



WakeMyPC Enterprise Server v5.2

Installation and Administration Guide

Release 5.2 January 2018

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

Website: www.datasynergy.co.uk
Email: sales@datasynergy.co.uk
Telephone: 08456 435 035

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

Contents

WakeMyPC Enterprise Server Installation and Administration	6
Overview.....	6
Relationship with Data Synergy PowerMAN power management software	7
Wake-on-LAN Technology and complementary tools.....	8
New in WakeMyPC Enterprise Server v5.2	8
Prerequisites	10
Deployment Prerequisites	10
Deployment Components.....	10
Deployment Assumptions.....	11
Getting Started	11
SQL Database Configuration Walkthrough	12
SQL Server 2008 Database Procedure	12
SQL Server 2014 (and later) Database Procedure	16
Internet Information Services (IIS) Configuration Walkthrough	18
Windows Server 2008 IIS Setup Procedure.....	18
Windows Server 2012 (and later) IIS Setup Procedure	19
Installing WakeMyPC Server Website	22
Website installation procedure	22
Securing website with SSL (https) procedure	26
Advanced SQL Server Configurations	30
Using a remote SQL Server	30
Using a named instance SQL Server	32
Configuring WakeMyPC Server Website	32
Basic web.config settings	32
Wake-up configuration web.config settings.....	33
Email configuration web.config settings	35
Advanced web.config settings.....	36
Minimal web.config settings	37
Configuring WakeMyPC Enterprise Server Logging	38

Securing access to the WakeMyPC Server Website.....	38
WakeMyPC Server Testing.....	43
Basic Website Testing.....	43
Email Testing.....	43
Database Testing	44
Checking Website Security	45
Checking SMTP Email Configuration.....	46
Temporary Website Maintenance (Server Offline).....	46
Configure WakeMyPC Server for your organisation.....	47
Using virtual sites to group computers (SiteGUID setting).....	47
PowerMAN integration (shared SiteGUID).....	48
Standalone computers (no SiteGUID).....	48
Manual computer registration.....	49
Manual administrative computer wake-up.....	50
WakeMyPC API for scripted or scheduled wake-up	51
Workstation Remote Access, Windows Remote Desktop and Terminal Services Gateway Integration	52
Legacy Remote Desktop Web Connection (Windows Server 2003 and later)	53
Terminal Services Gateway / Remote Desktop Web Connection Integration (Windows Server 2008 and later).....	54
Generic RDP:// Protocol Integration (Most browsers / operating systems)	54
Generic VNC:// Protocol Integration (Most browsers / operating systems)	54
WakeMyPC Workstation Availability Checker (Probe)	55
WakeMyPC Server SQL Database Maintenance.....	56
Database backup strategy.....	56
Database optimization strategy	58
Troubleshooting WakeMyPC Enterprise Server.....	60
Problem: Static test page is not displayed	60
Problem: Website reports – The page cannot be found	60
Problem: Website reports – Server Application Unavailable	60
Problem: /Secure webpage appears blank (and no error is displayed)	60
Problem: .NET Framework v4.0.30319 is not available when creating App Pool	61

WakeMyPC Server Installation and Administration Guide

OR Website reports - The current identity does not have write access to ...Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files.....	61
OR Website reports - The current identity does not have write access to ...Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files.....	61
OR "The page cannot be found" error message when you request an ASPX page.....	61
OR "HTTP Error 404 - File or Directory not found" error message when you request an ASPX page	61
Problem: Servercheck.aspx takes excessive time (>1 second) to display.....	61
OR Servercheck.aspx reports - An error has occurred while establishing a connection to the server (or similar)	61
Problem: Website reports - Sorry. A website error was detected. This cause of this error has been logged and will be investigated	62
Problem: Non-specific database connectivity problem.....	63
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	63
Problem: Website displays - Service Unavailable.....	64
Problem: The website reports an exception obtaining permission of type 'System.Web.AspNetHostingPermission'	64
Problem: Unrecognized attribute "targetFramework" reported when you request an ASPX page.....	65
OR <compilation debug="false" targetFramework="4.0"></compilation>	65
Problem: Website generated URLs fail to work correctly.	65
OR Website URLs contain additional, unrecognised symbols, such as %20.....	65
Problem: Website reports error 'Cannot find the object upClientRemoveStale, because it does not exist or your do not have permission'	65
Problem: The WakeMyPC website does not operate correctly with Internet Explorer 10	65
Problem: Target computer(s) wake-up but WakeMyPC does not recognize this and keeps attempting wake-up before timing out.	66
Appendix A – Data Synergy Remote Desktop Launcher	67
Overview.....	67
WakeMyPC Server Configuration	67
Appendix B – WakeMyPC Agent Data Protocol	68
XML Protocol.....	68
Appendix C – Supported WakeMyPC parameters (API)	69
Appendix D – Authenticating Workstation Wake-up	71
Enabling Authentication.....	71
Configuring IIS Integrated Windows Authentication.....	71
Using an external authentication provider.....	74
Appendix E - WakeMyPC Database Creation Script	75
Appendix F – Upgrade existing WakeMyPC v5.1.3.x server	76

WakeMyPC Enterprise Server Installation and Administration

Overview

WakeMyPC Enterprise Server provides a convenient way for both users and IT staff to remotely power-on or wake-up workstations via a simple web interface. This allows workstations to be powered-off (or in a low-power mode) when not required.

A common application for WakeMyPC is to maximize the benefits of workstation power management whilst also allowing workstations to be accessed whenever necessary. This removes a common barrier to effective power management and can deliver significant additional energy savings.

WakeMyPC Enterprise Server suite consists of three distinct components:

WakeMyPC Server is a web-based system providing:

- Ad-hoc workstation wake-up based upon computer name or recent user name
- Ad-hoc workstation wake-up by workstation group
- Scheduled workstation wake-up compatible with the Windows Task Scheduler
- Persistent workstation information storage database – avoiding manual re-input
- Optional integration with Data Synergy PowerMAN and PowerMAN Enterprise Server

WakeMyPC Agent is an optional component that automatically collects relevant workstation information and periodically uploads it to the WakeMyPC Server. This avoids the need to manually populate the WakeMyPC Enterprise Server with workstation information and also ensures that this information is always current. The WakeMyPC Agent is designed to impose minimal demands upon the enterprise network and will typically upload information that has changed since the last upload.

Remote Desktop Launcher is an optional internet protocol handler for the RDP:// protocol. This may be installed on end-user workstations and allows the Microsoft Terminals Services Client tool (MSTSC) to be conveniently launched from a suitably encoded HTTP page hyperlink.

Tip: WakeMyPC was originally codenamed “WakeMAN”. Technical references to WakeMAN refer to the WakeMyPC product. Previous editions of WakeMyPC supported a “Lite” edition for use specifically with Data Synergy’s PowerMAN product. Support for this SKU has now been discontinued and the features combined into the full Enterprise Edition product.

This document explains how WakeMyPC Enterprise Server operates and provides a full walk-through installation procedure. The instructions below are intended for a system / network administrator with experience 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.

The walk-through describes an installation on a typical Microsoft Windows Server 2008 or later system running IIS and MS SQL 2008 Standard Edition or later. It assumes that each of these products has been installed using the default settings. It also assumes that the server is only used for the WakeMyPC server platform. WakeMyPC has relatively low resource requirements and can co-exist on a server hosting other services. 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.

Further documents are available for:

- **WakeMyPC Operations Guide** - explains how to use the WakeMyPC Server software.
- **WakeMyPC Agent Installation Guide** – explains how to deploy the optional agent software
- **Wake-on-LAN Explained** - discusses WoL network implementation issues in further detail.

Tip: We strongly recommend that you read this entire guide before commencing a WakeMyPC Server deployment.

Relationship with Data Synergy PowerMAN power management software

Data Synergy's PowerMAN product is an ideal companion to a WakeMyPC deployment. PowerMAN is an advanced software product giving organisations of all sizes a simple and effective solution to manage PC running costs. PowerMAN complements the built-in power management features of Microsoft Windows® by providing:

- Comprehensive, centralised, configuration of PC power management
- Web-based, organisation-wide reporting of PC usage and costs

PowerMAN's innovative approach allows PC power features to be simply managed using familiar Windows tools. This dramatically reduces implementation time and delivers rapid results. PowerMAN's unique web-reporting system allows both IT and non-IT staff to monitor progress and identify areas for improvement.

PowerMAN is very lightweight and scales very well. The client software (power policy implementation) is configured using standard registry based settings or Windows Group Policy. This does not normally require any additional server resources and will scale to the largest Windows based networks with ease. The PowerMAN reporting (server) software is only used for reporting and can handle > 50,000 computers on a single server. PowerMAN has minimal bandwidth requirements and is designed to work alongside exist proxy and firewall systems. Typically, less than 500 bytes of network traffic is generated per client PC per day and around 1MB of data is logged per PC per year.

Wake-on-LAN Technology and complementary tools

Traditional Wake-on-LAN (WoL) technology may only be used in small, un-routed, networks and is not suitable for use over the internet. WakeMyPC server overcomes these limitations by implementing a web-based wake gateway.

Data Synergy also provides the following related tools:

- Free **WOLMAN command-line** tool for investigating and debugging WoL. This is included with the WakeMyPC Server and is also available directly from the Data Synergy website
- Commercial **DMCMOS32 utility** for configuring BIOS features, such as WoL, on large numbers of similar computers

New in WakeMyPC Enterprise Server v5.2

This release of WakeMyPC Enterprise Server include a number of changes and bug fixes. These are described in detail in the accompanying release notes. The changes include:

1. WakeMyPC no longer offers a separate “Lite” edition SKU. The unified product is called “WakeMyPC Enterprise Server”.
2. The WakeMyPC website has been redesigned to make better use of wide displays. The original screens were designed for a minimum 800x600 display. Technological developments mean these displays are now rare and consequently WakeMyPC is now designed for a minimum 1024x768 display. This removes the white side bars that were present on some systems.
3. WakeMyPC no longer requires separate 32-bit and 64-bit installations. This change reduces the installation footprint and simplifies the installation procedure. It also removes the install dependency on the Microsoft VC++ Runtime and PowerLib.dll. The software will automatically run in 64-bit mode when available.
4. This WakeMyPC Server installation guide has been updated to simplify website security configuration. Specific sections are now included for Windows Server 2012 and SQL Server 2014 and later.
5. An updated WakeMyPC Agent (WMCLIENT.EXE) is included. This supports Windows 10.0 RTM, provides a native 64-bit executable and SSL support. Full details of the v5.2.0 agent are listed in the separate agent release notes and install guide.
6. The most recent username is now displayed against each workstation. A complete list of recently logged on users is available on the ComputerSchedule.aspx page.
7. The most recent registered network card MAC address is now displayed against each workstation. A complete list of MAC addresses associated with the workstation is available on the ComputerSchedule.aspx page.
8. Wildcard searches are now optionally supported. This feature should be disabled on multi-domain servers to prevent cross domain searches.

9. Scripting support has been expanded by the addition of the optional ?Wake parameter to several website pages. Depending on context this will either force an immediate wake-up operation or force a non-JavaScript based (server only) wake operation. To use this parameter append ?Wake=True to the page query string. This feature is supported on the WakeSite.aspx, WakeComputer.aspx and WakeAll.aspx pages. This feature does not require JavaScript and is compatible with scripted wake-up tools such as WGET or similar. Full technical details are listed in an appendix at the end of this document.
10. Multiple workstations can now be awoken in one operation from the SiteSchedule.aspx page. To use this feature select the appropriate workstations and click Wake Selected.
11. Similarly, the WakeSeach.aspx page now allows multiple computers to be woken via the UI - Previously this was only possible when using query based search parameters. If multiple search results are found a new "Wake All" link is displayed.
12. Expanded bookmark support on WakeManual.aspx page for Chrome/Firefox browsers. Clicking Add Favourite now displays a shortcut dialog than can be copied and added the browser bookmarks/favourites. This approach is not required in Internet Explorer which supports in-page addition of favourites.
13. Added option to email quick wake-up link from the /User/WakeSearch.aspx page. This can be used to store the link for subsequent re-use. If a username is known and the EmailWakeDomain setting has been configured then the email address used is prepopulated to be username@EmailWakeDomain. The user may replace this email address with an alternative if appropriate.

Optionally, if the EmailWakeDomain setting is defined and the UsernameRequired setting is True then the email address is locked and the user is prevented from sending the email to an alternative address. The WakeManual.aspx page supports the same behaviour.
14. The WakeSeach.aspx page also now supports an optional WolMode parameter. This may be used to override the default operation mode. The available modes are described in an appendix at the end of this document.
15. The new ManualSearchPermitted setting may be used to disable the search UI. When this feature is disabled (set to False) the wake-up search UI is hidden and the search automatically generated based upon the user identity (if known). This may be combined with the UsernameRequired setting to ensure only authenticated users may perform wake-up operations and they may only proceed to wake-up computers previously associated with that user.
16. The WakeMyPC task log is now disabled by default. This simplifies the installation procedure. When enabled, the task log now supports logging of raw web requests as an additional audit measure. To enable this feature set the LogTaskHistory=True.

Prerequisites

Deployment Prerequisites

WakeMyPC Server has the following requirements:

- A server with at least 2GB of RAM running Windows Server 2008 or later. Larger installations may require more RAM.
- Internet Information Services with ASP.NET support and the Microsoft .NET 4 Framework.
- 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.
- Approximately 1KB of data storage per client workstation. e.g. 20,000 PCs will require approximately 20MB of storage.
- In-house 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.

The Microsoft .NET 4.5.2 Framework (required for Windows Server 2008) can be obtained from here:

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

Deployment Components

WakeMyPC Server is supplied as three components:

- WakeMyPC Website (hosted by Windows IIS). This is supplied as a ZIP file called **WakeMAN5 Website.zip**.
- Enterprise Server WakeMyPC Server master database hosted by MSSQL Server. This component is supplied as an SQL Server backup file called **WakeMAN5 Database.bak**. This must be restored on to your server.

NB: There are other means to distribute a SQL Server based system, however, a SQL database backup neatly encapsulates the more complex methods and is the most trouble free way to achieve a reliable deployment. An alternative SQL Script based deployment mechanism is described in an appendix at the end of this document. This is intended for advanced SQL system administrators.

- The Installation Guide (this document) which describes the system and a walk-through installation.

Deployment Assumptions

The installation walk-through below makes certain assumptions about the server configuration. These are as follows:

- The server prerequisite components are installed using their default settings
- The IIS website is configured to serve content on port **8000**, to allow anonymous access and to use an application pool running in the security context of the '**Network Service**' account
- The same server is used for the SQL database and the website
- 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:

<http://msdn.microsoft.com/en-us/library/aa174516.aspx>

- The SQL database is configured to use the Simple recovery model
- The Network Service account is a member of the database role called 'WMWebsite' – This provides the website with the limited database access necessary to function correctly. This configuration is described below.

