXE file name to highlight it, then press **Shift+Right-click** to open the menu.
4. Click **Run as different user** to open the Windows Security dialog.
5. In the **User name** field, type a user name that has the sysadmin role, then type the password for that user.
6. Click **OK** to open Database Manager.

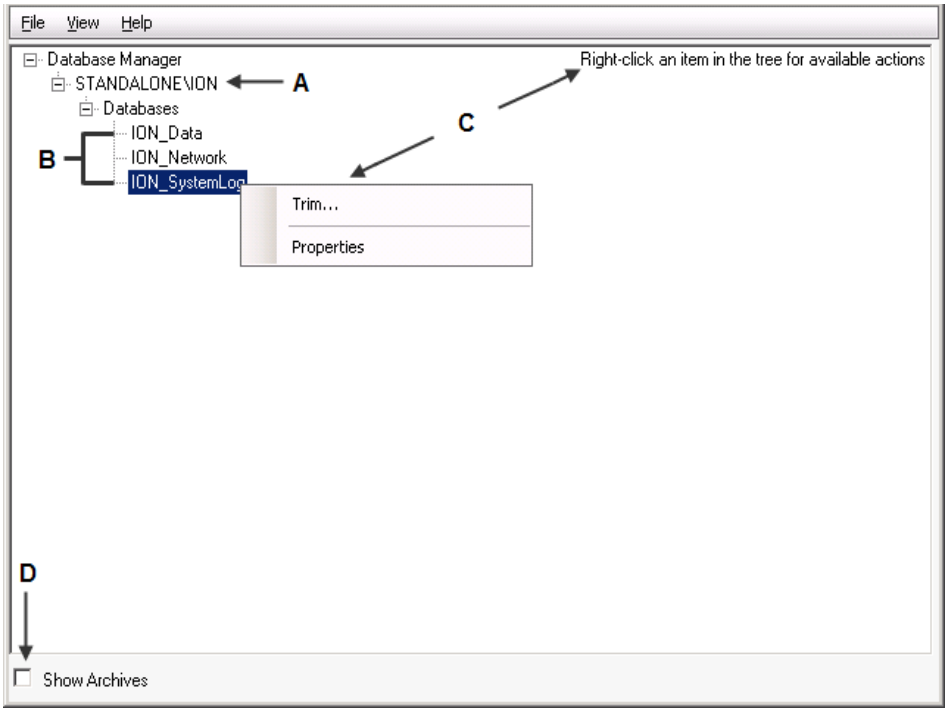
Database Manager interface

To access Database Manager, start Management Console then click **Tools > Database Manager**.

Note that the Windows user running Database Manager needs to be a member of the sysadmin SQL Server role.

Expand the items in the navigation tree to display the **Databases** for each instance.

Note that scheduled jobs are available only in Windows Task Scheduler. For further information, see Database maintenance.



A	SQL Server Instance	B	Databases	C	Options menu	D	Show Archives

SQL Server instance

The default SQL Server instance that the product uses for its databases is *COMPUTERNAME**INSTANCE*, where *COMPUTERNAME* is the name of the server, and *INSTANCE* is the SQL Server instance used with the product.

Databases

The **Databases** section lets you view information about the databases or perform manual actions on the databases.

For information on the manual actions you can perform, see Manual actions.

Viewing Database Properties

To view the properties of a particular database, right-click that database and select **Properties**. The properties are:

- **Size**: The current size of the database.
- **Primary File Location**: The file path for the primary database (.mdf) file.
- **Transaction Log Location**: The file path for the transaction log (.ldf) file.
- **Creation Date**: The date and time when the database was created.
- **Last Backup Date**: The date when the last backup was performed.
- **Disk Space Available**: The amount of free space available on the disk where the database resides.

- **Server Version**: The type and version of the SQL Server instance that is hosting the database.

Show archives

Select this check box (lower left-hand corner) if you want the list under **Databases** to include all archived databases along with the live databases. After **Show Archives** is selected, you can upgrade archived databases or view the properties of the archived databases.

Clear the **Show Archives** check box to hide the archived databases from view. This also prevents the database actions from being performed on database archives.

Manual actions

The following sections provide information on the manual actions that you can use to manage your databases.

