



PowerMAN Enterprise Server 5.5

Installation and Administration Guide

Release 5.5.4 November 2022. Revised March 2023

About Data Synergy



Data Synergy is a British company based in Sheffield. We have over fifteen years' experience developing and supporting software solutions for enterprise PC deployment and management. We do not resell other vendors' products and do all of our development, sales and support from our UK base.

Our products have evolved through listening to customer ideas and applying our unrivalled knowledge of PC internals. If you have a suggestion for a new product or feature we would love to talk to you.

Data Synergy UK Ltd
Cooper Buildings
Sheffield Technology Parks
Arundel Street
Sheffield
S1 2NS
United Kingdom

Website: www.datasynergy.co.uk
Email: sales@datasynergy.co.uk
Telephone: +44 (0)8456 435 035

Registered in England and Wales
Company Number 06682095
VAT Registration GB 939 7559 56

Contents

PowerMAN Enterprise Server Installation and Administration.....	6
Overview.....	6
New in PowerMAN Enterprise Server v5.5.....	7
Prerequisites	12
Deployment Components.....	12
Deployment Assumptions.....	13
Getting Started	14
SQL Database Configuration Walkthrough	14
SQL Server 2008/2012 Database Procedure	15
SQL Server 2014 and later Database Procedure	17
Internet Information Services (IIS) Configuration Walkthrough	19
Windows Server 2008 IIS Setup Procedure.....	19
Windows Server 2012 and later IIS Setup Procedure	21
Installing PowerMAN Enterprise Server Website.....	23
External hosting – Using SSL/TLS security (https)	28
Firewall Configuration for IIS	30
Advanced SQL Configuration	31
Using a remote SQL server.....	31
Using a named instance SQL Server.....	33
Configuring PowerMAN Enterprise Website	34
Common “web.config” settings.....	34
Email configuration “web.config” settings.....	35
Advanced “web.config” settings	36
Minimal “web.config” settings.....	37
Securing PowerMAN Website	38
Configuring User Authentication (Integrated Windows Authentication)	42
Testing Integrated Windows Authentication Mode.....	43

PowerMAN Website Testing	44
Checking Website Security	44
SMTP Configuration (Email and error reporting)	45
Configure PowerMAN Enterprise Server for your organisation	46
Configuring User Logins.....	47
Configuring Anonymous Access	47
Configuring Automatic Site Creation (AD Integration)	48
Error Log.....	49
Temporary Website Maintenance (Server Offline).....	50
SQL Database Optimization and maintenance.....	51
Database Backups	51
Periodic SQL Database Optimisation.....	53
Database Server Configuration	54
Manual SQL Database Backup.....	55
Troubleshooting PowerMAN Enterprise Server	57
Problem: Static test page is not displayed	57
Problem: Website reports – The page cannot be found.....	57
Problem: Website reports – Server Application Unavailable	57
Problem: /Secure webpage appears blank (and no error is displayed)	57
Problem: .NET Framework v4.0.30319 is not available when creating App Pool	58
OR Website reports - The current identity does not have write access to ...Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files.....	58
OR "The page cannot be found" error message when you request an ASPX page.....	58
OR "HTTP Error 404 - File or Directory not found" error message when you request an ASPX page	58
Problem: Servercheck.aspx takes excessive time (>1 second) to display	58
OR Servercheck.aspx reports - An error has occurred while establishing a connection to the server (or similar)	58
OR Website reports Server Error in '/' Application. Runtime Error. Description: An exception occurred while processing your request.	58
Problem: Website reports - Sorry. A website error was detected. This cause of this error has been logged and will be investigated	59
Problem: Non-specific database connectivity problem.....	59
OR Website reports error 'A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: SQL Network Interfaces, error: 25 - Connection string is not valid)' or similar	59
Problem: Website displays - Service Unavailable	60

PowerMAN Enterprise Server v5.5

Problem: The website reports an exception obtaining permission of type 'System.Web.AspNetHostingPermission'	60
Problem: Unrecognized attribute "targetFramework" reported when you request an ASPX page.....	61
OR <compilation debug="false" targetFramework="4.0"></compilation>	61
Problem: Website generated URLs fail to work correctly.	61
OR Website URLs contain additional, unrecognised symbols, such as %20.....	61
Problem: Computers appear to be reporting correctly but are not showing on the reporting system	61
OR The SQL database contains data but this is not visible in the web-based reports	61
Problem: How do I migrate from the PowerMAN hosted reporting system to the (on-premise) PowerMAN Enterprise Server system?	61
Problem: How do I migrate from the (on-premise) PowerMAN Enterprise Server reporting system to the hosted PowerMAN reporting system?	62
Problem: How do I migrate a PowerMAN Enterprise Server (PMES) system from one server to another?	63
Problem: Windows Integrated Authentication Mode does not work as expect.....	63
OR PMES reports 'Unknown User' when Windows Integrated Authentication Mode is enabled.....	63
OR The/CurrentIdentity.aspx page displays no username when Windows Integrated Authentication Mode is enabled	63
Problem: The PMES website does not operate correctly with Internet Explorer 10	63
Appendix A: PowerMAN5 Database Creation Script (v5.5.x)	64
Appendix B: PowerMAN5 Upgrade Procedure (v5.4.x to v5.5.x)	65
Appendix C: Very large (>50k workstations) deployments	68
Appendix D: PowerMAN System Architecture	69
Appendix E: PowerMAN Authentication API	70
Authentication API Operation	70
Authentication API Output	70
Testing Authentication API	71
Demand Reporting API Authentication	71
Appendix F: SQL Server Default Installation Procedure	72
SQL Server Installation Walkthrough	72
SQL Server Remote Access / Remote PMES (IIS) website	75
Firewall Configuration for remote SQL Server	76
SQL Server Management Studio (SQL 2016 and later)	77

PowerMAN Enterprise Server Installation and Administration

Overview

PowerMAN Enterprise Server (PMES) complements the PowerMAN client software by giving you powerful, organisation-wide, reporting of PC energy usage, costs and waste. The software, which is identical to that used for Data Synergy's hosted cloud reporting service, provides your organisation with its own **private** reporting platform.

The reporting system is optional – the PowerMAN client software will function fully without it. However, the reports can be extremely useful to monitor the on-going effectiveness of your PowerMAN installation and determine where further improvements can be made.

There are several reasons you may want to run your own reporting platform:

- **More cost effective** - PMES can be more cost effective for larger organisations
- **Internal security requirements** – It is normally impractical for police forces, central government or the military to use the hosted service
- **Integration** – Running your own reporting platform allows your organisation to integrate your own MIS systems with the raw data for added business benefit

This document explains how PMES operates and provides a full walkthrough installation. The instructions below are intended for an experienced system / network administrator with knowledge of Microsoft Windows Server configuration and security, Internet Information Services (IIS) and Microsoft SQL Server (MSSQL). This document is not a training course on these technologies – it is assumed that the reader is already familiar with these products. Data Synergy can support any organisation with the appropriate skills but cannot, unfortunately, provide formal training in these technologies.

The walkthrough describes an installation on a typical Microsoft Windows Server 2008 (or later) system running IIS and Microsoft SQL 2008 (or later) Standard Edition. It assumes that each of these products has been installed using following the default settings. It also assumes that the server is only used for the PowerMAN reporting platform. PMES has relatively low resource requirements and can co-exist on a server hosting other services or be deployed in a virtualised environment. Whilst this scenario is not described in this document the basic approach discussed can be adapted to install the software on any of the supported environments with appropriate minor changes.

A separate document, called **PowerMAN Server Management Reporting Platform Guide**, explains how to manage everyday use of the reporting system.

Please remember that the PMES server is only used for reporting. It is not used to deploy PowerMAN and has no role in the active management of the client software. This must be done using the appropriate deployment and management software as described in the **PowerMAN Installation and Administration Guide**.

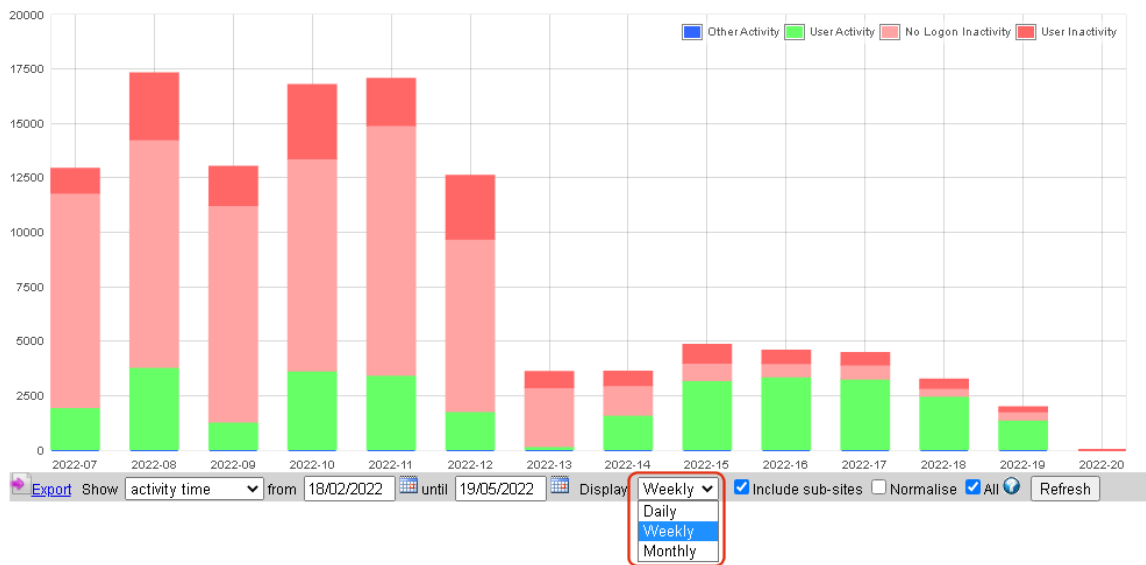
We recommend that you read this entire guide before commencing a PowerMAN Enterprise Server deployment.

New in PowerMAN Enterprise Server v5.5

PowerMAN Enterprise Server v5.5 (PMES) includes several new features. These include:

1. A new **monthly summary report**. This complements the existing daily and weekly reports. Some of the charts have been redesigned to improve readability and are now displayed in a stacked bar chart format and the reporting API has also been extended to support the new chart types:

Weekly Activity / Hours



2. PMES now provides a **Notifications** tab:



The notifications tab can be used to configure optional **email summary notification reports**. These can be sent daily, weekly, monthly or annually to notify stakeholders of recent energy saving performance:

:

	Week commencing 23/10
Unique computers	2163
User active hours	19641 (27 %)
Other active hours (Defined by system administrator)	0 (0 %)
User inactive hours	52597 (73 %) 18536 due no user logon (26 %) 34060 due to inactivity whilst user logged on (47 %)
Total hours	72237 (100 %)
Inactive cost (estimated)	£ 573.02
Suggestion	PowerMAN "Default Power Policy" may reduce inactivity when user is logged on. For example: This could logout an inactive user after a period of time or place the computer in a power saving mode.

PowerMAN Enterprise Server v5.5

- PMES now provides a **Logins** tab. It can be used create, delete and reset other user accounts:



Login Administration

Email Address	Home Site	Parent Access	Access Level
admin@example.com	None	Enabled	Site Administrator Password Impersonate Delete
fred@example.com	None	Enabled	Viewing Only Password Impersonate Delete
bob@example.com	Customer Service	Disabled	Viewing Only Password Impersonate Delete

- The **Devices** tab now provides a convenient search feature to locate workstations by name. This supports * and ? wildcard characters and includes a date filter to limit results to only certain assets:

Demonstration Devices

Client Version: Computer Name: (Use * and ? for wildcards)

OS Version: CPU:

Battery: Logical Cores:

Vendor: RAM: to GB

Product/Code: Hard Disks:

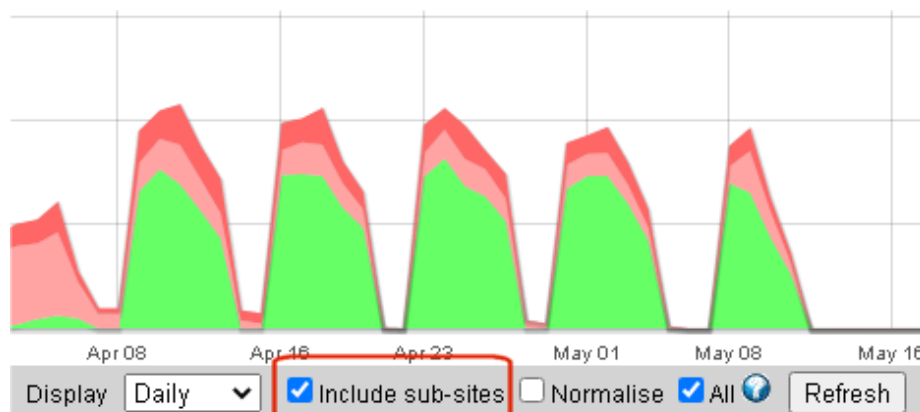
BIOS: Optical Drives:

BIOS Version: Free System Drive: GB

Show Computers last status from until Include sub-sites Showing 60 of 329 available records

Computer	Version	OS	Battery	Vendor	Product/Code	BIOS	Version	CPU	Logical Cores	RAM MB	Hard Disks	Optical Drives	Free System Drive MB	Last Status
Workstation021	5.4.0.5932	10.0.9200	False	HP	8299	HP	P01 Ver. 02.04	Intel(R) Core(TM) i5-7500 CPU @ 3.40GHz	4	3975	1	1	434540	19/03/2020
Workstation042	5.4.0.5932	10.0.9200	False	HP	8299	HP	P01 Ver. 02.04	Intel(R) Core(TM) i5-7500 CPU @ 3.40GHz	4	3975	1	1	428626	10/05/2020
Workstation044	5.4.0.5932	10.0.9200	False	HP	8299	HP	P01 Ver. 02.04	Intel(R) Core(TM) i5-7500 CPU @ 3.40GHz	4	3975	1	1	435733	09/05/2020
Workstation045	5.4.0.5932	10.0.9200	False	HP	8299	HP	P01 Ver. 02.04	Intel(R) Core(TM) i5-7500 CPU @ 3.40GHz	4	3975	1	1	428607	11/05/2020

- The main activity chart now includes the option to exclude data from child sub-sites:



- Similarly, the computers report now includes the option to directly include computers from child sub-sites. On supported browsers, clicking a specific computer will open the detailed computer report in a new browser tab:

PowerMAN Enterprise Server v5.5



Computers

Computer	Client Version	Last Status	Inactive %	Inactive Hours	Active Hours	<input type="checkbox"/> No Logon	<input type="checkbox"/> Inactive User	<input type="checkbox"/> User	<input type="checkbox"/> Other	WakeAll
Workstation274	5.4.0.5932	10/05/2022	40.00	4.50	6.75	<div style="width: 100%; height: 10px; background-color: #f00;"></div>	<div style="width: 100%; height: 10px; background-color: #0f0;"></div>			Wake
Workstation138	5.4.0.5932	11/05/2022	47.37	4.50	5.00	<div style="width: 100%; height: 10px; background-color: #f00;"></div>	<div style="width: 100%; height: 10px; background-color: #0f0;"></div>			Wake
Workstation117	5.4.0.5932	10/05/2022	51.52	4.25	4.00	<div style="width: 100%; height: 10px; background-color: #f00;"></div>	<div style="width: 100%; height: 10px; background-color: #0f0;"></div>			Wake
Workstation012	5.4.0.5932	10/05/2022	18.89	4.25	18.25	<div style="width: 100%; height: 10px; background-color: #f00;"></div>	<div style="width: 100%; height: 10px; background-color: #0f0;"></div>			Wake
Workstation006	5.4.0.5932	11/05/2022	13.18	4.25	28.00	<div style="width: 100%; height: 10px; background-color: #f00;"></div>	<div style="width: 100%; height: 10px; background-color: #0f0;"></div>			Wake

Show computers from until Include computers in sub-sites

- PMES now optionally reports computer network information. The report includes the most recent network interface adapter name(s) together with associated MAC (hardware) address, IP address(s) and, if appropriate, subnet mask(s). The feature supports both IP v4 and IP v6:

Network Information

Description	Physical/MAC	Active	Hardware	Addresses
 Realtek PCIe GBE Family Controller	5CE0C52AB190	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.200.190/24, FE80:0000:0000:0000:ABCD:1234:0190:64
 Intel(R) Dual Band Wireless-AC 7265 WIFI	C860008C1190	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	192.168.202.190/24

- The computer summary report has been redesigned to be easier to understand. The page has been split into sub-categories for basic information, general hardware information and power management specific information. Each sub-category now includes the date and time it was last updated.

Operations / Workstation072

Site	Operations	OU=Operations,OU=Desktop,DC=corp,DC=local
Name	Workstation072 Wake	CN=Workstation072,OU=Operations,OU=Desktop,DC=corp,DC=local
Registered	06/02/2022	Windows® Version 6.1.7601 Service Pack 1
Last Live Status (Local)	14/05/2022 09:44:45	Live Status User Activity
Last Status	11/05/2022	Last Startup 11/05/2022 10:05:42
Client Version	5.4.0.5932	Battery No Battery (Desktop)
Platform	x86 (32-bit)	Timezone 0.0 hour(s) UTC

Hardware

CPU Sockets/Cores/Logical	1 / 4 / 4 2893 MHz	CPU Model	Intel(R) Core(TM) i5-3470S CPU @ 2.90GHz
System RAM	3476 MB	System Model / Vendor	3398 / Hewlett-Packard
Fixed / Optical Drives	1 / 1	BIOS Vendor	Hewlett-Packard

Last Updated: 11/05/2022 10:05:42

Power Management Capabilities

Supports States	S345	Supports Wake from	S1234
Supports "Modern/Connected" Standby	Not supported	Supports always connected PC	Not supported
Hardware Buttons	Power	Disk Standby	Supported
Hibernation File (S4)	Present	System HDD Free	261,601 MB
Hybrid Sleep (Fast S4)	Not supported	Fast Startup (Hiberboot)	Not supported

Last Updated: 11/05/2022 10:05:42

- The PMES **demand or "pull" reporting API** has been extended to support optional sub-sites, a new monthly summary report and a new detailed (per 15-minute report). The revised API syntax is documented in the PowerMAN Platform Reporting Guide.
- The sub-sites report now shows the number of computers reporting data in the last 90-days (or most recently available 90-days if applicable):

PowerMAN Enterprise Server v5.5

Sub-Sites

Site	Computers (90-days)	Last Status	Inactive Hours	Active Hours	<input type="checkbox"/> No Logon <input type="checkbox"/> Inactive User <input type="checkbox"/> User <input type="checkbox"/> Other
Operations	76	11/05/2022	315.25	635.75	
Sales	72	11/05/2022	68.00	322.50	
Marketing	13	12/05/2022	64.00	111.25	
Administration	15	11/05/2022	62.50	150.00	

Similarly, the site information panel now breaks down the number of computers present and reporting data into separate 30/90 day categories. These may be exported or used to investigate scenarios where the number of computers reporting has changed significantly:

Organisation	Demonstration 2022	OU=Desktop,DC=corp,DC=local
Created	01/01/2021	First Data 14/08/2021
Expires	Never	Last Data 12/05/2022
Data Retention	1835 days (Summary)	Total Computers 317 Export / Recent (30-days) 322 Export / Recent (90-days) Export All
	1835 days (Detail)	
	Total Sub-Sites	11 Export

- The live reporting feature has been extended to provide an alternative public PC availability report (SiteLiveAvailable.aspx). This is intended for use in public access dashboards and similar. The report is designed for unrestricted use and does not require a login. For added security, it does not include links to other PMES reports:

Live Computer Status

Computer Name	<input type="checkbox"/> Unknown	<input checked="" type="checkbox"/> Available	<input type="checkbox"/> Not Available
Workstation001	<input checked="" type="checkbox"/>	Workstation021	<input checked="" type="checkbox"/> Workstation058
Workstation002	<input checked="" type="checkbox"/>	Workstation038	<input checked="" type="checkbox"/> Workstation070
Workstation003	<input checked="" type="checkbox"/>	Workstation041	<input checked="" type="checkbox"/> Workstation080
Workstation004	<input checked="" type="checkbox"/>	Workstation044	<input checked="" type="checkbox"/> Workstation088
Workstation005	<input checked="" type="checkbox"/>	Workstation046	<input checked="" type="checkbox"/> Workstation112
Workstation010	<input checked="" type="checkbox"/>	Workstation048	<input checked="" type="checkbox"/> Workstation114
Workstation013	<input checked="" type="checkbox"/>	Workstation056	<input checked="" type="checkbox"/> Workstation115
Workstation016	<input checked="" type="checkbox"/>	Workstation057	<input checked="" type="checkbox"/> Workstation124
Workstation017	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/> Workstation137
			<input checked="" type="checkbox"/> Workstation160
			<input checked="" type="checkbox"/> Workstation163
			<input checked="" type="checkbox"/> Workstation167
			<input checked="" type="checkbox"/> Workstation207
			<input checked="" type="checkbox"/> Workstation213
			<input checked="" type="checkbox"/> Workstation223
			<input checked="" type="checkbox"/> Workstation225