WakeMyPC is flexible software and, within reason, can function in a variety of environments. You may choose to re-configure your server to use Windows Integrated Authentication for website access 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 WakeMyPC Server releases.

WakeMyPC 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 WakeMyPC system can be easily backed-up as a single entity and quickly transferred to another hardware platform.

Getting Started

Before starting to deploy WakeMyPC Server 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 WakeMyPC Server distribution files
- A WakeMyPC Server 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 the database files are to be located in C:\Database\WakeMAN5.

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

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

1. Create folder for database files: **C:\Databases\WakeMAN5**
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, MS SQL 2014 and later releases. The basic process is essentially the same and can be easily adapted to other MS SQL Server releases.

SQL Server 2008 Database Procedure

1. Configure the database name as: **WakeMAN5**
2. Select **From Device** and locate the **WakeMAN5 Database.bak** file
3. Select **Options** and modify the **Restore As** path to **C:\Databases\WakeMAN5**

Destination for restore

Select or type the name of a new or existing database for your restore operation.

To database:

To a point in time:

Source for restore

Specify the source and location of backup sets to restore.

☐ From database:

☒ From device:

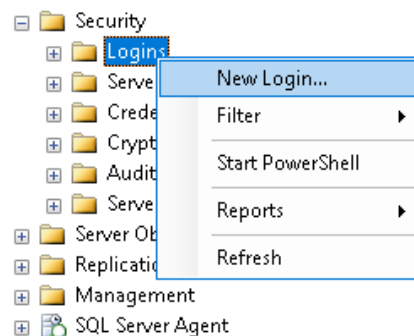
Select the backup sets to restore:

Restore	Name	Component	Type	Server	Database
<input checked="" type="checkbox"/>	WakeMAN5-Full Database Backup	Database	Full	SERVER2008S	WakeMAN5

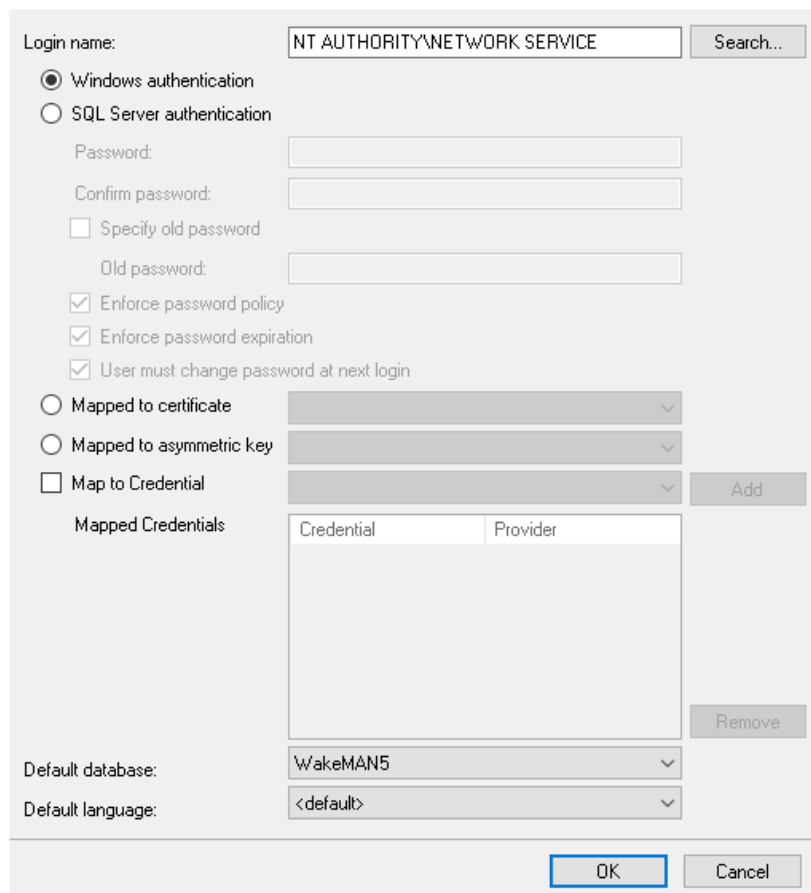
4. Click **OK** to restore the database. On a typical server this will take only a few seconds.

Following database installation (including via the script method described in Appendix E) 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 **WakeMAN5** as the default database
7. Confirm the Network Service account is listed (as shown below) and click **OK** again



Login name:

☒ Windows authentication
☐ SQL Server authentication

Password:

Confirm password:

☐ Specify old password

Old password:

☒ Enforce password policy
☒ Enforce password expiration
☒ User must change password at next login

☐ Mapped to certificate
☐ Mapped to asymmetric key
☐ Map to Credential

Mapped Credentials

Credential	Provider
------------	----------

Default database:
Default language:

8. Navigate to **Databases\WakeMAN5\Security\Users**
9. Right click and select **New User**
10. Click the top search ... button and locate the **Network Service** user
11. Select the **WMWebsite** database role

User name: Network Service

☒ Login name: NT AUTHORITY\NETWORK SERVICE ...

☐ Certificate name: ...

☐ Key name: ...

☐ Without login

Default schema: dbo ...

Schemas owned by this user:

Owned Schemas

<input type="checkbox"/>	db_accessadmin
<input type="checkbox"/>	db_backupoperator
<input type="checkbox"/>	db_datareader
<input type="checkbox"/>	db_datawriter
<input type="checkbox"/>	db_ddladmin
<input type="checkbox"/>	db_denydatareader
<input type="checkbox"/>	db_denydatawriter

Database role membership:

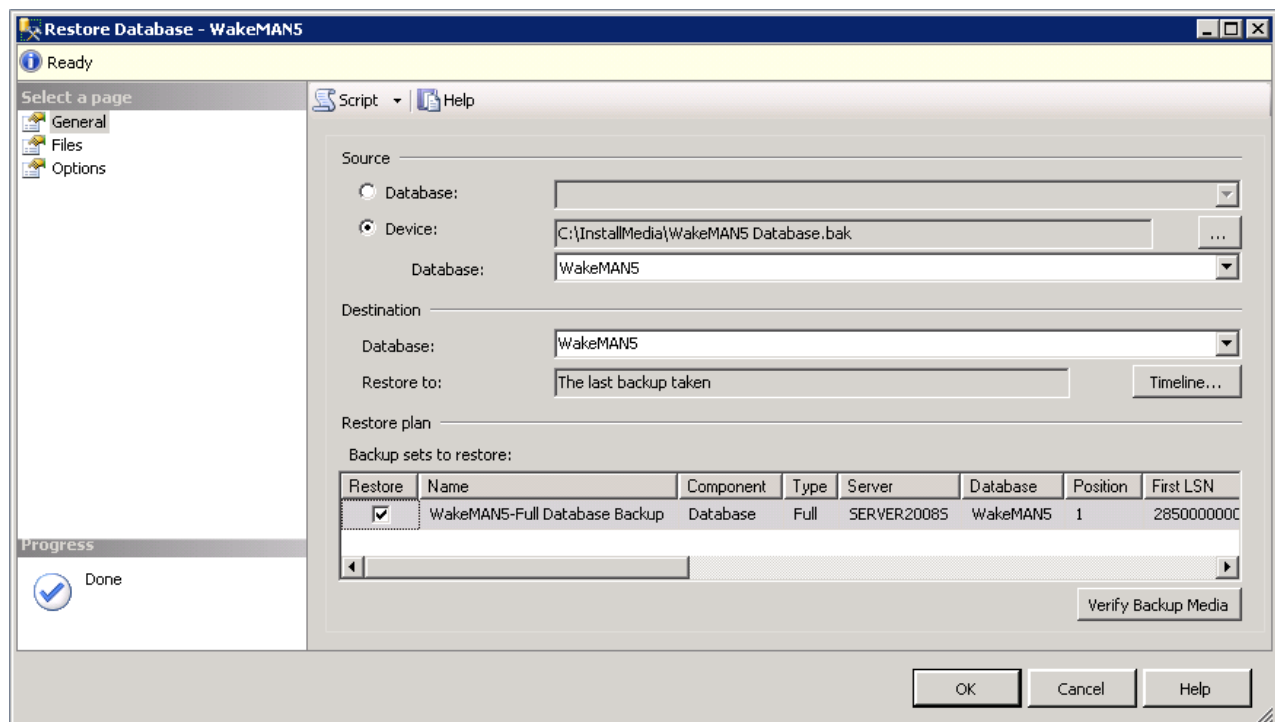
Role Members

<input type="checkbox"/>	db_datawriter
<input type="checkbox"/>	db_ddladmin
<input type="checkbox"/>	db_denydatareader
<input type="checkbox"/>	db_denydatawriter
<input type="checkbox"/>	db_owner
<input type="checkbox"/>	db_securityadmin
<input checked="" type="checkbox"/>	WMWebsite

12. Click **OK**

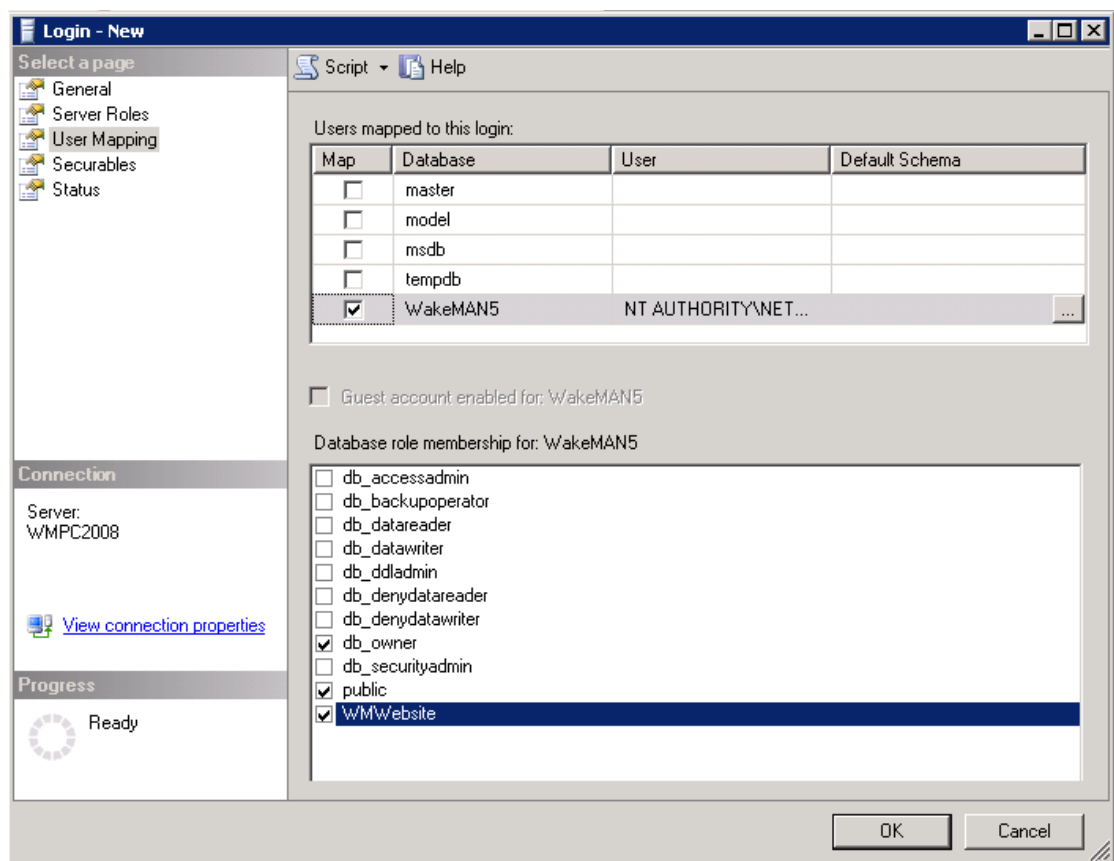
SQL Server 2014 (and later) Database Procedure

1. Select **Device** and locate the **WakeMAN5 Database.bak** file
2. Configure the destination database name as: **WakeMAN5**
3. Select **Files** and modify **Restore As** to **C:\Databases\WakeMAN5**
4. Click **OK** to restore the database. On a typical server this will take just a few seconds



Following database installation (including via the script method described in Appendix E) 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 **WakeMAN5** as the default database
6. Select the **User Mapping** page
7. Highlight the **WakeMAN5** database and tick the **Map** checkbox (see below)
8. Tick the **WMWebsite** role (located at the bottom)
9. Click **OK**



The 'WMWebsite' database role has the limited database access rights to operate the WakeMyPC 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 Server 2008 or later. It assumes that the website files are located in C:\Websites\WakeMAN5.

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.

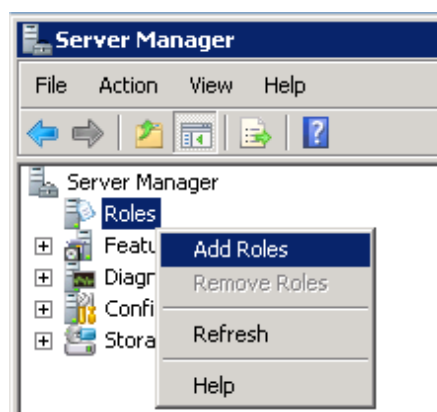
If you deviate from this assumption please remember that the **/Public** folder, as a minimum, must be accessible to the anonymous WakeMyPC clients. The one exception to this is that the **/Secure** folder should be restricted to provide access only to appropriate website Administrators. The procedure for this is described later in this document. 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** and locate **Roles**
2. Right click and select **Add Roles**



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 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"/> 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 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 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 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 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"/> 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 checked="" 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"/> 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>

Tip: If you installed IIS after the .NET Framework you will need to re-register .NET with IIS using the following command:

```
%windir%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -i
```

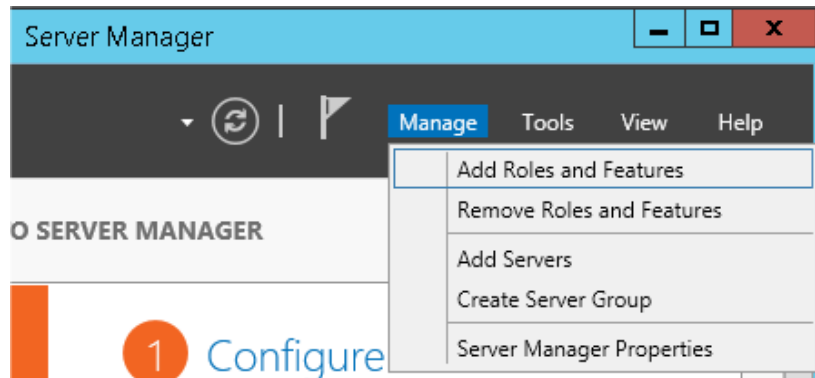
Or, if testing WakeMyPC on a 32-bit system, use the following command:

```
%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -i
```

