StruxureWare™

Power Monitoring Expert 8.2

IT Guide

7EN42-0155-00

03/2017

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 an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

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

⚠ CAUTION

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

NOTICE

NOTICE is used to address practices not related to physical injury. The safety alert symbol shall not be used with this signal word.

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 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 because communication delays can occur between the time a control is initiated and when that action is applied.
- Do not use the software to control remote equipment without securing it with an authorized access level, and without including a status object to provide feedback about the status of the control operation.

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

⚠ WARNING

INACCURATE DATA RESULTS

- Do not incorrectly configure the software, as this can lead to inaccurate reports and/or data results.
- 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

- Change default passwords to help prevent unauthorized access to device settings and information.
- Disable unused ports/services and default accounts to help minimize pathways for malicious attackers.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cyber security best practices (for example: least privilege, separation of duties) to help prevent unauthorized exposure, loss, or modification of data and logs, or interruption of services.

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

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.

Product documentation

The following Power Monitoring Expert documentation is applicable to this version of the product.

- *What's New*, document number 7EN12-0302-00.
- *Before Installing your Software*, document number 7EN52-0406-00.
- *Using the SQL Server 2012 DVD*, document number 7EN52-0391-00.
- *Using the SQL Server 2016 DVD*, document number 7EN52-0432-00.
- *Installation Guide*, document number 7EN02-0392-00.
- *User Guide*, document number 7EN02-0391-00.
- *Hierarchy Manager – Help Topics*, document number 7EN52-0413-00.
- *Web Applications – Help Topics*, document number 7EN52-0412-00.

The following documents are available through the Power Monitoring Expert Exchange Community. Contact your Schneider Electric representative for further information.

- *Design Guide*, document number 7EN42-0141-00.
- *IT Guide*, document number 7EN42-0155-00.
- *Licensing Guide*.
- Documentation related to product upgrades.

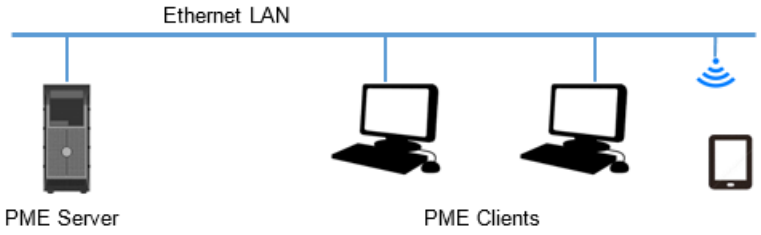
Online information available in the product includes:

- *Power Monitoring Expert Help* – accessible from within installed components, such as Management Console, Vista, and Designer.
- *Alarm Configuration Help* – accessible in a browser-based help format from the Alarm Configuration application.
- *Hierarchy Manager Help* – accessible in a browser-based help format from the Hierarchy Manager application.
- *Web Applications Help* – accessible in a browser-based help format from the Web Applications application.

Architecture and setup types

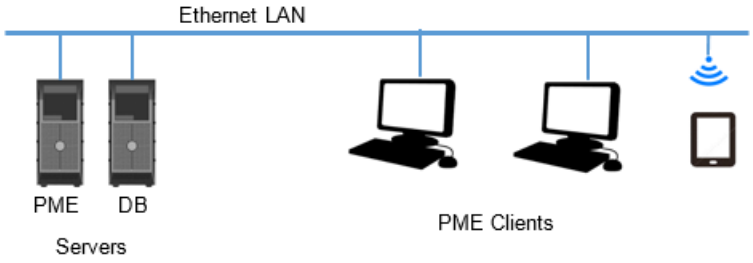
PME is deployed in one of two basic architectures: standalone or distributed database.

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. Users 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 PME database files. Users access the power monitoring data through clients.

PME setup types

Reflecting the different deployment architectures, the PME installer provides the following setup type options:

Setup Type	Architecture	Description
Standalone Server	Standalone	A Standalone Server hosts PME configuration files and services, the IIS server, and a SQL Server instance for the PME databases.

