



WakeMyPC Lite Server & WakeMyPC Enterprise Server v5.1 Installation and Administration Guide

Release 5.1.3 June 2011

About Data Synergy



Data Synergy is a British company based in Sheffield. We have over 10 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 Server Overview	6
WakeMyPC Lite Server and WakeMyPC Enterprise Server Editions.....	6
Wake-on-LAN Technology and complementary tools.....	8
WakeMyPC Server Installation (All Editions)	9
Installation Prerequisites	9
WakeMyPC Server Deployment Components.....	9
Deployment Assumptions.....	10
Installation Checklist.....	11
Walkthrough - Website Configuration Windows Server 2003.....	12
Walkthrough - Website Configuration Windows Server 2008.....	17
WakeMyPC Enterprise Server Installation Steps	22
SQL Database Configuration Walk-through.....	22
Using a remote SQL Server	25
Using a named instance SQL Server.....	27
Securing the WakeMyPC Enterprise Server Website.....	27
Walkthrough: Securing the website - Windows 2003.....	27
Walkthrough: Securing the website - Windows 2008.....	31
Configuring WakeMyPC Server	33
WakeMyPC Lite Server and Enterprise Server Common Settings	33
WakeMyPC Enterprise Server Specific Settings	36
Configuring WakeMyPC Server Logging	37
WakeMyPC Workstation Availability Checker (Probe)	38
WakeMyPC Scripting and scheduling	38
Workstation Remote Access, Windows Remote Desktop and Terminal Services Gateway Integration	39
Remote Desktop Web Connection.....	40
Terminal Services Gateway / Remote Desktop Web Connection Integration (Windows Server 2008 only)	41
Generic RDP:// Protocol Integration (Most browsers / operating systems)	41
Generic VNC:// Protocol Integration (Most browsers / operating systems)	41

WakeMyPC Server Testing.....	42
WakeMyPC Server Website Testing.....	42
WakeMyPC Server Email Testing.....	42
WakeMyPC Enterprise Server Database Testing.....	43
Checking WakeMyPC Enterprise Server Website Security.....	44
Checking SMTP Email Configuration.....	44
Temporary Website Maintenance (Server Offline).....	46
WakeMyPC Enterprise Server SQL Database Maintenance.....	47
Database backup strategy.....	47
Database optimization strategy.....	50
Troubleshooting WakeMyPC Server.....	51
Problem: Static test page is not displayed.....	51
Problem: Website reports – The page cannot be found.....	51
Problem: Website reports – Server Application Unavailable.....	51
Problem: Servercheck.aspx takes excessive time (>1 second) to display.....	52
Problem: Servercheck.aspx reports - An error has occurred while establishing a connection to the server (or similar).....	52
Problem: Website reports - Sorry. A website error was detected. This cause of this error has been logged and will be investigated.....	52
Problem: Non-specific database connectivity problem.....	53
Problem: Website reports - The current identity does not have write access to ...Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files.....	53
Problem: Website displays - Service Unavailable.....	54
Problem: The website reports an exception obtaining permission of type 'System.Web.AspNetHostingPermission'.....	54
Problem: "HTTP Error 404 - File or Directory not found" error message when you request an ASPX page.....	55
Problem: Unrecognized attribute "targetFramework" reported when you request an ASPX page.....	55
Problem: Website reports - Could not load file or assembly 'PowerLib' or one of its dependencies. An attempt was made to load a program with an incorrect format.....	55
Problem: "The application has failed to start because its side-by-side configuration is incorrect. Please see the application event log or use the command-line sxstrace.exe tool for more detail. Exception from HRESULT: 0x800736B1" error message when you request an ASPX page.....	55
OR Could not load file or assembly 'PowerLib.dll' or one of its dependencies. The specified module could not be found.....	55
Problem: Website generated URLs fail to work correctly.....	56
Website URLs contain additional, unrecognised symbols, such as %20.....	56
Appendix A – Data Synergy Remote Desktop Launcher.....	57
WakeMyPC Server Configuration.....	57
Appendix B – WakeMyPC Agent Data Protocol.....	58
XML Protocol.....	58

Appendix C – Supported WakeMyPC webpage parameters	59
Appendix D – Authenticating Workstation Wake-up	61
Enabling Authentication.....	61
Configuring IIS Integrated Windows Authentication.....	61
Using an external authentication provider	62
Appendix E – Upgrading existing WakeMyPC / WakeMAN Servers	63
Appendix F – WakeMyPC Database v5.1.x Update Procedure.....	63



WakeMyPC Server Overview

WakeMyPC 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 use for WakeMyPC is to maximize the benefits of workstation power management by allowing workstations to be accessed whenever necessary. This removes the most common barrier to effective power management and delivers significant additional energy savings.

WakeMyPC Lite Server and WakeMyPC Enterprise Server Editions

Data Synergy distributes the WakeMyPC Server software in two forms:

WakeMyPC Lite Server is a basic product providing manual workstation wake-up only. The product does not include any persistent data storage (database) and therefore workstation technical details must be manually entered and then either stored in an Internet browser bookmark or re-entered on a subsequent occasion. This product is ideal for small scale deployments and Wake-On-LAN testing. Lite Server is available as a free download and does not include any technical support.

WakeMyPC Enterprise Server is a fully featured enterprise-class product providing:

- Ad-hoc workstation wake-up based upon computer name, 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
- Optional workstation agent to automatically gather and update workstation information

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. WakeMyPC Agent is not available with WakeMyPC Lite Server

WakeMyPC Server Installation and Administration Guide

This Installation and Administration Guide covers both products. Where a section is applicable to both products the term WakeMyPC Server is generally used. Where a specific section only applies to one product this is explained in the text. Where specific differences exist they are covered in the text. For instance, the database features and majority of customisable settings are only applicable to WakeMyPC Enterprise Server. The supplied license keys are also different. WakeMyPC was originally codenamed WakeMAN. Technical references to WakeMAN refer to the WakeMyPC product.

This document explains how WakeMyPC server operates and provides a full walk-through installation. The instructions below are intended for a system / network administrator with experience of Microsoft Windows Server configuration and security, Internet Information Services (IIS) and, for Enterprise Server only, 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 2003/2008 system running IIS and MSSQL 2005 Standard Edition. 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.

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

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 wake gateway. The software may be used with any version of Windows IIS from Windows XP onwards.

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

Data Synergy's PowerMAN product is an ideal companion for any 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.

WakeMyPC Server Installation (All Editions)

Installation Prerequisites

WakeMyPC Server has the following requirements:

- A server with at least 2GB of RAM running Windows Server 2003 or 2008. Larger installations may require more RAM. The server may be either x86 or x86-64 based.
- Internet Information Services with ASP.NET support and the Microsoft .NET 4.0 Framework.

WakeMyPC Enterprise Server additionally requires:

- WakeMyPC Enterprise Server additionally requires Microsoft® SQL Server Express Edition 2005/2008 or greater with the most recent service pack installed.
- 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 (Enterprise Server only)

It is your responsibility to obtain the necessary Windows Server and Microsoft SQL Server product licenses.

The Microsoft .NET 4.0 Framework can be obtained from the following location:

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=0a391abd-25c1-4fc0-919f-b21f31ab88b7>

WakeMyPC Server Deployment Components

WakeMyPC Server is supplied as three components:

- WakeMyPC Website (hosted by Windows IIS). This is supplied in two ZIP files (only one is required).

The appropriate file must be extracted and configured using IIS:

WakeMAN5 Website x86.zip is for 32-bit operating system platforms

WakeMAN5 Website x64.zip is for 64-bit operating system platforms

- 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 backup file neatly encapsulates the more complex methods and is the most trouble free way to achieve a reliable deployment.

- 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 following additional assumptions apply to WakeMyPC Enterprise Server only:

- 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.

Installation Checklist

Before starting to deploy WakeMyPC 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 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

NB: This product key is a demonstration key and will not function on a live system. Please remember the client product key and the server product keys **are different**.