Show detailed activity status

- PMES now reports the last computer start-up (boot) time. This may be useful to identify workstations that have not rebooted for some time. This feature requires client v5.5.3.0 or later.
- PMES now allows individual computer names to be hidden for either individual sub-sites or all sites. This is intended to enhance user privacy where this is a concern and a user could be identified from the computer name. When this feature is enabled, it is no longer possible to view individual computer names, export lists of computers, view computers on the "Live" tab or view the "Device" tab. This feature may be enabled via the **Show Computers** setting on the **Configuration** tab:

PowerMAN Enterprise Server v5.5

Configuration

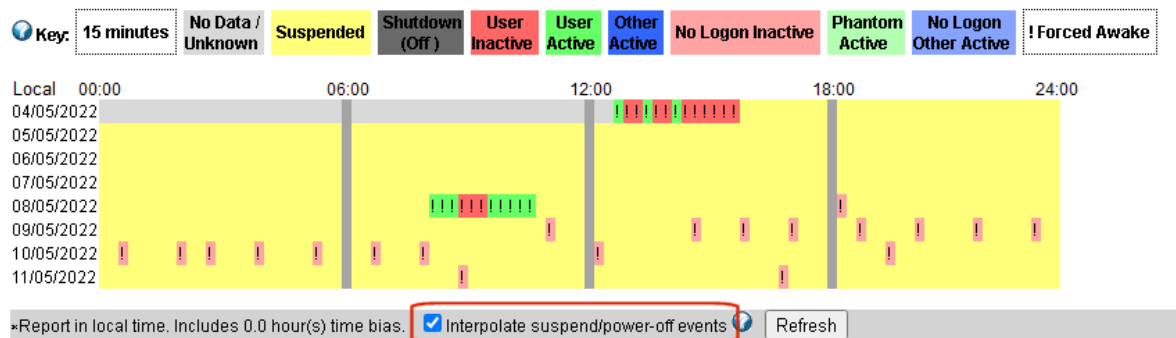
Auto Computer Move	<input checked="" type="checkbox"/> Enable computer auto-move	<input checked="" type="checkbox"/> Update sub-sites	Save
Show Computers	<input checked="" type="checkbox"/> Show computers	<input checked="" type="checkbox"/> Update sub-sites	Save
Auto Site Creation	<input type="checkbox"/> Enable auto site creation (OU Based)		Save
Anonymous Viewing	<input checked="" type="checkbox"/> Permitted		Save

14. PMES now reports the availability of the following additional power management capabilities. This feature requires client v5.5.3 or later:

- Hybrid sleep support (Fast S4)
- Fast start-up (Hiberboot)
- Support for “modern” standby (AoAC)
- Support for Windows “always-on connected” feature-set (e.g. AoAC connected)

15. The detailed computer activity report now provides an **Interpolate** option to show the assumed state of a computer when it was turned off/asleep (previously this was implicit):

Detailed Activity Report



16. The latest PMES also includes several bug fixes. Please see Release Notes for a detailed list.

PowerMAN Enterprise Server v5.5

Prerequisites

PowerMAN Enterprise Server has the following requirements:

- A server with at least 4GB of RAM running Windows Server 2008 or later. Larger installations may require more RAM. The server may be either 32-bit (if available) or 64-bit. Please note that SQL Server 2019 and later require Windows 10 / Server 2016 or later.
- Internet Information Services with ASP.NET support and the Microsoft .NET 4.x Framework.
- Approximately 1MB of data storage per client computer per year. e.g. 20,000 PCs will require approximately 20GB of storage per annum.
- Microsoft® SQL Server Standard Edition 2008 or later with the most recent service pack installed. Smaller deployments (<10,000 workstations) may also use the free SQL Express Edition. In the situation, we suggest using the “SQL Express with Tools” variant. Please remember that SQL Express has a 10 GB maximum database size.
- Skills to configure Windows Server, IIS and MS SQL Server

It is your responsibility to obtain the necessary Windows Server and Microsoft SQL Server product licenses. In an enterprise environment, the costs associated with this should be small compared to the potential savings from using PowerMAN. However, if the costs of these components are prohibitive, it may be more appropriate to use the PowerMAN cloud (hosted) reporting platform.

For older Windows Server 2008 systems, the Microsoft .NET 4.5.2 Framework can be obtained from the following location. It is built-in to later Windows Server releases.

<https://www.microsoft.com/en-gb/download/details.aspx?id=42642>

Deployment Components

PowerMAN Enterprise Server is supplied as three components:

- PowerMAN Enterprise Server Database hosted by MS SQL Server. This is supplied as an SQL Server backup file called **PowerMAN5x Database.bak**. This must be restored on to your server.

NB: An alternative SQL Script based deployment mechanism is described in Appendix A. This is intended for advanced SQL system administrators.

- PowerMAN Enterprise Website (hosted by IIS). This is supplied in a ZIP file called **PowerMAN5x Website.zip**. The same file may be used for both 32-bit and 64-bit operating system platforms
- The Installation Guide (this document) which describes the system and a walkthrough installation.

PowerMAN Enterprise Server v5.5

Deployment Assumptions

The walkthrough below makes certain assumptions about the server configuration. These are as follows:

- The server prerequisite components are installed using their default settings
- The same physical/virtual server is used for the SQL database and the IIS website
- The SQL Server is installed with default settings. Please see the Appendix at the end of this guide for an example SQL Server installation procedure.
- The SQL Server is configured as the default instance and uses Windows Integrated Authentication (or mixed authentication). The use of default and named instances is described in the following document:

<https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/database-engine-instances-sql-server>

- The SQL database is configured to use the Simple recovery model and use compatibility level 100 or greater
- The website is configured to serve content on port 8080, to allow anonymous access (except to the Secure folder) and to use an application pool running in the security context of the Network Services account
- The Network Services account is a member of the SQL database role called 'Website' – This provides the website with the limited database access necessary to function correctly. This configuration is described below.

PMES is flexible software and, within reason, can function in a variety of environments and configurations. You may choose to re-configure your server to use Windows Integrated Authentication for all website access (except the essential PostStatus.aspx file) or otherwise change the assumptions used in this document. Whilst there may be many organisation specific reasons for doing this we would recommend that you initially deploy the software using the method presented and consider the impact of re-integrating future PowerMAN Enterprise Server releases.

PMES can be used in a virtualised environment. This has the advantage that a standalone server can be quickly configured, using the methods described in this document, without impacting on any pre-existing systems. This technique also has the advantage that the PMES system can be easily backed-up as a single entity and quickly transferred to another hardware platform.

Getting Started

Before starting to deploy PMES please check that you have the following:

- A hardware/software platform meeting the requirements described
- An understanding of the installation process (read this document)
- The PMES distribution files (supplied as a ZIP file)
- A PMES product key. For the purposes of this document the following fictitious information is used:

Organisation: Example Corporation Limited
Product Key: XGHK-GABQ-GDTH-UJKQ-HYJK-DBKY

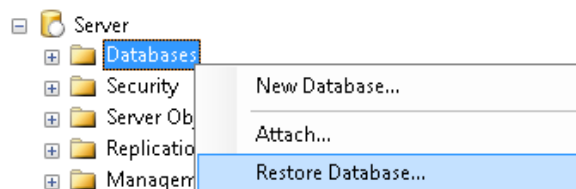
SQL Database Configuration Walkthrough

The following steps walk through a typical deployment using Microsoft SQL Server 2008 or later. It assumes that SQL Server has been installed with default settings and the database files are to be located in C:\Database\PowerMAN5. If you are unfamiliar with SQL Server installation, please see the Appendix at the end of this guide for an example installation procedure.

Tip: An alternative, script based, SQL deployment mechanism is described in Appendix A. This is intended for advanced SQL administrators.

The pre-configured SQL database can be installed using the following steps:

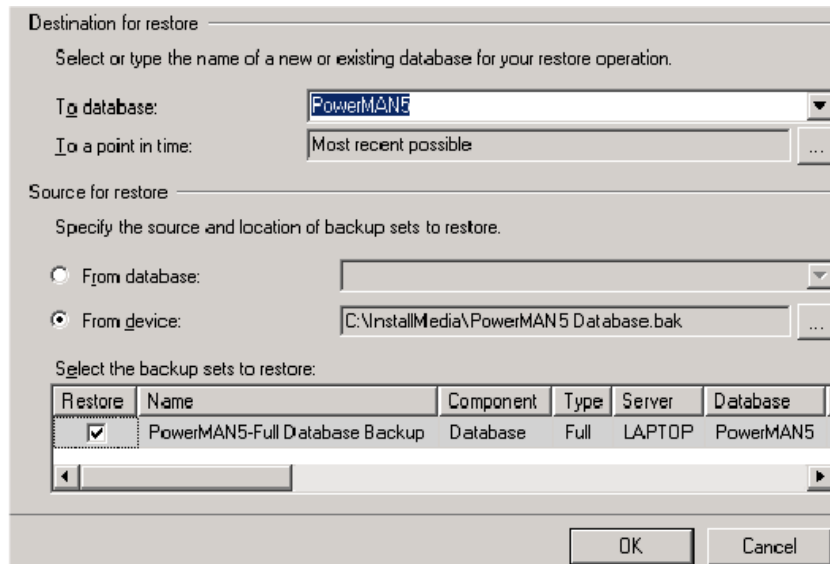
1. Create folder for database files. C:\Databases\PowerMAN5
2. Open **SQL Server Management Studio**
3. Right click on **Databases** and select **Restore Database:**



The Restore Database process is slightly different for later MS SQL Server releases. The following sections describe the key steps for MS SQL 2008/2012 and MS SQL 2014 and later releases. Regardless of version, the basic procedure is similar and can be easily adapted to other MS SQL Server releases.

SQL Server 2008/2012 Database Procedure

1. Configure the database name as: **PowerMAN5**
2. Select **From Device** and locate the **PowerMAN5 Database.bak** file
3. Select **Options** and modify the restore path to **C:\Databases\PowerMAN5**



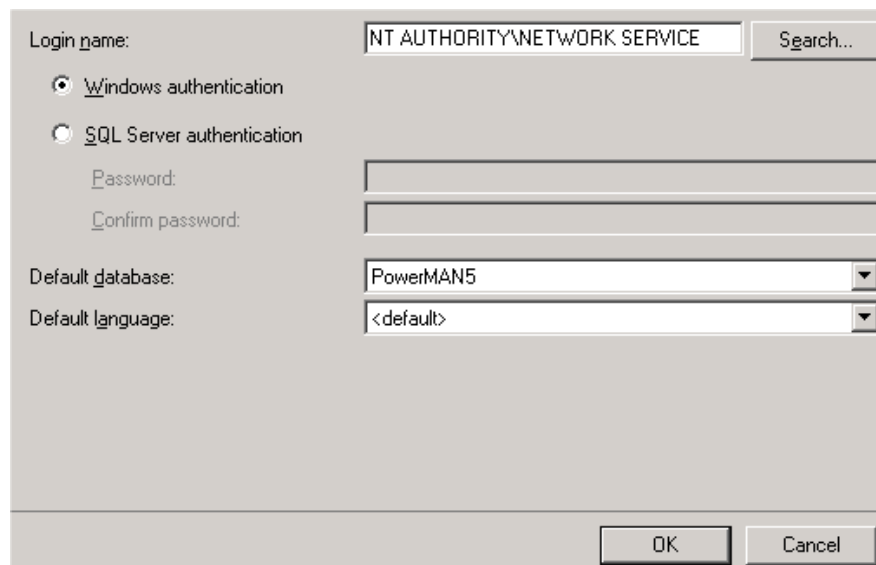
4. Click **OK** to restore the database. On a typical server this will take only a few seconds. Following database installation (including via the script method described in Appendix A) the website/database user login should be configured using the following procedure.

1. Open **SQL Server Management Studio**
2. Navigate to **Security\Logins**
3. Right click and select **New Login**



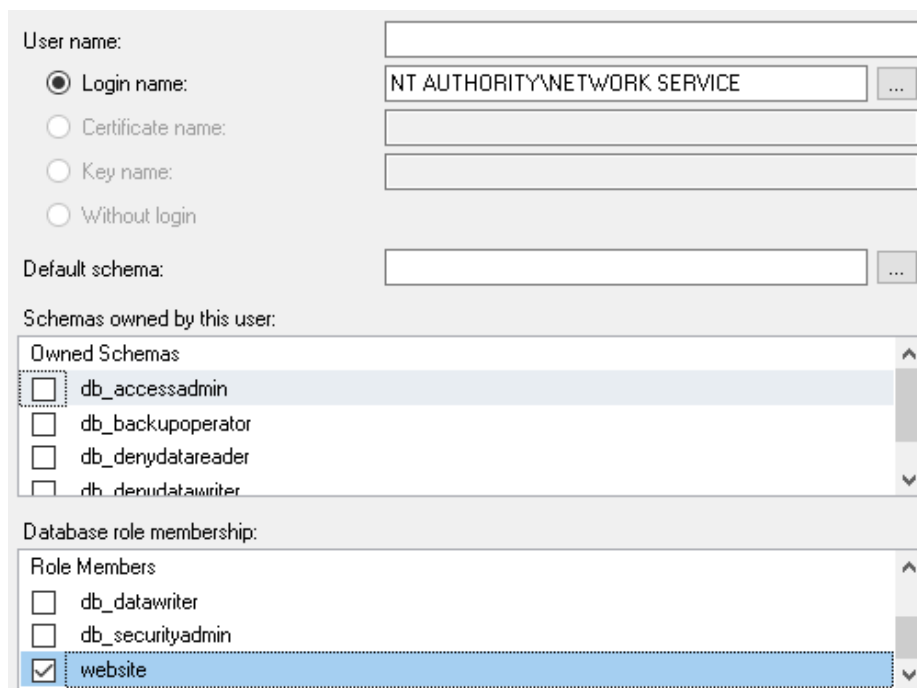
4. Click **Search**
5. Enter **Network Service** and click **OK**
6. Select **PowerMAN5** as the default database
7. Confirm the Network Service account is listed (as shown below) and click **OK** again

PowerMAN Enterprise Server v5.5



Login name: Search...
 Windows authentication
 SQL Server authentication
 Password:
 Confirm password:
 Default database:
 Default language:

8. Navigate to **Databases\PowerMAN5\Security\Users**
9. Right click and select **New User**
10. Click the top search ... button and locate the **Network Service** user



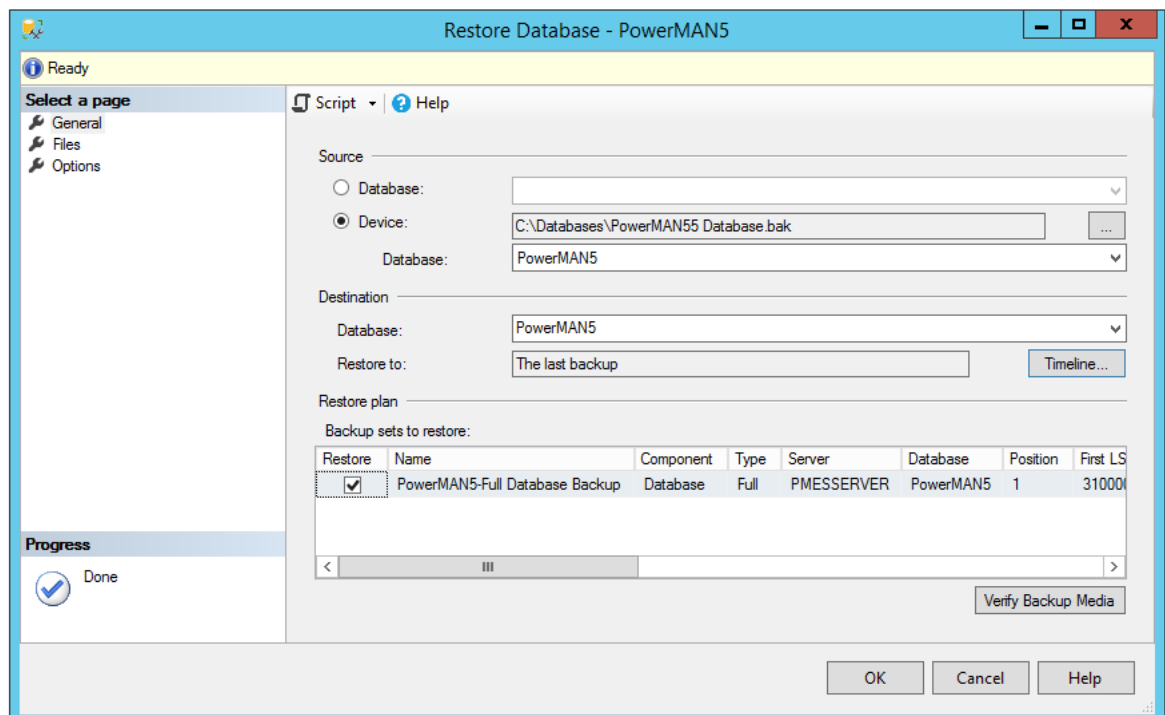
User name:
 Login name: ...
 Certificate name:
 Key name:
 Without login
 Default schema: ...
 Schemas owned by this user:
 Owned Schemas
 db_accessadmin
 db_backupoperator
 db_denydatareader
 db_denudatawriter
 Database role membership:
 Role Members
 db_datawriter
 db_securityadmin
 website

11. Select the **Website** database role
12. Click **OK**

SQL Server 2014 and later Database Procedure

Tip: SQL Server 2019 and later requires Windows 10 / Windows Server 2016 or later. Please see: <https://learn.microsoft.com/en-us/troubleshoot/sql/general/use-sql-server-in-windows>

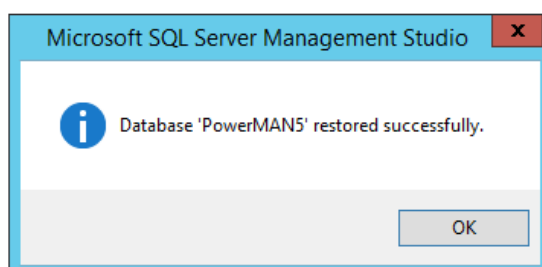
1. Select **Device**, click ..., click **Add**, locate the **PowerMAN5 Database.bak** file and click **OK**
2. Configure the destination database name as: **PowerMAN5**



3. Select **Files** and set **Restore As** to the target folder: **C:\Databases\PowerMAN5**

Logical File Name	File Type	Original File Na...	Restore As
PowerMAN5	Rows Data	c:\databases\...	c:\Databases\PowerMAN5\PowerMAN5.mdf
PowerMAN5_log	Log	c:\databases\...	c:\Databases\PowerMAN5\PowerMAN5_1.ldf

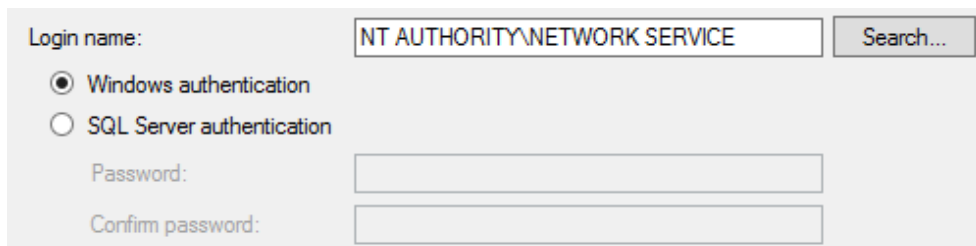
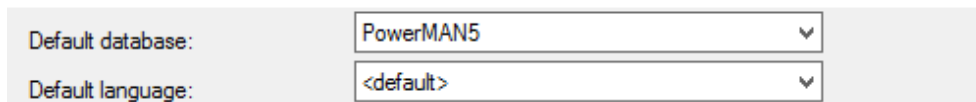
4. Click **OK** to restore the database. On a typical server this will take only a few seconds



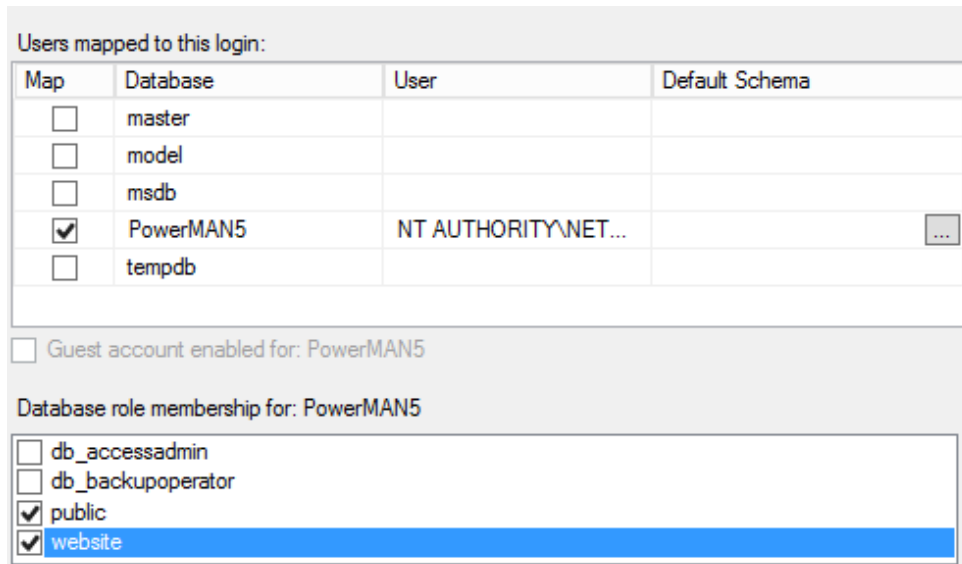
PowerMAN Enterprise Server v5.5

Following database installation (including via the script method described in Appendix A) the website/database user login should be configured using the following procedure.