Setup Type	Architecture	Description
Application Server	Distributed database	An Application Server hosts the PME configuration files and services, and the IIS server. It communicates with the remote database server to access the PME databases.
Secondary Server	Custom	Secondary Server installations are not common, and are used only in exceptional circumstances.
Client (optional component)	Both	Clients are designed for administrators and power users. An Engineering Client provides access to the PME thick client UIs and the Excel-based Reporter component. A Reporting Client lets users generate reports using the Excel-based Reporter component of PME.

Desktop or mobile Web clients do not require any software installation. Using a supported browser, Web clients access PME power monitoring data through the web server running on the PME server.

For information on how to design a PME system, see the *Power Monitoring Expert Design Guide*.

Prerequisites and dependencies

Installation sequence

An instance of SQL Server must be installed before PME can be installed.

The PME standalone or application server must be installed before PME clients can be installed.

SQL Server considerations

PME can work with newly installed, or existing SQL Server systems.

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. Follow the installation instructions for SQL Server in the *Power Monitoring Expert Installation Guide*.
New SQL Server Express	The PME installer provides the option to install an instance of SQL Server 2014 Express. This is a free version of SQL Server. All required resources for the installation are included with the PME installer. The installation of SQL Server Express is seamlessly integrated into the PME install process.
Existing SQL Server Standard	To use an existing instance of SQL Server Standard with PME, the SQL Server setup wizard must be rerun to configure the software correctly for use with PME. Follow the installation instructions for SQL Server in the *Power Monitoring Expert Installation Guide*.
Existing SQL Server Express	The PME installer can add a new instance to an existing SQL Server Express for use with PME.

Distributed database install

In a distributed database installation, the SQL Server is installed on a different computer than the PME software. PME must be able to create and access databases in an existing folder location on the SQL Server computer.

Resource requirements

The hardware requirements for a PME server depend on the power monitoring system size and configuration as well as performance expectations. The PME databases will grow over time as data is being collected and stored.

The network bandwidth requirement for communication between PME server and clients depends on the type, frequency, and amount of data requested by the clients.

The network bandwidth requirement for device communication depends on the device types, device configuration, and communication methods.

See the *Power Monitoring Expert Design Guide* for system specification details.

Software licensing

PME uses a feature based licensing model.

A newly installed PME system includes a 90-day trial license for all features of the product. After 90 days some software functionality is disabled if the required purchased licenses are not activated.

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. Licenses can only be returned and reactivated once per calendar year.

See the *Power Monitoring Expert Licensing Guide* details.

Other considerations

Naming the server

Verify that the computer name for the server conforms to Windows naming conventions. A computer name is limited to 15 characters and it must not contain blank spaces or any of the following prohibited characters:

\ (backslash)	; (semi-colon)
/ (slash)	< (less than)
* (asterisk)	> (greater than)
+ (plus)	? (question mark)
= (equals)	" (quotation mark)
| (vertical bar)	_ (underscore)
: (colon)	

For compatibility with Power Monitoring Expert software, use only letters and numbers, starting the name with a letter, for example `MyServer123`.

NOTE: The computer name must not be changed after the Power Monitoring Expert software is installed. If the computer name is changed after the install, the software ceases to function correctly. Should this occur, contact Technical Support for assistance.

Database backups

The power monitoring data collected by PME is a business asset and must be secured against accidental loss. The PME databases should be backed up regularly, using standard SQL Server backup procedures. PME databases can reach 100s of GB in size. Appropriate backup locations must be provided to accommodate this database size.

Display resolution

The minimum display resolution for PME user interfaces is 1024 x 768 pixels.

Operating environment

PME must be used with Microsoft Windows and Microsoft SQL Server software. Other operating system or database software is not supported.

Supported environments and software

PME supports a variety of Windows operating systems, SQL Server editions, and other supporting software. Any limitations on combinations of Windows operating systems with SQL Servers set by Microsoft apply.