To perform an action manually, do one of the following:

- Right-click **Databases** and select the action from the menu, or
- Right-click the specific database and select the action you want to perform from the pop-up menu.

When you right-click **Databases** and select an action, a dialog specific to that action opens. The databases listed in the dialog are those to which the action applies.

When you right-click a specific database, only the actions that apply to that database appear in the menu and the database is selected by default in the dialog for the action.

Archive

The Archive action creates an archive of the selected database.

Before proceeding, ensure that you have write access to the archive directory location.

1. Right-click **Databases** or **ION_Data** and select **Archive** to open the **Database Archive** dialog. If necessary, select the database that you want to archive.
2. Select the directory where the archive will be saved.

   For **standalone** environments:

   a. In **Save archive to**, click the browse button  to select the directory where the archive will be saved.

   `...\Power Monitoring Expert\Database\Archives\Data` is the default directory for the saved archive, but you can specify another local directory.

   b. (Optional) Specify a different local directory.

   NOTE: You can only save an archive to a directory on the local machine, not to a location on the network.

   c. (Optional) Edit the default archive filename to follow your naming conventions.

   NOTE: The database name is restricted to characters A-Z, a-z, 0-9, and _ (underscore).

For **distributed** environments:

a. In **Save archive to**, enter an existing directory path on the server and a valid filename for the archive.

For example: `C:\Archives\ION_Data_January.mdf`. The path – in the example `C:\Archives` – must exist on the Database Server.

NOTE: The database name is restricted to characters A-Z, a-z, 0-9, and _ (underscore).

3. Select the data types that you want to archive.
4. Specify the date range of the data that you want to archive. For **Start**, select **The beginning of the database** or select **Date** and enter a date and time. Enter a date and time for **End Date**.
5. Under **Trim after archive** select whether or not you want to remove archived data from the database.

You need to select **The beginning of the database** for the start date range for trimming the live database, otherwise the **Trim after archive** option is disabled.

6. Click **OK**.

The **Progress** field displays the current progress of the archive process. If a manual archive does not succeed, a message appears and the **Database Archive** dialog remains open with the **OK** button grayed out — examine the **Progress** field to discover where the process did not succeed. If the archive is successful, the dialog closes automatically.

Export Registry Setting

The Export Registry Setting action exports settings to a registry (.reg) file. This is useful if you need to set up client computers in a system where the primary server's database settings (server instance name and database name) are customized. After you export the settings to the registry (.reg) file, you can import that registry file on the client computer.

1. Right-click **Databases** and select **Export Registry Setting** to open the **Database Registry Key Export** dialog.
2. Type the path and filename for the file or click the browse button  to specify the location for the saved the database registry key.

The directory ...\Power Monitoring Expert\config\cfg\ is the default save location for the exported database registry key.

3. Click **OK**.

New ION_Data Database

The New ION_Data Database action creates a new, blank version of the ION_Data database.

1. Right-click **Databases** and select **New ION_Data Database** to open the **New Historical Database** dialog.
2. Type a name for your new database.

NOTE: Do not name it “ION_Data” as this is the default name for the existing ION database. Database names are restricted to characters A-Z, a-z, 0-9, and _ (underscore).

3. Click the browse button  to specify a location for the database.
4. Click **OK**.

Trim

The Trim action removes data from a database.

NOTICE
LOSS OF DATA • Back up the database at regular intervals. • Back up the database before upgrading or migrating the system. • Back up the database before trimming it. • Back up the database before making manual database edits. • Verify correct database behavior after making database or system changes. **Failure to follow these instructions can result in permanent loss of data.**

1. Right-click **Databases**, **ION_Data** or **ION_SystemLog** and select **Trim** to open the **Trim Database** dialog.
2. Select the database you want to trim from the **Database to trim** list.
3. Under **Trim Range**, specify the date range of data you want to trim (for the ION_Data database) or set the maximum data age in days (for the ION_SystemLog database).
4. For the ION_Data database, select the data types you want to trim (**Data Records**, **Waveforms**, **Events**) in the **Data Types** section. You can select any combination of data types to trim.
5. Click **OK**. A message appears to notify you that the selected data will be removed. Click **Yes** to continue or **No** to cancel.

Upgrade Database

The Upgrade Databases action upgrades the selected database to the latest database schema.