1. Open **SQL Server Management Studio**
2. Navigate to **Security\Logins**
3. Right click and select **New Login**
4. Click **Search** and locate the **Network Service** user
5. Select **PowerMAN5** as the default database

6. From the left hand menu, select the **User Mapping** page
7. Highlight the **PowerMAN5** database and tick the **Map** checkbox
8. Tick the **Website** role



Map	Database	User	Default Schema
<input type="checkbox"/>	master		
<input type="checkbox"/>	model		
<input type="checkbox"/>	msdb		
<input checked="" type="checkbox"/>	PowerMAN5	NT AUTHORITY\NET...	
<input type="checkbox"/>	tempdb		

Guest account enabled for: PowerMAN5

Database role membership for: PowerMAN5

- db_accessadmin
- db_backupoperator
- public
- website

9. Click **OK**

PowerMAN Enterprise Server v5.5

The **'Website'** database role has the limited database access rights to operate the PowerMAN Enterprise Server system. For security reasons not all database objects are accessible to this database role. More advanced configuration and database maintenance must be manually performed using the SQL Server Management Studio.

You **MUST** also configure an appropriate database performance optimization and backup strategy. An example procedure is explained later in this document.

Internet Information Services (IIS) Configuration Walkthrough

The following sections walk through a typical website deployment on a system running Windows 2008 or later. It assumes that the website files are located in C:\Websites\PowerMAN5.

The procedure below assumes that the majority of the website is configured to allow anonymous access (the default). In IIS7 anonymous access is authenticated using the special **IUSR** user account. This account is a member of the Users group and the instructions below assume this is the case.

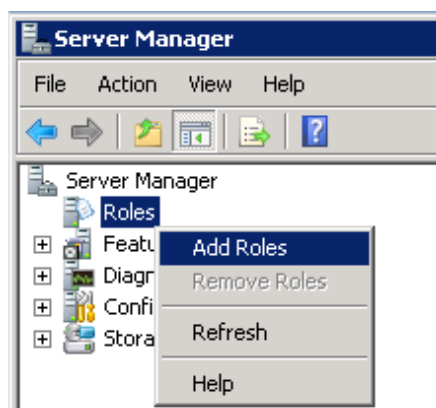
If you deviate from this assumption please remember that the **/PostStatus.aspx** file, as a minimum, must be accessible to the anonymous PowerMAN clients. One exception to this is that the **/Secure** folder must be restricted to provide access only to appropriate website Administrators. This is typically done using NTFS permissions. Please contact Technical Support if you require further advice on this issue.

Please follow the instructions below to configure IIS. If IIS is already installed please run through the instructions to confirm the required IIS components are installed and make any necessary component adjustments.

Windows Server 2008 IIS Setup Procedure

On Windows Server 2008, please proceed as follows:

1. Open **Server Manager** (ServerManager.exe) and locate **Roles**
2. Right click and select **Add Roles**



PowerMAN Enterprise Server v5.5

3. Click **Next**
4. Select **Web Server (IIS)** and click **Next**
5. If applicable, read the notes on IIS and click **Next** again
6. Select the following *minimum* IIS components below (it is ok to select additional components if that is appropriate):

<ul style="list-style-type: none"> <input type="checkbox"/> <input checked="" type="checkbox"/> Web Server <ul style="list-style-type: none"> <input type="checkbox"/> <input checked="" type="checkbox"/> Common HTTP Features <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Static Content <input checked="" type="checkbox"/> Default Document <input type="checkbox"/> Directory Browsing <input checked="" type="checkbox"/> HTTP Errors <input checked="" type="checkbox"/> HTTP Redirection <input type="checkbox"/> WebDAV Publishing <input type="checkbox"/> <input checked="" type="checkbox"/> Application Development <ul style="list-style-type: none"> <input checked="" type="checkbox"/> ASP.NET <input checked="" type="checkbox"/> .NET Extensibility <input type="checkbox"/> ASP <input type="checkbox"/> CGI <input checked="" type="checkbox"/> ISAPI Extensions <input checked="" type="checkbox"/> ISAPI Filters <input checked="" type="checkbox"/> Server Side Includes <input type="checkbox"/> <input checked="" type="checkbox"/> Health and Diagnostics <ul style="list-style-type: none"> <input checked="" type="checkbox"/> HTTP Logging <input type="checkbox"/> Logging Tools <input type="checkbox"/> Request Monitor <input type="checkbox"/> Tracing <input type="checkbox"/> Custom Logging <input type="checkbox"/> ODBC Logging 	<ul style="list-style-type: none"> <input type="checkbox"/> <input checked="" type="checkbox"/> Security <ul style="list-style-type: none"> <input type="checkbox"/> Basic Authentication <input checked="" type="checkbox"/> Windows Authentication <input type="checkbox"/> Digest Authentication <input type="checkbox"/> Client Certificate Mapping Authentication <input type="checkbox"/> IIS Client Certificate Mapping Authentication <input type="checkbox"/> URL Authorization <input checked="" type="checkbox"/> Request Filtering <input type="checkbox"/> IP and Domain Restrictions <input type="checkbox"/> <input checked="" type="checkbox"/> Performance <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Static Content Compression <input type="checkbox"/> Dynamic Content Compression <input type="checkbox"/> <input checked="" type="checkbox"/> Management Tools <ul style="list-style-type: none"> <input checked="" type="checkbox"/> IIS Management Console <input type="checkbox"/> IIS Management Scripts and Tools <input type="checkbox"/> Management Service <input type="checkbox"/> IIS 6 Management Compatibility <ul style="list-style-type: none"> <input type="checkbox"/> IIS 6 Metabase Compatibility <input type="checkbox"/> IIS 6 WMI Compatibility <input type="checkbox"/> IIS 6 Scripting Tools <input type="checkbox"/> IIS 6 Management Console <input type="checkbox"/> <input type="checkbox"/> FTP Server <ul style="list-style-type: none"> <input type="checkbox"/> FTP Service <input type="checkbox"/> FTP Extensibility <input type="checkbox"/> IIS Hostable Web Core
---	--

7. Click **Next** and then click **Install**

Following IIS configuration please install the .NET framework:

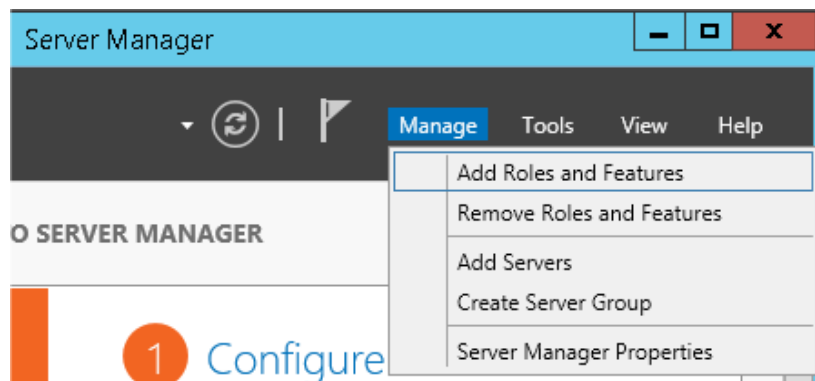
8. Download and install the .NET 4.5.2 Framework. This is available from the following Microsoft website:

<https://www.microsoft.com/en-gb/download/details.aspx?id=42642>

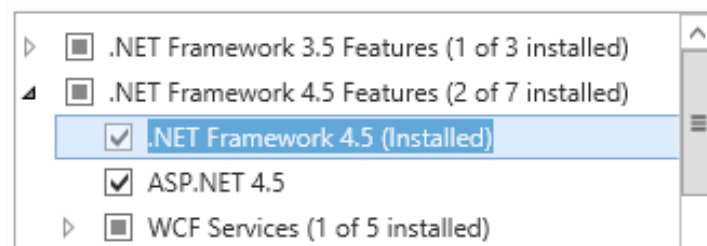
Windows Server 2012 and later IIS Setup Procedure

On Windows Server 2012 please proceed as follows:

1. Open **Server Manager** (ServerManager.exe)
2. Click **Manage** and select **Add Roles and Features**:



3. Click **Next**
4. Select **Role-based or feature-based installation**
5. Click **Next**
6. Select the local server and click **Next** again
7. Select **Web Server (IIS)** and when prompted **Add Features** and then **Next**
8. Confirm the **.NET Framework 4.x** and **ASP.NET 4.x** components are checked:



9. Click **Next** again
10. If applicable, read the notes on IIS and click **Next** again
11. Select the following *minimum* IIS components below (it is ok to select additional components if that is appropriate):

PowerMAN Enterprise Server v5.5

<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Web Server <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Common HTTP Features <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Default Document <input type="checkbox"/> Directory Browsing <input checked="" type="checkbox"/> HTTP Errors <input checked="" type="checkbox"/> Static Content <input checked="" type="checkbox"/> HTTP Redirection <input type="checkbox"/> WebDAV Publishing <input checked="" type="checkbox"/> Health and Diagnostics <ul style="list-style-type: none"> <input checked="" type="checkbox"/> HTTP Logging <input type="checkbox"/> Custom Logging <input type="checkbox"/> Logging Tools <input type="checkbox"/> ODBC Logging <input type="checkbox"/> Request Monitor <input type="checkbox"/> Tracing <input checked="" type="checkbox"/> Performance <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Static Content Compression <input type="checkbox"/> Dynamic Content Compression <input checked="" type="checkbox"/> Security <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Request Filtering <input type="checkbox"/> Basic Authentication <input type="checkbox"/> Centralized SSL Certificate Support <input type="checkbox"/> Client Certificate Mapping Authentication <input type="checkbox"/> Digest Authentication <input type="checkbox"/> IIS Client Certificate Mapping Authentication <input type="checkbox"/> IP and Domain Restrictions <input type="checkbox"/> URL Authorization <input checked="" type="checkbox"/> Windows Authentication 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Application Development <ul style="list-style-type: none"> <input type="checkbox"/> .NET Extensibility 3.5 <input checked="" type="checkbox"/> .NET Extensibility 4.5 <input type="checkbox"/> Application Initialization <input type="checkbox"/> ASP <input type="checkbox"/> ASP.NET 3.5 <input checked="" type="checkbox"/> ASP.NET 4.5 <input type="checkbox"/> CGI <input checked="" type="checkbox"/> ISAPI Extensions <input checked="" type="checkbox"/> ISAPI Filters <input checked="" type="checkbox"/> Server Side Includes <input type="checkbox"/> WebSocket Protocol <input type="checkbox"/> FTP Server <ul style="list-style-type: none"> <input type="checkbox"/> FTP Service <input type="checkbox"/> FTP Extensibility <input checked="" type="checkbox"/> Management Tools <ul style="list-style-type: none"> <input checked="" type="checkbox"/> IIS Management Console <input type="checkbox"/> IIS 6 Management Compatibility <input type="checkbox"/> IIS Management Scripts and Tools <input type="checkbox"/> Management Service
---	---

Note: ASP.NET 4.5 is default on Windows Server 2012. NET v4.6 is available on later operating systems and also available as an optional update for Windows Server 2012 R2. See: <https://support.microsoft.com/en-us/topic/the-net-framework-4-6-1-for-windows-server-2012-r2-on-windows-update-b1b1638f-47ba-e436-81f0-fe23de52d579>. Windows Server 2019 ships with ASP.NET v4.7 and Windows Server 2022 ships with ASP.NET v4.8. PMES supports v4.5 and later.

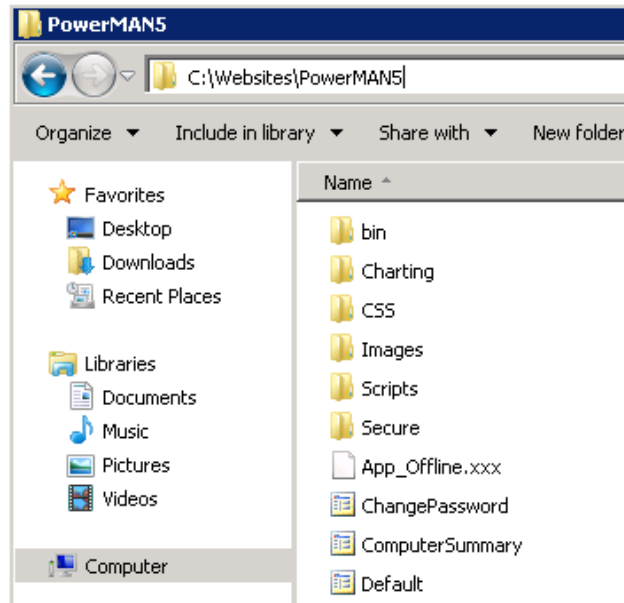
12. Click **Next**
13. Optionally, check **Restart the destination server automatically if required**
14. Click **Install**



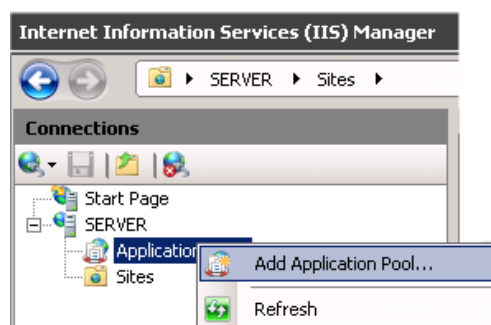
Installing PowerMAN Enterprise Server Website

Following successful IIS configuration and .NET Framework installation the PowerMAN reporting website may be configured. The procedure is the same for Windows Server 2008 and later. Please proceed as follows:

1. Create folder for website files: C:\Websites\PowerMAN5
2. Extract the contents of “PowerMAN5x Website.zip” file to this folder:

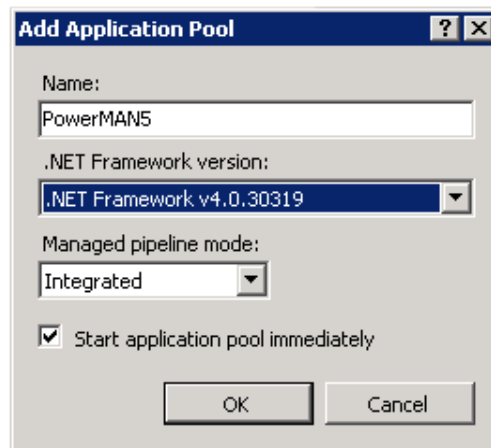


3. Open the **Internet Information Services (IIS) Management snap-in (INETMGR.EXE)**
4. Expand the left hand tree view
5. Navigate to **Application Pools**
6. Right click and select **Add Application Pool**



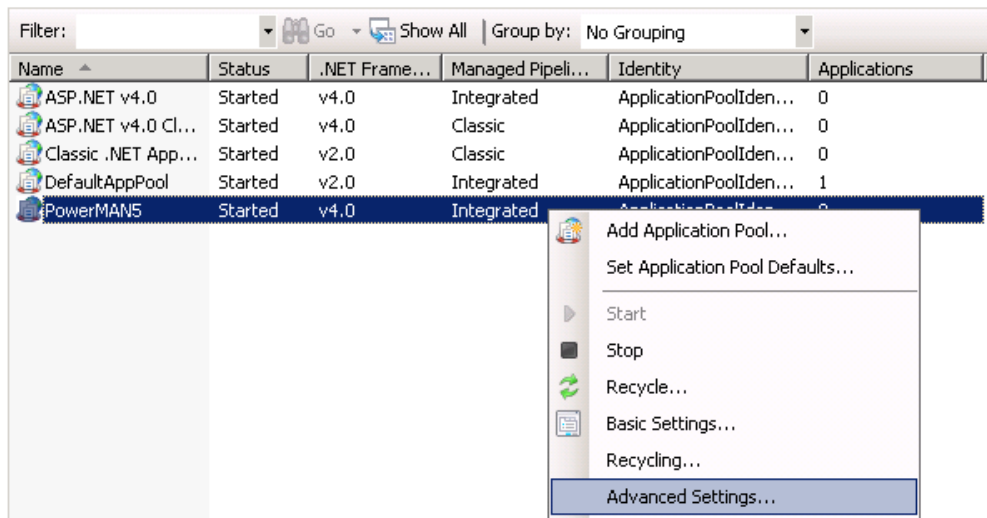
7. Enter the pool name: **PowerMAN5** and select **.NET Framework v4.0.x** and **Integrated** mode:


PowerMAN Enterprise Server v5.5



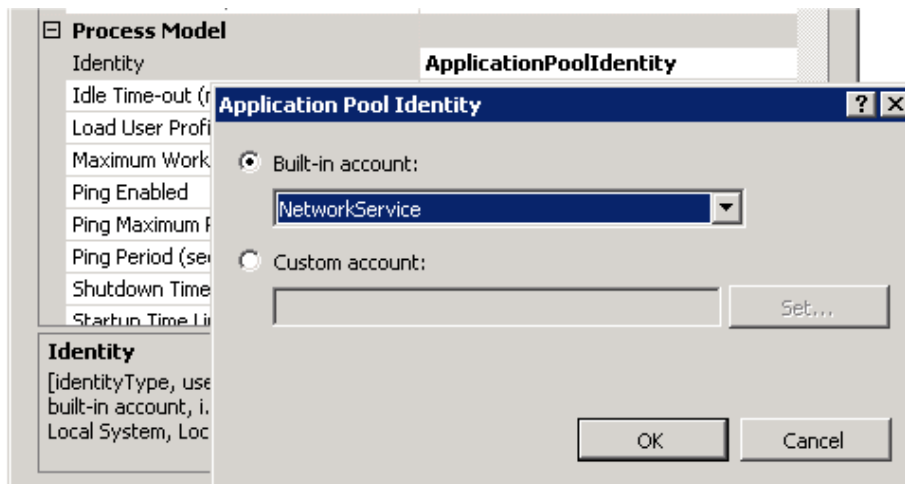
Tip: If .NET v4.0 is not listed this may be because .NET was installed before IIS. Please see the troubleshooting section to resolve this.

8. Click **OK** to close the dialog
9. Navigate to the newly created **PowerMAN5** application pool
10. Right click and select **Advanced Settings**



11. Navigate to the **Identity** setting and press 
12. Select **Built-in account: Network Service** and then click **OK**

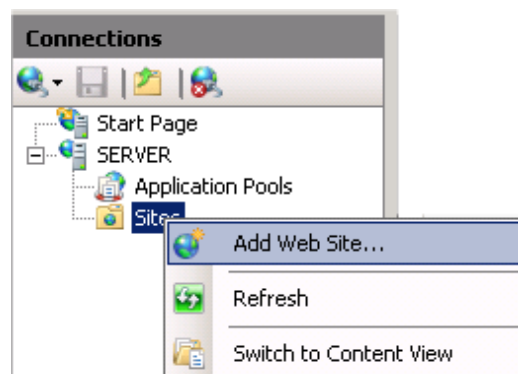
PowerMAN Enterprise Server v5.5



Tip: If the SQL database is located on a remote server you must also change the Load User Profile option to **True**.