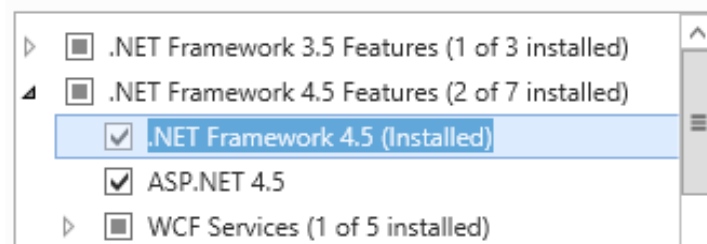
Windows Server 2012 (and later) IIS Setup Procedure

On Windows Server 2012 and later please proceed as follows:

1. Open **Server Manager**
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 4.5** and **ASP.NET 4.5** 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):

<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
---	--

12. Click **Next**

13. Optionally, check **Restart the destination server automatically if required**

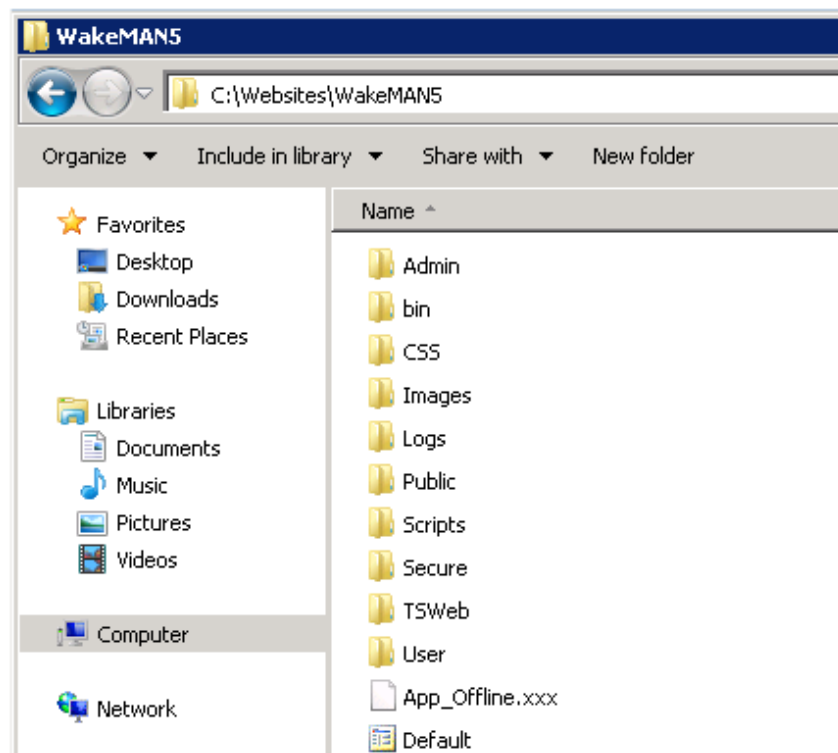
14. Click **Install**

Installing WakeMyPC Server Website

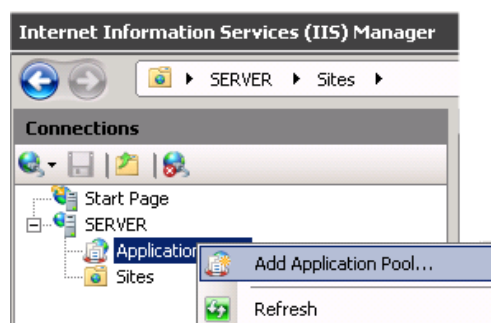
Website installation procedure

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

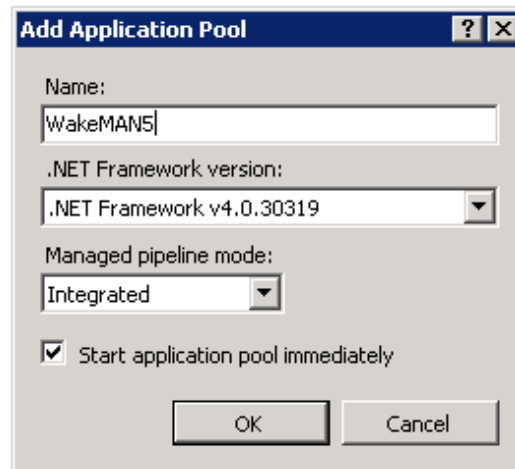
1. Create folder for website files: **C:\Websites\WakeMAN5**
2. Extract the contents of “WakeMAN5x Website.zip” file to this folder:



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**

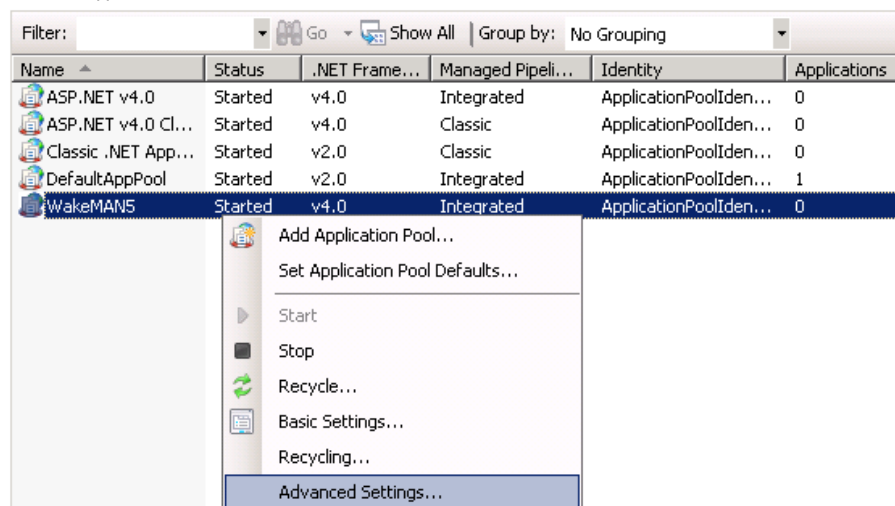



7. Enter the pool name: **WakeMAN5** and select **.NET Framework v4.0.30319** and **Integrated** mode:

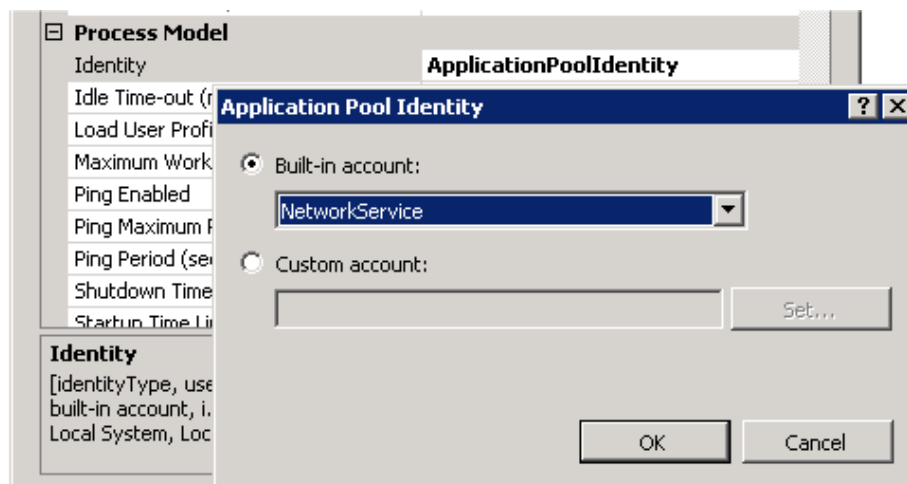


Tip: If .NET v4.0 is not listed this may be because .NET was installed before IIS. Please see the troubleshooting section to resolve this.

8. Click **OK** to close the dialog
9. Navigate to the newly created **WakeMAN5** application pool
10. Right click and select **Advanced Settings**



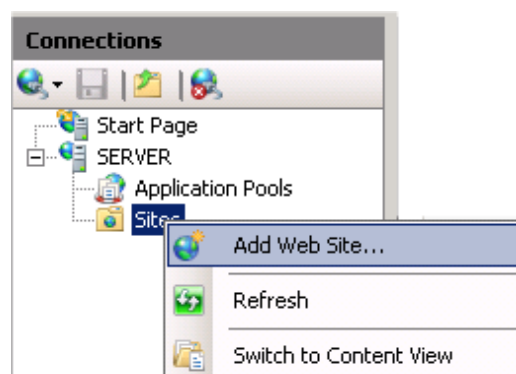
11. Navigate to the **Identity** setting and press 
12. Select **Built-in account: Network Service** and then click **OK**



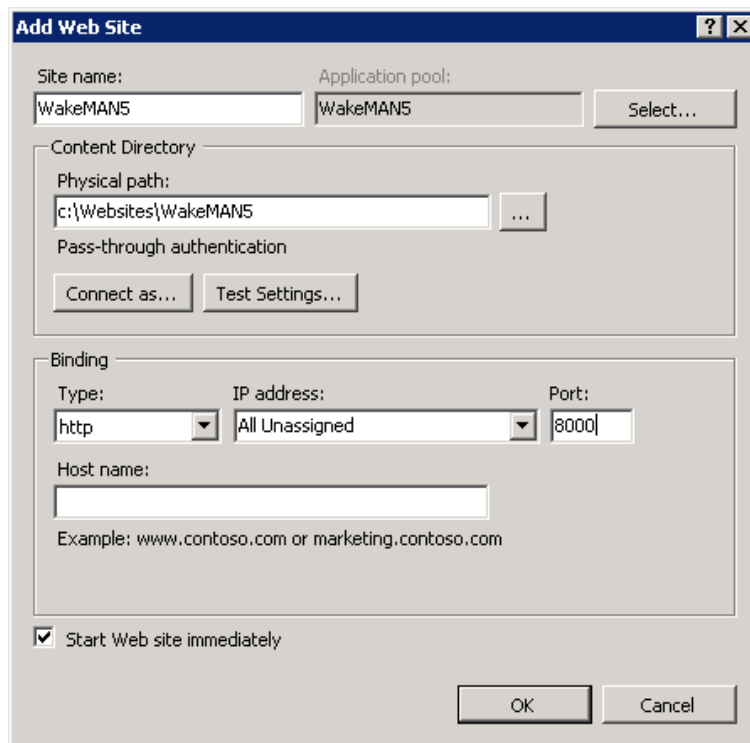
Tip: If the SQL database is located on a remote server you must also change the **Load User Profile** option to **True**:

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**



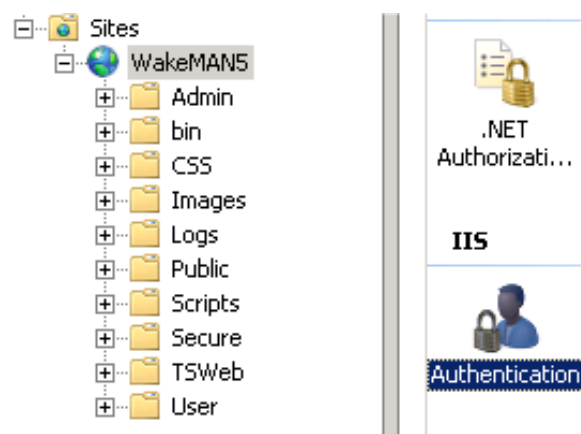
16. Enter the Site Name: **WakeMAN5**
17. Select the Application Pool: **WakeMAN5**
18. Select the appropriate website path, application pool, server IP address range and port number. The default WakeMyPC Enterprise Server port is **8000**. Click **OK**:



The 'Add Web Site' dialog box is shown. It has a title bar with a question mark and a close button. The 'Site name' field contains 'WakeMAN5'. The 'Application pool' dropdown is set to 'WakeMAN5' with a 'Select...' button. The 'Content Directory' section has a 'Physical path' field with 'c:\Websites\WakeMAN5' and a browse button (...). Below it is a 'Pass-through authentication' section with 'Connect as...' and 'Test Settings...' buttons. The 'Binding' section has a 'Type' dropdown set to 'http', an 'IP address' dropdown set to 'All Unassigned', and a 'Port' field with '8000'. There is a 'Host name' field with an example: 'www.contoso.com or marketing.contoso.com'. At the bottom, there is a checkbox 'Start Web site immediately' which is checked, and 'OK' and 'Cancel' buttons.

Important: The website **MUST** be accessible to the computers running the WakeMyPC agent 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 **WakeMAN5** website. In the right hand pane 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:



Authentication

Group by: No Grouping		
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.

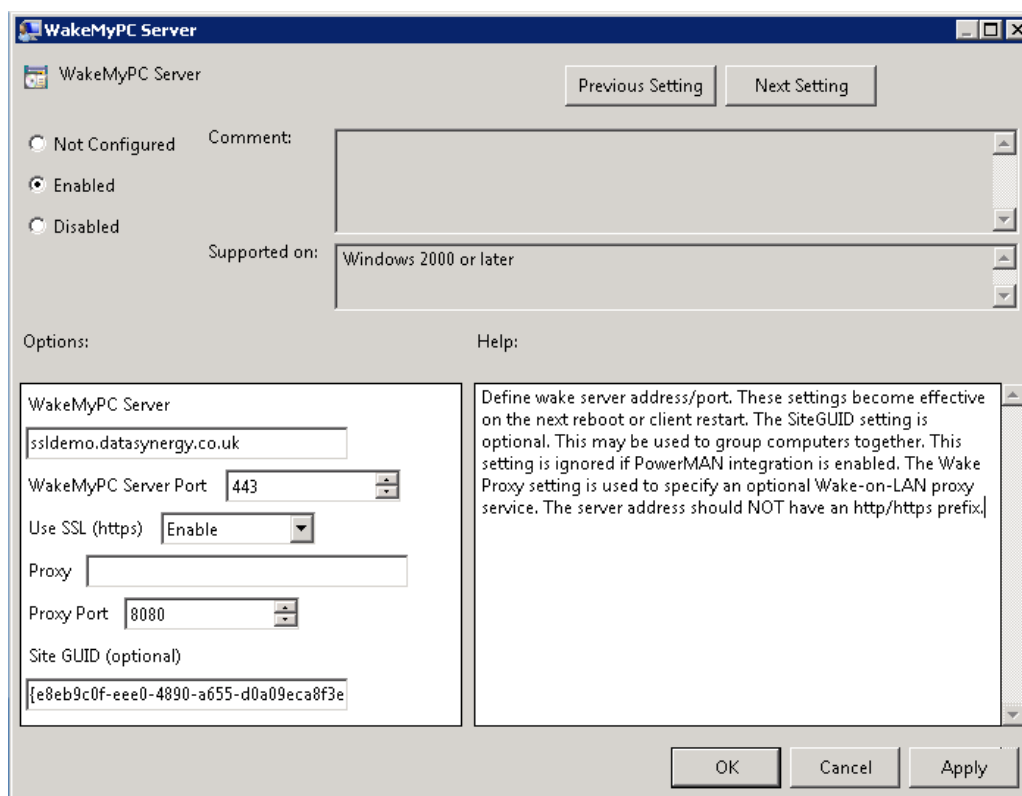
Securing website with SSL (https) procedure

The WakeMyPC website can optionally be secured using Secure Sockets Layer (SSL). This technique encrypts traffic to the website and prevents a network eavesdropper from accessing sensitive information such as workstation network details and user passwords. The additional layer of security may be unnecessary in a strictly controlled corporate network environment but is otherwise highly desirable, especially if the website is accessed over the public internet.