1. Right-click **Databases** and select **Upgrade Databases** to open the **ION Database Upgrade** dialog.

   The Power Monitoring Expert installer automatically upgrades your databases with the new database schemas when you install Power Monitoring Expert on an existing server. If you install the latest version of the product on a different server so that you can manually copy older database files to the new computer, you can run this action on the older databases (that is, on the ION_Data, ION_SystemLog, and ION_Network databases, and archives) to upgrade them with the new schema.
2. Select the database in the list that you want to upgrade and click **OK**.

Restoring a database

You can restore a database from a backup by logging in to SQL Server Management Studio as a user with syadmin access authority for the **Restore Database** function. (Database backups are specified as a scheduled job in Windows Task Scheduler. See Database maintenance for more information.)

Restoring the latest database

Complete the following to restore a database from the latest backup:

1. Stop all ION services.
2. Open **SQL Server Management Studio**, enter your password if required and click **Connect** to access your SQL Server.
3. In the **Object Explorer** pane on the left, expand **Databases**, right-click the database you want to restore and click **Tasks > Restore > Database** to open the **Restore Database** dialog.
4. Under **Source**, select **Database** and click the database you want to restore in the dropdown list if it is not already selected.
5. Under **Backup sets to restore**, select the checkbox in the **Restore** column for the database you want to restore.
6. Click **Options** in the **Select a page** pane on the left.
7. On the **Options** page:
   - Under **Restore options**, select **Overwrite the existing database (WITH REPLACE)**.
   - For **Recovery state**, select **RESTORE WITH RECOVERY** from the dropdown list.

     RESTORE WITH RECOVERY is described as **Leave the database ready to use by rolling back uncommitted transactions. Additional Transaction logs cannot be restored**.
8. Click **OK** to begin the restore operation.

   A message indicates that the database has been restored successfully. If the restore operation is not successful, the database reverts to its original state.

   NOTE: After you restore the database, you need to assign its ownership to the ION user as follows:

   a. In SQL Server Management Studio, right-click the restored database and click **Properties** in the menu to open the Database Properties dialog.
   b. Click **Files** under **Select a page**.
   c. Click the button on the right of the **Owner** field to open the Select Database Owner dialog.
   d. Type ION in the field labeled **Enter the object names to select** and click **Check Names** to adjust the format of your entry to [ION].
   e. Click **OK** to update the owner of the database.

f. Click **OK** to close the Database Properties dialog.

9. Restart all ION services.

Restoring a specific database

Complete the following to restore a specific database:

1. Repeat steps 1 through 3 from Restoring the latest database above.
2. Under **Source**, select **Device** and click **Browse** to open the **Select backup devices** dialog.
3. Select **File** in **Backup media type** list if it is not already specified and then click **Add** to open the **Locate Backup File** dialog.
4. Navigate to and select the backup file you want to restore and click **OK**.
5. Verify that the file referenced in the **Specify Backup** dialog is the one you selected and click **OK** to return to the **Restore Database** dialog.
6. Under **Select the backup sets to restore**, select the checkbox in the **Restore** column for the database you are restoring.
7. Click **Options** in the **Select a page** pane on the left.
8. On the **Options** page:
   - Under **Restore options**, select **Overwrite the existing database (WITH REPLACE)**.
   - Under **Recovery state**, select **RESTORE WITH RECOVERY** from the dropdown list.

     RESTORE WITH RECOVERY is described as **Leave the database ready to use by rolling back uncommitted transactions. Additional Transaction logs cannot be restored**.
9. Click **OK** to begin the restore operation.

   A message indicates that the database has been restored successfully. If the restore operation is not successful, the database reverts to its original state.

   NOTE: After you restore the database, you need to assign its ownership to the ION user as follows:

   a. In SQL Server Management Studio, right-click the restored database and click **Properties** in the menu to open the Database Properties dialog.
   b. Click **Files** under **Select a page**.
   c. Click the button on the right of the **Owner** field to open the Select Database Owner dialog.
   d. Type ION in the field labeled **Enter the object names to select** and click **Check Names**.

      The format of your entry changes to [ION].
   e. Click **OK** to update the owner of the database.
   f. Click **OK** to close the Database Properties dialog.
10. Restart all ION services.