Walkthrough - Website Configuration Windows Server 2003

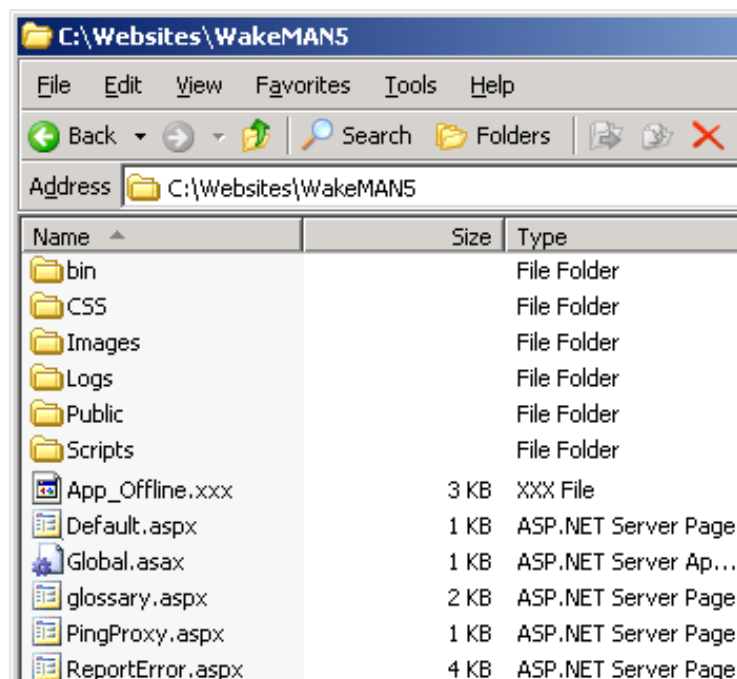
The following steps walk through a typical deployment on a system running Windows 2003 / IIS. It assumes that the website files are located in C:\Websites\WakeMAN5.

The procedure below assumes that the majority of the website is configured to allow anonymous access (the default). If you deviate from this assumption please remember that the **/Public** directory, as a minimum, must be available to anonymous clients. The one exception to this assumption is that the **/Secure** folder is configured to provide access only to appropriate Administrators. This is described in the procedure below.

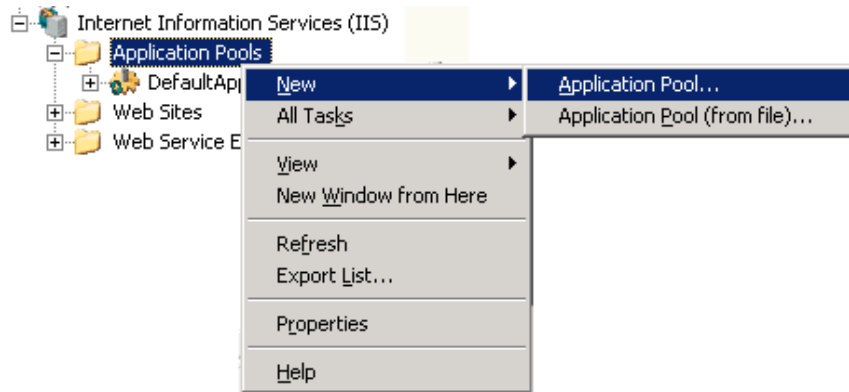
Before proceeding to configure the website please **confirm that the Microsoft .NET 4.0 Framework is installed**. The quickest way to do this is to check for the presence of the following folder: C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319

To configure the website proceed as follows:

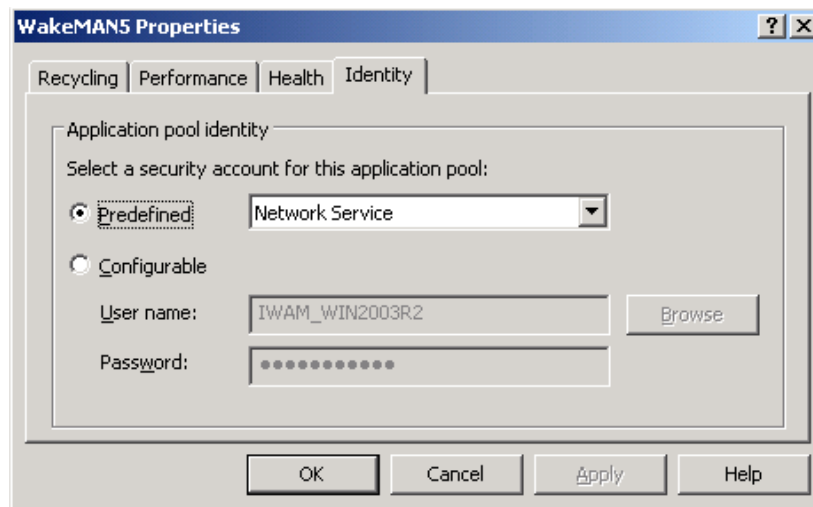
1. Create folder for website files: C:\Websites\WakeMAN5
2. Extract the appropriate WakeMAN5 Website ZIP file (x86 or x64) to this folder



3. Open the IIS Management snap-in
4. Navigate to Internet Information Servers\Application Pools
5. Right click and select **New\Application Pool**



6. Enter the pool name: **WakeMAN5** and click **OK**
7. Navigate to the newly created **WakeMAN5** application pool
8. Right click and select **Properties**
9. Navigate to the Identity tab
10. Select 'Predefined: Network Service' and click **OK**

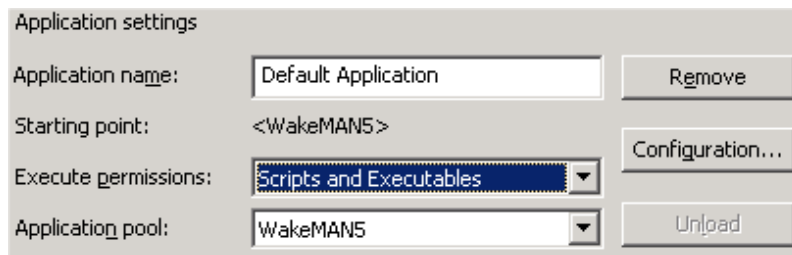


11. Navigate to **Websites**
12. Right click and select **NewWebsites**
13. Click **Next** and enter the website name: **WakeMAN5**. Click **Next** again.
14. Select the appropriate server IP address range (The default 'All Unassigned' is usually sufficient) and port number. The default port is **8000**. Click **Next**.

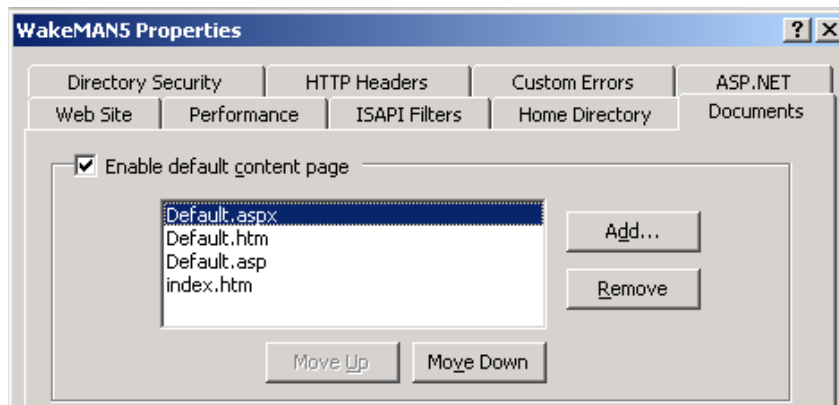
Important: The website **MUST** be accessible to remote users and the computers running the WakeMyPC client software. If the IIS server is behind a firewall please remember to ensure you have granted the appropriate access. If necessary you can configure the website to accept connections on more than one port.

WakeMyPC Server Installation and Administration Guide

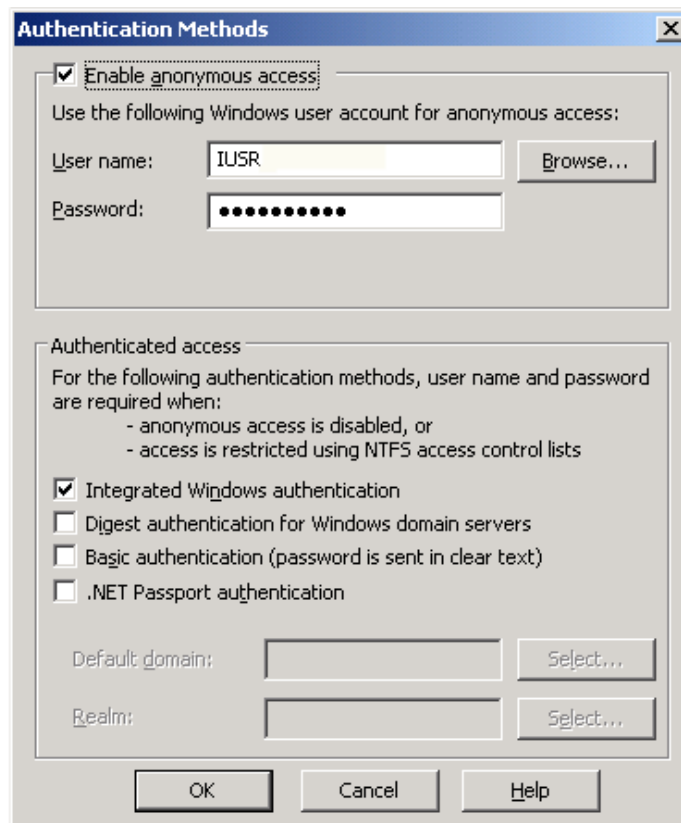
15. Enter the appropriate website file path: **C:\Websites\WakeMAN5**
16. Ensure 'Allow anonymous access to this website' is selected. Click **Next**
17. Ensure 'Read' is ticked. Click **Next** and then **Finish**
18. Right click on the newly created WakeMAN5 website and select **Properties**
19. Navigate to the **Home Directory** tab
20. Select '**Scripts and Executables**' (under Execute Permissions)