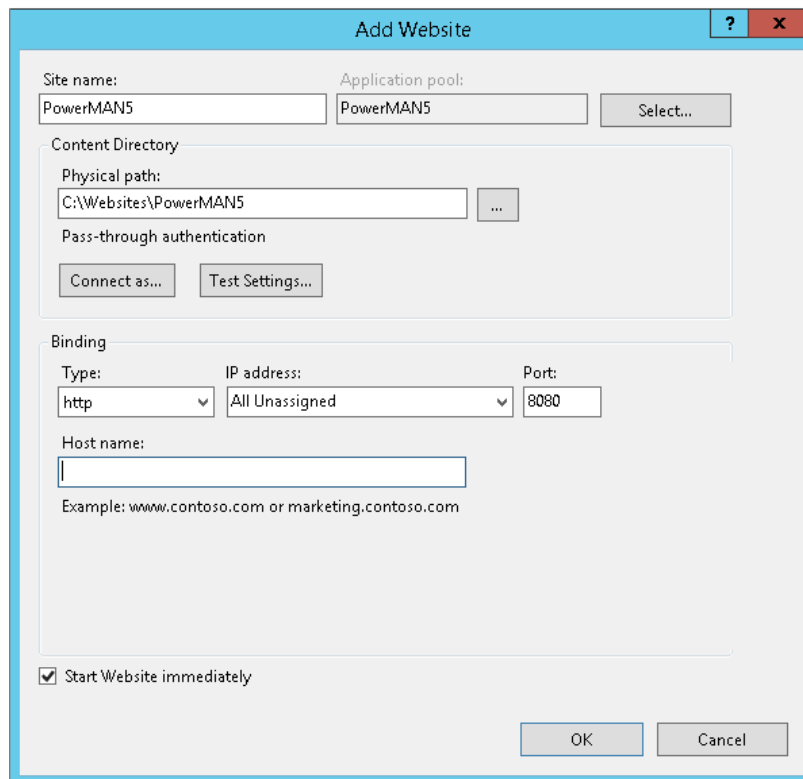
Idle Time-out (minutes)	20
Load User Profile	True
Maximum Worker Processes	1

13. Close the Application Pool settings by clicking **OK**
14. Navigate to **Sites**
15. Right click and select **Add Web Site**



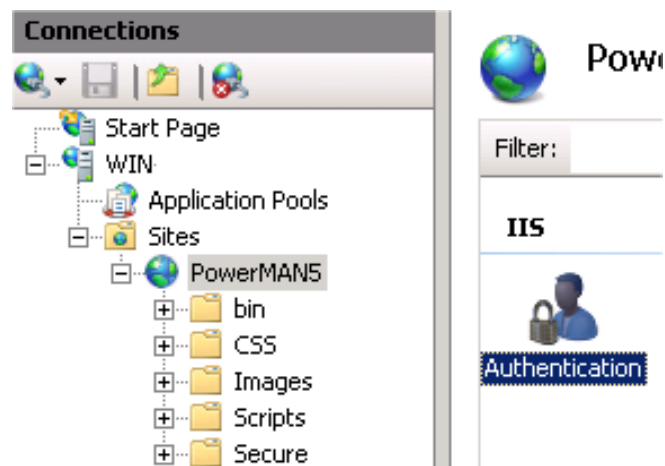
16. Enter the Site Name: **PowerMAN5**
17. Select the Application Pool: **PowerMAN5**
18. Select the appropriate website path, application pool, server IP address range and port number. The default port is **8080**. Click **OK**:

PowerMAN Enterprise Server v5.5

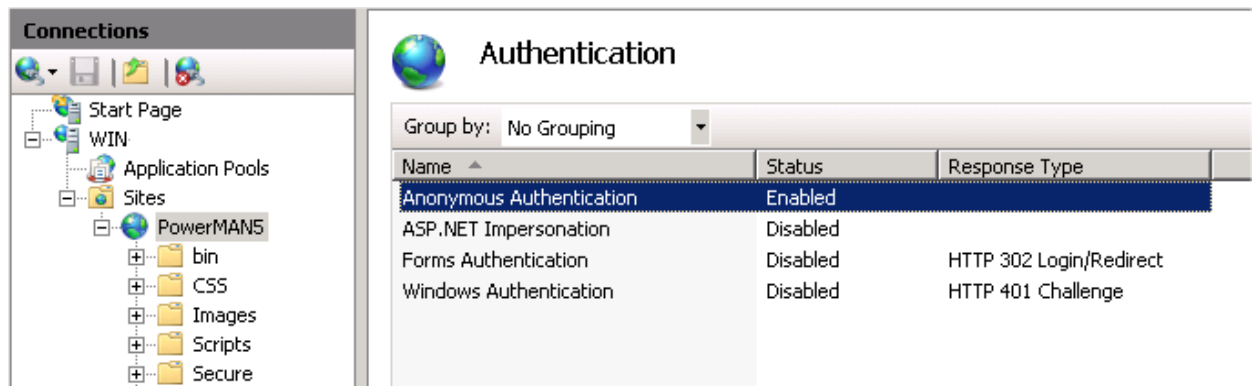


Important: The website **MUST** be accessible to the computers running the PowerMAN client software. If the IIS server is behind a firewall please remember to create a firewall rule. If necessary you can configure the website to accept connections on more than one port.

19. Expand the **Sites** tree and locate the **PowerMAN5** website. In the right hand pane double click the **Authentication** icon:



20. Confirm that **Anonymous Authentication** only is enabled. At this stage we recommend that **Windows Authentication** is NOT enabled. This step is discussed later:



Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

Tip: IIS 7 and later include a number of changes over previous IIS releases. In particular the way anonymous website access operates has changed. The built-in **IUSR** account replaces the legacy IUSR_MachineName account. This account is a member of the Users group and you will NOT normally need to explicitly configure anonymous website access. This is explained further here:

<http://learn.iis.net/page.aspx/140/understanding-the-built-in-user-and-group-accounts-in-iis-70/>

21. Navigate to **Logging** and configure the IIS logging settings appropriate to your organisation.

Tip: IIS logging should normally be enabled. This feature can be very useful when troubleshooting any website problems in the future.

External hosting – Using SSL/TLS security (https)

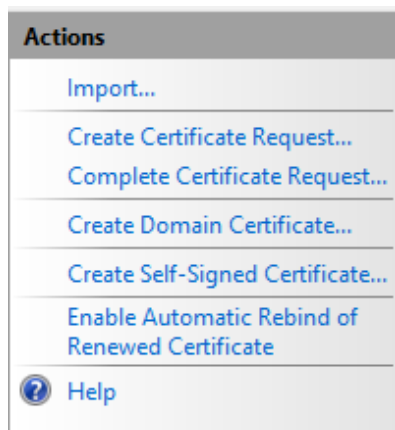
The walkthrough above describes a configuration where the IIS website uses port 8080 and where the traffic is not encrypted. This is typically acceptable for an internal installation of PMES. If you plan to publish your PMES system on the internet, we would recommend that you consider publishing the site using a certificate. This will ensure all traffic is encrypted and prevent an eavesdropper from monitoring the (mostly anonymous) PowerMAN traffic.

To enable SSL/TLS security proceed as follows:

1. Open the **Internet Information Services (IIS) Management tool (INETMGR.EXE)**
2. Select the server name from the left hand menu
3. Double click **Server Certificates**



4. Click **Create Certificate Request**



5. Follow the on-screen instructions to create a CSR. The precise settings will depend on your certificate provider. For example:

<https://www.digicert.com/kb/csr-creation-ssl-installation-iis-10.htm>

<https://sectigo.com/resource-library/generate-csr-microsoft-iis-8-x>

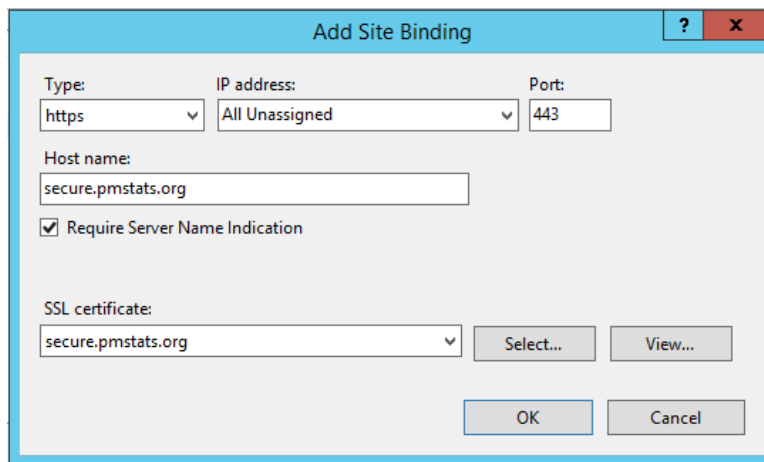
<https://uk.godaddy.com/help/iis-10windows-server-2016-generate-csrs-certificate-signing-requests-27348>

6. Click **Complete Certificate Request**
7. Click ... and locate your certificate (it may also be necessary to change the file extension filter)
8. Click **OK** to load the certificate onto the server

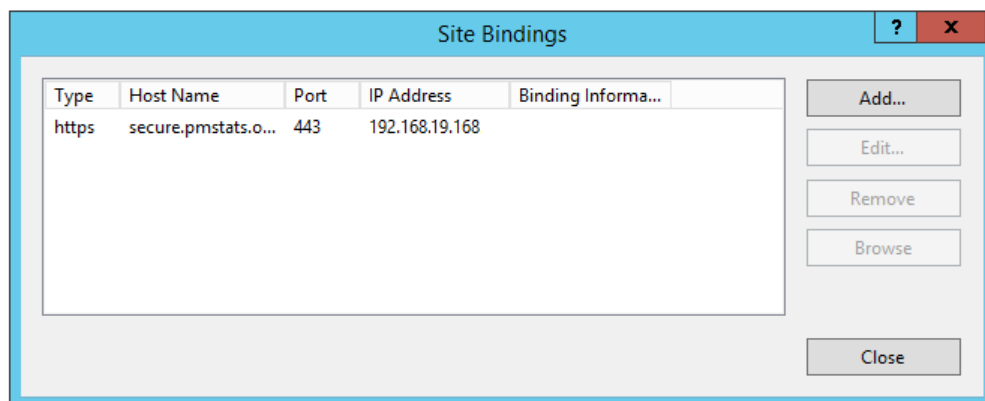
PowerMAN Enterprise Server v5.5

Once the certificate is available, it may be associated with the PowerMAN website as follows:

1. Expand the **Sites** tree
2. Locate the **PowerMAN5** website
3. Right-click and select **Edit Bindings**
4. Click **Add**
5. Select **https** and the desired IP address(s) and port (typically 443)
6. Enter a host name (which should match the certificate) and select the certificate:

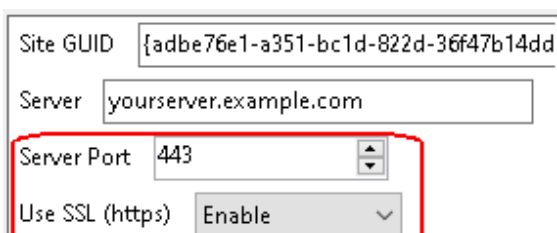


7. Optionally, check the **Required Server Name Indication** checkbox and click **OK**
8. Remove any other unnecessary bindings (e.g. port 8080) and click **Close**



Type	Host Name	Port	IP Address	Binding Informa...
https	secure.pmstats.o...	443	192.168.19.168	

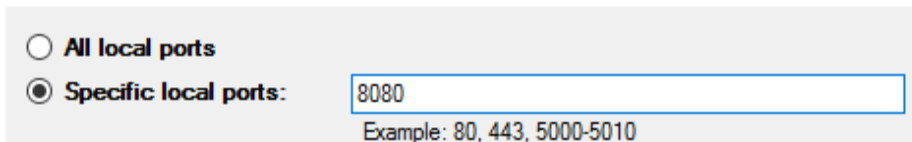
Tip: If you use an SSL/TLS certificate, please remember to make complementary changes to your PowerMAN client reporting configuration via Group Policy or similar:



Firewall Configuration for IIS

Windows Server includes a built-in firewall. If this feature is enabled, a firewall rule must be created to permit the PowerMAN traffic to reach the PMES website. To create a rule, proceed as follows:

1. Open **Windows Firewall with Advanced Security** (WF.MSC)
2. From the left-hand menu, select **Inbound Rules**
3. From the right-hand menu, select **New Rule**
4. Select **Port** and click **Next**
5. Enter the port number (typically 8080 or 443):

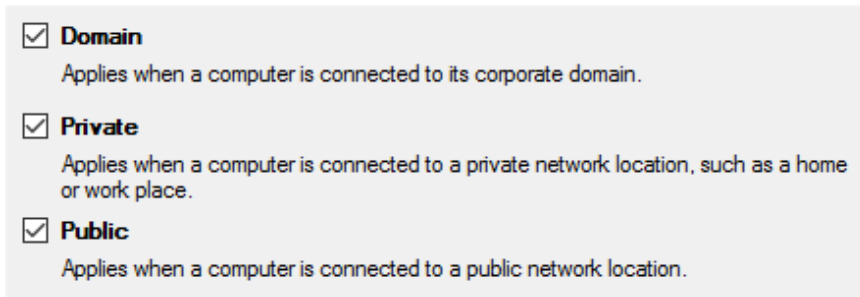


All local ports

Specific local ports:

Example: 80, 443, 5000-5010

6. Select **Allow the connection** and click **Next**
7. Select the desired **Profiles**:



Domain
Applies when a computer is connected to its corporate domain.

Private
Applies when a computer is connected to a private network location, such as a home or work place.

Public
Applies when a computer is connected to a public network location.

8. Click **Next**
9. Enter a name e.g. **PowerMAN Enterprise Server**
10. Click **Finish**

Advanced SQL Configuration

Using a remote SQL server

The walkthrough above describes a configuration where the website and database are located on the same physical server. This approach allows the Network Service account to be used to access the database. The following section explains, briefly, the changes necessary to configure the website to operate with a SQL server located on another server.

You can ignore this section if the web server and SQL server are running on the same server.

This section assumes that both the web server and SQL server are members of the **same Windows domain**. The procedure below replaces the Network Service account with a standard domain user account.

To create this account, proceed as follows:

1. Open the **Active Directory Users and Computers** snap-in
2. Right click on Users and select **New\User**
3. Enter an appropriate username, for instance **PowerMAN**, and click **Next**
4. Enter an appropriate password (twice)
5. Ensure **User must change password at next logon** is NOT selected
6. Select other configuration settings appropriate for your organisation. Typically the account should be configured to avoid password expiry as this will result in the server failing.
7. Click **Next** and then click **Finish**

The domain user account can now be configured for the PowerMAN5 application pool:

8. Open the **IIS Management** snap-in
9. Navigate to the **PowerMAN5** application pool
10. Right click and select **Properties**
11. Navigate to the **Identity** tab
12. Select **Configurable**
13. Click **Browse** and locate the domain user (PowerMAN) account. Click **OK**
14. Enter the appropriate password
15. Click **Apply** and enter the password again

Windows 2008: You must also change the application pool Local User Profile option to **True**.

PowerMAN Enterprise Server v5.5

The domain user account must be granted read access to the website files. This is configured as follows:

1. Open the IIS Management snap-in
2. Navigate to **Websites\PowerMAN5**
3. Locate the Secure folder in the right hand pane
4. Right click and select **Permissions**
5. Click **Add** and locate the domain user account (PowerMAN). Click **OK**
6. Select **Read** (deselect all other options) and then click **OK**

Finally, the domain user account can be made a member of the **website** role of the database:

1. Open SQL Server Management Studio
2. Navigate to **Security\Logins**
3. Right click and select **New Login**
4. Click **Search**
5. Locate the recently created domain user account (PowerMAN) and click **OK**
6. Change the default database to **PowerMAN5** and click **OK** again
7. Navigate to **Databases\PowerMAN5\Security\Users**
8. Right click and select **New User**
9. Click the top search ... button and locate the domain user account
10. Select the 'Website' database role
11. Click **OK**

Using a named instance SQL Server

Microsoft SQL Server supports both default and named database instances. Named instances permit multiple SQL server engines to be installed on the same server. A default instance has no name and therefore only one default instance can exist per server.

This following Microsoft document explains database instances further:

<https://learn.microsoft.com/en-us/sql/database-engine/configure-windows/database-engine-instances-sql-server>

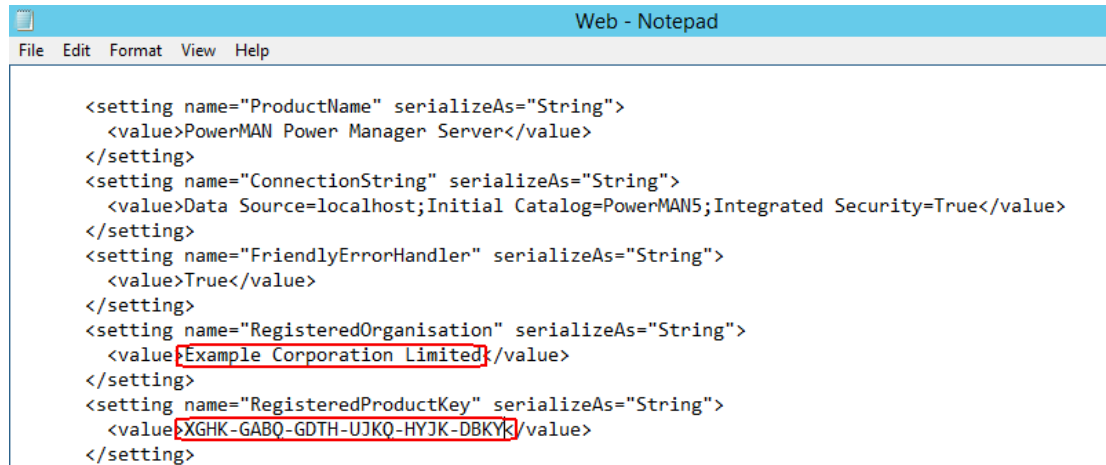
The SQL walkthrough in this document assumes that the SQL server is running as a default instance.