Configure database connection encryption

You can configure PME to use encryption for the communication between the application server and the database server. You can also specify if PME trusts self-signed server certificates on the database server or not. For more information on setting up encryption for database connections, see Set up encrypted database communication for Distributed Database architectures.

NOTE: Before editing the settings in the registry, confirm that your PME system has been taken out of service and that all system services have been stopped.

To enable or disable encryption for database connections:

1. Open the Windows Registry Editor.
2. Navigate to the following registry key:`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Schneider Electric\Power Monitoring Expert\10.0\Databases`
3. Set the `UseEncryption` value to 1, to enable encryption, or to 0, to disable encryption.

To configure the software to trust or not trust self-signed certificates on the database server:

1. Open the Windows Registry Editor.
2. Navigate to the following registry key:`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Schneider Electric\Power Monitoring Expert\10.0\Databases`
3. Set the `TrustServerCertificate` value to 1, to trust self-signed certificates, or to 0, to not trust self-signed certificates.

Database growth calculations

Factory default measurement logging

A measurement record in the database uses approximately **75 bytes** of disk space. Based on the factory default data logging configurations, we can calculate the database growth for data logged from different device types.

Example

Device Type	Daily Growth Rate (kB)	Number of Devices	Total Daily Growth (MB)	Total Annual Growth (GB)
ION7650	780	10	7.62	2.72
PM8000	950	20	19.00	6.94
PM3200	85	70	5.81	2.07
TOTAL	-	100	32.43 MB	11.84 GB

NOTE: Use the Database Growth Calculator tool to estimate the database growth for your system. The tool is available through the Exchange Community. See Resources for link information.

Custom measurement logging

Custom measurement logging can be configured in the monitoring devices and, as software based logging, in PME. A measurement record in the database uses approximately **75 bytes** of disk space.

The following shows the database growth estimate for logging of a single measurement every 15 minutes:

$$Single\ Measurement\ (MB) = \frac{365\ \frac{Days}{Year} * 24\ \frac{Hours}{Day} * 4\ \frac{Measurement}{Hour} * 75\ \frac{bytes}{Measurement}}{1{,}048{,}576\ \frac{bytes}{MB}}$$

$$= 2.51\ MB\ /\ YR$$

NOTE: Use the Database Growth Calculator tool to estimate the database growth for your system. The tool is available through the Exchange Community. See Resources for link information.

Power quality event logging

Power quality (PQ) events and waveform capture recording is event driven, which makes it impossible to accurately predict their impact on database growth. In our experience, power quality data accounts for approximately 10% - 20% of the total database size.

NOTE: Use the Database Growth Calculator tool to estimate the database growth for your system. The tool is available through the Exchange Community. See Resources for link information.

Adding idle detection to custom Web Application links

PME automatically times out inactive client sessions. If custom content links are added to the Web Applications framework, then the custom content must implement the idle detection, or activity on that content is not registered and the Web client session can time out unexpectedly.

Prerequisite: The custom application must be in the same Application Pool as the regular PME applications, and must use the same authentication configuration.

To add idle detection to custom content:

1. In the custom Web application, Add references to jquery and jquery.idle.js.
2. Create an IdleDetection object when the document has loaded.

> **NOTE**: If you want your application to take part in keeping PME non-idle, but you do not want your application to log itself out after the idle period, you can add the following JSON as a parameter to the idle() method: `{enableLogoutRedirection: false;}`

Example web.config for an application in the PME Application Pool:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
 <system.web>
 <compilation debug="true" targetFramework="4.6" />
 <httpRuntime targetFramework="4.6" requestValidationMode="2.0"
enableVersionHeader="false" />
 <authentication mode="Forms">
 <forms name=".APPLICATIONFRAMEWORK" loginUrl="/SystemDataService/Auth"
defaultUrl="/SystemDataService/Auth/GenerateAuthUrl" timeout="2880"
protection="All" enableCrossAppRedirects="true" />
 </authentication>
 <machineKey decryption="AES" decryptionKey="AutoGenerate"
validation="HMACSHA256" validationKey="AutoGenerate" />
 <authorization>
 <deny users="?" />
 </authorization>
</system.web>
</configuration>
```

Example minimal page that has idle detection added to it:

test.html