Software	Supported versions/editions
Operating system	Windows 7 Professional/Enterprise, SP1 Windows 8.1 Professional/Enterprise Windows 10 Professional/Enterprise Windows Server 2008 R2 Standard/Enterprise, SP1 Windows Server 2012 Standard/Enterprise Windows Server 2012 R2 Standard Windows Server 2016 Standard
Database system	SQL Server 2008 R2 Express, SP3* SQL Server 2012 Express, SP3* SQL Server 2014 Express, SP1 SP2* SQL Server 2016 Express, SP1* SQL Server 2008 R2 Standard/Enterprise, SP3 SQL Server 2012 Standard/Enterprise/Business Intelligence, SP3 SQL Server 2014 Standard/Enterprise/Business Intelligence, SP1 SP2 SQL Server 2016 Standard/Enterprise/Business Intelligence, SP1
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

Software	Supported versions/editions
Microsoft Excel	Microsoft Excel 2010, 2013, or 2016
Desktop Web browser	Microsoft Internet Explorer versions 10 and 11*** Microsoft Edge Google Chrome version 42 and later Mozilla Firefox version 35 and later Apple Safari versions 7 or 8 and later
Mobile Web browser	Safari on iOS7 and iOS8 operating systems Browsers on Android operating systems 4.4 - 4.4.4, and 5.0
.NET Framework	4.6 for Power Monitoring Expert 3.5 (or 3.5 SP1) for the Power Monitoring Expert installer 4.0 for the Power Monitoring Expert licensing component
Microsoft Silverlight	Microsoft Silverlight 5.0 or later

* Express editions of SQL Server can only be used for standalone PME installations. They cannot be used for distributed database installations.

** Virtual environments must be configured 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.

*** Only Internet Explorer 10/11 can access the Alarms and Tables apps in the web application framework. These applications require Microsoft Silverlight technology which is not available on other browsers.

Localization

PME supports the following languages:

English, Chinese (Traditional and Simplified), Czech, French, German, Italian, Polish, Russian, and Spanish.

Use PME with an operating system (OS) and SQL Server of the same language. For example, Spanish PME with Spanish OS and Spanish SQL Server.

The English version of PME can be used with a supported language, non-English OS and SQL Server. For example, English PME with Italian OS and Italian SQL Server.

Operating system and SQL Server updates

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

Network connectivity

TCP port requirements

PME depends on certain TCP 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.

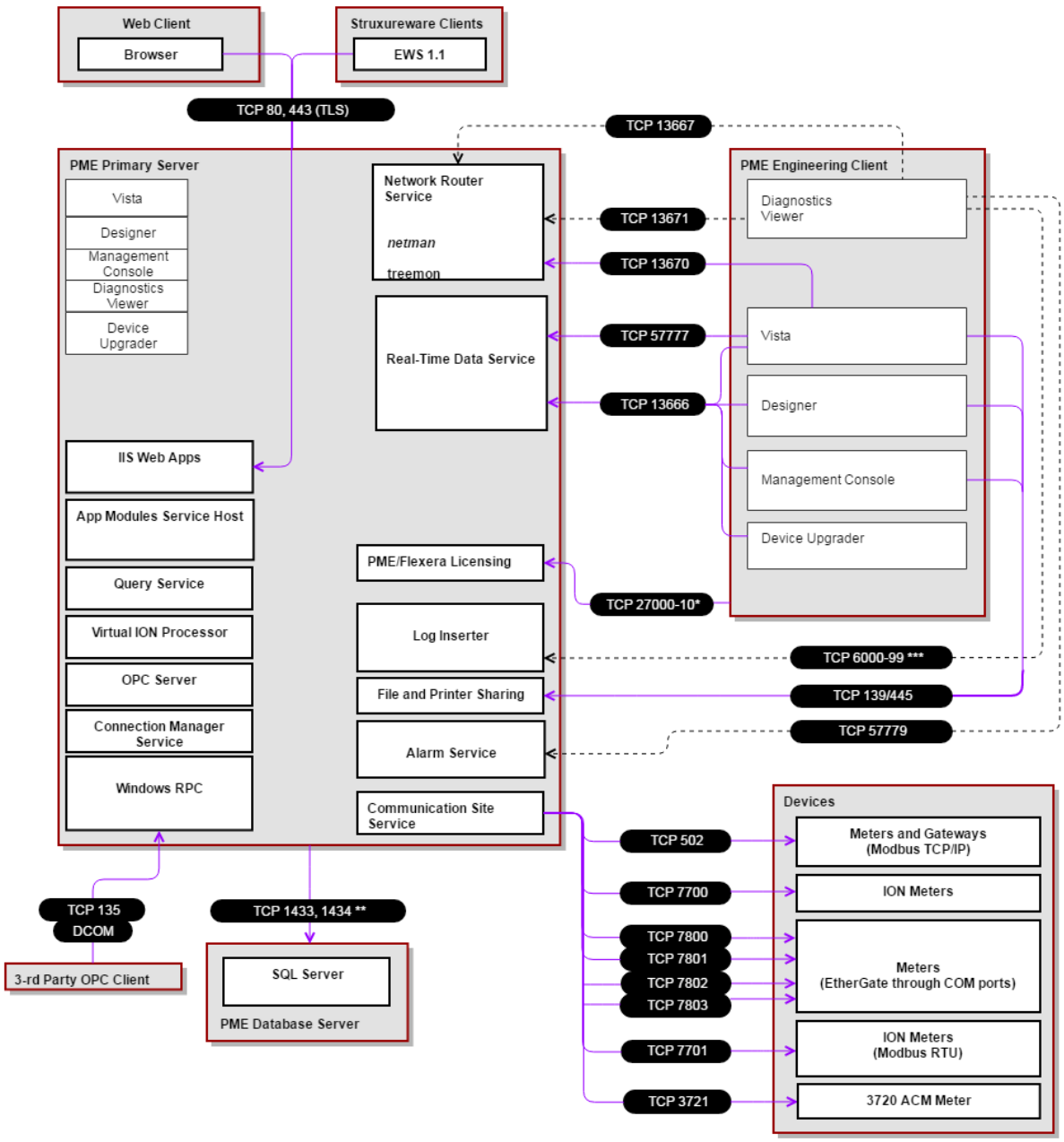
The following table lists all ports and their functions:

Function	Type	Protocol	Port	Configurable	Location
SQL Server instance	Core	TCP	1433	No	Database Server
SQL Server Browser	Core	UDP	1434	No	Database Server
IIS Server	Core	HTTP	80	Yes	PME Server
IIS Server	Core	HTTPS	443	No	PME Server
PME Vista	Core	TCP	13666	No	Engineering Client
PME Vista	Core	TCP	13670	No	Engineering Client
PME Vista	Core	TCP	57777	No	Engineering Client
PME Designer	Core	TCP	13666	No	Engineering Client
PME Management Console	Core	TCP	13666	No	Engineering Client
PME Device Upgrader	Core	TCP	13666	No	Engineering Client
Power Meter Comms	Core	Modbus TCP	502	No	Power Meter
Power Meter Comms	Core	Modbus RTU	7701	No	Power Meter
Power Meter Comms	Core	ION	7700	No	Power Meter
Power Meter Comms	Core	PML	3721	No	Power Meter
Ecostruxure Web Services	Core	HTTP	80	Yes	PME Server
Flexera Licensing	Core	TCP	27010	Yes	PME Server
PME OPC Client	Core	OPC	135	No	PME Server
File and Printer Sharing	Core	NetBIOS/SMB	139/445	No	PME Server
PME Diagnostics Viewer	Diagnostic	TCP	13667	No	Engineering Client

Function	Type	Protocol	Port	Configurable	Location
PME Diagnostics Viewer	Diagnostic	TCP	13671	No	Engineering Client
PME Diagnostics Viewer	Diagnostic	TCP	6000-99	No	Engineering Client
PME Diagnostics Viewer	Diagnostic	TCP	57779	No	Engineering Client
Ethergate gateway	Optional	Modbus/ION/PML	7800-03	No	Gateway
Power Meter	Optional	Telnet	23	No	Power Meter
Power Meter	Optional	FTP	20/21	No	Power Meter
Power Meter	Optional	TFTP	69	No	Power Meter
Power Meter	Optional	SMTP	25	No	Power Meter
Power Meter	Optional	HTTP	80	No	Power Meter
Power Meter	Optional	HTTPS	443	No	Power Meter

* The direction of a port is determined by the communication initiation request which will establish the communication socket.

The following image shows the ports and the components they are associated with:



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. The Database Manager is an optional tool, used for managing the PME databases.

PME does not support Windows Active Directory services.

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 dual stack IPv4/IPv6 network adapters.