To use a specific named database instance the **ConnectionString** setting, stored in the web.config file, must be amended accordingly (see next section). For instance to use a remote database instance named 'SqlExpress' this would be:

Data Source=Server\SqlExpress;Initial Catalog=PowerMAN5;Integrated Security=True

Configuring PowerMAN Enterprise Website

The majority of the remaining PMES configuration is contained in the website **web.config** file. This is located in the root of the website and can be edited with Notepad or a similar text editor program. The settings in the web.config file are stored in XML format. We recommend that you backup this file before making any changes. For example:



```

<setting name="ProductName" serializeAs="String">
  <value>PowerMAN Power Manager Server</value>
</setting>
<setting name="ConnectionString" serializeAs="String">
  <value>Data Source=localhost;Initial Catalog=PowerMAN5;Integrated Security=True</value>
</setting>
<setting name="FriendlyErrorHandler" serializeAs="String">
  <value>True</value>
</setting>
<setting name="RegisteredOrganisation" serializeAs="String">
  <value>Example Corporation Limited</value>
</setting>
<setting name="RegisteredProductKey" serializeAs="String">
  <value>XGHK-GABQ-GDTH-UJKQ-HYJK-DBKY</value>
</setting>

```

As supplied the file must be manually edited to include the settings appropriate for the installation. A basic PMES server requires relatively few common settings. These are described below:

Common “web.config” settings

Setting	Meaning
RegisteredOrganisation	The name of the registered organisation. For instance: <i>Example Corporation Limited</i>
RegisteredProductKey	The product key. For instance: <i>XGHK-GABQ-GDTH-UJKQ-HYJK-DBKY</i>
ConnectionString	The MS SQL database connection string. For a local (default instance) database this is typically: <i>Data Source=localhost;Initial Catalog=PowerMAN5;Integrated Security=True</i> For a local database instance called ‘SqlExpress’ this would be: <i>Data Source=.\SqlExpress;Initial Catalog=PowerMAN5;Integrated Security=True</i> For a remote database instance called ‘SqlExpress’ located on a PC called ‘Server’ this would be: <i>Data Source=Server\SqlExpress;Initial Catalog=PowerMAN5; Integrated Security=True</i>

SiteRoot	The URL of the web server. <i>e.g. www.examplecorp.com or 192.168.200.10</i>
SecurePath	The URL of the secure administration folder. This is prefixed with a tilde character: <i>e.g. ~/Secure</i>
IntegratedWindowsAuthentication	The user authentication method. This may be: True – Use integrated Windows authentication False – Use email address + password authentication <i>e.g. False</i>

Email configuration “web.config” settings

Setting	Meaning
BugEmail	The email address to send website error reports. Please see the section on SMTP server configuration below. This feature is optional. <i>e.g. support@yourcompany.com</i>
WebsiteEmail	The email account from which to send email bug reports and user notifications. If SMTP authentication is enabled on the email server then this must be a recognised account. <i>e.g. powerman@yourcompany.com</i>
SMTPServer	The SMTP server used for sending emails. This feature also requires that the BugEmail and WebsiteEmail settings are configured: <i>e.g. localhost</i>
SMTPUsername	The username to use for SMTP authentication. This may be blank if authentication is not required.
SMTPPassword	The password to use for SMTP authentication. This may be blank if authentication is not required.
SMTPPort	The TCP port used for SMTP server access. This is normally port 25. <i>e.g. 25</i>
SMTPEnableSSL	Use SSL to access the SMTP server. This is required by some SMTP servers as an additional security measure. This feature is disabled by default. <i>e.g. False</i>

Advanced “web.config” settings

The following advanced settings are provided. The default values are typically sufficient but may be amended if required:

Setting	Meaning
FriendlyErrorHandler	<p>This feature allows detailed error reports to be displayed on the server console.</p> <p><i>e.g. True</i></p>
CommandTimeoutSeconds	<p>Specifies the SQL database command timeout. This is the period of time a complex operation may take before timing out. 120 seconds is sufficient in almost all cases. If complex operations frequently take longer than this it may indicate a problem with SQL server configuration (disk configuration, memory or indexes)</p> <p><i>e.g. 120</i></p>
ServerMaintenanceMessage	<p>Defines maintenance message that is displayed to all users at the top of the PMES screen. This is normally blank.</p> <p><i>e.g. This server will be unavailable for scheduled maintenance on Tuesday 5th July.</i></p>
XMLLogPath	<p>The file system path to log all client XML data uploads. This feature may be used to debug upload problems from the server-side. It should normally be disabled as this feature will impose a performance penalty on the server. The website application pool user (typically Network Service) should have write access to this folder.</p> <p><i>e.g. D:\PMESXML</i></p>
LiveStatusHistoryRetainDays	<p>The number of days to retain live history information. This is used for troubleshooting and should typically be zero. It will be removed in a future release.</p> <p><i>e.g. 0</i></p>
EmailFooterHTML	<p>The text to display at the bottom of PMES notification emails. This may be required to comply with data protection / anti-SPAM regulations e.g. GDPR in the EU.</p> <p><i>e.g. You have received this email because you or your system administrator has registered for this service. Please contact your system administrator to unregister.</i></p>

Minimal “web.config” settings

At a minimum the following settings must be configured:

- **RegisteredOrganisation**
- **RegisteredProductKey**
- **SiteRoot**

In addition, the following settings may need amendment:

- **ConnectionString** – This may need to be changed if the database is located on another server or is not using the default SQL instance
- **SMTPServer, BugEmail and WebsiteEmail** – This will need to be configured if you are using the email error reporting feature

The web.config file may also contain some additional settings not described above. These are used internally by PMES and should not normally be changed.

Securing PowerMAN Website

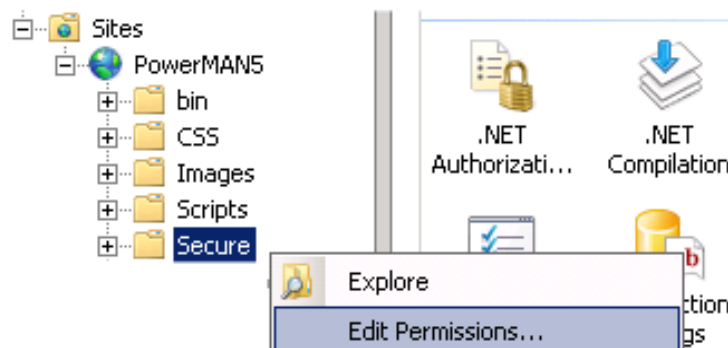
The following section explains how to secure the website on Windows 2008 or later. It describes a default configuration. You may wish to use a different approach to comply with your own organisation requirements.

The PMES website incorporates a **/Secure** folder that contains tools only for administrator use. The pages within this folder are used to perform the initial online server configuration and to subsequently administer the PMES system. These pages **MUST be secured** as they must not be available for anonymous access. This is typically done using Windows Integrated Authentication.

Tip: You can also rename the **/Secure** folder for added security. It is not required for day-to-day server use.

To disable anonymous access for this folder proceed as follows:

9. Open the **Internet Information Services (IIS) Management tool (INETMGR.EXE)**
10. Navigate to **Sites**
11. Locate the **PowerMAN5** site and expand the folder tree
12. Locate the **Secure** folder, right click and select **Edit Permissions:**



13. Select the **Security** tab
14. Click **Advanced**

On Server 2008:

15. Click **Changed Permissions**
16. Un-check **'Include inheritable permissions from this objects parent'** and then click **OK** (if prompted by a warning click **Remove** and then **Yes**) and then **OK** again

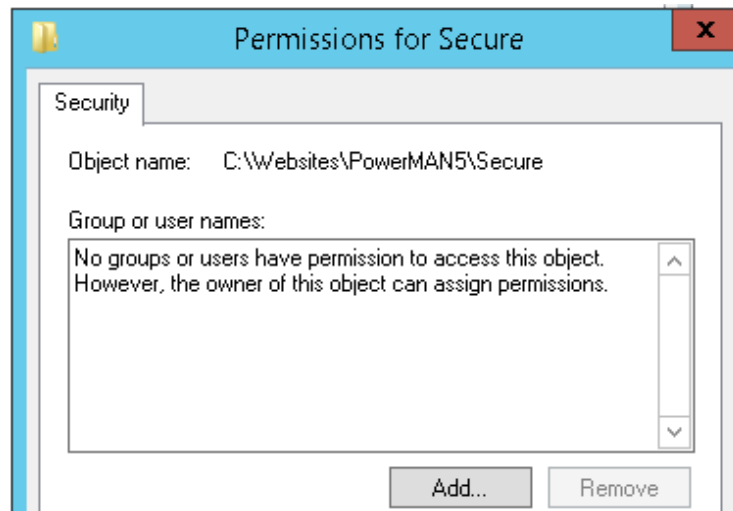
On Server 2012 and later:

17. Click **Disable Inheritance**
18. Select **Remove all inherited permissions from this object** and then click **OK** (if prompted by a warning click **Yes**)

PowerMAN Enterprise Server v5.5

19. Click **Edit**

The following dialog should now be visible:



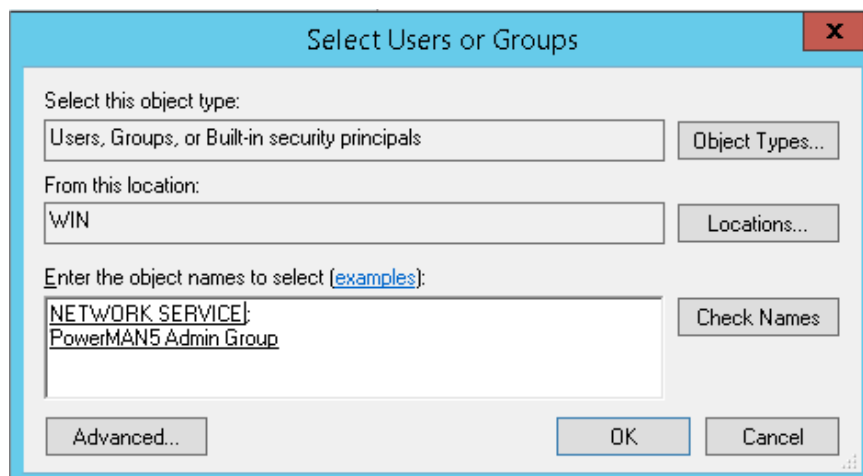
20. Click **Add**.

Tip: We recommend you create a specific local group for the PowerMAN administrators. Historically it was common to use the built-in Administrators group for this purpose but this can be ineffective when User Access Control (UAC) is enabled. Alternatively, you use specific user names.

The following example uses a group called **PowerMAN5 Admin Group**.

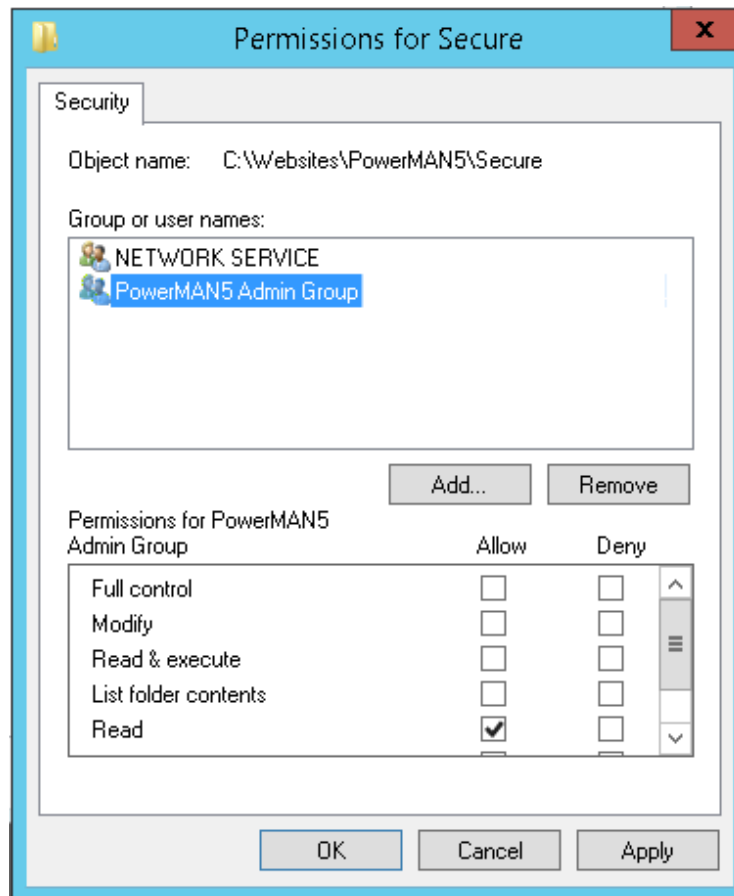
21. Locate the users or groups who will be allowed access to the secure website pages. This should include the account used by the PowerMAN5 application pool user (typically Network Service).

For instance **Network Service** and **PowerMAN 5 Admin Group**:



22. Click **OK**

23. Confirm the selected groups/users have **Read access** (you can also deselect Read & Execute and List Folder Contents, these are not required)



24. Click **OK** and close the dialog
9. Expand the **Sites** tree and select the **Secure** folder again.
10. In the right hand pane double click the **Authentication** icon
11. Enable **Windows Authentication** and ensure that that **Anonymous Authentication** is disabled. This ensures that only the authorised users/groups can access the content:

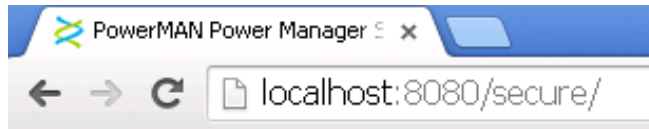
Authentication

Group by: No Grouping		
Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

PowerMAN Enterprise Server v5.5

Finally, confirm the security restriction is operational as follows:

12. Open the **Secure** page using the web browser. For instance:



13. If prompted, enter your login credentials:

Sign in

Username

Password

14. Confirm the page loads normally
15. Repeat this check from a remote workstation and confirm the page loads normally for an approved user.
16. Finally, log in as another user and confirm the page is **NOT** accessible.

Tip: Please remember the Network Service **MUST** be included in the user list for the website to function correctly. The Users group and the IUSR user account should NOT normally be granted read access to /Secure folder.

Alternatively, you could remove or rename the **/Secure** folder for added security. It is not required for day-to-day server use.

Tip: You can also rename the **/Secure** folder for added security. It is not required for day-to-day server use.

Configuring User Authentication (Integrated Windows Authentication)

The PMES software supports both native and Windows integrated authentication:

1. **Native mode (default)** - PMES requires an email address and password to authenticate users for non-anonymous reports. This is simpler to setup. The password is stored in an encrypted format in the PMES database.

To enable this mode modify the web.config file setting:

IntegratedWindowsAuthentication = False

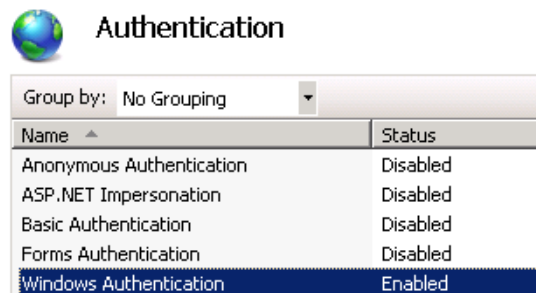
2. **Windows integrated mode (advanced)** - PMES uses the Windows credentials supplied by a compatible Windows browser (Internet Explorer, Chrome and Firefox all support this feature). This allows report access to be seamlessly linked to a Windows logon and avoids the requirement to store any password information in the PMES database.

To enable this mode:

- i. Modify the **web.config** file setting:

IntegratedWindowsAuthentication = True

- ii. Open IIS Manager and select the **PowerMAN5** website
- iii. Navigate to **Authentication** and double click.
- iv. Confirm the default authentication for the site: Set **Windows Authentication** to enabled and **Anonymous Authentication** to disabled:



- v. Click **Content View** (bottom of screen)
- vi. Locate **PostStatus.aspx**, right click and select **Switch to Features View**. PostStatus.aspx should now be visible in the left hand pane.
- vii. Select PostStatus.aspx in the left hand pane and click **Authentication**.
- viii. Configure an authentication exception for the PostStatus.aspx file: Set **Anonymous Authentication** to enabled and set **Windows Authentication** to disabled.
- ix. Close the **Internet Information Services (IIS)** Management tool

Testing Integrated Windows Authentication Mode

PMES includes a diagnostic feature to resolve problems related to Windows Integrated Authentication mode. To confirm this feature is working correctly please proceed as follows:

1. Logon to a client workstation with a Windows user account. Typically this will be the domain account you wish to use for integrated authentication.
2. Open the page <http://yourserver:8080/CurrentIdentity.aspx>
3. Confirm that PMES displays the Windows username of the currently logged on user

PowerMAN Enterprise Server v5.5

PowerMAN Website Testing

Now that the server has been configured it can be tested. There are several test pages provided to check that the database and website functionality.

Assuming you are testing the server locally you can use the following URL:

<http://localhost:8080/statictest.htm>

This page should display a message indicating that the web server is functioning. If this process is not successful you must check the basic IIS configuration before proceeding further.

Tip: If the web server does not display the static test page it may be because you have forgotten to grant the PowerMAN5 application pool read access to the website root folder.

Similarly, after the web server has been checked you can confirm the database is functioning using the following URL:

<http://localhost:8080/servercheck.aspx>

If the system is correctly configured this will report: **Server is available**

Tip: If the server does not respond you may need to investigate the cause of the problem. The most common problems are caused by incorrectly configured database connections or security settings. The **servercheck.aspx** page uses a stored procedure called **upServerCheckInfo**. You (or a suitably qualified DBA) can use the **SQL Server Profiler** tool to trace the website access to this procedure and determine the cause of the problem.

If the **statictest.htm** page check is successful but the **servercheck.aspx** page fails, this may be because the wrong ASP.NET framework is selected in the application pool or a required IIS/ASP.NET component is missing. Please check the preceding sections to confirm the correct configuration.

Checking Website Security

Before proceeding further it is essential to verify the security of the PMES system. Assuming the installation steps above have been followed you can do this as follows from **another** computer (not the server) using arbitrary user credentials:

- Check the page <http://yourserver:8080> is available to any user
- Check the page <http://yourserver:8080/Secure> is only accessible to the user/group(s) you have selected
- If Windows Integrated Authentication mode is enabled check that the page <http://yourserver:8080/CurrentIdentity.aspx> displays the Windows username of the current logged on user

This step completes the basic configuration of the PMES system. Most day-to-day configuration and management can now be performed using the website itself.

PowerMAN Enterprise Server v5.5

SMTP Configuration (Email and error reporting)

PowerMAN Enterprise Server allows users to file error reports in the event on a server problem. These are sent by email and may be investigated using the server database and IIS logs. This feature is optional.

To use this feature you must configure the **SMTPServer**, **BugEmail** and **WebsiteEmail** settings in the web.config file. You can test the email notification using a webpage located in the secure area. To use this feature proceed as follows:

1. Navigate to <http://yourserver:8080/Secure/ServerTools.aspx>
2. Click the **Test** link
3. Confirm a test email is delivered (this may take several minutes)

Configuration	Server Tools	Error Log
---------------	--------------	-----------

Setting	Value
ConnectionString	Data Source=localhost;Initial Catalog=PowerMAN5;Integrated Security=True
SMTPServer	smtp.yourdomain.com
BugEmail	support@yourdomain.co.uk Test

Parameter	Value
Application Pool Identity	NT AUTHORITY\NETWORK SERVICE
Scheduler last run	12:44:28 Run now

Configure PowerMAN Enterprise Server for your organisation

Before proceeding to configure the system for your own organisation please:

- Obtain a PowerMAN **client** software product key (this is different to the PMES server PID)
- Decide if you wish to allow anonymous access to view the management reports
- Decide if you wish to use PMES native (email address + password) or Windows integrated user authentication mode. This is configured with the **WindowsIntegratedAuthentication** setting in the PMES web.config file.
- Decide if you wish to manually create reporting sites (groups) or automatically create them using the workstation's Active Directory tree (requires client 5.2.6 or later)
- Decide which currency to use for reporting estimated energy costs

Tip: Anonymous access to the management reporting tool allows the system to be used by a variety of users without configuring a specific login. Anonymous access does not allow any configuration changes to be made. Anonymous access is usually used when customers evaluate the PowerMAN hosted reporting system as it simplifies initial configuration and allows the reporting system to be quickly shared by a number of users.

To register your client key in PMES and create your organisation, proceed as follows:

1. Open the Secure configuration page: <http://yourserver:8080/Secure>
2. Enter your **organisation name** and PowerMAN **client** software product key

Register New Organisation

Registered Organisation Name	<input type="text" value="Example Corporation Limited"/>
Registered Client PID key	<input type="text" value="DQTJ-KXCP-QJCX-ABTK-CWDK"/>
Allow anonymous viewing	<input checked="" type="checkbox"/>
Currency Symbol	<input type="text" value="USD United States Dollars"/>
<input type="button" value="Create"/>	

3. Select the appropriate settings for anonymous access and reporting currency
4. Click **Create**

Organisation Configuration

Export Organisations	Expires After: <input type="text" value="05/05/2022"/>	<input type="button" value="Refresh"/>				
Organisation	Client PID	Created	Sites	Computers		
Example Corporation Limited	DQTJ-KXCP...	01/11/2022	1	0	Super User Rename Delete	

Configuring User Logins

The PowerMAN reporting software requires a user login to make configuration changes. To create the first user login, proceed as follows:

1. Open the Secure configuration page: <http://yourserver:8080/Secure>
2. Identify the organisation
3. Click **Super User**



4. Click the **Logins** tab
5. Follow the instructions in the PowerMAN Management Reporting Platform Guide to complete login creation.

Tip: When Windows integrated mode is enabled the qualified user name should be entered instead of a login email address (no password is required). This is in following the format:

domain\username

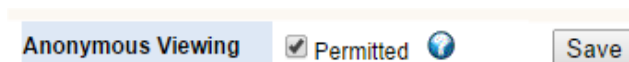
A helper page is provided to display the current qualified user name as communicated by the browser. Please visit the following page to display the current logon:

<http://yourserver:8080/currentidentity.aspx>

Configuring Anonymous Access

To change the anonymous access feature proceed as follows:

1. Open the Secure configuration page: <http://yourserver:8080/Secure>
2. Identify the organisation
3. Click **Super User**
4. Click the **Configuration** tab
5. Select the appropriate viewing setting (and optionally update sub-sites):



6. Click **Save**

Configuring Automatic Site Creation (AD Integration)

PMES allows reporting sites (groups) to be manually created or automatically created based upon the workstation Active Directory tree. This feature requires client version 5.2.6 or later. The reporting site is created based upon the workstations AD 'distinguished name (DN)'. For instance the computer PC2723 could have the DN:

CN=PC2723,OU=Workstations,OU=Management,OU=Head Office Staff,OU=Departments,DC=Customer,DC=local

This would place the workstation in the following reporting location:


Root -> Departments -> Head Office Staff -> Management -> Workstations

When automatic site creation is enabled PowerMAN will automatically generate any necessary reporting sub-sites and arrange them accordingly. This feature is disabled if the workstation is located within a sub-site that has the auto move setting disabled.