```
<!DOCTYPE html>
<html>
<head>
    <title>Example Application for Idle Detection</title>
    <script src="/SystemDataService/Content/External/jquery/jquery-2.1.4.modified.js"></script>
    <script src="/SystemDataService/Content/External/jquery/jquery.idle.js"></script>
    <script>
        $(document).ready(function() {
            $(document).idle();
        });
    </script>
</head>
<body>
   Example Application
</body>
</html>
```

Diagnostics and Usage Services

Diagnostics and Usage anonymously sends data to a secure server. Schneider Electric uses this data to help improve our software by understanding how you use it.

The diagnostics and usage service collects and sends data to Schneider Electric weekly on Monday at 2:00 a.m. (server time), over HTTPS at port 443. Each time the service runs, it creates a log file in the `system\bin` folder in the Power Monitoring Expert install location.

This operation is enabled by default.

NOTE: All diagnostics and usage data are sent to Schneider Electric anonymously. None of the collected information identifies you or your company. For more information on the Schneider Electric Privacy Policy, see the Schneider Data Privacy and Cookie Policy.

The following diagnostic and usage data is collected when it is enabled:

Diagnostic Data	Usage Data
• Power Monitoring Expert version • Operating system version and type (32- or 64-bit) • Number of CPU cores • System memory (RAM) • .NET Framework version • SQL Server version • Distributed or local database • City or region • Number of monitors in use • Client screen resolution • Screen DPI	• Total number of devices • Device type count • Number of users

To disable the sending of data:

1. Open Web Applications and click **Settings > Registration & Analytics > Diagnostics and Services**.
2. Select **Disable** in the dropdown list and click **Save** to apply the change.

Decommissioning Reference

This section contains detailed instructions for decommissioning your system. For an overview, see Decommission.

NOTICE

UNINTENDED DATA LOSS OR LOSS OF SOFTWARE FUNCTION

- Only decommission PME systems that are no longer needed.
- Archive important PME data and files before decommissioning. You cannot recover, reinstall, or otherwise retrieve any part of PME after decommissioning.

Failure to follow these instructions can result in irreversible damage to software and databases.

Choose **Destroy** or **Overwrite** to decommission your system.

You must decommission PME on all PME Servers, Database Servers, and PME Clients.

Decommissioning does not completely restore your computers to the state they were in before PME was installed. Decommissioning does not remove third-party software used by PME (for instance, the .NET framework), even if this software was installed using the PME installer.

NOTE: Decommissioning will not remove PME data that has been exported from PME or PME information in third-party software. This includes, but is not limited to:

- Data exported to other systems using EcoStruxure Web Services (EWS), OPC DA server, ETL, ODBC, PQDIF or VIP.
- Registration information shared with Schneider Electric.
- Diagnostics and Usage data sent to Schneider Electric.
- System information sent to Schneider Electric for licensing.
- Archived configurations created with the Configuration Manager.
- PME System Key exported from the Installer.
- PME information configured in third-party whitelisting software.
- Files or data copied, backed-up, exported, or otherwise saved to a file location other than the PME folder.

Destroy

⚠ WARNING

HAZARD OF PHYSICAL INJURY

- Do not destroy hard drives without the proper safety training.
- Never burn a hard drive, put a hard drive in a microwave, or pour acid on a hard drive.

Failure to follow these instructions can result in death or serious injury.

NOTE: If you do not have the proper safety training, consult your IT department to select an asset disposal company.

To destroy hard drives:

1. Identify all computers where PME is installed. In a Distributed Database architecture, this includes all PME Servers, Database Servers, and PME Clients.
2. Remove all hard drives from the computers identified in the previous step.
3. Destroy each hard drive:
   a. Puncture, shatter, or sand the hard drive plates. Follow local regulations for proper disposal of the hard drive.