21. Select the recently created **WakeMAN5** application pool (as shown)
22. Click **Apply**
23. Navigate to the **Documents** tab
24. Confirm **Enable default content page** is selected and that a default entry is present for **Default.aspx**. If necessary click **Add** and add **Default.aspx**

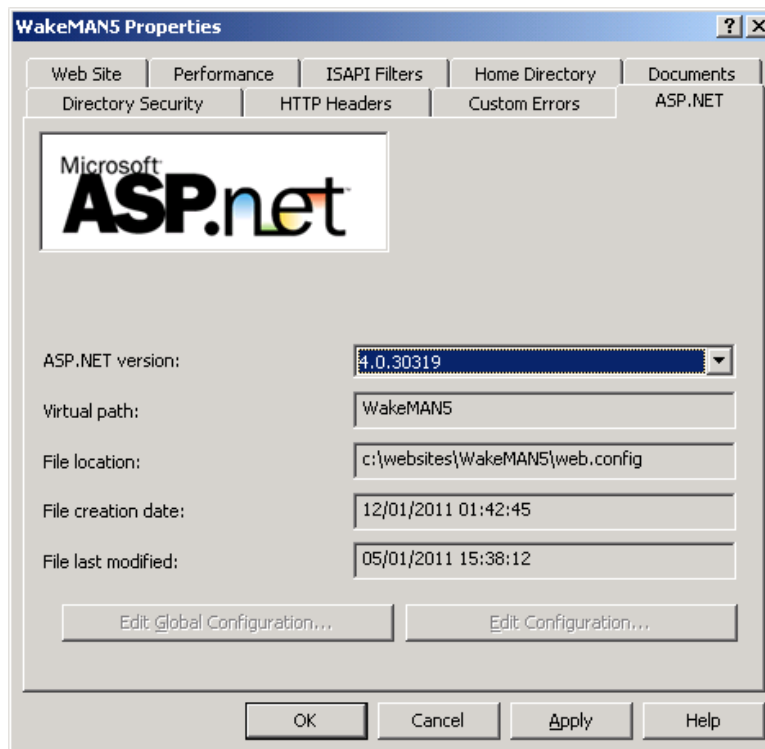


25. Click **Apply**
26. Navigate to the **Directory Security** tab and **press Authentication and Access Control\Edit**
27. Confirm that **Anonymous Access** and **Integrated Windows Authentication** are enabled and then click **Ok**:



28. Navigate to the **ASP.NET** tab.

29. Ensure that ASP.NET version is set to 4.0. If necessary change this and click **Apply**.



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\Framework\v4.0.30319\aspnet_regiis.exe -i
```

30. Navigate to the **Website** tab 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.

Walkthrough - Website Configuration Windows Server 2008

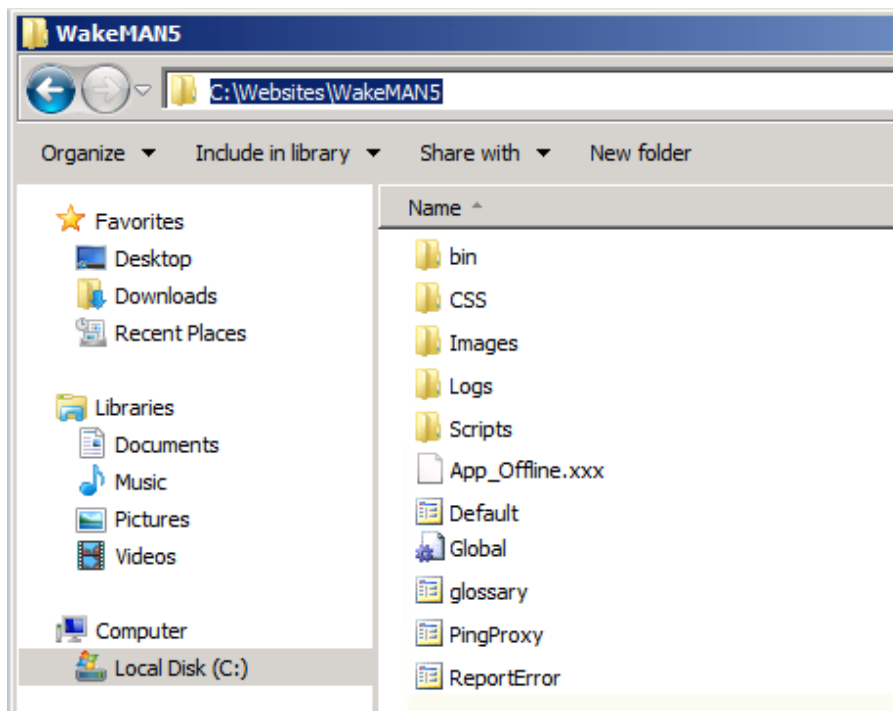
Windows Server 2008 (IIS 7) differs in several important respects from previous versions. The following steps walk through a typical deployment on a system running Windows 2008 / IIS 7. It assumes that the website files are located in C:\Websites\WakeMAN5.

The procedure below assumes that the majority of the website is configured to allow anonymous access (the default). If you deviate from this assumption please remember that the **/Public** directory, as a minimum, must be available to anonymous clients. The one exception to this assumption is that **the /Secure** folder is configured to provide access only to appropriate Administrators. This is described in the procedure below.

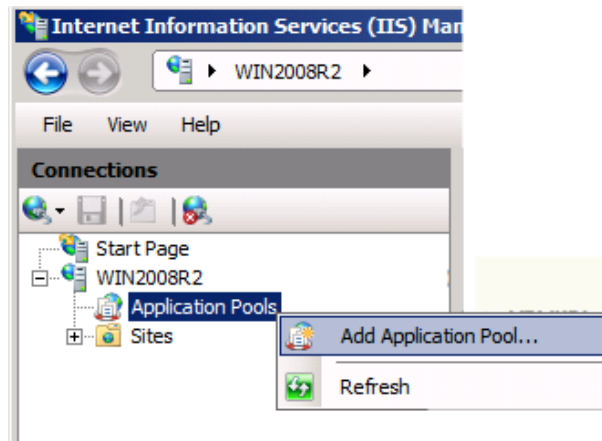
Before proceeding to configure the website please **confirm that the Microsoft .NET 4.0 Framework is installed**. The quickest way to do this is to check for the presence of the following folder: C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319

To configure the website proceed as follows:

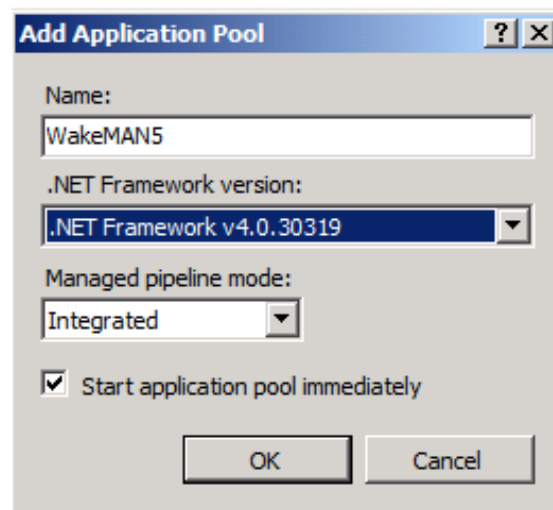
1. Create folder for website files: C:\Websites\WakeMAN5
2. Extract the appropriate WakeMAN5 Website ZIP file (typically x64) to this folder



3. Open the Server Manager
4. Locate the **Internet Information Services (IIS)** Management snap-in (INETMGR.EXE)
5. Navigate to **Application Pools**
6. Right click and select **Add Application Pool**



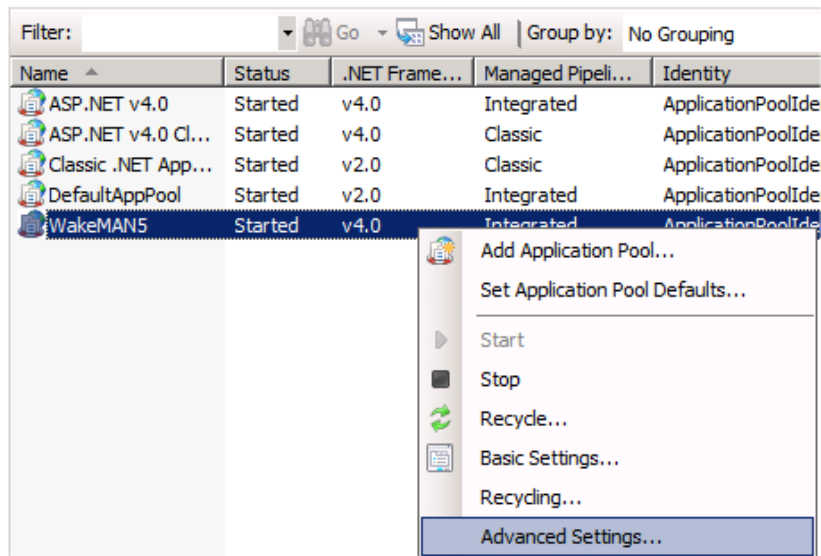
7. Enter the pool name: **WakeMAN5** and select **.NET Framework v4.0.30319**:



8. Navigate to the newly created **WakeMAN5** application pool

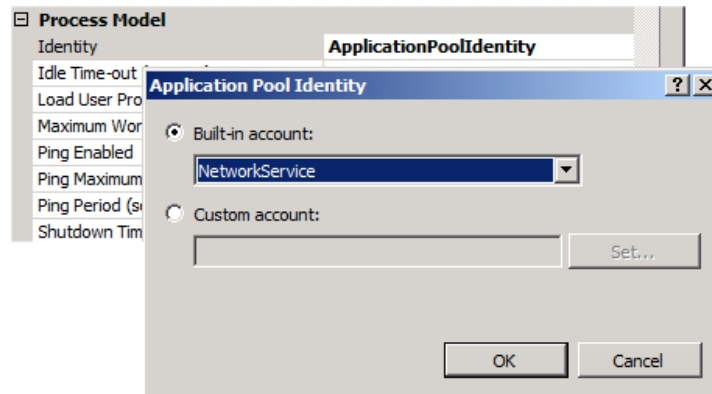
WakeMyPC Server Installation and Administration Guide

- Right click and select **Advanced Settings**



- Navigate to the **Identity** setting and press 

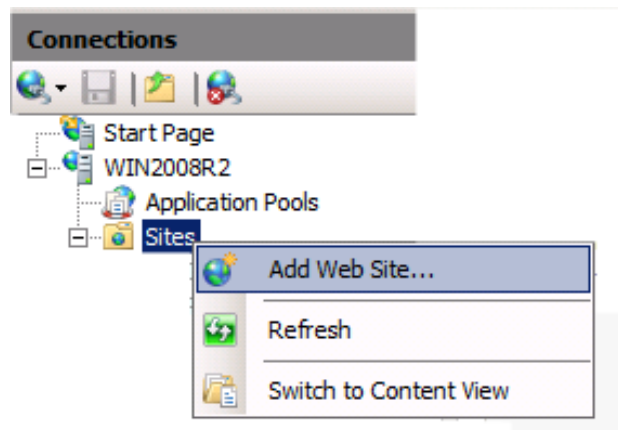
- Select **Built-in account: Network Service** and click **OK**



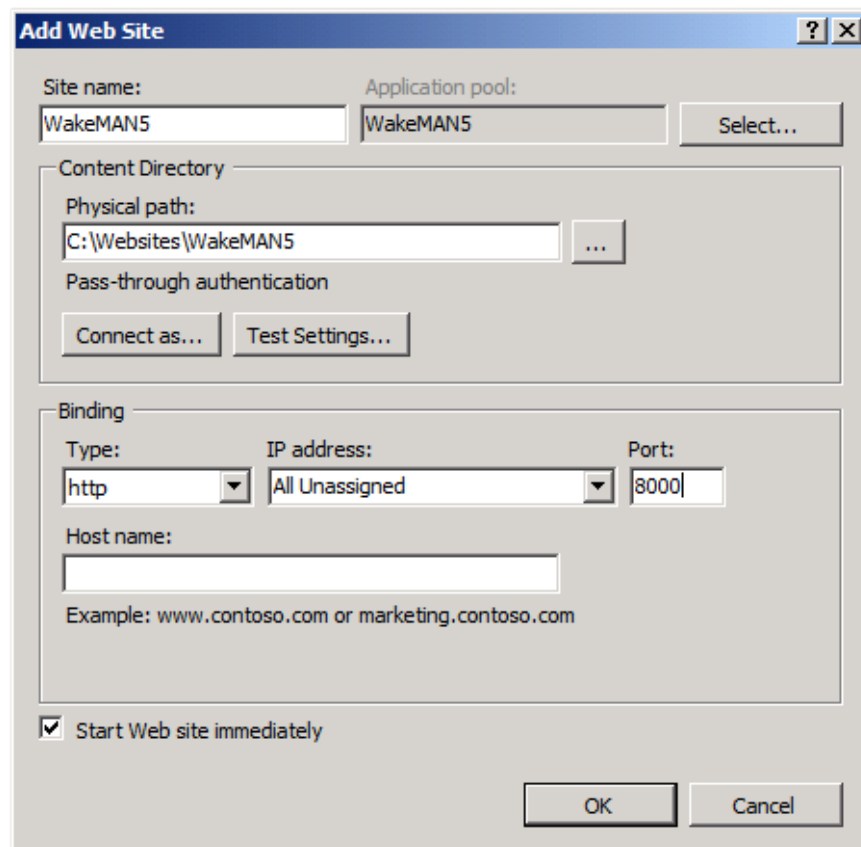
Tip: If the SQL database is located on a remote server you must also change the **'Load User Profile'** option to **True**:

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

- Close the Application Pool settings by selecting **OK**
- Navigate to **Sites**
- Right click and select **Add Web Site**



15. Enter the Site Name: **WakeMAN5**
16. Select the Application Pool: **WakeMAN5**
17. Select the appropriate website path, server IP address range (The default 'All Unassigned' is usually sufficient) and port number. The default port is **8000**. Click **OK**.



Add Web Site

Site name: Application pool:

Content Directory

Physical path:

Pass-through authentication

Binding

Type: IP address: Port:

Host name:

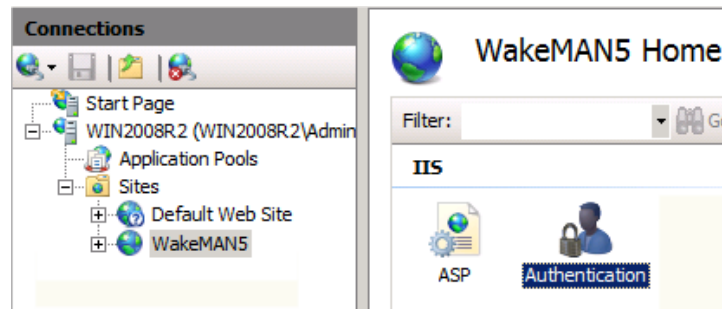
Example: www.contoso.com or marketing.contoso.com

Start Web site immediately

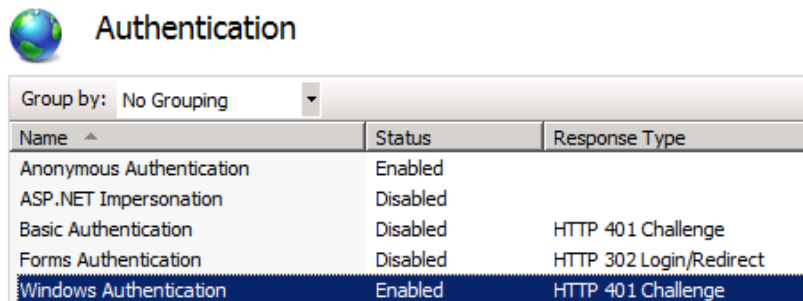
Important: The website **MUST** be accessible to the computers running the WakeMyPC client software. If the IIS server is behind a firewall please remember to ensure you have granted the appropriate access. If necessary you can configure the website to accept connections on more than one port.

WakeMyPC Server Installation and Administration Guide

18. Double click on the **WakeMAN5** website to open the site
19. Navigate to **Authentication** and double click



20. Confirm that **Anonymous Authentication** and **Windows Authentication** are both enabled (shown below):



Tip: IIS 7 includes a number of changes over previous versions. In particular the way anonymous website access operates has changed. The built-in IUSR account replaces the IUSR_MachineName account. 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.