Enabling SSL enhances security in two use cases:

- Encrypts user connections to the website UI (without VPN or similar)
- Encrypts sensitive network and user details transmitted over internet by the WakeMyPC agent

The v5.2 WakeMyPC agent and later supports SSL operation. The feature may be enabled by selecting the SSL option in the WakeMyPC agent settings and changing the port number (typically to 443). This is shown in the screenshot below and described in more detail in the separate agent Admin Guide.



SSL support on the WakeMyPC webserver requires an appropriate server security certificate. This may be purchased from a variety of vendors such as Symantec, GlobalSign, Digicert, Thawte or GoDaddy. In some cases it may also be possible to generate a certificate in-house.

Microsoft describes the procedure to request an Internet Server certificate here:

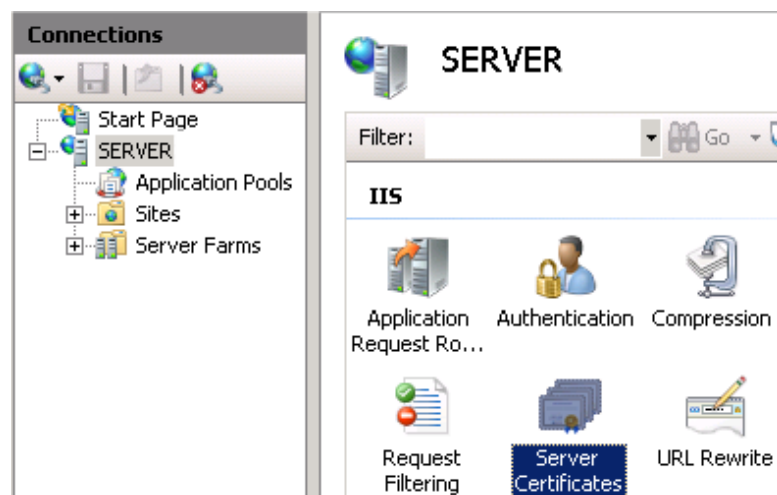
[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732906\(v=ws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732906(v=ws.10))

Similarly, the procedure to install a certificate on IIS7 is described here:

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771816\(v%3dws.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc771816(v%3dws.10))

The remainder of this section describes how to secure the WakeMyPC website using SSL. It assumes the security certificate is already installed on the IIS server. To secure the site, proceed as follows:

1. Open the **Internet Information Services (IIS)** Management tool (INETMGR.EXE)
2. Select the server name in the right hand tree
3. Click on **Server Certificates**:



4. Confirm the required certificate is installed on the server. For instance the following screenshot shows a certificate for the domain `ssldemo.datasynergy.co.uk`:

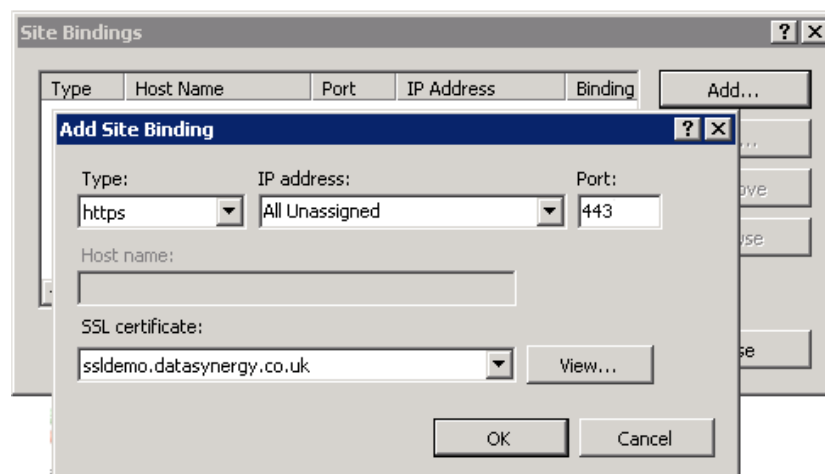


Server Certificates

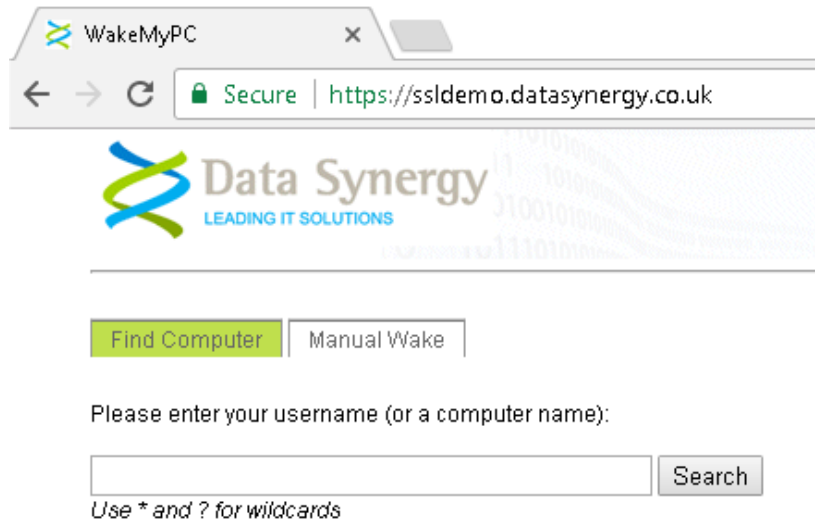
Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By	Expiration Date
ssldemo.datasynergy.co.uk	ssldemo.datasynergy.co.uk	COMCOM RSA Domain Validation...	19/07/2029 00:59:59

5. Navigate to **Websites\WakeMAN5**
6. Right click on the site and select **Edit Bindings**
7. Click **Add**
8. Select **https**, change the port number as required and select the SSL certificate from the drop-down list
9. Click **OK** and then **Close**



10. Open the WakeMyPC website in your browser and confirm it operates as expected with the https:// prefix. For instance:



Tip: It may be desirable to maintain non-https access to the WakeMyPC website inside your corporate network. For instance, this approach would allow older WakeMyPC agents to communicate with site whilst you transition to the v5.2 or later agent. If this facility is not required the http (typically port 80 or 8000) binding can be safely removed from the website.

Advanced SQL Server Configurations

Using a remote SQL Server

The walkthrough steps above describe 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 **WakeMAN**, 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 WakeMAN5 application pool:

8. Open the **IIS Management** snap-in
9. Navigate to the **WakeMAN5** 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 (WakeMAN) account. Click **OK**
14. Enter the appropriate password
15. Click **Apply** and enter the password again

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

WakeMyPC Server Installation and Administration Guide

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\WakeMAN5**
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 **WMWebsite** 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 **WakeMAN5** and click **OK** again
7. Navigate to **Databases\WakeMAN5\Security\Users**
8. Right click and select **New User**
9. Click the top search ... button and locate the domain user account
10. Select the '**WMWebsite**' database role
11. Click **OK**

Using a named instance SQL Server

Microsoft SQL server supports both default and named database instances. This following Microsoft document explains database instances:

<http://msdn.microsoft.com/en-us/library/aa174516.aspx>

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

Data Source=Server\SqlExpress;Initial Catalog=WakeMAN5; Integrated Security=True

Configuring WakeMyPC Server Website

The remaining WakeMyPC Server website configuration is contained in the **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.

Basic web.config settings

Setting	Meaning
RegisteredOrganisation	The name of the registered organisation. For instance: Example Corporation Limited
RegisteredProductKey	The product key. For instance: XGHK-GABQ-GDTH-UJKQ-HYJK-DBKY
ConnectionString	<p>The WakeMyPC server database connection string.</p> <p>For a local (default instance) database this is typically:</p> <p><i>Data Source=localhost;Initial Catalog=WakeMAN5;Integrated Security=True</i></p> <p>For a local database instance called 'SqlExpress' this would be:</p> <p><i>Data Source=.\SqlExpress;Initial Catalog=WakeMAN5; Integrated Security=True</i></p> <p>For a remote database instance called 'SqlExpress' located on a PC called 'Server' this would be:</p> <p><i>Data Source=Server\SqlExpress;Initial Catalog=WakeMAN5; Integrated Security=True</i></p>

Wake-up configuration web.config settings

WakeTimeoutSeconds	<p>The period of time, in seconds, allowed for a wake request before it is abandoned. Typically it will take up to 10 seconds for a computer that is asleep to respond and up to 120 seconds for a computer that is turned off:</p> <p>e.g. 120</p>
WakeRefreshSeconds	<p>The interval, in seconds, between each wake attempt. It may take a short period for a computer to start responding following power-on or wake-up. During this period WakeMyPC will periodically retry the computer to determine if it is available. Setting this value too low will increase the server workload.</p> <p>e.g. 5</p>
WakeConnectURL	<p>The URL used for post-wake activities. This is described further in subsequent sections.</p> <p>e.g. ~/TSWeb/?Server=\$computername\$.fqdomainsuffix&AutoConnect=1</p>
ProbeTimeoutMS	<p>The probe timeout, in milliseconds, to use when checking if a remote workstation is available. This is typically 500ms. Significantly increasing this value will reduce system performance.</p> <p>e.g. 500</p>
ProbeICMP	<p>Enable ICMP (Ping) probe of remote workstations. This should normally be enabled as ICMP provides the most reliable and secure way to determine if a remote workstation is available.</p> <p>NB: The target computer firewall must permit ICMP traffic.</p> <p>e.g. True</p>
ProbePorts	<p>A comma separated list of TCP ports to probe. It is recommended that this is used to complement the ICMP probe method in environments where ICMP may be disabled or blocked by intermediate firewalls. Generally ICMP is preferable. The list of ports should be restricted to only those ports absolutely necessary.</p> <p>e.g. 445, 3389</p>
ProbeAddressingMode	<p>The host addressing mode that should be used during probe operations. Supported values are:</p> <ul style="list-style-type: none"> 1 = Use IP address 2 = Use unqualified computer name (default) 3 = Use fully qualified computer name (requires FQDomainSuffix) <p>Generally the default option (2) will be sufficient for a corporate network with functioning DNS. The IP address option is useful for networks without functioning DNS. The fully-qualified option</p>

	allows the WakeMyPC server to be operated externally.
FQDomainSuffix	<p>The fully qualified internet domain suffix for the host network. This is required for off-network workstations to directly connect to internal workstations (where permitted by the network). This setting should not be prefixed by a dot character:</p> <p>e.g. domain.yourcompany.com</p>
DefaultWoLMode	<p>The type of WoL packet to send. The available options are:</p> <p>No wake-up. Just probe = 0 Local broadcast = 1 (default) Subnet directed broadcast = 2 Direct (unicast) packet = 3</p>
DefaultWoLPort	<p>The TCP/UDP port to which WoL requests should be directed. In most installations the selection of a port number is not relevant and any port number will function. In some installations a specific port number may be required to conform to local network routing rules or as part of a WoL network security strategy. The default port is 7.</p> <p>e.g. 7</p>
UsernameRequired	<p>Require user authentication to access pages within the /User folder and sub-folders. Optionally, if the <code>EmailWakeDomain</code> setting is also defined and the <code>UsernameRequired</code> setting is <code>True</code> then the email address is locked and the user is prevented from amending their email address. This is <code>False</code> by default.</p> <p>e.g. <code>False</code></p>
UsernameUnknownPage	<p>The page unauthenticated users are redirected to. This feature is only applicable when <code>UsernameRequired=True</code>. A default placeholder page is provided.</p> <p>e.g. <code>~/LoginRequired.aspx</code></p>
WildcardSearchPermitted	<p>Permit wildcards <code>*</code> and <code>?</code> to be used on the <code>/User/WakeSearch.aspx</code> and <code>/User/WakeManual.aspx</code> pages. This is <code>True</code> by default but may be disabled to prevent users abusing WakeMyPC to wake-up multiple computers.</p> <p>e.g. <code>True</code></p>
ManualSearchPermitted	<p>Permits the user to manually search for a target computer to wake-up. When this feature is disabled (set to <code>False</code>) the wake-up search UI is hidden and the search automatically generated based upon the user identity (if known). This may be combined with the <code>UsernameRequired</code> setting to ensure only authenticated users may perform wake-up operations and they may only proceed to wake-up computers previously associated with that user.</p> <p>Tip: If this approach is desired the following configuration is suggested to maximise security:</p> <ol style="list-style-type: none"> Lockdown the /User folder to only permit viewing by

	<p>permitted users. The Installation Guide describes how to do this using NTFS permissions.</p> <ul style="list-style-type: none"> b. Set ManualSearchPermitted=False c. Set WildcardSearchPermitted=False d. Set UsernameRequired=True
--	---

Email configuration web.config settings

BugEmail	<p>The email address to send website error reports to. Please see the section on SMTP server configuration below. This feature is optional.</p> <p>e.g. support@yourcompany.com</p>
WebsiteEmail	<p>The email address to send emails from. Please see the section on SMTP server configuration below:</p> <p>e.g. wakemypc@yourcompany.com</p>
SMTPServer	<p>The SMTP server used for sending emails. This feature also requires that the BugEmail and WebsiteEmail settings are configured:</p> <p>e.g. localhost</p>
SMTPUsername	<p>The username to use for SMTP authentication. This may be blank if authentication is not required.</p>
SMTPPassword	<p>The password to use for SMTP authentication. This may be blank if authentication is not required.</p>
SMTPPort	<p>The TCP port used for SMTP server access. This is normally port 25.</p> <p>e.g. 25</p>
SMTPEnableSSL	<p>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.</p> <p>e.g. False</p>
EmailWakeLink	<p>Allow workstation 'quick link' to be emailed to user. This requires a working SMTP server configuration:</p> <p>e.g. True</p>
EmailWakeDomain	<p>Where a user's name is known, specifies the email domain name that should be appended to the username to generate an email address suggestion for the user.</p> <p>This feature can be used to send an email containing a WakeMyPC link from the /User/WakeSearch.aspx and /User/WakeManual.aspx pages. Where the UsernameRequired setting is True the suggestion is mandatory and cannot be overridden by the user. This feature is optional.</p> <p>e.g. mydomain.com</p>

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	This feature allows detailed error reports to be displayed on the server console. e.g. True
LogTaskHistory	Enable the internal WakeMyPC task log. This can be used to debug wake-up problems and is (from v5.2) disabled by default. e.g. True
CommandTimeoutSeconds	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) e.g. 120
PowerMANConnectionString	The PowerMAN server database connection string. This setting is optional and may be blank if not required. Please see the PowerMAN Installation Guide for further details. Configuring this feature activates PowerMAN integration. This allows sites to be conveniently imported from a PowerMAN server and synchronised with the WakeMyPC server.
PostErrorURL	The fully qualified URL that users will be redirected to in the event of a software error: e.g. http://www.datasynergy.co.uk
LogPath	The relative path to the WakeMyPC event log folder. This is used to record significant runtime events. This should be prefixed with a ~ character: e.g. ~/Logs
LogRetainDays	The number of days to retain WakeMyPC event logs. The minimum period is 30 days: e.g. 90
DataRetainDays	The number of days to retain per-workstation information. The minimum period is 30 days: e.g. 60
SecurePath	The URL of the secure administration folder. This is prefixed with a tilde character: e.g. ~/Secure

Minimal web.config settings

As supplied the web.config must be manually edited to include the settings appropriate for the installation. At a minimum the following settings must be configured:

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

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, WebsiteEmail** and **BugEmail** – This will need to be configured if you intend to use the email features

The web.config file may also include some additional settings not described below. These are used internally by WakeMyPC and should not normally be changed.