   b. or, provide the hard drive to an asset disposal company.

Overwrite

NOTICE

UNINTENDED DATA LOSS OR LOSS OF SOFTWARE FUNCTION

- Only overwrite files and folders from PME.
- Back up important files from other software before overwriting PME.

Failure to follow these instructions can result in irreversible damage to software and databases.

To overwrite PME:

1. Open the Windows Control Panel and select Programs and Features.
2. Uninstall PME.
3. Select and install a data destruction tool. There are many commercial and open-source data destruction tools available. Consult your IT department if you are unsure about which tool to choose.
4. Detach PME database archives:
   a. Open **SQL Server Management Studio**, enter your password if required and click **Connect** to access your SQL Server.
   b. In the **Object Explorer** pane on the left, expand **Databases**, right-click the database archive you want to detach and click **Tasks > Detach**… to open the **Detach Database** dialog.
   c. In the **Detach Database** dialog, click **OK**.
   d. Repeat the above steps for all PME database archives.
5. Locate your PME folder under Program Files. The PME folder contains the following subfolders:
   - `\Applications`
   - `\config`
   - `\Database`

- \diagnostic
- \Diagnostics Tool
- \License Configuration Tool
- \Licenses
- \Setup
- \SetupLogs
- \system
- \Uninst_PowerMonitoringExpert
- \web

6. Follow instructions provided with your data destruction tool to overwrite the entire PME folder located in the previous step.
7. Locate any custom PME files in folders outside of the PME folder. This may include, but is not limited to, following file types:
   - Vista and Designer files: .cfg, .dgm, .wsn, .wsg
   - ION databases and archives: .LDF, .MDF
   - ION database backups: .bak
   - Custom report packs: .rdlc
   - PMESystem Key: .key
8. Follow instructions provided with your data destruction tool to overwrite the files located in the previous step.
9. Repeat the steps above on all PME Servers, Database Servers, and PME Clients.

IP Ports

The following table lists the ports used by PME for the communication between its components and the connected devices:

Port	Protocol	Location	Function	Configurable
20/21	FTP	Power Meter	Power meter access	No
23	Telnet	Power Meter	Power meter access	No
25	SMTP	Power Meter	Power meter access	No
69	TFTP	Power Meter	Power meter access	No
80	HTTP	(1) PME Server (2) Power Meter	(1) IIS server, EWS (2) Power meter access	(1) Yes (2) No
135	OPC	PME Server	OPC client	No
139/445	NetBIOS/SMB	PME Server	Engineering client (File and Printer Sharing)	No
443	HTTPS	(1) PME Server (2) Power Meter	(1) IIS Server, EWS, Cloud Agent (2) Power meter access	No
502	Modbus TCP	Power Meter	Power meter communication	No
1433	TCP	Database Server	SQL Server instance	No
1434	UDP	Database Server	SQL Server Browser	No
3721	PML	Power Meter	Power meter communication	No
6000-6099	TCP	PME Server	Log Inserter	No
7070	TCP	PME Server	Licensing	Yes
7176	TCP	PME Server	Diagnostics Viewer (LogSubsystem.Service.exe)	No
7700	ION	Power Meter	Power meter communication	No
7701	Modbus RTU	Power Meter	Power meter communications	No
7800	Modbus/ION/PML	Gateway	Ethergate (All meter COM ports)	No
7801	Modbus/ION/PML	Gateway	Ethergate (Meter COM1)	No
7802	Modbus/ION/PML	Gateway	Ethergate (Meter COM2 and COM 4)	No
7803	Modbus/ION/PML	Gateway	Ethergate (Meter COM3)	No
8090	TCP	PME Server	Web client browser	Yes
8523	TCP	PME Server	Logical devices (LogicalDevice.AutoConfig.ServiceHost.exe)	Yes
13666	TCP	PME Server	PMLNetman.exe	No
13667	TCP	PME Server	Diagnostics Viewer (Server access from client machine)	No
13668	TCP	PME Server	Secondary server	No
13666 13670 13671	TCP	PME Server	Services (Vista and Designer access from client machines)	No
23102	TCP	PME Server	Application Modules web services	No
57777	TCP	PME Server	(1) Real-time data service (to send data to clients) (2) SQL Server (for default instance)	Yes

Port	Protocol	Location	Function	Configurable
57778	TCP	PME Server	DataProcessorService.exe	Yes
57779	TCP	PME Server	Diagnostics Viewer (Alarm Service)	Yes
57780	TCP	PME Server	Diagnostics Viewer (Log Subsystem)	Yes
57781	TCP	PME Server	Diagnostics Viewer (Cloud Agent)	Yes

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+33 (0) 1 41 29 70 00

www.se.com

7EN02-0449-01 01/2022