To enable this feature proceed as follows:

1. Open the Secure configuration page: <http://yourserver:8080/Secure>
2. Identify the organisation
3. Click **Super User**
4. Click the **Configuration** Tab
5. Locate the **Auto Site Create** feature
6. Select **Enable auto site creation**

Auto Site Creation

Enable auto site creation (OU Based) 

Save

7. Click **Save**

Error Log

PMES includes an error log feature. This is accessible from the /Secure page and records both minor and serious server errors for later review. This feature can be useful for debugging PMES configuration problems.

TIP: It is quite normal for some client upload operations to timeout during busy periods or when only partial data is uploaded. These errors are typically associated with PostStatus.aspx. Please contact Data Synergy Technical for further information on specific error messages.

PowerMAN Power Manager Server Error Log

Configuration | Server Tools | **Error Log**

Important: The error log is for Technical Support use. It is normal for some errors (especially PostStatus data upload timeouts) to be logged during normal operation. This does not indicate a fault.

Date/Time	FunctionName	Description	ExtraInfo
14/08/2010 20:18:44	Throw	Unexpected end of file while parsing Name has occurred. Line 16, position 841.	http://pmstats.org:8080/PostStatus.aspx?ClientGUID={4f3a2f9b-a3bf-4f3a-b7cd-0019d1561109}&SiteGUID={4f3a2f9b-a3bf-4f3a-b7cd-35b23c9eb8ae}
14/08/2010 19:41:38	Throw	Unexpected end of file while parsing Name has occurred. Line 16, position 841.	http://pmstats.org:8080/PostStatus.aspx?ClientGUID={4f3a2f9b-a3bf-4f3a-b7cd-0019d1561109}&SiteGUID={4f3a2f9b-a3bf-4f3a-b7cd-35b23c9eb8ae}

Temporary Website Maintenance (Server Offline)

PowerMAN Enterprise Server incorporates a simple feature that can be used to notify users if the server is temporarily unavailable for maintenance. You may wish to enable this feature if you are performing a software upgrade or other maintenance task. To notify users proceed as follows:

1. Locate the **App_Offline.xxx** file in the root of the website
2. Rename it to **App_Offline.htm**
3. Remember to rename the file to App_Offline.xxx when your offline task is complete

This technique is explained further in the following Microsoft document:

<http://msdn.microsoft.com/en-us/library/bb398992.aspx>

SQL Database Optimization and maintenance

There are several additional steps required to ensure reliable and optimal functioning of the PMES MS SQL database:

- Database backup strategy
- Database optimization strategy
- Database configuration

Database Backups

As supplied the PowerMAN5 database is configured to use the **Simple Recovery Model**. This model is simple to configure but may result in some data loss in the event of a server malfunction. In this model any data changed after the last backup is subject to possible loss. In many scenarios the minor discontinuity in the logged data that would result from a malfunction may be acceptable.

Tip: When it would be unacceptable to lose any PowerMAN data the solution is to use the **Full Recovery Model**. This stores separate database and transaction log backups to an alternative physical location and means that it is possible to restore all database changes since the last full backup. This approach, although more complicated, may also be appropriate for your system. It is your responsibility to configure the necessary transaction log backups.

The following Microsoft article provides additional guidance on selecting the appropriate backup strategy:

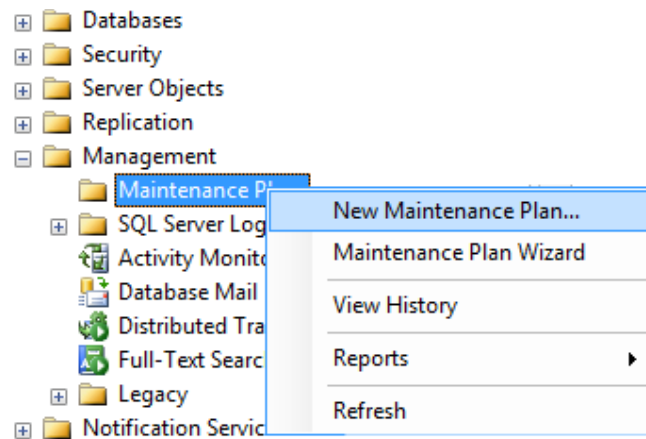
<https://learn.microsoft.com/en-us/sql/relational-databases/backup-restore/recovery-models-sql-server>

You must decide the appropriate database backup strategy for your PMES deployment.

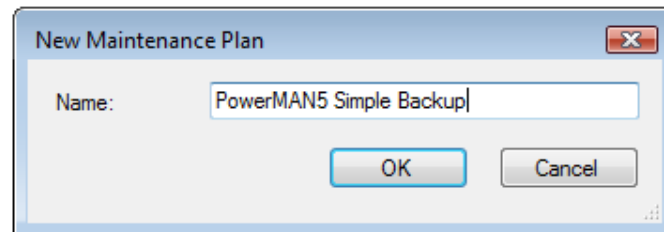
The following steps describe a procedure to configure regular backups using the Simple Recovery Model:

1. Open SQL Server Management Studio
2. Navigate to Management\Maintenance Plans
3. Right click and select New Maintenance Plan

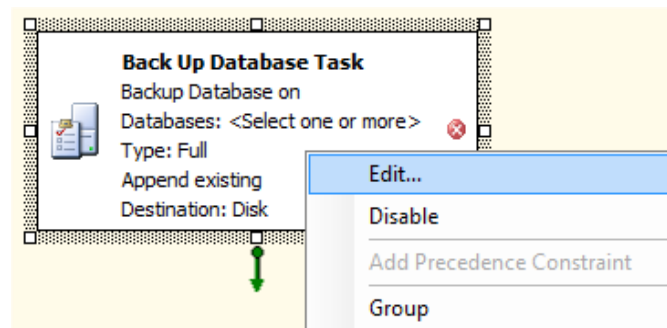
PowerMAN Enterprise Server v5.5



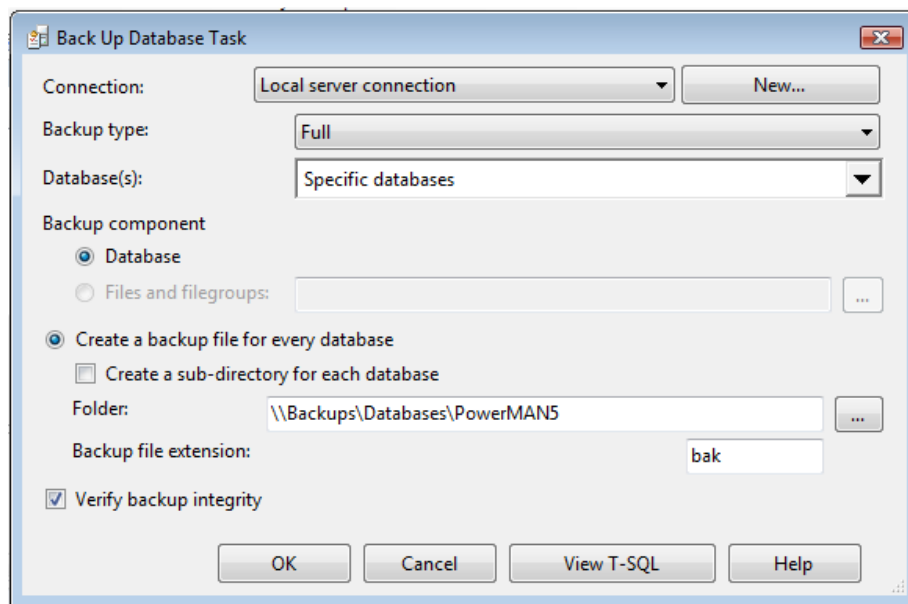
4. Enter an appropriate plan name: **PowerMAN5 Simple Backup**



5. Drag the 'Backup Database Task' to the main pane (located bottom right)
6. Right click on the task and select Edit



7. Select the PowerMAN5 database
8. Select an appropriate backup location e.g. [\\Backups\Databases\PowerMAN5](#)
9. Click OK



10. Click the Calendar icon
11. Select an appropriate backup schedule and click OK. (Typically the backup should occur once per day)

Important: Adequate database backups are essential to avoid unacceptable data loss. You are responsible for configuring a suitable backup strategy. When configuring the backup system you should consider the possibility of hardware failure on the server. You can mitigate this problem by configuring the backup to a remote location. The ideal time to configure a backup is between 8 and 10pm. This is usually after most client computers have been switched off and before midnight when any active computers will start to report data.

It is not necessary to keep historic backups forever and in practice only the last few backups (for instance the last 7 days) need to be retained.

Periodic SQL Database Optimisation

The PowerMAN database makes extensive use of indexes to improve performance. Over time these can become fragmented which can lead to a decrease in performance and website timeouts. It is good practice to periodically optimize these indexes. This can be done either by reorganising or rebuilding the indexes. Each technique has both advantages and disadvantages. These are discussed further in the following Microsoft article:

[http://msdn.microsoft.com/en-us/library/aa964133\(SQL.90\).aspx](http://msdn.microsoft.com/en-us/library/aa964133(SQL.90).aspx)

The most appropriate technique will depend upon the size of your PowerMAN database and the level of index fragmentation. The following procedure explains how to configure the indexes to rebuild once per week. This technique, which will make the database temporarily inaccessible, is the simplest technique to ensure optimal performance.

You must determine the most appropriate database optimisation technique for your server. This decision is primarily determined by the size of the database and the amount of database downtime you will accept. In many scenarios it would be acceptable to optimize the indexes less frequently than once per week.

PowerMAN Enterprise Server v5.5

To configure the database to rebuild the indexes once per week proceed as follows:

1. Open **SQL Server Management Studio**
2. Navigate to **Management\Maintenance Plans**
3. Right click and select **New Maintenance Plan**
4. Enter an appropriate plan name: **PowerMAN5 Index Task**
5. Drag the **'Rebuild Index Task'** to the main pane
6. Right click on the task and select **Edit**
7. Select the **PowerMAN5** database
8. Select **Tables and Views** and click **OK**
9. Click the **Calendar** icon
10. Select an appropriate backup **schedule** and click **OK**. (Typically the index rebuild should occur once per week)

Important: It is easy to overlook the importance of effective index optimization. The strategy above is probably excessive for most standard databases but will result in regularly optimized databases indexes. As the database may be inaccessible during the index rebuild operation this task should normally be carried out during a regular maintenance period or when the server is not required.

Database Server Configuration

PMES is designed to have low hardware resource requirements. Smaller PMES systems (<10,000 workstations) may use SQL Express edition and run with satisfactory performance using a default configuration on desktop (rather than server) class hardware. In such installations no specific database server configuration is required.

In larger PMES systems (database >10GB) it is necessary to use SQL Standard (or Enterprise) edition. In such installations a significant performance improvement may be obtained by correctly configuring the SQL server. The improvement achievable through careful configuration can be several times greater than that obtainable from higher performance server hardware alone. Depending upon system scale the following best practices may deliver significant advantages:

- PMES and TempDB database and transaction log files be located on physically separate drives.
- Backups run during non-peak times (typically after 6pm and before midnight)
- Server RAM be at least 4GB (10,000 workstations), 8 GB (25,000) workstations) or 16GB (50,000 workstations and above)
- All drives have ample free space
- The SQL server is used for SQL alone and no other services (e.g. not IIS, AD etc.)

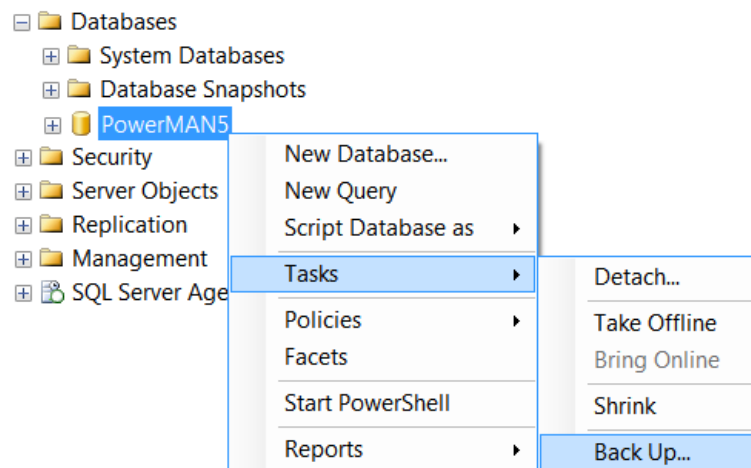
Please contact Data Synergy Technical Support if you require any further advice.

PowerMAN Enterprise Server v5.5

Manual SQL Database Backup

The PowerMAN SQL database may be manually backed up at any time by following the procedure below:

1. Open **SQL Server Management Studio**
2. Navigate to **Databases\PowerMAN5**
3. Right click and select **Tasks\Back Up**



4. Select Backup type: **Full**
5. Click **Add**
6. Select an appropriate backup destination folder
7. Enter an appropriate backup name: **PowerMAN5-Full Database Backup**
8. Click **OK**

PowerMAN Enterprise Server v5.5

Source

Database: PowerMAN5

Recovery model: FULL

Backup type: Full

Copy-only Backup

Backup component:

Database

Files and filegroups: ...

Backup set

Name: PowerMAN5-Full Database Backup

Description:

Backup set will expire:

After: 0 days

On: 01/03/2012

Destination

Back up to: Disk Tape

d:\PowerMAN5.bak

TIP: SQL Database backup files can be quite large. Often they will compress very significantly using tools such as ZIP or WinRAR. Please compress SQL backup files before sending them to Data Synergy Technical Support.

Troubleshooting PowerMAN Enterprise Server

PowerMAN Enterprise Server (PMES) has undergone many thousands of hours of development and testing. The software is very reliable but problems do sometimes happen. This walkthrough installation in this document makes some basic assumptions about the PMES deployment environment and, in a real-world deployment; additional complications may cause configuration problems. This section describes common problems, how to investigate, and ultimately resolve them.

Tip: For security reasons the web.config file supplied with PMES is configured to display only limited client error messages. If you experience problems with the PMES website it can be very helpful to view the problem pages directly on the web server via <http://localhost:8080/>. If this is not practical you can **temporarily** configure additional error messages to be displayed on client browsers by changing the following setting in the web.config file:

```
customErrors mode="RemoteOnly" -> customErrors mode="Off"
```

Please remember that this step will expose your system to additional security threats and should only be performed in a controlled environment.

Problem: Static test page is not displayed

Problem: Website reports - The page cannot be found

Problem: Website reports - Server Application Unavailable

The static test page (statictest.htm) is provided to test the basic functionality of the web server. It does not use the SQL database and therefore avoids the additional complications that can occur due to database connectivity problems. If this page does not display please check the following:

- The application pool identity (usually Network Service) has read access to the folder containing the website. If you have configured the application pool to use a domain user account then this account must have read access to the website.
- The server firewall (if running) allows access to the web server (usually port 8080)
- There may be additional useful information in the System and Application event logs

Problem: /Secure webpage appears blank (and no error is displayed)

This problem can occur when the ConnectionString configuration setting is incorrect. Please review the steps in the Website Testing section above and in particular confirm that the <http://localhost:8080/servercheck.aspx> page functions as expected.

Problem: .NET Framework v4.0.30319 is not available when creating App Pool

OR Website reports - The current identity does not have write access to ...Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files

OR "The page cannot be found" error message when you request an ASPX page

OR "HTTP Error 404 - File or Directory not found" error message when you request an ASPX page

This message can be displayed if the Internet Information Service (IIS) was installed after the .NET framework. It indicates that the .NET framework is not correctly registered with IIS. You can correct this problem by executing the following OS specific command:

32-bit OS: %windir%\ Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -i

or

64-bit OS: %windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -i

If this step is necessary please also remember to check that the correct .NET framework is configured for the website (in the ASP.NET tab).

Problem: Servercheck.aspx takes excessive time (>1 second) to display

OR Servercheck.aspx reports - An error has occurred while establishing a connection to the server (or similar)

OR Website reports Server Error in '/' Application. Runtime Error. Description: An exception occurred while processing your request.

This class of problem is usually associated with database connectivity issues. This may be because the database server is not accessible or because the security configuration is incorrect. The following may be helpful:

- If the problem is sporadic please consider other tasks the server may be doing. If the computer hosting the SQL server is used for other services please consider providing a separate sever for the PowerMAN database. The database must reliably respond in <5 seconds for PowerMAN clients to be able to successfully log data.
- Check the network connection from the IIS server to the SQL server
- Check the IIS application pool identity (usually Network Service for local databases and a domain user account for remote databases) is a member of the Website database role.
- Disable 'friendly' error messages (see below) and review the detailed error data reported. It may also be helpful to check tblErrorLog in the PowerMAN5 database.

Problem: Website reports - Sorry. A website error was detected. This cause of this error has been logged and will be investigated

This error is generated when the PMES software encounters an error. The most common cause of this problem is a timeout accessing the database. This can happen due to incorrect database configuration or under very heavy database load conditions. PowerMAN logs most errors (except timeouts) in the tblErrorLog database table. You can query this table to determine the cause of the error.

To investigate the cause of this error further you can also disable the 'friendly' error message and configure PMES to display the full error message. This information may be useful to Technical Support.

To display detailed error information:

- Edit the web.config file and change the value of the FriendlyErrorHandler to 'False'. This will allow detailed error reports to be displayed on the server console.
- To enable display detailed error information on remote browsers (not necessary for localhost) you can edit the web.config file and change the customErrors 'mode' setting from "RemoteOnly" to "Off".

Please remember that both of these changes will make the PMES server less secure. They should only be performed under controlled conditions and certainly not when the PMES server is accessible from the internet.

Problem: Non-specific database connectivity problem

OR Website reports error 'A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: SQL Network Interfaces, error: 25 - Connection string is not valid)' or similar

Database connectivity issues can sometimes be difficult to resolve. The basic PMES configuration is quite simple but complexity can dramatically increase if the SQL server is located in a remote location or either server is shared with other services.

To re-cap, the general configuration is normally as follows:

1. The website is run in the context of a separate application pool
2. This application pool uses a specific user account (often Network Service).
3. The user account must have Read access to the website root folder
4. The user account must be a member of the Website database role

You can investigate connectivity problems using a combination of the following steps:

- Check the basic configuration above. In particular confirm the identity used for the application pool and that this user account has the necessary file system and database access

PowerMAN Enterprise Server v5.5

- If you have recently made configuration changes it can sometimes help to recycle the application pool and restart the IIS service. This is described elsewhere in this document.
- Use the <http://localhost:8080/secure/ServerIdentity.aspx> to confirm the identity that the web server is currently using. This should match that configured in the application pool
- Use the <http://localhost:8080/ServerCheck.aspx> page to confirm the database connection is operational
- Use the SQL Server Profiler tool to monitor the IIS interaction with the SQL server. This can often expose security related problems.
- If PMES displays the 'friendly' error page consider disabling this feature (see above) to see more detailed error information.

Problem: Website displays - Service Unavailable

This message is displayed when the PowerMAN5 application pool is incorrectly configured. This message may also be displayed if the application pool has recently been re-configured to use a domain user account. Please check the following:

- The application pool identity is correctly configured. If a domain user account is being used try re-entering the password.
- The application pool identity (domain user) is a member of the local **IIS_USRS** group
- After making any changes you can restart the application pool by right clicking on it and selecting **Recycle**.
- Similarly it can sometime help, after making several related changes, to restart the website or even IIS itself. This can be done by right clicking on the site and selecting **Stop** and then **Start**. To restart IIS right click on Internet Information Services and select **All Tasks/Restart IIS**
- There may be additional useful information in the System event log

Problem: The website reports an exception obtaining permission of type 'System.Web.AspNetHostingPermission'

This problem can occur on Windows 2008 (IIS7). It can be problematic to resolve because unless **customErrors** setting has been modified it is only displayed when the web page is viewed on the local server.

This problem can occur when the SQL database is located on a remote server and the application pool is operating under the identity of a domain user. To resolve the problem change the application pool setting **Load User Profile** to **True**.