Other considerations

Network communications

PME server, database server, and clients must be able to communicate with each other over a high bandwidth 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 PME is connected to, 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 and Reporting 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.

Accounts and permissions

PME

PME uses role based, password protected, user accounts.

One supervisor account (highest privilege level) is created during the installation of PME with a user defined password. No other accounts are created by default.

PME does not support Windows Active Directory services.

Windows

User Accounts

The following tables list the Windows accounts and permissions required for PME installation, operation, and maintenance:

Account	Permissions	Machine	Notes
Login used to install PME	Member of local Administrator group	PME Server	If possible, the local Administrator account should be used.
Login used to access PME applications	Needs to be a member of Users group	Engineering Client	Used to access the PME client applications.
Login to run application engineering tools	Needs to be a member of local Administrators group	PME Server	An example is the Configuration Manager Tool, which may be used for system upgrades.

Service Accounts (Non-interactive)

Account	Permissions	Machine	Notes
IONUser	No group membership. Has List/Read/Write/Execute permissions on the PME share folder. Needs access to the folder where subscriptions are saved.	PME Server	Created during the installation of PME. Used to run report subscriptions.
IONMaintenance	Member of local Users group (user login is blocked)	PME Server	Created during the installation of PME. Used to run database maintenance jobs in Windows Task Scheduler.

Account	Permissions	Machine	Notes
SQL Server Agent service	NT AUTHORITY\SYSTEM	Database Server	Permissions are required during PME installation to allow access to the database folder(s) and the installer user's Temp folder. Permissions can be lowered after PME is installed.
SQL Server Database Engine service	NT AUTHORITY\SYSTEM	Database Server	Permissions are required during PME installation to allow access to the database folder(s) and the installer user's Temp folder. Permissions can be lowered after PME is installed.

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
ApplicationModules AlarmServiceHost	Manual	Local System
ApplicationModules CoreServicesHost	Automatic	Local System
ApplicationModules DataServicesHost	Automatic	Local System
ApplicationModules ProviderEngineHost	Automatic	Local System
ION Alert Monitor	Manual	Local System
ION Component Identifier Service	Manual	Local System
ION Connection Management Service	Manual	Local System
ION Diagnostics and Usage Service	Automatic	Local System
ION Event Watcher Service	Automatic	Local System
ION Log Inserter Service	Automatic	Local System
ION Managed Circuit Service	Automatic	Local System
ION Network Router Service	Automatic	Local System
ION OPC Data Access Server	Manual	Local System
ION PQDIF Exporter Service	Manual	Local System
ION Query Service	Automatic	Local System
ION Real Time Data Service	Automatic	Local System
ION Report Subscription Service	Automatic (Delayed Start)	Local System
ION Site Service	Automatic	Local System
ION Software Alarm Service	Automatic	Local System
ION Software Modbus Gateway Service	Manual	Local System

Service Name	Startup type	Log on Account
ION Virtual Processor Service	Automatic	Local System
ION Virtual Processor Service – NVIP.PQADVISOR	Automatic	Local System
ION Virtual Processor Service –NVIP.Data_Center*	Automatic	Local System
ION Virtual Processor Service –NVIP.Data_Center_Alarming*	Automatic	Local System
ION XML Subscription Service	Automatic	Local System
ION XML Subscription Store Service	Automatic	Local System
ImadminSchneider	Automatic	Local System
SQL Server (ION)	Automatic	Local System

* These services are only present in the Data Center edition of PME.

For a detailed description of these services, see the *Power Monitoring Expert Design Guide*.

IIS

The PME 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	Local System	Dashboards EWS (Ecostruxure Web Services) Hierarchy Manager Slideshow System Data Service Trends Web
ION App Pool	Local System	Alarm Configuration ION ION/diagrams ION Report Data Service Web Services
Web Reporter App Pool	Local System	Rate Editor Reporter

SQL Server

The database server hosts several databases for PME. The following table lists the SQL Server logins and permissions created for PME:

Login	Authentication	Server Role	Database	Membership
AMUser	SQL	Public	ApplicationModules	AMApplicationRole, public

Login	Authentication	Server Role	Database	Membership
ION	SQL	Public	ApplicationModules	db_owner, public
			ION_Data	db_owner, public
			ION_Network	db_owner, public
			ION_SystemLog	db_owner, public
			msdb *	SQLAgentOperatorRole, SQLAgentReader Role, SQL AgentUserRole, public
ionedsd	SQL	Public	ION_Data	ION_DSD_Reader, public
			ION_Network	NOM_DSD_Reader, public
Report	SQL	Public	ION_Data	db_datareader, ION_ Reader, public
			ION_Network	db_datareader, public
IONMaintenance**	Windows	Public	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

* In SQL Standard version only.