WakeMyPC Enterprise Server Installation Steps

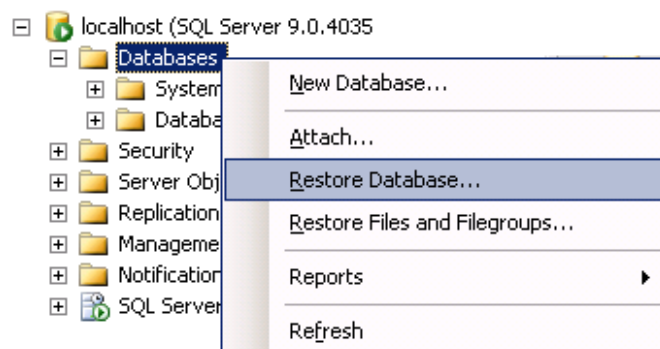
The following additional database configuration steps apply to WakeMyPC Enterprise Server only. **No database component is required for WakeMyPC Lite Server Edition.**

SQL Database Configuration Walk-through

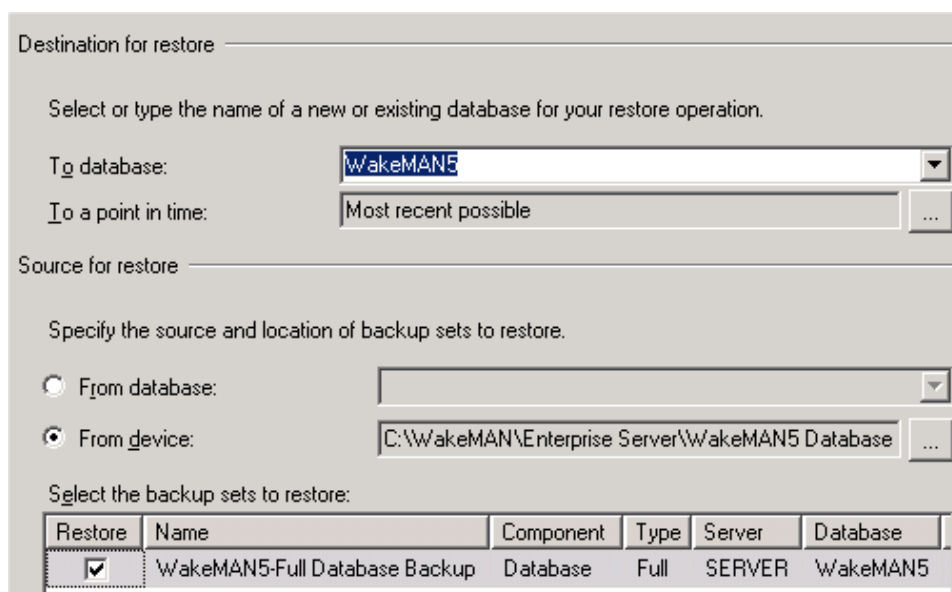
The following steps walk through a typical deployment using Microsoft SQL 2005/2008 Server. It assumes that the database files are to be located in C:\Database\WakeMAN5.

The database can be installed using the following steps:

1. Create folder for database files. C:\Databases\WakeMAN5
2. Open SQL Server Management Studio
3. Start the database restore wizard

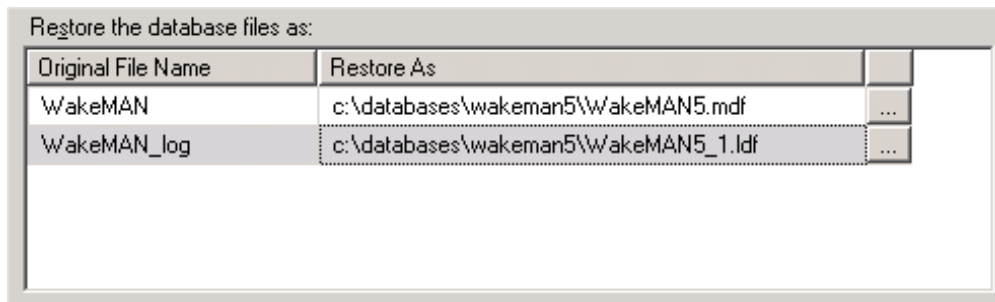


4. Configure the database name as: WakeMAN5
5. Select **From Device**, click ... and locate the **WakeMAN5 Database.bak** file

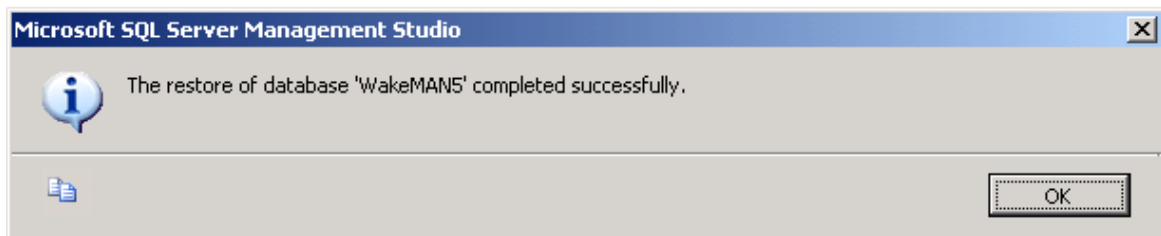


WakeMyPC Server Installation and Administration Guide

6. Select **Options** and modify the restore path to the required folder e.g. C:\Databases\WakeMAN5

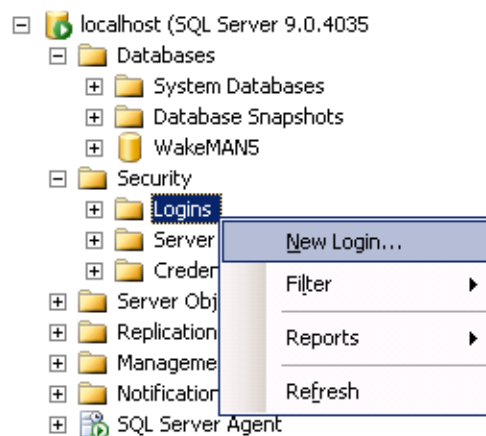


7. Click **OK** to restore the database. On a typical server this will take only a few seconds:



The database should be configured using the following procedure:

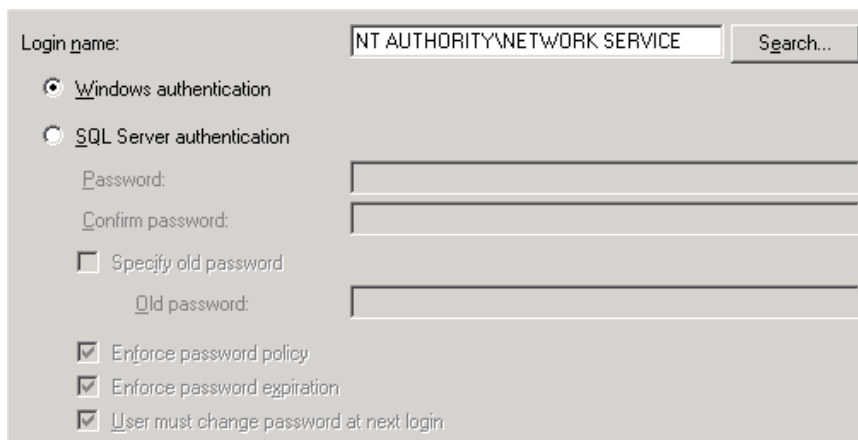
1. Open **SQL Server Management Studio**
2. Navigate to **Security\Logins**
3. Right click and select **New Login**



4. Click **Search**
5. Enter **Network Service** in the box and click **OK**

WakeMyPC Server Installation and Administration Guide

6. Confirm the local '**Network Service**' account is listed (as shown below) and click **OK** again



Login name:

Windows authentication
 SQL Server authentication

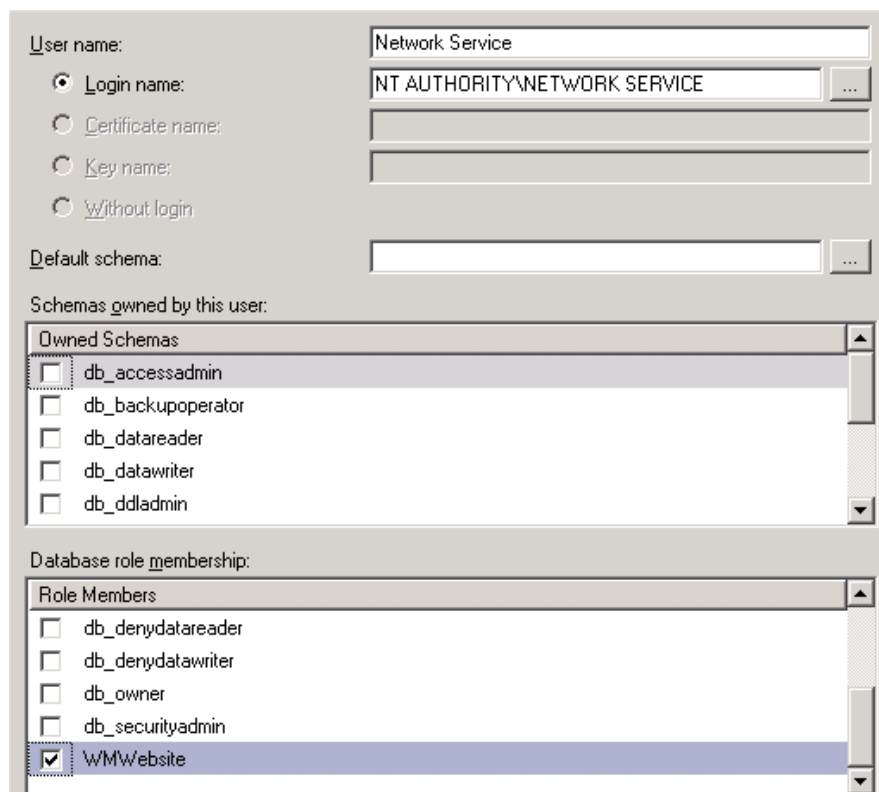
Password:
 Confirm password:

Specify old password
 Old password:

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

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

Tip: If the Network Service user already exists in the WakeMAN5 database right click on the Network Service user, select **Properties** and confirm the '**WMWebsite**' role is assigned as shown below.



User name:

Login name:
 Certificate name:
 Key name:
 Without login

Default schema:

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

Database role membership:

Role Members	
<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

WakeMyPC Server Installation and Administration Guide

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.

Using a remote SQL Server

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

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

This section assumes that both the web server and SQL server are members of the **same Windows domain**. The procedure below replaces the Network Service account with a standard domain user account. This account provides secured database access to the WakeMyPC Server website. The procedure described is for Windows 2003. An almost identical procedure may be used for later releases.

To create the domain user account proceed as follows:

1. Open the **Active Directory Users and Computers** snap-in
2. Right click on Users and select **NewUser**
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

WakeMyPC Server Installation and Administration Guide

12. Select **Configurable**
13. Click **Browse** and locate the domain user (e.g. 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**.

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 (e.g. WakeMAN). Click **OK**
6. Select **Read** (deselect all other options) and then click **OK**

Windows 2003: You must also add the application pool identity (domain user) to the local **IIS_WPG** group.

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

1. Open **SQL Server Management Studio**
2. Navigate to **Security\Logins**
3. Right click and select **New Login**
4. Click **Search**
5. Locate the recently created domain user account (e.g. WakeMAN) 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 'Website' 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
```