Idle Time-out (minutes)	20
Load User Profile	True
Maximum Worker Processes	1

Problem: Unrecognized attribute “targetFramework” reported when you request an ASPX page**OR <compilation debug="false" targetFramework="4.0"></compilation>**

This problem can occur if IIS application pool is running under an incorrect version of the .NET framework. To resolve this problem confirm that that WakeMAN5 application pool is running under the v4 .NET framework. If necessary install the v4 .NET framework.

Problem: Website generated URLs fail to work correctly.**OR Website URLs contain additional, unrecognised symbols, such as %20**

This problem occurs URL settings in the web.config file contain leading, trailing or embedded spaces or other unprintable characters. In some rare circumstances embedded spaces may be necessary but generally well-formed URLs should avoid spaces and unprintable characters. Check that no unexpected characters exist in between <value> and </value> for the **PostErrorURL** and **WakeConnectURL** settings.

Problem: Computers appear to be reporting correctly but are not showing on the reporting system**OR The SQL database contains data but this is not visible in the web-based reports**

This problem can happen if the SiteGUID being used by client computers is not registered on the server. In this situation data is still logged correctly but is not displayed.

To register a SiteGUID with the system proceed as follows:

- Login to the reporting system (or click ‘Super User’ on the secure administration page)
- Navigate to the site you wish to use as the parent of the new site-site
- Click **Add / Move Site**
- Enter the new SiteGUID including the {braces} and a suitable site name
- Click **Add / Create Site**

Problem: How do I migrate from the PowerMAN hosted reporting system to the (on-premise) PowerMAN Enterprise Server system?

Many organisations use the hosted PowerMAN reporting system for either evaluation purposes or as a complete live system. The hosted platform has many advantages and is generally cost effective for organisations with less than approximately 2,000 computers. In some situations it may be desirable to move from the hosted environment to the on-premise PowerMAN Enterprise Server (PMES) system. Data Synergy offer a free data transfer service for customers upgrading to PMES. The following procedure explains the transfer procedure

PowerMAN Enterprise Server v5.5

for a live installation that is currently using the hosted reporting platform:

Setup your own PMES server using the blank database supplied.

1. Confirm the system is working with test data. The simplest way to do this is to manually configure a single PC to report to the server using Local Group Policy. Confirm the PMES server is working satisfactorily
2. Stop the IIS server e.g. not accepting data from clients. Confirm that the website is inaccessible
3. Prevent the clients from reporting to the hosted system. The best way to do this (if possible) is via the external firewall by blocking pmstats.org. If this is not possible please contact Technical Support
4. Confirm that data has stopped flowing to the hosted system - this should happen instantly
5. Ask Data Synergy Technical Support to prepare a database export
6. Restore the exported database to your SQL server replacing the test database previously used
7. Update the client settings to use the new (private) reporting server
8. Allow clients to start reporting to private server. This will happen after the next client reboot or PowerMAN service restart

NB: Step 2 is essential. This is to ensure that the changeover is clean. There are 28 days (by default) from this point before there is any risk of data discontinuity.

Problem: How do I migrate from the (on-premise) PowerMAN Enterprise Server reporting system to the hosted PowerMAN reporting system?

Data Synergy offer a free data transfer service for customers transferring to the hosted reporting system from PMES. The following procedure explains the transfer procedure for a live installation that is currently using PMES. The procedure is very similar to that described above for transfer to PMES:

1. Disable your existing PMES server. The easiest way to do this is to disable the IIS website or block traffic with the server's local firewall
2. The client software will continue to record data locally and periodically attempt to transfer this to the server. This is harmless. Do NOT configure your client software to report to our hosted system just yet
3. Backup your local PMES database and compress it (ZIP is ideal)
4. Email Data Synergy Technical Support the compressed database. If the database is too large to email please contact Technical Support for advice
5. We will extract the data from your database and load it into the hosted system
6. We will then confirm the hosted system is ready to accept data from your deployment
7. Update the client settings to use the new hosted reporting platform (pmstats.org)
8. Allow clients to start reporting to hosted system (for instance by unblocking the external firewall). Data will start to flow after the next client reboot or PowerMAN service restart

NB: The most important step is point 2. This is vital to ensure that the changeover is clean. There are 28 days (by default) from this point before there is any risk of data discontinuity.

PowerMAN Enterprise Server v5.5

Problem: How do I migrate a PowerMAN Enterprise Server (PMES) system from one server to another?

To move the PowerMAN PMES IIS web component to another IIS server proceed as follows:

1. Disable your existing PMES server. The easiest way to do this is to disable the IIS website or block traffic with the server's local firewall
2. Install PMES on the new server following the instructions in the Platform Installation Guide
3. Configure the appropriate settings (including SQL database 'connection string') in the web.config file
4. Update the client settings to use the new reporting server address
5. Allow clients to start reporting to hosted system. This will happen after the next client reboot or PowerMAN service restart

NB: The most important step is point 1. This is vital to ensure that the changeover is clean. There are 28 days (by default) from this point before there is any risk of data discontinuity

To move the PowerMAN SQL database to another SQL server proceed as follows:

1. Disable your existing PMES server. The easiest way to do this is to disable the IIS website or block traffic with the server's local firewall
2. Backup the SQL database following the instructions in the PMES Platform Installation Guide
3. Restore the database to the new SQL server
4. Update the SQL database 'connection string' in the web.config file to point to the new SQL server
5. Re-enable the PMES server (for instance restart the website)

Problem: Windows Integrated Authentication Mode does not work as expect

OR PMES reports 'Unknown User' when Windows Integrated Authentication Mode is enabled

OR The/CurrentIdentity.aspx page displays no username when Windows Integrated Authentication Mode is enabled

This problem can occur when Anonymous Windows authentication is enabled. To disable this proceed as follows:

- On Windows Server 2008/2012: Open **IIS Manager** and select the **PowerMAN5** website. Navigate to **Authentication** and double click. Confirm that **Anonymous Authentication** is disabled.

Problem: The PMES website does not operate correctly with Internet Explorer 10

This problem can occur if the Windows server hosting PMES has not been updated. IE10 may not be recognised by the built-in ASP.NET browser definition files. This problem can be resolved by installing any pending Windows updates. The specific update that resolves this problem is available from the following link:

<http://support.microsoft.com/kb/2600088>

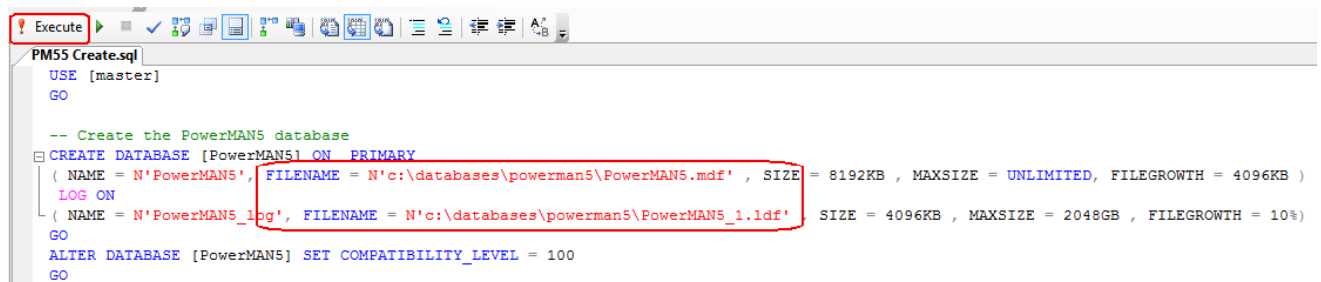
Appendix A: PowerMAN5 Database Creation Script (v5.5.x)

Advanced SQL administrators may wish to create the PowerMAN5 database using a SQL script rather than by restoring the pre-supplied database backup file. A script is supplied in the **Advanced** folder of the PMES distribution. To create the databases using a scripted method, proceed as follows:

1. Open SQL Server Management Studio
1. Open the supplied **PM55 Create.sql** script file. This is located in the **Advanced** folder of the PMES distribution.
2. Amend the database and transaction log file locations as required (see diagram below)

NB: We recommend best practice is to place these files on separate physical disks. This will improve both performance and recoverability in the event of a disk failure. This is may not be necessary on smaller deployments.

3. Click **Execute**



```
PM55 Create.sql
USE [master]
GO
-- Create the PowerMAN5 database
CREATE DATABASE [PowerMAN5] ON PRIMARY
( NAME = N'PowerMAN5', FILENAME = N'c:\databases\powerman5\PowerMAN5.mdf' , SIZE = 8192KB , MAXSIZE = UNLIMITED, FILEGROWTH = 4096KB )
LOG ON
( NAME = N'PowerMAN5_log', FILENAME = N'c:\databases\powerman5\PowerMAN5_1.ldf' , SIZE = 4096KB , MAXSIZE = 2048GB , FILEGROWTH = 10%)
GO
ALTER DATABASE [PowerMAN5] SET COMPATIBILITY_LEVEL = 100
GO
```

4. Confirm no error messages are reported
5. Perform the steps described in the **Database Login Configuration** section above. This will add the user used for the IIS website application pool to the PowerMAN5 database 'website' role
6. Perform the subsequent website configuration steps described above

Appendix B: PowerMAN5 Upgrade Procedure (v5.4.x to v5.5.x)

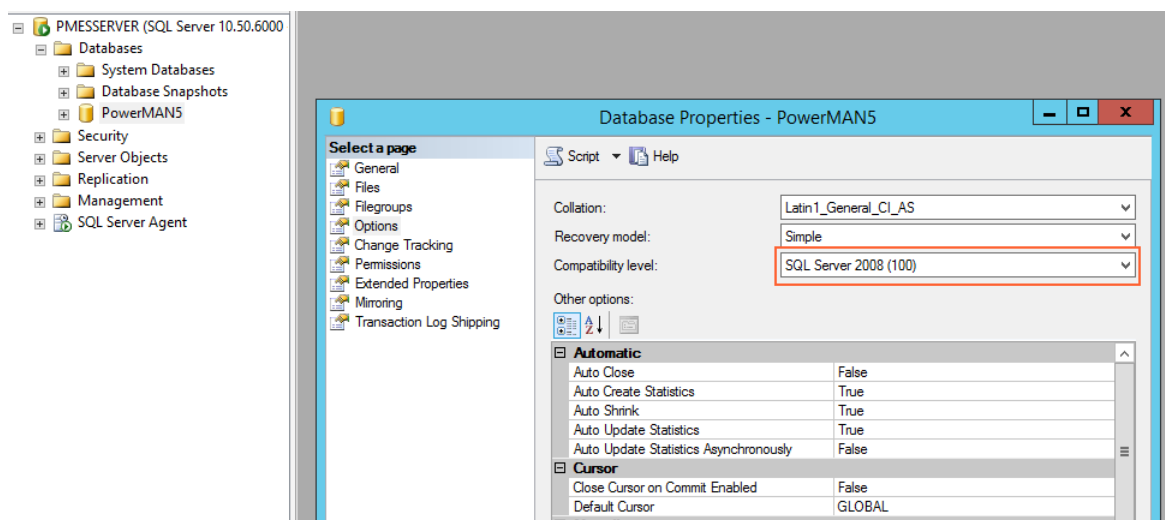
To upgrade from PowerMAN Enterprise Server v5.4.x to v5.5 it is necessary to update both the website and the underlying PowerMAN database.

To upgrade the website please follow the procedure below:

1. Backup the existing website and, if possible, save / print the “web.config” configuration file for reference
2. Delete the existing website
3. Follow the procedure above to install a new PMES website and configure it appropriately. In some cases, it may be useful to refer to the previous “web.config” configuration file.
4. Temporarily, disable the website (for instance, stop it using IIS Manager or use the Offline.htm file) before proceeding with the database update below.

A script is supplied in the **Advanced** folder of the PMES distribution to update the PowerMAN database to the new format. To update the database, please proceed as follows:

1. Confirm the website has been temporarily disabled
2. Open SQL Server Management Studio
3. Expand the treeview on the left hand side to show the available databases
4. Determine the name of the existing PowerMAN database. It is normally called **PowerMAN5**. If the database name is not PowerMAN5 then the update script must be amended accordingly. This is explained further below.
5. Right click on the database (e.g. PowerMAN5) and select **Properties**
6. Select the **Options** page and check the database **Compatibility Level**. In previous releases, this may have been 80/90. We recommend this is set to 100 now. If necessary, change the Compatibility Level and click **OK**:



7. Right click on the database and select **New Query**

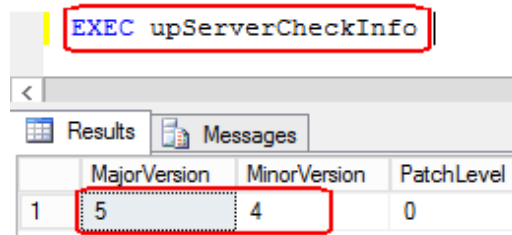
PowerMAN Enterprise Server v5.5

- Enter the command:

```
EXEC upServerCheckInfo
```

- Click **Execute**

- Confirm the database is version 5.4. **This update is NOT suitable for other releases:**



	MajorVersion	MinorVersion	PatchLevel
1	5	4	0

- If not done already, backup the existing database to a safe location
- Open the supplied **PM55 Upgrade.sql** script file. This is located in the **Advanced** folder of the PMES distribution.
- If necessary amend the database [name], contained in square brackets, located at the top of the script (see diagram below):

```

/*
PowerMAN Enterprise Server Upgrade Script

Update PMES 5.4.x DB to 5.5.4 DB

(c) Data Synergy UK Ltd 2008-2022

Notes:

1. This procedure makes minor changes to an existing PMES v5.4.x database and should execute very quickly.
   The script should not be used in any other scenario and should only be executed once.

2. This script does not change the SQL compatibility level. The default for new installations of PMES v5.5.x is 100
   [This level is supported on SQL Server 2008 and later. To change the compatibility level use the following:

USE [PowerMAN5]
GO
EXEC dbo.sp_dbcmptlevel @dbname=N'PowerMAN5', @new_cmptlevel=100
GO

*/
USE [PowerMAN5]
GO

```

- Click **Execute**

- Allow the update to proceed - This may take some time on a larger database. Do not cancel the update.

- Confirm no error was reported:

PowerMAN Enterprise Server v5.5

```
Messages
Altering extended properties
Creating extended properties
Altering permissions on [dbo].[qryClientNetworkAddresses]
Altering permissions on [dbo].[upClientNetworkAdaptersRefresh]
Altering permissions on [dbo].[upSiteChangeParentOrganisationAutoSiteCreationType]
Altering permissions on [dbo].[upClientNetworkAdapterAddUpdate]
Altering permissions on [dbo].[upClientNetworkAdaptersDelete]
Altering permissions on [dbo].[upSiteChangeParentOrganisationChangeAnonymousLoginLevel]
Altering permissions on [dbo].[upLoginHistoryAdd]
Altering permissions on [dbo].[upOrganisationGetAllLoginHistory]
Altering permissions on [dbo].[upServerGetAllLoginHistory]
Altering permissions on [dbo].[upSiteChangeHideClients]
Altering permissions on [dbo].[upSiteGetBestWorstClientUtilization]
Altering permissions on [dbo].[upOrganisationGetAllNotifications]
Altering permissions on [dbo].[upNotificationCreate]
Altering permissions on [dbo].[upNotificationDelete]
Altering permissions on [dbo].[upNotificationUpdateHomeSite]
Altering permissions on [dbo].[upNotificationUpdateDisabled]
Altering permissions on [dbo].[upNotificationUpdateSalutation]
Altering permissions on [dbo].[upNotificationUpdateDatePartCode]
Altering permissions on [dbo].[upNotificationRecordRun]
Altering permissions on [dbo].[upServerGetPendingNotifications]
Altering permissions on [dbo].[upSiteGetMonthlyStatusSummary]
The database update succeeded
```

<

✔ Query executed successfully.

17. Re-enable the PowerMAN website
18. Confirm the database and website function as expected

Tips: The database upgrade is an advanced operation and may take some time to execute. If you are not familiar with Microsoft SQL please contact Technical Support for assistance.

Following the update, the first report may take some extra time to display. Please be patient and, if necessary, click refresh to try again.

Appendix C: Very large (>50k workstations) deployments

In very large PowerMAN deployments we recommend that the following SQL database script is executed prior to production deployment.

This modifies the PMES database to (conservatively) support over 50,000 workstation data years (the data generated by 50,000 workstations in one year). This modification has a small server performance penalty and is therefore not enabled by default. This modification is not recommended for systems with less than 10,000 workstations.

To perform this update proceed as follows:

1. Open SQL Server Management Studio
2. Open a new query window
3. Paste in the SQL script below
4. Click Execute
5. Confirm no error messages are reported

```
USE PowerMAN5  
GO
```

```
ALTER TABLE tblClientStatusDetail  
DROP CONSTRAINT PK_tblClientDetail
```

```
ALTER TABLE tblClientStatusDetail  
ALTER COLUMN ClientStatusDetailId BIGINT NOT NULL
```

```
ALTER TABLE tblClientStatusDetail  
ADD CONSTRAINT PK_tblClientDetail PRIMARY KEY (ClientStatusDetailId)
```

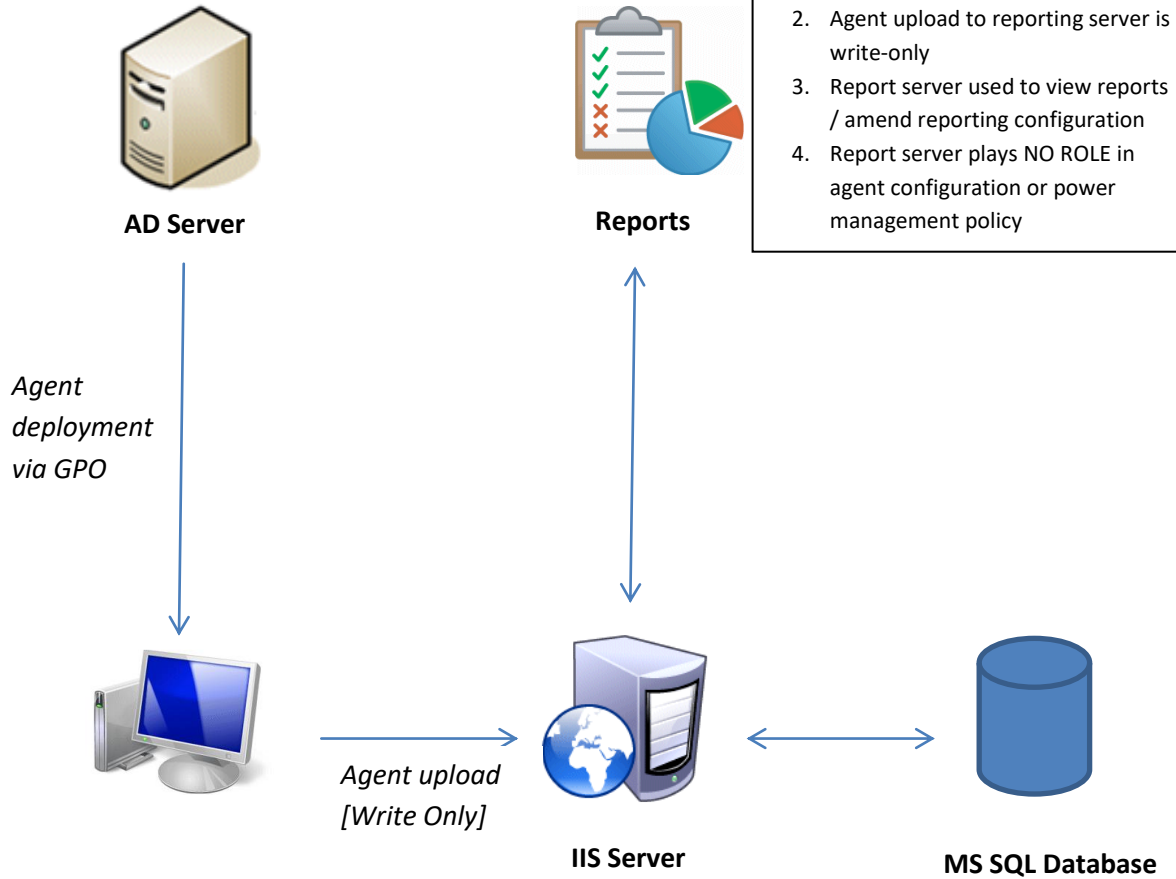
```
ALTER TABLE [dbo].[tblClientStatusDetail] WITH CHECK ADD CONSTRAINT  
[FK_tblClientStatusDetail_tblClient] FOREIGN KEY([ClientId])  
REFERENCES [dbo].[tblClient] ([ClientID])
```

```
ALTER TABLE [dbo].[tblClientStatusDetail] CHECK CONSTRAINT  
[FK_tblClientStatusDetail_tblClient]  
GO
```

Tip: This script can be run at any time but will take a considerable time to execute on an existing large database. It will only take a few seconds to execute on an empty database and is therefore best run prior to production deployment.