** This Login only exists on standalone systems where the PME server resides on the same computer as the database server.

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.

Domain

A domain account is required for an upgrade from an ION E 6.0.1 to a PME 8.2 distributed system using the Configuration Manager tool.

The 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 PME database instance.

Cybersecurity

Network security

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

Data encryption

At Rest

PME protects the passwords of its user accounts, as well as the Windows and SQL Server accounts using SHA-256 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

By default, PME uses a regular HTTP connection for server/Web client communication.

PME can be configured to work with TLS 1.2, using secure HTTPS connections between the PME server and its Web clients. Both self-signed and authority issued certificates are supported.

NOTE: TLS 1.0 is required for PME to function correctly and cannot be disabled.

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

Malware detection

PME can be used with antivirus (AV) software.

NOTE: Special configuration of the AV software may be required.

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. Issues during the installation of PME have been observed, where the AV scan delays caused timeouts and failures in the PME installation process.

PME has not been tested with whitelisting software products.

Password management

During the installation of PME, a single **supervisor** account is created. The password for this account is user defined. Any other user accounts must be created after the installation, using the **supervisor** login and the User Manager application in PME. The supervisor account password can be reset through the User Manager, or through the PME installer at any time.

The Windows and SQL Server accounts used by PME have unique, default passwords, that are generated during the installation of PME. These passwords can be changed at any time through the PME installer.

If SQL Server Express is installed through the PME installer, a sa account with a unique, default password is created. It is a good practice to change this default password for the sa account immediately after the installation of PME is complete.

Other considerations

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 PME.

Diagnostics and Usage feature

PME includes a feature for the PME R&D team to collect basic usage statistics on PME. The collected information does not include any customer or user identification. Users can decide to disable this feature during the installation of PME or any time after, through the PME Web application settings.

The information collected by this feature is sent to a secure cloud database once a week (default is Monday, 2AM), over HTTPS at port 443. The following information is collected:

Country, .NET Framework version, number of CPU cores, number of device types, number of PME users, number of monitors in use, number of devices, OS version, PC memory, PME architecture (standalone vs. distributed database), PME version, screen resolution, SQL Server version

Network Shares

PME Engineering and Reporting 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 as well.

PME installer

PME uses an automated installer which:

- Runs pre-installation checks
- Installs the required .NET Framework (if needed)
- Provides the option to install SQL Server Express
- Allows users to set the PME, Windows, and SQL Server account passwords
- Installs and configures all PME application files and services.

The installer produces a detailed installation log file which is saved inside the PME folder structure on the PME server.

The installer can also be run at any time after the installation of PME to change the account passwords or export a copy of the system key.

Device networks

PME must be connected to a network of power monitoring devices to collect the data to fulfill its intended purpose of providing power system information to users.

PME supports a large number of different device types. Devices can be connected through serial or Ethernet communication.

Ethernet device networks

Ethernet 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 IP addresses (IPv4 or IPv6) and ports, or device names, requiring some form of name resolution mechanism. Bandwidth requirements per device are typically low, but depend heavily on the amount and type of data requested from the device by PME.

Device communications are based on encapsulated Modbus or ION protocol and are not encrypted. TLS connections to devices are not supported.

Devices require fixed IP addresses. Dynamic address assignment is typically not supported by the device.

Serial device networks

Serial communication is the traditional way of connecting devices to PME. Often a hybrid approach is used with Ethernet-to-Serial gateway devices.

Serial device communications are based on Modbus RTU or ION protocol and are not encrypted.

PME also supports communication through telephone modems.

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison – France
www.schneider-electric.com

7EN42-0155-00 03/2017