Configuring WakeMyPC Enterprise Server Logging

WakeMyPC include an optional internal event logging system to aide in debugger wake-up issues and Technical Support. The event logs are created in text file format in the **Logs folder**. The IIS WakeMAN application pool must have read/write access to this folder. This can be configured as follows:

To configure website access for this folder proceed as follows:

1. Open the IIS Management snap-in
2. Navigate to **Websites\WakeMAN5**
3. Locate the **Logs** folder in the right hand pane
4. Right click and select **Permissions**
5. Click **Advanced**
6. Click **Add** and select user account used by the WakeMAN application pool (typically Network Service)
7. Select **Full Control**
8. Click **OK**
9. Open the website's "web.config" file
10. Locate the **LogTaskHistory** setting
11. Change the setting to **True**
12. Save the "web.config" file

Securing access to the WakeMyPC Server Website

This section explains how to secure the website on Windows 2008 or later.

The WakeMyPC Server website groups functionality into four distinct areas. Each of these is located in a separate website folder and may be independently secured as required. The folders are:

- **/Secure** – Administration tools for initial setup and server maintenance. This is generally only required during initial setup and should not be accessible to standard users.
- **/Admin** – Administration tools for day-to-day administration. This is required for day-to-day WakeMyPC administration and should not be accessible to standard users.
- **/User** – User-driven wake-up and workstation registration pages. This is required for day-to-day user wake-up operations (e.g. self wake-up). Options to secure this folder are described in Appendix D.
- **/Public** – Used by the WakeMyPC agent for data upload. This folder must permit anonymous access.

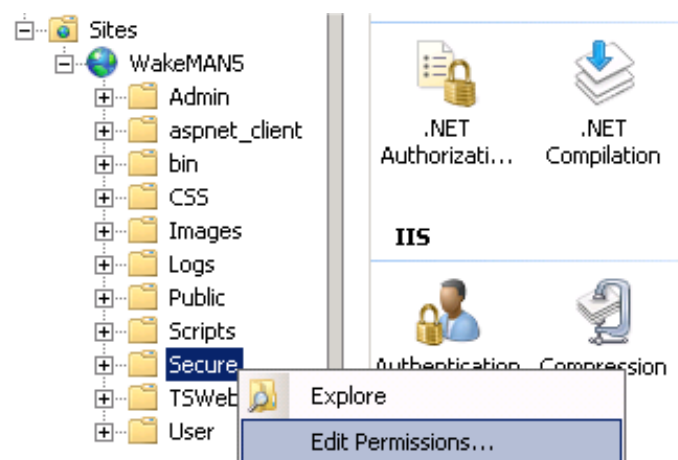
Each of these folders may be secured using IIS Integrated Windows Authentication. This limits access to the users/groups that are specified. In practice most installations will apply strict security to the /Secure and /Admin folders and less (or no) security to the /User folder.

The **/Secure** folder contains tools **only** for administrator use. The pages within this folder are used to perform the initial online server configuration and to administer the WakeMyPC Server system. These pages **MUST be secured** as they must not be available for anonymous access. The same technique may be used to secure both /Admin and, if necessary, the /User folders. We recommend the **/Admin** folder is also secured to prevent unauthorised system changes.

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

To disable anonymous access to the /Secure folder, proceed as follows:

1. Open the **Internet Information Services (IIS)** Management tool (INETMGR.EXE)
2. Navigate to **Sites**
3. Locate the **WakeMAN5** site and expand the folder tree
4. Locate the **Secure** folder, right click and select **Edit Permissions**:



5. Select the **Security** tab
6. Click **Advanced**

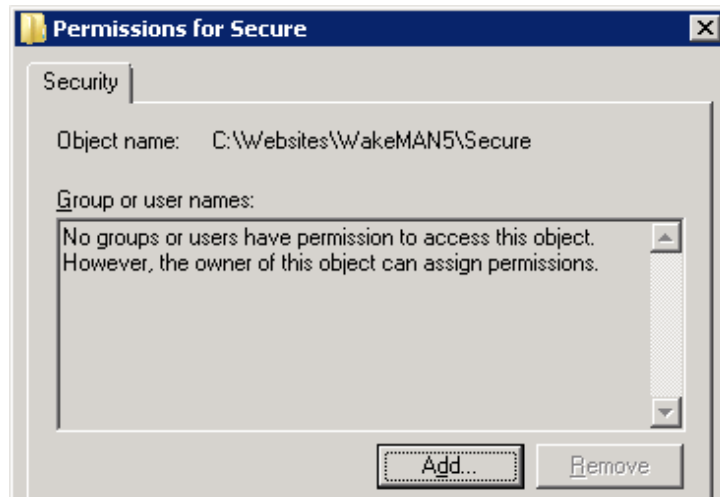
On Windows Server 2008:

7. Click **Changed Permissions**
8. Un-check '**Include inheritable permissions from this objects parent**' and then click **OK** (if prompted by warnings click **Remove** and then **Yes**) and then **OK** again
9. Click **Edit**

On Windows Server 2012 and later:

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

The following dialog should now be visible:



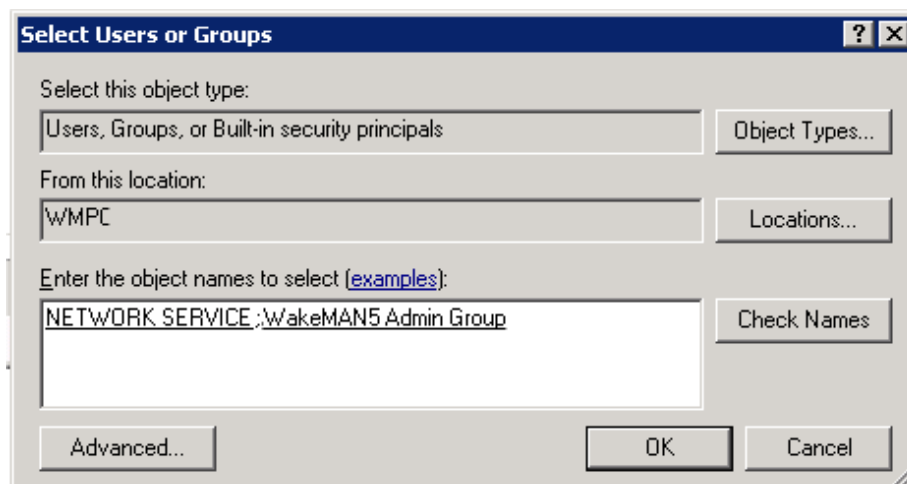
13. Click **Add**

Tip: We recommend you create a specific local group for the WakeMyPC 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. Please remember to make **yourself a member** of this group. Alternatively, you can configure folder security using specific user names.

The following example uses a group called **WakeMAN5 Admin Group**.

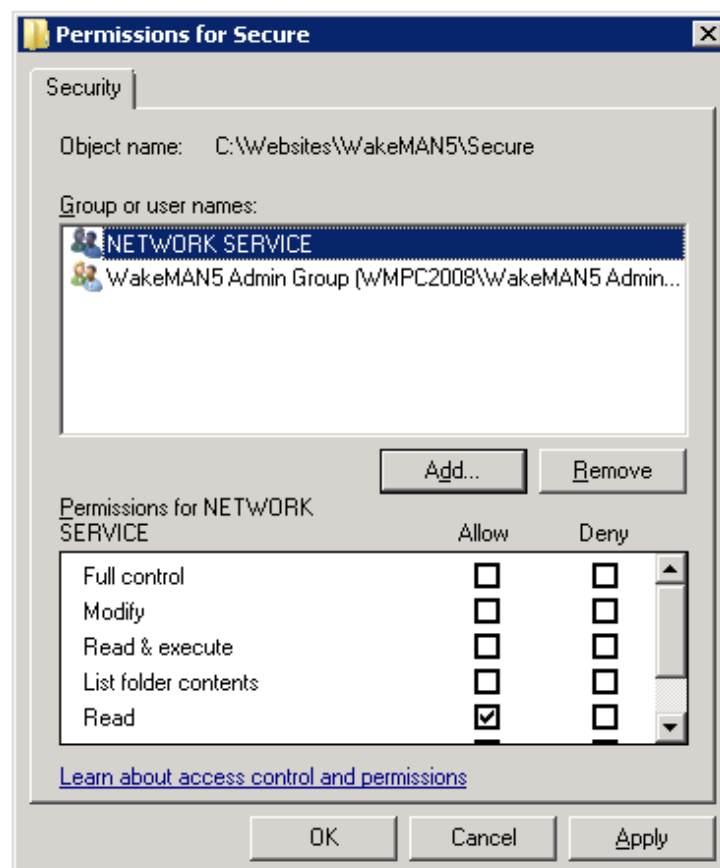
14. Locate the users or groups who will be allowed access to the secure website pages. This should include the account used by the WakeMAN5 application pool user (typically Network Service).

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



15. Click **OK**

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




17. Click **OK** and close the dialog

1. Expand the **Sites** tree and select the **Secure** folder again. In the right hand pane click the **Authentication** icon

WakeMyPC Server Installation and Administration Guide

2. 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

Finally, confirm the security restriction is operational as follows:

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



4. If prompted, enter your login credentials
5. Confirm the page loads normally
6. Repeat this check from a remote workstation and confirm the page loads normally for an approved user
7. Finally, log in as another user and confirm the page is NOT accessible.
8. **Repeat** this procedure to secure the **/Admin** folder

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 the **/Secure** folder.

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

Tip: Methods to authenticate the **/User** folder are described in Appendix D. These optional techniques may be used to limit which users can use the wake-up service.

WakeMyPC Server Testing

Basic 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:8000/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 WakeMAN5 application pool read access to the website root folder.

Email Testing

WakeMyPC Server utilizes email to provide several features. These include sending website error reports to a configurable support notification address and emailing workstation wake-up links to users. To operate correctly the WakeMyPC SMTP server email settings must be correctly configured.

To test the basic email system use the procedure below. This checks the SMTP server settings and the **WebsiteEmail** setting:

1. Navigate to the **/user/wakemanual.aspx** page
2. Enter some workstation details
3. Click the 'Email' link and enter your email address and confirm email arrives.
4. Confirm an email is delivered

To test the BugEmail setting:

1. Navigate to the **/secure/servertools.aspx** page
2. Click **Test**.
3. Confirm an email is delivered to the address defined by the **BugEmail** setting

Database Testing

Following the web server above you can confirm the WakeMyPC Enterprise Server database is functioning correctly with the following test URL:

<http://localhost:8000/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 **servercheck.aspx** page fails to load and the browser reports the page was not found (error 404) this may be because ASP.NET is not correctly configured. Please see the following Microsoft article for a resolution:

<http://support.microsoft.com/kb/315122>

Checking Website Security

Before proceeding further it is essential to verify the security of the WakeMyPC Enterprise Server 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:8000> is available to any user
- Check the page <http://yourserver:8000/Secure> prompts for a login and is only accessible to the user/group(s) you have selected
- If applicable, check that the pages <http://yourserver:8000/User> and <http://yourserver:8000/Admin> prompts for a login and is only accessible to the user/group(s) you have selected

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



WakeMyPC Configuration

Licensed Organisation	Example Corporation Limited
Support Reference	C1B2B9
License Expiry	1/1/2030
License Edition	Enterprise
License Limits	1000 computers
Registered	0 computers (0 in last 30 days)

Checking SMTP Email Configuration

WakeMyPC Enterprise Server can email users bespoke workstation wake-up links and also email the system administrator error reports in the event on a server problem. These may be investigated further 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. In some cases it may be necessary to configure further SMTP server settings such as authentication. You can test the email system using a webpage located in the secure area. To use this feature proceed as follows:

1. Navigate to <http://yourserver:8000/Secure/ServerTools.aspx>
2. Click the **Test** link
3. Confirm a test email is delivered (this may take several minutes)

Server Tools

Setting	Value
ConnectionString	Data Source=localhost;Initial Catalog=WakeMAN5;Integrated Security=True
SMTPServer	smtp.yourdomain.com
BugEmail	support@yourdomain.co.uk Test
WildcardSearchPermitted	True
Application Pool Identity	NT AUTHORITY\NETWORK SERVICE

Temporary Website Maintenance (Server Offline)

WakeMyPC 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>

Configure WakeMyPC Server for your organisation

The WakeMyPC website can be used to:

- Manually register computers for subsequent wake-up
- Prepare for automatic computer registration using the WakeMyPC agent
- Group larger numbers of computers together into virtual “sites” for management purposes of group wake-up
- Search for a computer or groups of computers by name or recent logged on user
- Wake-up single computers or groups of computers
- Remove computers from the system when they are no longer required

This section describes how to setup the WakeMyPC website for initial use. Separate documents explain how to use the web interface to search for and wake-up computers and how to install and configure the WakeMyPC agent.

Using virtual sites to group computers (SiteGUID setting)

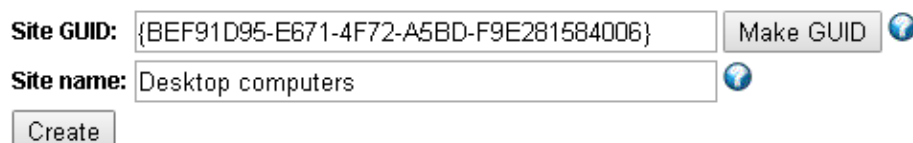
WakeMyPC permits computers to be grouped into virtual “sites” for management purposes. These sites may be based on any convenient grouping such as physical location, business function or similar. To create a new site, proceed as follows:

1. Open the Secure configuration page: **/Secure**
2. Click **Make GUID** to generate a unique site identity

NB: This SiteGUID may be used when deploying the WakeMyPC agent to configure computers to register automatically with the site.