Securing the WakeMyPC Enterprise Server Website

This section explains how to secure the WakeMyPC website. The following sections explain this in more details for Windows 2003 and Windows 2008.

The WakeMyPC Enterprise Server website groups functionality into three 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
- **/Admin** – Administration tools for day-to-day administration
- **/User** – Used-driven wake-up and workstation registration pages

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.

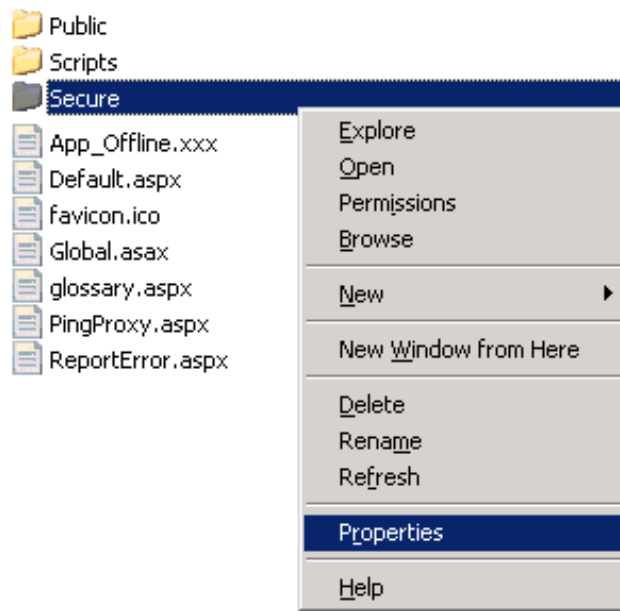
The **/Secure** folder contains tools **only** for administrator use. The pages within this folder are used to perform the initial online server configuration and to administer the WakeMyPC Server system. These pages **MUST be secured** as they must not be available for anonymous access.

Walkthrough: Securing the website - Windows 2003

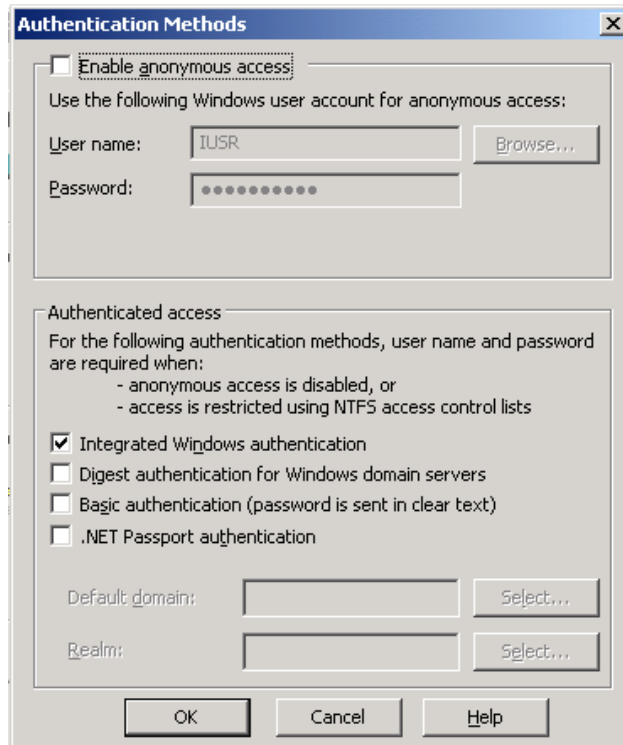
This section explains how to secure the /Secure folder on Windows 2003. The same technique may be used to secure both /Admin and, if necessary, the /User folders. The subsequent section explains the same process for Windows 2008.