Appendix D: PowerMAN System Architecture

PowerMAN Agent & Server Architecture



Appendix E: PowerMAN Authentication API

PowerMAN Enterprise Server v5.2.5 introduced an external user authentication API.

Authentication API Operation

The authentication API may be used to integrate existing intranet systems with the PowerMAN reporting system. The authentication API is available on the hosted (cloud) based system provided by Data Synergy and selected solution resellers. **This feature is not available on private PMES installations running in Windows integrated authentication mode.**

The authentication API is exposed as two simple web services:

Method	Explanation
Query String	<p>A username and password may be passed to the API by using the Username and Password parameters in the query string. For instance the following HTTP GET request:</p> <p>e.g. http://yourserver/loginapi.aspx?Username=fred&Password=12345</p> <p>This is less secure than HTTP POST but may be acceptable for internal intranet solutions. This approach is not recommended for the (hosted) PMES system over the public internet.</p>
HTTP POST	<p>A username and password may be passed to the API by POSTing the data to the target page. This approach is more secure than the simpler query string approach as the login data is not visible to the user. For instance the following HTTP POST request:</p> <p>e.g. http://yourserver/loginapi.aspx Content: Username=fred&Password=12345</p>

Authentication API Output

The API is implemented as a simple web service.

- On success, it return `OK`: followed by a URL to redirect the user to (in the current session):

`OK:/SiteSummary.aspx?SiteGUID=e4f3d29b0b444293b58aa4d9d245efff`

- On failure, it returns `ERR`: followed by a brief explanation:

`ERR:Unsuccessful logon`

Testing Authentication API

A test page is provided to test queries to the login API. To access the page visit:

<http://yourserver/logintest.aspx>

To use the test page proceed as follows:

1. Open the logintest.aspx page
2. Enter appropriate username and password details
3. Click the QS button to simulate logon via the query string method
4. Click the POST button to simulate logon via the POST method
5. The page displays the API result

email/username

.....

Logon QS
Logon POST

Demand Reporting API Authentication

The on-demand reporting API may be used to “pull” reports from the reporting system. This may be used to automate or script report requests. The on-demand API is fully integrated with authentication API. This has the following consequences:

Authentication Required	Consequence
No	Anonymous access to “pull” reports is available. It is not necessary to authenticate. NB: Anyone with the appropriate SiteGUID can download reports
Yes	The authentication API must be used prior to making a report request.

Appendix F: SQL Server Default Installation Procedure

PowerMAN Enterprise Server currently supports Microsoft SQL Server 2008 and later. The installation walkthrough in this guide assumes the SQL Server has been installed using a default configuration. The procedure below explains how to install SQL Server (2019) in such a configuration. The procedure for other SQL Server releases is very similar.

The current edition of SQL Server / SQL Server Express can be downloaded here:

<https://www.microsoft.com/en-us/sql-server/sql-server-downloads>

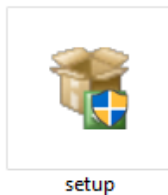
The current release of SQL Server Management Studio can be downloaded here:

<https://learn.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms>

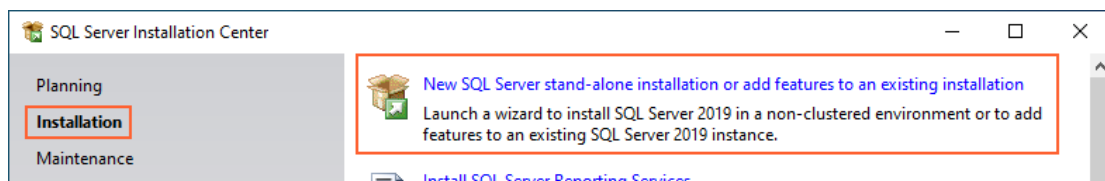
SQL Server Installation Walkthrough

To install SQL Server / SQL Server Express 2019 with default settings, please proceed as described below. A similar procedure can be used for other SQL releases:

1. Login using an account with Administrator rights.
2. Launch the SQL Server setup program:



3. When prompted, click **Installation** and **New SQL Server stand-alone installation**:

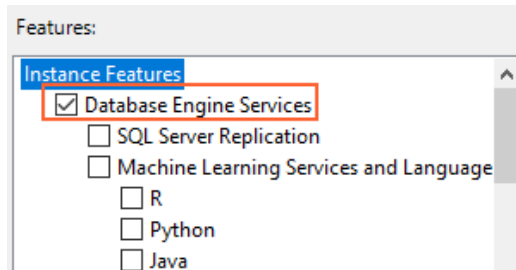


4. If prompted, select the desired SQL Server edition and/or enter your product key and then click **Next**.
5. Accept the license and then click **Next**.
6. If prompted, select the appropriate update configuration and click **Next**.
7. Review the installation rules (prerequisites), resolve any missing components / problems and click **Re-Run** or **Next**:

NB: The wizard may warn about the firewall configuration. SQL Server typically requires [port 1433](#) to be open for remote management. This port is not required if remote access is not required.

PowerMAN Enterprise Server v5.5

8. If prompted, select **SQL Server Feature Installation** and click **Next**.
9. Select the **Database Engine Services** component:



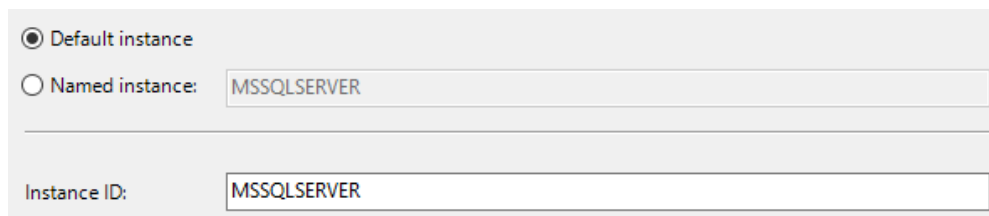
10. If available, select the **Management Tools – Complete** component and then click **Next**:

- Management Tools - Basic
- Management Tools - Complete

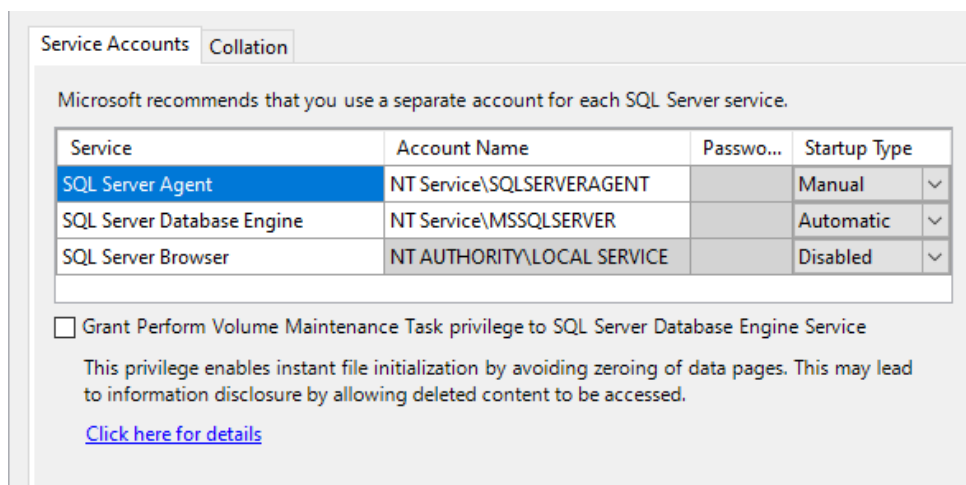
NB: This is not available in SQL Server 2016 and later. This requires a separate installation of SQL Server Management Studio (see below)

11. Select the instance mode – SQL Server supports a single “default” instance and multiple other “named” instance and click **Next**.

NB: PMES supports either case but will require a minor configuration change to support a specific named instance:



12. Confirm the Service Accounts configuration and click **Next**:



Service	Account Name	Passwo...	Startup Type
SQL Server Agent	NT Service\SQLSERVERAGENT		Manual
SQL Server Database Engine	NT Service\MSSQLSERVER		Automatic
SQL Server Browser	NT AUTHORITY\LOCAL SERVICE		Disabled

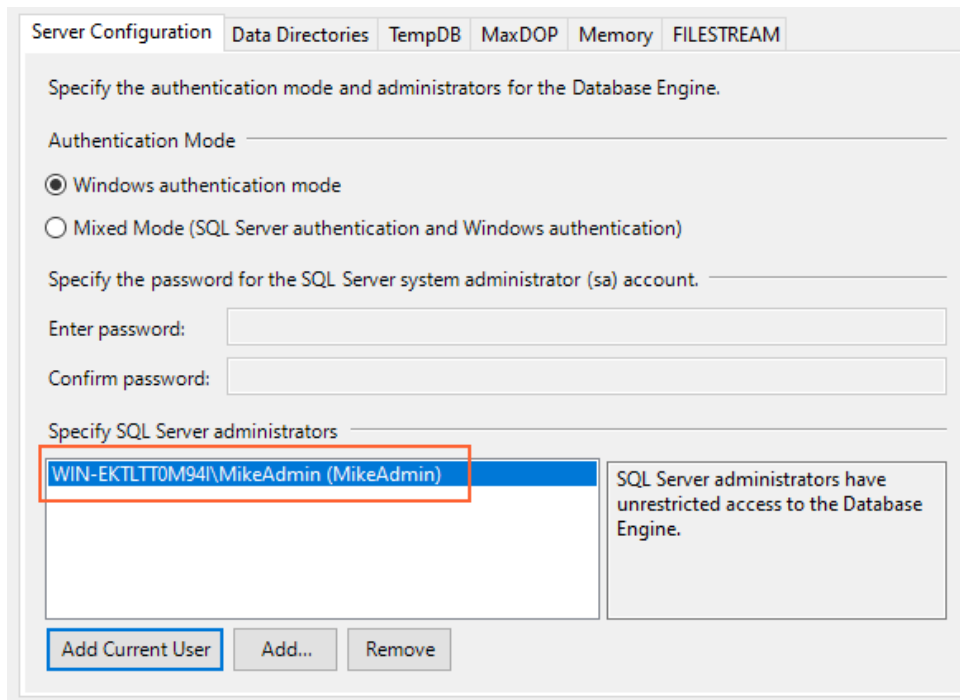
Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service

This privilege enables instant file initialization by avoiding zeroing of data pages. This may lead to information disclosure by allowing deleted content to be accessed.

[Click here for details](#)

PowerMAN Enterprise Server v5.5

- Click **Add Current User** to add yourself to the list of SQL administrators:



Server Configuration | Data Directories | TempDB | MaxDOP | Memory | FILESTREAM

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

Windows authentication mode

Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password:

Confirm password:

Specify SQL Server administrators

WIN-EKTLT0M94!\MikeAdmin (MikeAdmin)	SQL Server administrators have unrestricted access to the Database Engine.
--------------------------------------	--

- Optionally, use the **Add** button to add any other required administrator users and then click **Next**.
- Click **Install** to finalise the installation.
- Click **Close**:

Information about the Setup operation or possible next steps:

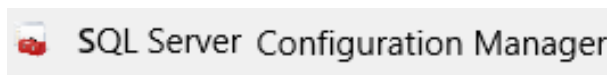
Feature	Status
<input checked="" type="checkbox"/> Database Engine Services	Succeeded
<input checked="" type="checkbox"/> SQL Browser	Succeeded
<input checked="" type="checkbox"/> SQL Writer	Succeeded
<input checked="" type="checkbox"/> SQL Client Connectivity SDK	Succeeded
<input checked="" type="checkbox"/> SQL Client Connectivity	Succeeded

SQL Server Remote Access / Remote PMES (IIS) website

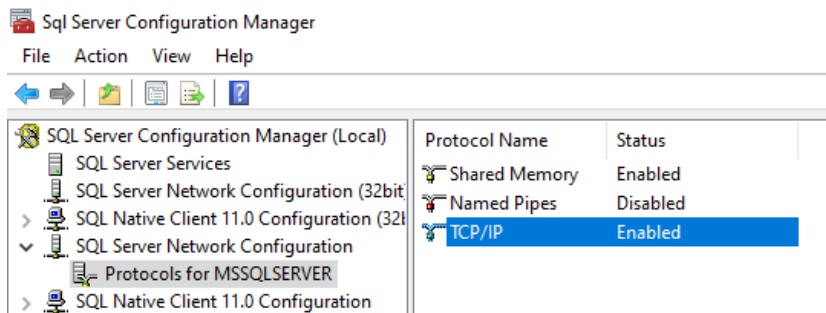
SQL Server supports remote administration but, for security reasons, this is disabled by default. If you wish to access the SQL Server remotely or host the PMES website on another computer, it will be necessary to enable remote access.

The typical process to enable remote SQL access is as follows:

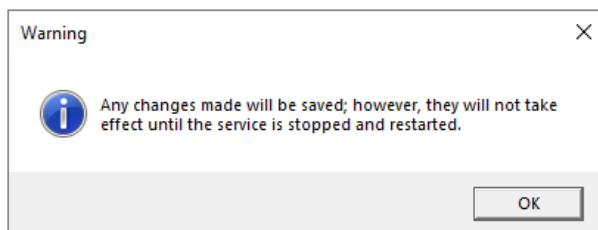
1. Login to the server using an account with Administrator rights.
2. Launch the **SQL Server Configuration Manager** tool (SQLServerManagerXX.msc)



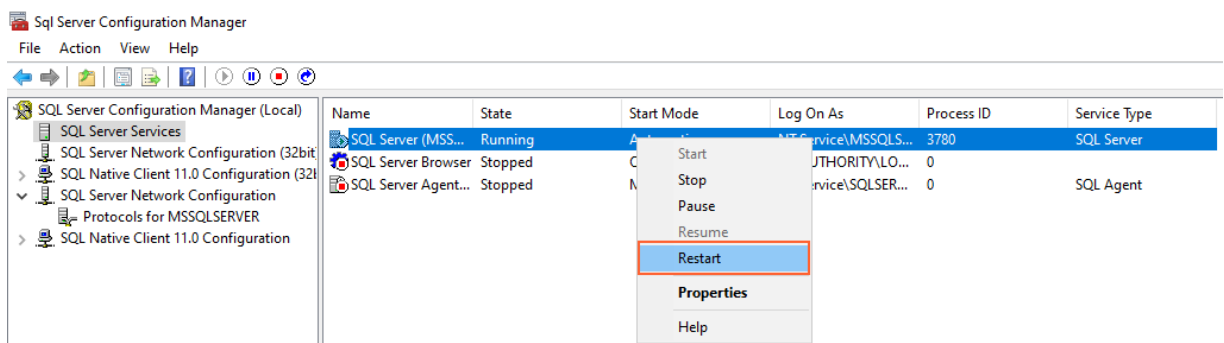
3. Navigate to **SQL Server Network Configuration**, expand the instance name, select TCP/IP, right click and select **Enable**:



4. The software will report that any changes require the SQL Server to be restarted:



5. To complete the process, navigate to **SQL Server Services**, select the SQL Server instance, right-click and select **Restart**:

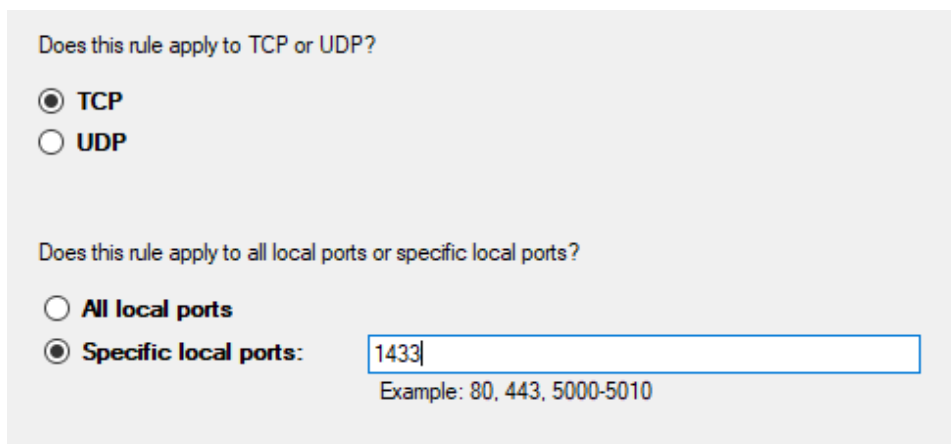


PowerMAN Enterprise Server v5.5

Firewall Configuration for remote SQL Server

Windows Server includes a built-in firewall. If this feature is enabled, a firewall rule must be created to permit the remote SQL Server access. To create a rule, proceed as follows:

1. Open **Windows Firewall with Advanced Security** (WF.MSC)
2. From the left-hand menu, select **Inbound Rules**
3. From the right-hand menu, select **New Rule**
4. Select **Port** and click **Next**
5. Enter the port number (typically 1433):



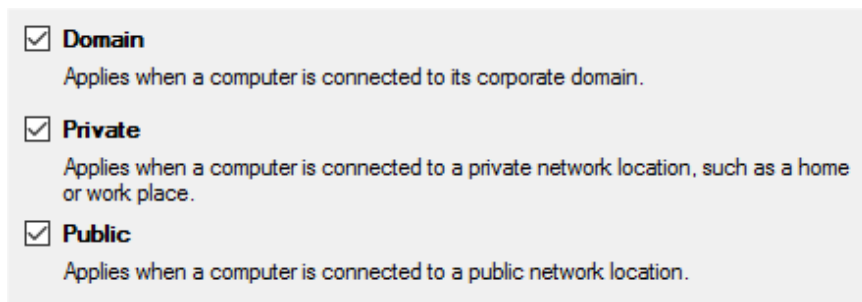
Does this rule apply to TCP or UDP?

TCP
 UDP

Does this rule apply to all local ports or specific local ports?

All local ports
 Specific local ports:
Example: 80, 443, 5000-5010

6. Select **Allow the connection** and click **Next**
7. Select the desired **Profiles**:



Domain
Applies when a computer is connected to its corporate domain.

Private
Applies when a computer is connected to a private network location, such as a home or work place.

Public
Applies when a computer is connected to a public network location.

8. Click **Next**
9. Enter a name e.g. **MS SQL**
10. Click **Finish**

SQL Server Management Studio (SQL 2016 and later)

The SQL Server Management Studio (SSMS) can be installed on the server or on another workstation to perform remote administration.

In SQL Server 2014 and earlier, the SSMS tool was included in the main SQL Server installation. In SQL Server 2016 and later, the tool is no longer included and must be installed separately.

To install SSMS, proceed as follows:

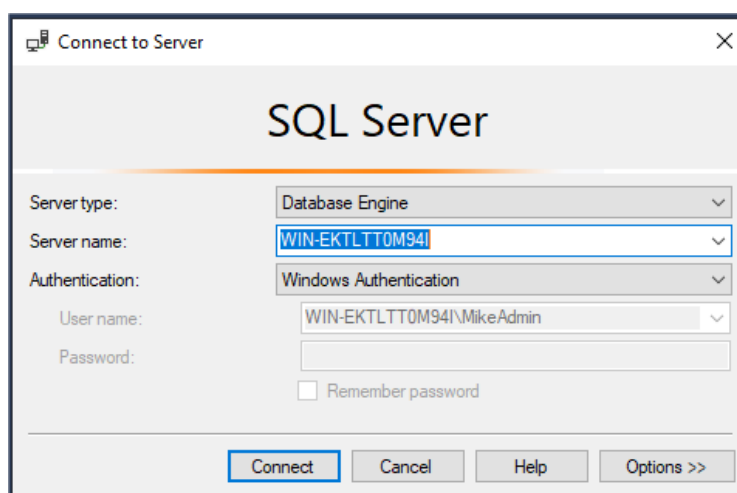
1. Launch the SSMS setup program:



2. Click **Install**
3. If prompted, click **Restart** to restart the computer

To use SSMS, proceed as follows:

1. Login using an account with SQL Administrator rights (granted when SQL Server was previously installed)
2. Launch the SQL Server Management Studio application (SSMS.exe)
3. Select the target server name (or localhost) and click **Connect**:



PowerMAN Enterprise Server v5.5

4. Expand the left-hand tree and perform the desired database administration task(s):