3. Enter an appropriate site name:

Create Site



Site GUID: {BEF91D95-E671-4F72-A5BD-F9E281584006} Make GUID ⓘ

Site name: Desktop computers ⓘ

Create

4. Click **Create**
5. Click on the newly created site name to administer the site, manually register new computers or remotely wake-up systems. For instance:

Available Sites

Site	Computers	Last Data	Delete Wake
Desktop computers	840	16/05/2017	<input type="checkbox"/>

PowerMAN integration (shared SiteGUID)

WakeMyPC may be optionally integrated with Data Synergy's PowerMAN software. In this configuration the PowerMAN computer groups or "virtual" sites are used instead of specific WakeMyPC sites. PowerMAN integration is enabled by default if the WakeMyPC agent is used. The feature may be optionally disabled by changing the agent configuration. This is described in the WakeMyPC Agent Admin Guide.

Tip: When PowerMAN integration is used the WakeMyPC agent automatically uses the ClientGUID/SiteGUID deployed with PowerMAN. This allows both systems to share information about the target computer and link seamlessly from PowerMAN to WakeMyPC. This operating mode is compatible with both the hosted or "cloud" PowerMAN reporting service and the private PowerMAN Enterprise Server software.

PowerMAN integration does not automatically name the PowerMAN sites on the WakeMyPC server. This is because this information is not publically available from the hosted PowerMAN system. In this case the sites will initially display as "Unnamed [date]" and must be renamed manually on the WakeMyPC server. Alternatively, if you run a private PowerMAN Enterprise Server you can configure the PowerMANConnectionString setting to automatically link through to the PowerMAN database. Please contact Technical Support for advice on setting up this feature.

Standalone computers (no SiteGUID)

Grouping computers together into "virtual" sites is recommended but not strictly required for user based wake-up scenarios. The feature may be useful when WakeMyPC is used alongside Data Synergy's PowerMAN product or to provide group based wake-up.

Computers that are registered with WakeMyPC but not linked to a site are listed on the **/Secure** page under **Unallocated Computers**. For instance:

Unallocated Computers

Computer	Last Data	Permanent	Delete Move
WINDOWS7N	22/01/2018	No	<input type="checkbox"/>

Manual computer registration

The WakeMyPC Agent may be deployed to Windows-based computers to enable automatic registration with WakeMyPC. This approach is ideal for large numbers of computers. Alternatively, computers can also be registered manually. This approach is ideal for small numbers of computers or when registering Linux / Apple based systems. To register a computer manually, proceed as follows:

1. If you are the system administrator, open the **/Secure** page and click the desired site name.

OR

If you are not the system administrator, open the **/Admin** page, enter the SiteGUID and click **Configure Site**

2. Navigate to the section captioned **Add Computer**
3. Enter the desired computer details and click **Submit**

Add Computer

Permanent	<input checked="" type="checkbox"/>
Client GUID:	<input type="text" value="{52B1C4D5-F616-4886-BBDF-CCC217160F4A}"/> <input type="button" value="Make GUID"/>
Name	<input type="text" value="Linuxbox"/>
Description	<input type="text" value="My example Linux box"/>
Timezone:	<input type="text" value="0"/> <input type="button" value="▼"/> hours UTC
MAC Address:	<input type="text" value="ABCD12345678"/>
Network Address:	<input type="text" value="IPv4"/> <input type="button" value="▼"/>
IP Address:	<input type="text" value="192.168.60.120"/>
Subnet Mask:	<input type="text" value="255.255.0.0"/> (IPv4 only)
<input type="button" value="Submit"/>	

Manual administrative computer wake-up

WakeMyPC may be used by both normal users and system administrators to wake-up computers. Users typically access the system via the /User/WakeSearch.aspx or /User/WakeManual.aspx pages. These are described elsewhere in this document and in the accompanying Operations Guide.

System Administrators can also wake-up computers directly via a number of different routes. For instance,

- To wake-up a single computer click the associated **Wake** link:

WINDOWS7N

Computer	WINDOWS7N	Update
Description		Change
Site / Group	None	
WakeMyPC version	5.2.0.326	
Windows® version	6.1.7601 Service Pack 1	
First registered	22/01/2018	
Timezone	0.0 hour(s) UTC	
Permanent	No	
Recent Users	1	
Last User		
Schedules	0	
Wake Proxy		
Last wake success	Never	Wake

Recent Users:

Network Addresses:

- To wake-up a group of computers, select the desired group(s) by checking the box and click **Wake** in the header bar:

Site	Computers	Last Data	Delete Wake
Desktop computers	840	16/05/2017	<input checked="" type="checkbox"/>

WakeMyPC API for scripted or scheduled wake-up

The primary function of WakeMyPC is to perform user driven, ad-hoc, wake-up of single workstations and groups of workstations. Typically wake-up operations are launched using the web interface. In some cases it may also be desirable to script or schedule the wake-up operation. This may be useful to system administrators for maintenance tasks such as updates, backups and AV scans.

WakeMyPC supports several different interfaces suitable for use with a script or Windows scheduled task. The following website pages are provided for this purpose:

- /WakeComputer.aspx – Immediately wake a single workstation
- /WakeSite.aspx – Immediately wake a group (site) of workstations
- /Admin/WakeAll.aspx – Immediately wake all known workstations

The full syntax for each page is documented in an appendix at the end of this guide. To wake a group of workstations the following syntax may be used:

```
WakeSite.aspx?SiteGUID={4381d7b7-90b1-4d1f-ad71-571234567890}
```

Where the SiteGUID is the SiteGUID assigned by the administrator. The {brace} characters are optional. The wake-up operation commences immediately.

This operation can be scripted by using the built-in Windows START program. For instance:

```
START "Wake-up" "http://server:8000/WakeSite.aspx?SiteGUID=4381d7b7-90b1-4d1f-ad71-571234567890"
```

This launches the wake-up task for the server located at <http://server:8000> and the site specified by SiteGUID=. The task will execute until it succeeds or times out. In normal operation the wake-up is designed for user monitoring. When executed via a script the WakeMyPC server will automatically timeout the page after 10 minutes of inactivity. This avoids the propagation of stale wake-up processes on the server.

Similarly a specific computer can also be woken using the registered ClientGUID:

```
WakeComputer.aspx?ClientGUID=4381d7b7-90b1-4d1f-ad71-571234567890
```

Appending the &Wake=True parameter forces an immediate, non-Javascript, based wake-up. This improves support for scripted wake-up and the WGET tool. For instance:

```
WakeComputer.aspx?ClientGUID=4381d7b7-90b1-4d1f-ad71-571234567890&Wake=True
```

The /User/WakeSearch.aspx and /User/WakeManual.aspx pages also support scripted operation. This can be useful to automate more complex scenarios that could otherwise be performed manually using the web interface. These pages also support the optional &Wake=True parameter and wildcards. For instance:

```
WakeSearch.aspx?ClientGUID=431db06d-5922-4093-9c70-6fb583846832
```

```
WakeSearch.aspx?ComputerName=Workstation*&Wake=True
```

```
WakeSearch.aspx?SiteGUID=edb1c22a-a9bf-46be-a907-1618bd27bf90&Wake=True
```

The complete web API is documented in an appendix at the end of this document.

Workstation Remote Access, Windows Remote Desktop and Terminal Services Gateway Integration

WakeMyPC Server allows users to wake a remote workstation and then immediately, and conveniently, connect to that workstation via remote desktop or similar. The software is designed to be compatible with several remote access systems such as Microsoft Remote Desktop / Terminal Services and VNC.

The workstation connection feature may be configured using the **WakeConnectURL** setting. This supports dynamic expansion of the following variables. Each of these is substituted for the specific computer:

Variable	Meaning
\$ipaddress\$	IP address of the remote host
\$computername\$	Unqualified computer name
\$fqdomainsuffix\$	Fully qualified network domain suffix This setting is required for remote clients (without local DNS access) to connect to workstations within the internal network.

The following section explains how to configure this feature for several common remote desktop systems.

Legacy Remote Desktop Web Connection (Windows Server 2003 and later)

Note: In the current release this feature is enabled by default. In the subsequent releases Data Synergy may be unable to freely ship the Microsoft Remote Desktop Web Connection software and it will be the customer's responsibility to download and install this product from Microsoft.

Microsoft Remote Desktop (RD) Web Connection allows a remote desktop session to be accessed directed from a web browser. The RD Web software is implemented as an ActiveX control that may be hosted on a Windows IIS web server. The control provides a web based remote desktop experience very similar to the built-in MSTSC.EXE program. The RD Web software is a free download from Microsoft. The most recent version (which also supports Windows 2008 and later) is available from the following link:

<http://www.microsoft.com/en-us/download/details.aspx?id=14531>

To current ActiveX control supports the v5.1 RDP protocol. This provides general remote desktop features and will be appropriate for many environments. However, this software has now been superseded (see below) and does have some limitations:

- Requires Internet Explorer browser
- Does not support more advanced remote multimedia features
- Does not support RDP via the SSL (secure) protocol or Terminal Services Gateway

To install the Microsoft Remote Desktop Web Connection proceed as follows:



tswebsetup.exe

- Download the RD Web Connection software from Microsoft
- Rename the TSWebsetup.exe file to **TSWebsetup.zip**
- Extract the file to the **TSWeb** folder on the WakeMyPC server
- Set the **WakeConnectURL** setting to:

~/TSWeb/?Server=\$computername\$. \$fqdomainsuffix\$&AutoConnect=1

Terminal Services Gateway / Remote Desktop Web Connection Integration (Windows Server 2008 and later)

Windows Server 2008 introduces the Terminal Services (TS) Gateway. This component is similar to the previous ActiveX approach but is built-in to Windows Server and is not available via a separate download. The updated software supports the v6.x version of the RDP protocol and includes support for SSL secured connections via a central TS Gateway. Like the previous release this software is only compatible with Internet Explorer.

To enable Terminal Services Gateway integration proceed as follows:

- Follow the Windows Server documentation to configure and test the TS gateway
- Configure the **WakeConnectURL** to the fully qualified URL of your TS gateway
e.g. **http://tsgateway.\$fqdomainsuffix\$**

Generic RDP:// Protocol Integration (Most browsers / operating systems)

The RDP:// pseudo-protocol provides a generic, browser and operating system independent, way to support Windows Remote Desktop. To use this method a protocol 'handler' must be registered on the client computer. This configures the workstation to open the appropriate program (e.g. MSTSC.EXE on Windows) when the user clicks an RDP:// encoded link.

Data Synergy provides the Remote Desktop Launcher utility. This is supplied as an MSI file that will install an RDP:// protocol handler on Microsoft Windows systems. Similar protocol handlers can be configured for other platforms. Please see Appendix A for further information.

To enable generic RDP:// integration proceed as follows:

- Ensure that an RDP:// protocol handler is installed / registered on the client workstation
- Configure the **WakeConnectURL** to
e.g. **rdp://\$computername\$. \$fqdomainsuffix\$**

Generic VNC:// Protocol Integration (Most browsers / operating systems)

Similarly, the VNC:// pseudo-protocol provides a generic, browser and operating system independent, way to support Virtual Network Computing (VNC). To use this method a protocol 'handler' must be registered on the client computer. This configures the workstation to open the appropriate program (e.g. VNCVIEWER.EXE on Windows) when the user clicks an VNC:// encoded link.

To enable generic VNC:// integration proceed as follows:

- Ensure that an VNC:// protocol handler is registered on the client workstation
- Configure the **WakeConnectURL** to
e.g. **vnc://\$computername\$. \$fqdomainsuffix\$**

WakeMyPC Workstation Availability Checker (Probe)

The WakeMyPC website includes a built-in workstation availability checker. As WakeMyPC attempts to wake or power-on a remote workstation it also probes the workstation to determine if it is available. This process repeats every few seconds until the workstation is detected or the pre-set timeout (WakeTimeoutSeconds) expires.

WakeMyPC supports two complementary probe methods:

- **ICMP (Ping) Probe** – Sends a 'Ping' request to the workstation. This is the default operation.
- **TCP Probe** – Sends a TCP 'connect' message to selected ports on the workstation. Services listening on these ports will accept this message and reply indicating that the workstation is available.

ICMP is designed for this purpose and therefore is the primary mechanism that should be used. The TCP probe method is provided to complement ICMP in environments where ICMP may be disabled or blocked by intermediate firewalls.

The workstation probe feature is configured by the following four settings:

```
ProbeTimeoutMS  
ProbeICMP  
ProbePorts  
ProbeAddressingMode
```

WakeMyPC Server SQL Database Maintenance

There are two additional steps required to ensure reliable and optimal functioning of the WakeMyPC Enterprise Server database:

- Database backup strategy
- Database optimization strategy

Database backup strategy

As supplied the WakeMAN5 Enterprise Server database is configured to use the **Simple Recovery Model**. This model is the easiest to configure but will result in some data loss in the event of a server malfunction. The Simple Recovery Model creates a database backup as configured in the server schedule (typically daily). Whilst very simple to understand and configure any data changes, between backups, are lost in the event of a server problem. In most scenarios the minor discontinuity in the logged data that would result from a database malfunction will be acceptable.

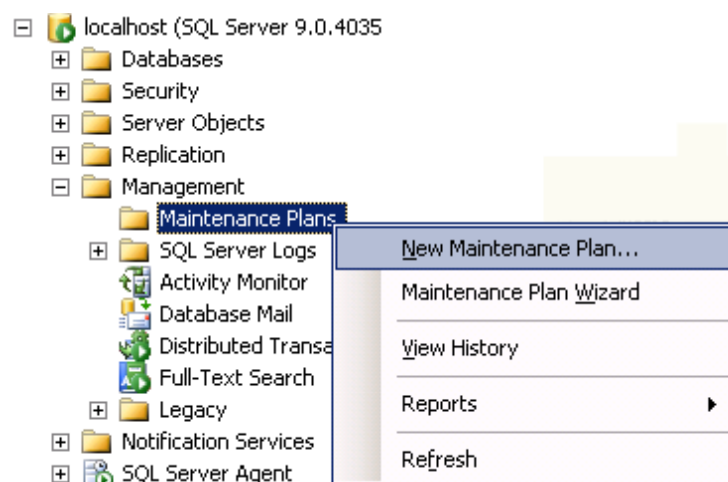
The following Microsoft article provides additional guidance on selecting the appropriate backup strategy:

<http://msdn.microsoft.com/en-us/library/aa173531.aspx>

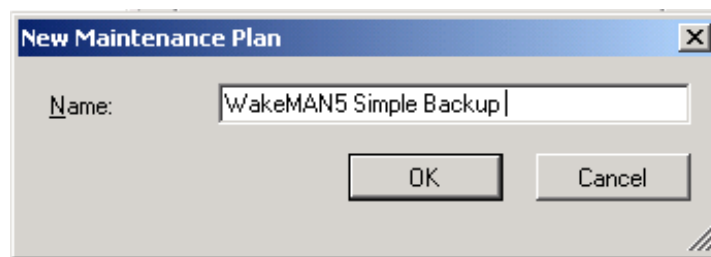
You must decide the appropriate database backup strategy for your WakeMyPC Enterprise Server deployment.