To disable anonymous access for this folder proceed 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 **Properties**



5. Navigate to the Directory Security tab and press **Edit**
6. Untick **'Enable Anonymous Access'**
7. Ensure **'Integrated Windows Authentication'** is selected.
8. Click **OK**

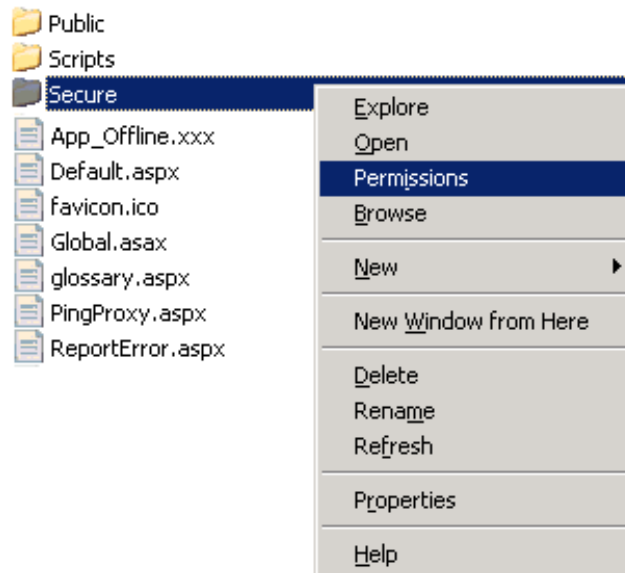


To configure the specific users / groups permitted to access this folder proceed as follows:

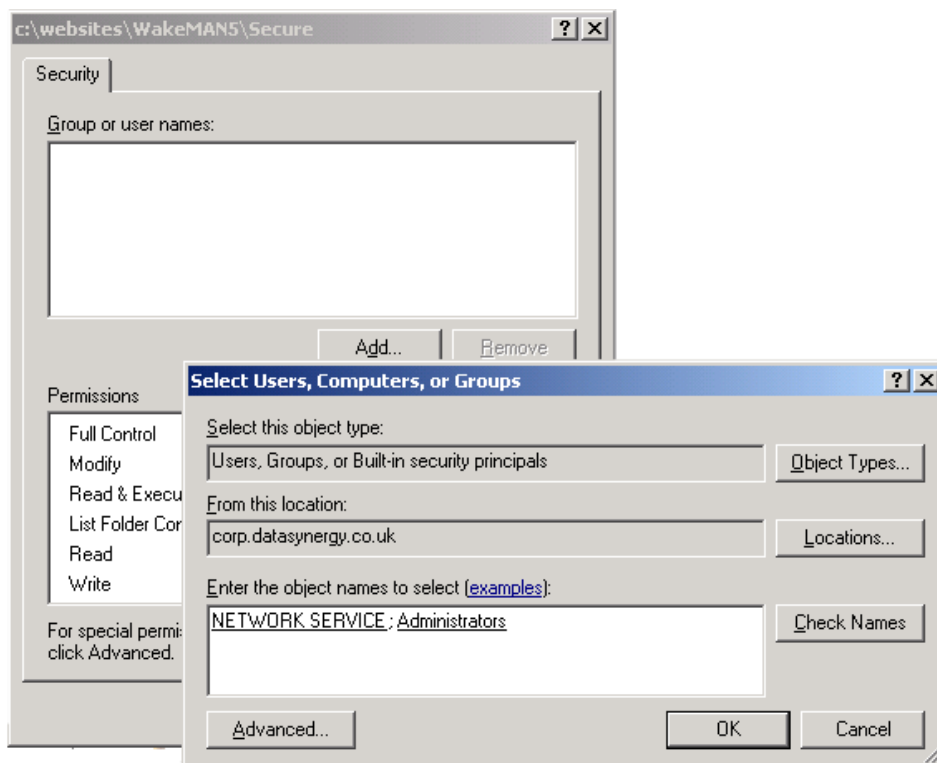
9. Open the IIS Management snap-in

WakeMyPC Server Installation and Administration Guide

10. Navigate to **Websites\WakeMAN5**
11. Locate the **Secure** folder in the right hand pane
12. Right click and select **Permissions**



13. Click **Advanced**
14. Un-tick '**Allow inheritable permissions from the parent to propagate**'
15. If prompted, click **Remove** and then click **OK** (if prompted by a warning click **Yes**)
16. Click **Add** and select the users or groups who will be allowed access to the secure website pages. For instance: **Network Service** and **Administrators**:



17. Click **OK**

18. Confirm the selected users have **Read access** (you can deselect Read & Execute and List Folder Contents) and click **OK**

NB: Please remember the Network Service **MUST** be included in the user list for the website to function correctly.

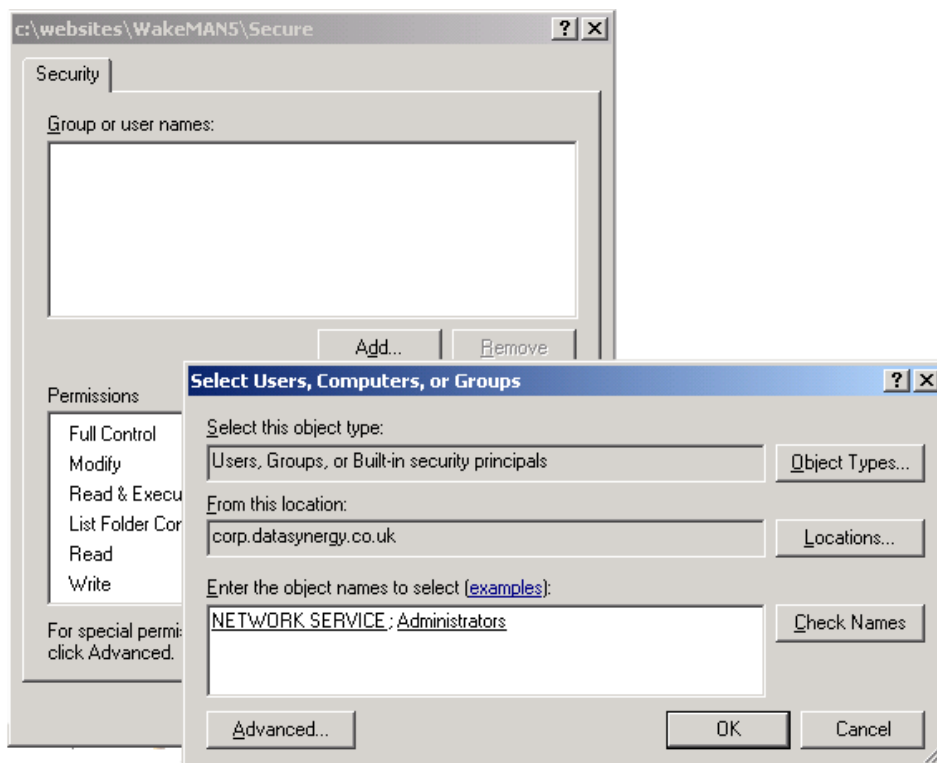
Tip: You can also remove or rename the **Secure** folder for added security. It is not required for day-to-day server use.

Walkthrough: Securing the website - Windows 2008

This section explains how to secure the /Secure folder on Windows 2003. The same technique may be used to secure both /Admin and, if necessary, the /User folders. This is very similar to the previous section describing Windows 2003 with minor changes.

To disable anonymous access for this folder proceed as follows:

1. Open the Server Manager
2. Locate the **Internet Information Services (IIS)** Management snap-in (INETMGR.EXE)
3. Navigate to **Sites**
4. Locate the **WakeMAN5** site
5. Select **Content View**
6. Locate the **Secure** folder
7. Right click and select **Edit Permissions**
8. Navigate to the **Security** tab and press **Edit**
9. Click **Advanced**
10. Click **Changed Permissions** (if necessary)
11. Un-tick '**Include inheritable permissions from this objects parent**'
12. Click **Remove** and then click **OK** (if prompted by a warning click **Yes**)
13. Click **Add** and select the users or groups who will be allowed access to the secure website pages. For instance **Network Service** and **Administrators**:



14. Click **OK**

15. Confirm the selected users have **Read access** (you can deselect Read & Execute and List Folder Contents) and click **OK**

NB: Please remember the Network Service **MUST** be included in the user list for the website to function correctly.

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

Configuring WakeMyPC Server

The remaining WakeMyPC Server 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.

As supplied the file 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 will normally be required with Enterprise Server edition:

- **SMTPServer, WebsiteEmail and BugEmail** – This will need to be configured if you intend to use the email features
- **ConnectionString** (Enterprise Server only) – This may need to be changed if the database is located on another server or is not using the default SQL instance

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.

WakeMyPC Lite Server and Enterprise Server Common Settings

The following settings apply to both WakeMyPC Lite Server and Enterprise Server editions.