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

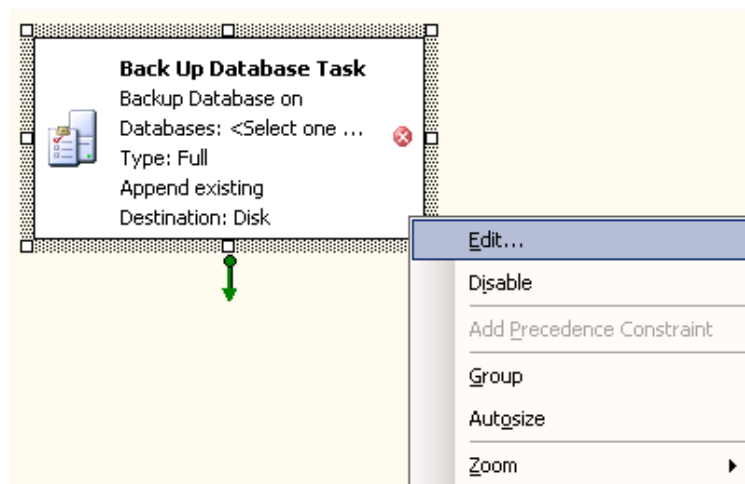
1. Open SQL Server Management Studio
2. Navigate to Management\Maintenance Plans
3. Right click and select New Maintenance Plan



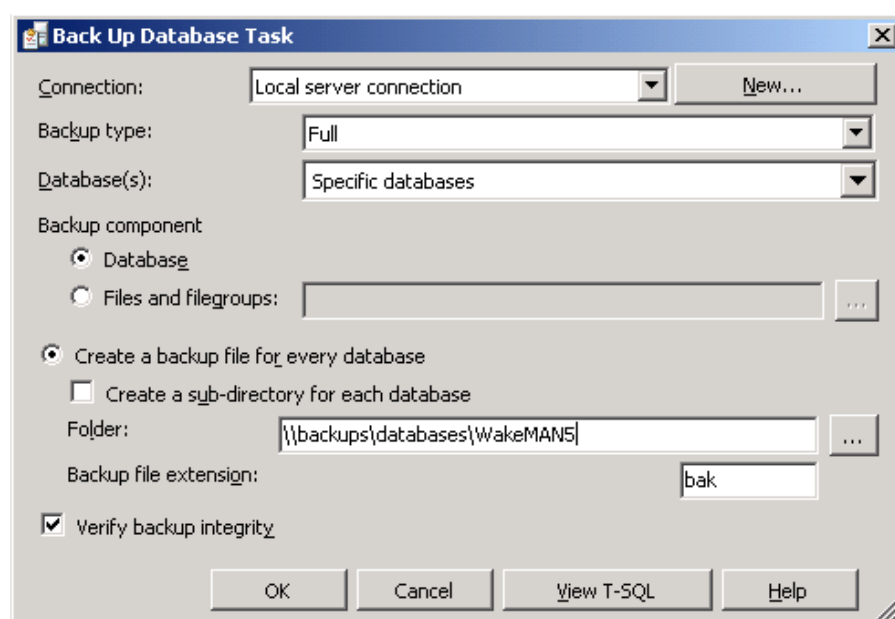
4. Enter an appropriate plan name: **WakeMAN5 Simple Backup**



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 WakeMAN5 database
8. Select an appropriate backup location e.g. [\\Backups\Databases\WakeMAN5](#) and click **OK**



9. Click the Calendar icon



10. 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.

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.

Database optimization strategy

The WakeMyPC Enterprise Server 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 WakeMAN5 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. This procedure may not be essential in smaller deployments.

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: **WakeMAN5 Index Task**
5. Drag the 'Rebuild Index Task' to the main pane
6. Right click on the task and select Edit
7. Select the WakeMAN5 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.

Troubleshooting WakeMyPC Enterprise Server

WakeMyPC Server has undergone many hours of development and testing. The software is very reliable but problems do sometimes happen. This walk-through installation in this document makes some basic assumptions about the WakeMyPC 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 WakeMyPC is configured to display only limited client error messages. If you experience problems with the WakeMyPC website it can be very helpful to view the problem pages directly on the web server via <http://localhost:8000/>. 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 access 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 8000)
- 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:8000/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\Framework\v4.0.30319\Temporary ASP.NET Files

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)

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 WakeMAN5 database. The database must reliably respond in <5 seconds for WakeMyPC agents to be able to successfully log data.
- Check the network connection from the IIS server to the SQL server
- Check the 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 /Logs folder or the tblErrorLog in the WakeMAN5 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 WakeMyPC software encounters an error. The most common cause of this problem is connection problem or timeout accessing the SQL database. This can happen due to incorrect database configuration or under very heavy database load conditions. WakeMyPC Enterprise Server logs most errors (except timeouts) in the tblErrorLog database table. Activity logs may also be recorded in the /Logs folder of the deployment. You can examine these logs or query the database 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 WakeMyPC Server 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 server less secure. They should only be performed under controlled conditions and certainly not when the 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 WakeMyPC Server configuration is simple but complexity can 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 ConnectionString setting in the web.config file refers to the correct database server and database. Confirm that the ConnectionString is spelt correctly.
- 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
- 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:8000/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:8000/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 WakeMyPC Server 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 WakeMAN5 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 occurs 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: Website reports error ‘Cannot find the object upClientRemoveStale, because it does not exist or your do not have permission’

This problem occurs due to a problem in the original v5.1.3.0 release of WakeMyPC. If you have this version installed please install the v5.1.3.1 hotfix or later release. This hotfix is only appropriate for v5.1.3.0.

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

This problem can occur if the Windows server hosting WakeMyPC has not been updated. IE10 is not 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>

Problem: Target computer(s) wake-up but WakeMyPC does not recognize this and keeps attempting wake-up before timing out.

This problem can occur when the target computer does not respond to any of the probes sent by WakeMyPC to determine if the system is operational. WakeMyPC supports two distinct probe mechanisms. These may be used in combination if desired. The mechanisms are:

- Probe using ICMP (network “ping”) – This feature is enabled by setting the `ProbeICMP` setting to True. Target computers may require a specific firewall rule to permit ICMP traffic. This can be checked by manually “pinging” the target computer. If this operation works then ICMP is enabled for that computer and WakeMyPC will be able to probe the computer.
- Probe ports (service scan) – This feature allows WakeMyPC to determine if a target computer is available by scanning specific network ports. This may be preferable in some circumstances because it avoids the need to enable ICMP traffic. The list of ports to check is specified by the `ProbePorts` setting. For instance, Microsoft networks typically have port 445 present.

When both mechanisms are enabled (or multiple probe ports specified) WakeMyPC will try all available checks and report a computer as available when any one check confirms the target computer is available. Once this is confirmed further checks are terminated to minimise network traffic.

Network probing may also fail because WakeMyPC cannot address the target computer. The addressing mode is configured by the `ProbeAddressingMode` setting. This may be one of the following:

- 1 = Use IP address
- 2 = Use unqualified computer name (default)
- 3 = Use fully qualified computer name (requires `FQDomainSuffix` setting)

Appendix A – Data Synergy Remote Desktop Launcher

Overview

The optional Remote Desktop Launcher provides an internet protocol handler for the RDP:// protocol. This may be installed on end-user workstations. The software allows the user to conveniently launch the Microsoft Terminals Services Client tool (MSTSC) from a suitably encoded HTTP page hyperlink.

For instance the following link would launch a remote desktop session to a computer called OfficePC:

```
<a href='rdp://officepc'>Open OfficePC</a>
```

Remote Desktop Launcher provides browser independent protocol translation to support the following browsers:

- Microsoft Internet Explorer
- Google Chrome
- Mozilla Firefox

Remote Desktop Launcher is suitable for use on both x86 and x64 based systems running Windows 2000 and later.

WakeMyPC Server Configuration

The Remote Desktop Launcher installs a generic protocol handler. To configure Data Synergy WakeMyPC server to use the handler configure the **WakeConnectURL** setting to:

```
rdp://$computename$. $fqdomainsuffix$
```

Appendix B – WakeMyPC Agent Data Protocol

WakeMyPC Agent is an optional component for use with WakeMyPC Server Enterprise Edition. The agent automatically collects relevant workstation information and periodically uploads it to the WakeMyPC Server. This optional component avoids the need to manually populate the WakeMyPC Enterprise Server with workstation information and also ensures that this information is always current. The WakeMyPC Agent is designed to impose minimal demands upon the enterprise network and will typically upload information that has changed since the last upload.

The information collected is the minimum required to perform workstation wake-up based upon either computer or username. No information about specific users or their activity is recorded. The information is uploaded in XML format using the industry standard HTTP POST protocol.

This document explains the operation of the protocol. This document assumes the reader is reasonably familiar with the Microsoft Windows SDK, the C/C++ programming language and XML. The protocol is very similar to that used by the Data Synergy PowerMAN product.

XML Protocol

Uploads are performed in XML format using the industry standard HTTP POST protocol. WakeMyPC Agent normally contacts the logging server either once every 24 hours or when a significant change is detected (for instance a new IP address). The XML upload consists of the following key elements:

- **<ClientInfo> node** – This includes static information about the workstation and installed agent version
- **<NetworkInfo> node** – This includes one or more <NetworkAdapter> nodes. Each of these represents a single adapter. Each adapter has exactly one MacAddress and one or more IP4Address or IP6Address elements
- **<UserList> node** – This contains the list of currently logged on users as an array of <UserName> elements

If you require further details of the WakeMyPC data transfer format please contact Data Synergy Technical Support.

Appendix C – Supported WakeMyPC parameters (API)

The **WakeMyPC Server** website features many pages that accept URL (query string) parameters. These may be used to pre-populate the page or launch an automatic action.

The following table summarises the parameters supported:

Page	Function and supported parameters
WakeComputer.aspx	<p>Wake specified workstation. This page is intended for use with third-party software such as the Windows Task Scheduler.</p> <p>Supported parameters:</p> <p>ClientGUID – Unique computer GUID Wake – Optionally forces immediate wake-up (JavaScript not required)</p> <p>Examples:</p> <pre>WakeComputer?ClientGUID={5fff352d-413a-4510-ba28-ebd4488df735}</pre> <pre>WakeComputer?ClientGUID={5fff352d-413a-4510-ba28-ebd4488df735}&Wake=True</pre>
WakeSite.aspx	<p>Wake specified site (workstation group). This page is intended for use with third-party software such as the Windows Task Scheduler.</p> <p>Supported parameters:</p> <p>SiteGUID – Unique site (computer group) GUID Wake – Optionally forces immediate wake-up (JavaScript not required)</p> <p>Example:</p> <pre>WakeSite?SiteGUID={8a63b6b9-f031-4f6e-a3f8-2c7f409c747f}</pre> <pre>WakeSite?SiteGUID={8a63b6b9-f031-4f6e-a3f8-2c7f409c747f}&Wake=True</pre>
Admin\WakeAll.aspx	<p>Wake all workstations in all sites. This page is intended for use with third-party software such as the Windows Task Scheduler. It is located in the Admin folder to prevent unauthorised use.</p> <p>Supported parameters:</p> <p>Wake – Optionally forces immediate wake-up (JavaScript not required)</p>
User\ComputerSetup.aspx	<p>Add or update an existing workstation. This is intended for self-service scenarios built-in to in-house user setup/registration processes.</p> <p>Supported parameters:</p> <p>ComputerName – Target computer name</p>

	<p>IPAddress – Target computer static/dynamic IP address SubnetMask – Target computer network subnet MacAddress – Target computer MAC (hardware) address Username (optional) – User's name ClientGUID (optional) – Specific unique client identity</p> <p>Example:</p> <pre>ComputerSetup.aspx ?ClientGUID={3ad36a85-1d48-4f58-9d61-d346f0977d00} &ComputerName=Accounts&UserName=Brenda &IPAddress=192.168.100.67&SubnetMask=255.255.255.0 &MacAddress=0026C7561234</pre>
User\WakeManual.aspx	<p>Wake a specific workstation using known network information. This page also supports wildcards * and ?.</p> <p>Supported parameters:</p> <p>ComputerName – Target computer name MacAddress – Target computer MAC (hardware) address IPAddress (required for subnet directed and direct modes) SubnetMask (required for subnet directed and direct modes) Wake – Optionally forces immediate wake-up (JavaScript not required) WolMode – Override the default wake-up method. This may be one of;</p> <pre>No wake-up. Just probe = 0 Local broadcast (default) = 1 Subnet directed broadcast = 2 Direct (unicast) packet = 3</pre> <p>Example:</p> <pre>Wakemanual.aspx?ComputerName=Accounts &IPAddress=192.168.100.67&SubnetMask=255.255.255.0 &MacAddress=0026C7561234&WolMode=2&Wake=True</pre>
User\WakeSearch.aspx	<p>Find and then wake a workstation. This page also supports wildcards * and ?.</p> <p>Supported parameter (any combination):</p> <p>ComputerName – Target computer name ClientGUID – Unique computer GUID SiteGUID – Unique site (computer group) GUID Wake – Optionally forces immediate wake-up (JavaScript not required) WolMode – Specifies the wake-up method.</p> <p>Examples:</p> <pre>WakeSearch.aspx?ComputerName=Accounts WakeSearch.aspx?ComputerName=Technical*&Wake=True WakeSearch.aspx?ClientGUID={431db06d-5922-4093-9c70-6fb583846832}&Wake=True</pre>

Appendix D – Authenticating Workstation Wake-up

The **WakeMyPC Server** website allows user workstation wake-up operations to be authenticated using a variety of methods:

- No authentication required (Default)
- IIS Integrated Windows Authentication (NTLM) on the **/User** folder
- External login provider

Enabling Authentication

Authentication is disabled by default. To enable authentication configure the following setting in the web.config file:

```
UsernameRequired=True
```

Unauthenticated users are redirected to a login holding page. A default place-holder page is required. This can be amended or alternatively the user redirected elsewhere. This is configured by the following setting:

```
UsernameUnknownPage=~/LoginRequired.aspx
```

Configuring IIS Integrated Windows Authentication

The user-based wake-up pages are all located in the **/User** folder. This may be secured using folder permissions to ensure only authorised users have access. The procedure is essentially the same as that used to secure the **/Secure** and **/Admin** folders. For instance to secure the **/User** folder on a Windows 2008 or later server proceed as follows:

1. Open the **Internet Information Services (IIS) Management tool (INETMGR.EXE)**
2. Navigate to **Sites**
3. Locate the **WakeMAN5** site and expand the folder tree
4. Locate the **/User** folder, right click and select **Edit Permissions:**
5. Select the **Security** tab
6. Click **Advanced**

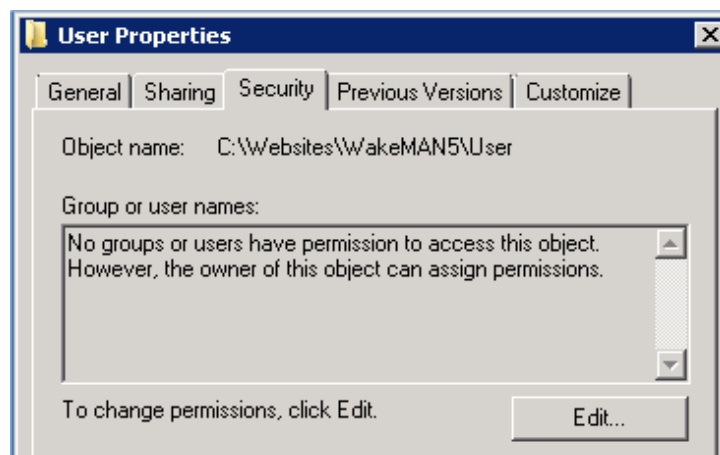
On Windows Server 2008:

7. Click **Changed Permissions**
8. Un-check '**Include inheritable permissions from this objects parent**' and then click **OK** (if prompted by warnings click **Remove** and then **Yes**) and then **OK** again
9. Click **Edit**

On Windows Server 2012 and later:

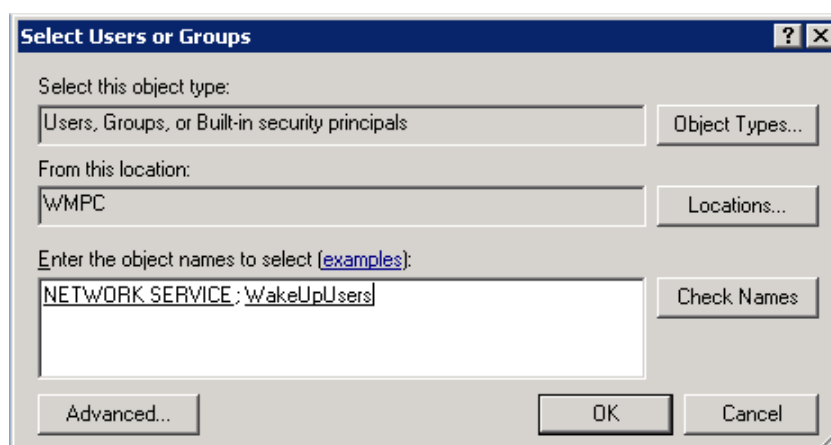
10. Click **Disable Inheritance**
11. Select **Remove all inherited permissions from this object** and then click **OK** (if prompted by a warning click **Yes**)
12. Click **Edit**

The following dialog should now be visible:

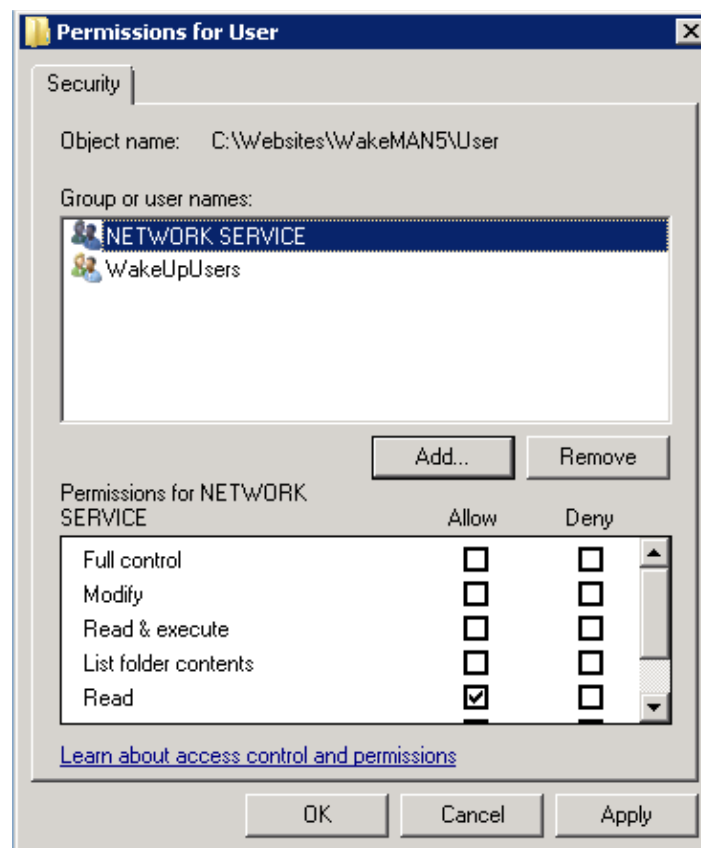


13. Click **Add**
14. Locate the users or groups who will be allowed access to the user website pages. This should include the account used by the WakeMAN5 application pool user (typically Network Service).

For instance **Network Service** and **WakeUpUsers**:



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



17. Click **OK** and close the dialog
9. Expand the **Sites** tree and select the **/User** folder again. In the right hand pane click the **Authentication** icon
10. 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	

Using an external authentication provider

WakeMyPC also supports an external authentication provider interface. This allows WakeMyPC to be integrated with third-party software or an existing user credentials system. When combined with the `UsernameRequired` setting this feature ensures that only authorised users who have previously been registered with WakeMyPC may use the wake-up service. All of the pages in the `/User` folder support this feature.

This feature maybe used in either of the following ways:

1. HTTP POST a 'username' to the relevant `/User` page. For example:

```
<!-- Example login interface using Form/POST -->
<form action="user/wakesearch.aspx" method="post">
  Username:
  <input type="text" name="username" /><input type="submit" value="Login" />
</form>
```

2. Append `?Username` to the URL. For example:

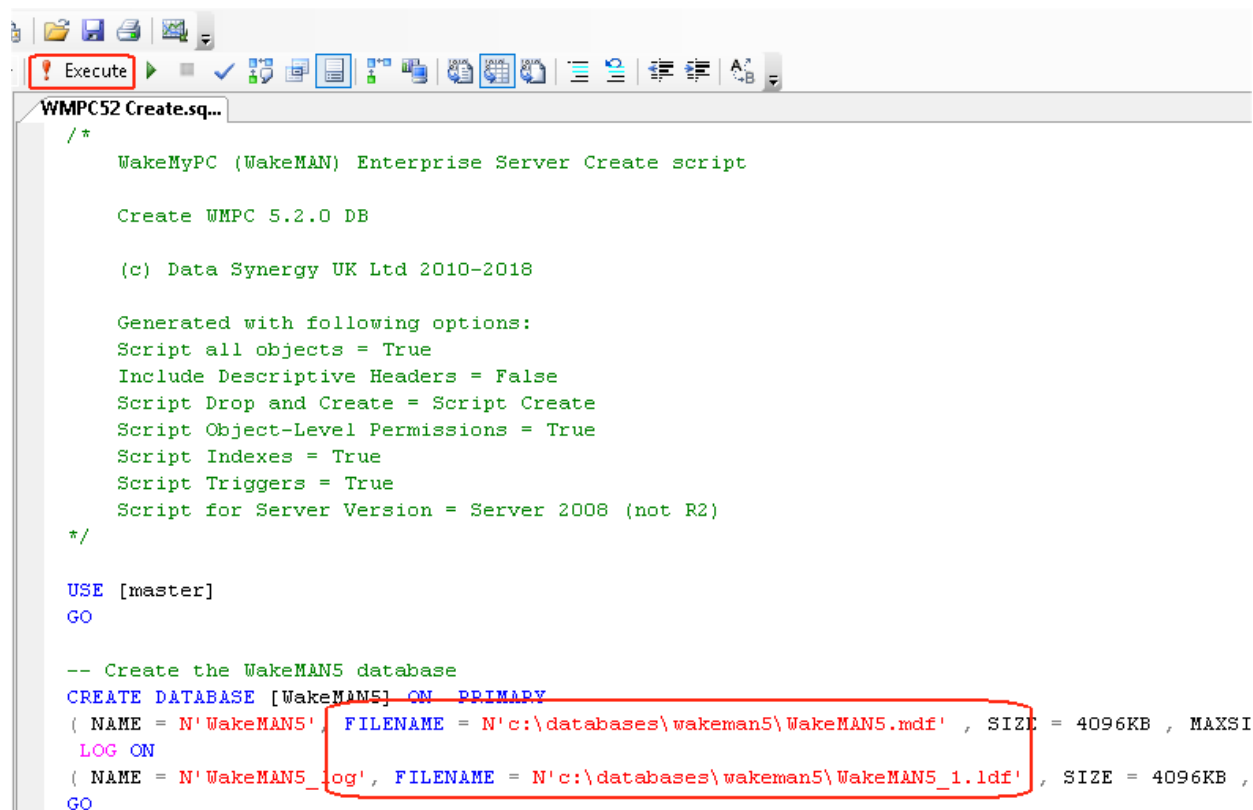
```
WakeSearch.aspx?Username=Brenda
```

Appendix E - WakeMyPC Database Creation Script

Advanced SQL administrators may wish to create the WakeMyPC 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 WakeMyPC distribution. To create the databases using a scripted method proceed as follows:

1. Open **SQL Server Management Studio**
1. Open the supplied **WMPC52 Create.sql** script file. This is located in the **Advanced** folder of the software distribution.
2. Amend the database and transaction log file locations as required (see diagram below)

NB: In critical deployments we would recommend best practice is to place these files on separate physical disks. This is not necessary on small test deployments.
3. Click **Execute**
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 WakeMAN5 database 'WMWebsite' role
6. Perform the subsequent website configuration steps described above



```

/*
WakeMyPC (WakeMAN) Enterprise Server Create script

Create WMPC 5.2.0 DB

(c) Data Synergy UK Ltd 2010-2018

Generated with following options:
Script all objects = True
Include Descriptive Headers = False
Script Drop and Create = Script Create
Script Object-Level Permissions = True
Script Indexes = True
Script Triggers = True
Script for Server Version = Server 2008 (not R2)
*/

USE [master]
GO

-- Create the WakeMAN5 database
CREATE DATABASE [WakeMAN5] ON PRIMARY
( NAME = N'WakeMAN5', FILENAME = N'c:\databases\wakeman5\WakeMAN5.mdf' , SIZE = 4096KB , MAXSI
LOG ON
( NAME = N'WakeMAN5_log', FILENAME = N'c:\databases\wakeman5\WakeMAN5_1.ldf' , SIZE = 4096KB ,
GO
  
```

Appendix F – Upgrade existing WakeMyPC v5.1.3.x server

To upgrade from WakeMyPC Enterprise Server v5.1.3.x to v5.2.0 it is necessary to update both the website and the underlying WakeMAN database. This can be accomplished as follows:

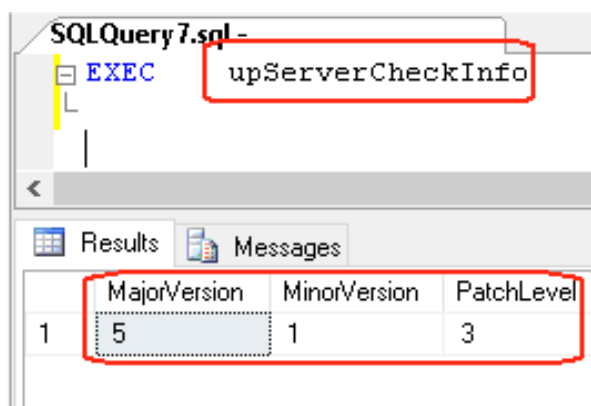
1. Backup the existing website and, if possible, print the “web.config” file
2. Delete the existing website
3. Follow the appropriate procedure above to install a new WakeMyPC website and configure it as required. In some cases it may be useful to refer to the previous “web.config” file.
4. Temporarily 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 WakeMyPC distribution to update the WakeMAN 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. Determine the name of the existing WakeMAN database. It is normally called WakeMAN5. If the database name is not WakeMAN5 then each update script must be amended accordingly. This is explained further below.
4. Right click on the database and select **New Query**
5. Enter the command:

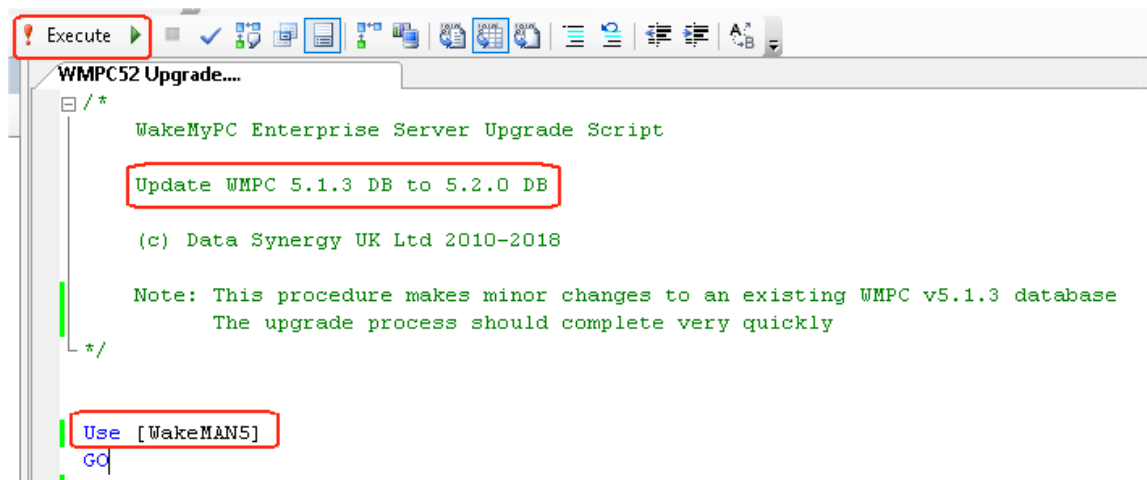
```
EXEC upServerCheckInfo
```

6. Click **Execute**
7. Confirm the database is version 5.1.3 **This update is NOT suitable for other releases:**

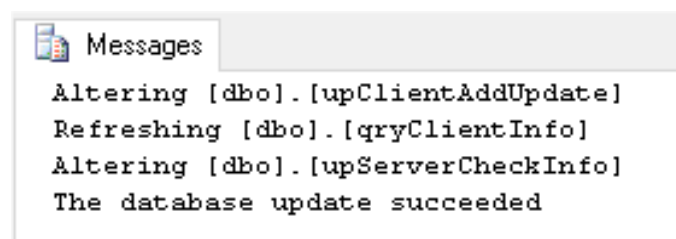


Tip: Please contact Technical Support for advice if you wish to upgrade a different WakeMyPC database revision to the latest release.

8. Backup the existing database to a safe location
9. Open the supplied **WMPC52 Upgrade.sql** script file. This is located in the **Advanced** folder of the WakeMyPC distribution.
10. If necessary amend the database [name], contained in square brackets, located at the top of the script (see diagram below):



11. Click **Execute**
12. Allow the update to proceed - This may take some time on a larger database. Do not cancel the update.
13. Confirm no error was reported:



14. Re-enable the WakeMyPC website
15. Confirm the database and website function as expected

Tip: The database upgrade is an advanced operation. If you are not familiar with Microsoft SQL or wish to upgrade another legacy version of WakeMyPC / WakeMAN please contact Technical Support for assistance.