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
PostErrorURL	The fully qualified URL that users will be redirected to in the event of a software error: <i>e.g. http://www.datasynergy.co.uk</i>
WakeTimeoutSeconds	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: e.g. 120
WakeRefreshSeconds	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. e.g. 5
WakeConnectURL	The URL used for post-wake activities. This is described further in

	<p>subsequent sections.</p> <p>e.g. ~/TSWeb/?Server=\$computername\$. \$fqdomainsuffix\$&AutoConnect=1</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>
LogPath	<p>The relative path to the WakeMyPC event log folder. This is used to record significant runtime events. This should be prefixed with a ~ character:</p> <p>e.g. ~/Logs</p>
LogRetainDays	<p>The number of days to retain WakeMyPC event logs. The minimum period is 30 days:</p> <p>e.g. 90</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>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> <p>1 = Use IP address 2 = Use unqualified computer name (default) 3 = Use fully qualified computer name (requires FQDomainSuffix)</p> <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 allows the WakeMyPC server to be operated externally.</p>
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>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</p>

	<p>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>
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>
UsernameRequired	<p>Require user authentication to access pages within the /User folder and sub-folders. This is False by default.</p> <p>e.g. False</p>
UsernameUnknownPage	<p>The page unauthenticated users are redirected to. This feature is only applicable when UsernameRequired=True. A default placeholder page is provided.</p> <p>e.g. ~/LoginRequired.aspx</p>
SMTPServer	<p>The SMTP server used for sending emails:</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>
STMPEnableSSL	<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>

WakeMyPC Enterprise Server Specific Settings

The following settings apply to only to WakeMyPC Enterprise Server. They may be present in other editions but will have no effect:

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>
PowerMAN ConnectionString	<p>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.</p> <p>Configuring this feature activates PowerMAN integration. This allows sites to be conveniently imported from a PowerMAN server and synchronised with the WakeMyPC server.</p>
DataRetainDays	<p>The number of days to retain per-workstation information. The minimum period is 30 days:</p> <p>e.g. 60</p>
SecurePath	<p>The URL of the secure administration folder. This is prefixed with a tilde character:</p> <p>e.g. ~/Secure</p>

Configuring WakeMyPC Server Logging

WakeMyPC include an 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**

WakeMyPC Workstation Availability Checker (Probe)

WakeMyPC Server 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.

WakeMyPC Scripting and scheduling

The primary function of WakeMyPC is to perform user driven, ad-hoc, wake-up of single workstations and groups of workstations. In some cases it may also be desirable to 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 – Wake a single workstation
- /WakeSite.aspx – Wake a group (site) of workstations
- /Admin/WakeAll.aspx – Wake all known workstations

The full syntax for each page is documented in the 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.

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.

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.

Remote Desktop Web Connection

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 Server) is available from the following link:

<http://www.microsoft.com/downloads/details.aspx?familyid=e2ff8fb5-97ff-47bc-bacc-92283b52b310>

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=\$computename\$. \$fqdomainsuffix\$&AutoConnect=1

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

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 Server Testing

WakeMyPC Server 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.

WakeMyPC Server 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

WakeMyPC Enterprise Server 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 WakeMyPC Enterprise Server 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	
License Expiry	01/01/2012
License Limits	10000 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)

WakeMyPC Server Tools

Setting	Value
ConnectionString	Data Source=localhost;Initial Catalog=WakeMAN5;Integrated Security=True
SMTPServer	localhost
BugEmail	example@yourcompany.com Test
Exit	

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>

WakeMyPC Enterprise 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.

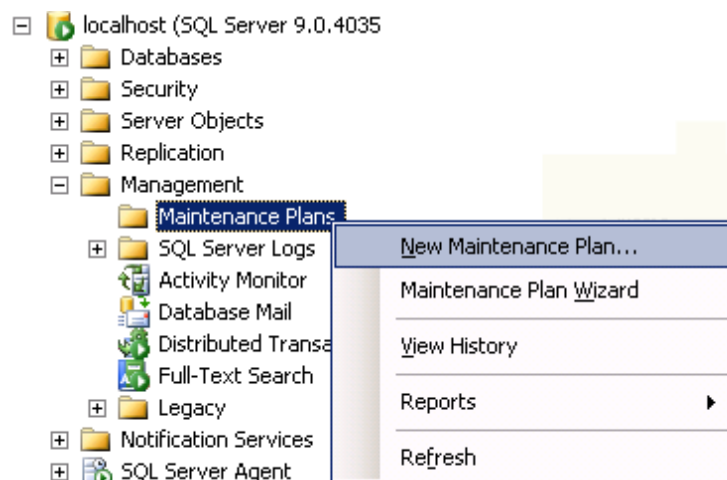
The following Microsoft article provides additional guidance on selecting the appropriate backup strategy:

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

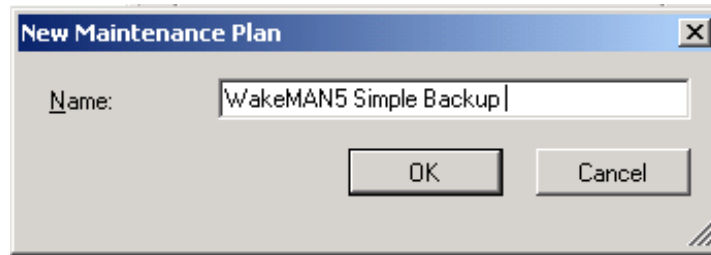
You must decide the appropriate database backup strategy for your WakeMyPC Enterprise Server deployment.

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

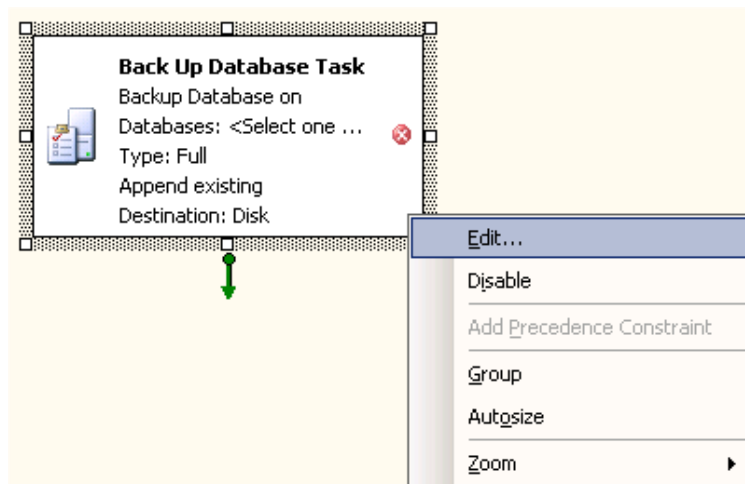
1. Open SQL Server Management Studio
2. Navigate to Management\Maintenance Plans
3. Right click and select New Maintenance Plan



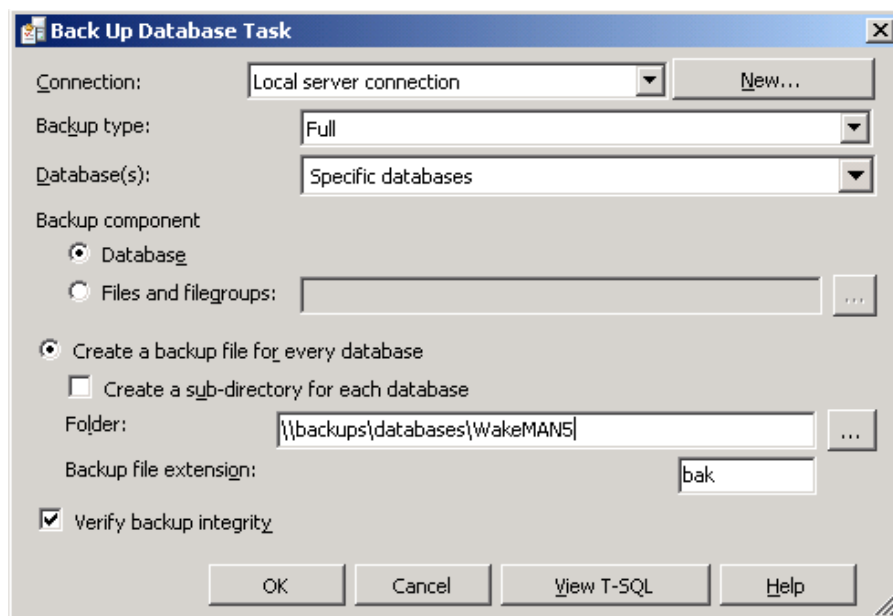
4. Enter an appropriate plan name: **WakeMAN5 Simple Backup**



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.

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 Server

WakeMyPC Server has undergone many thousands of hours 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: Servercheck.aspx takes excessive time (>1 second) to display**Problem: 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. WakeMyPC Lite and Enterprise Server both log errors to the /Logs folder. 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

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

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

```
%windir%\Microsoft.NET\Framework\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: 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_WPG** 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: "HTTP Error 404 - File or Directory not found" error message when you request an ASPX page

This problem can occur if ASP.NET was installed prior to IIS. This happens because, by default, when IIS is installed on any version of the Windows Server 2003 family, IIS only serves static content (HTML).

Support for ASP.NET must be manually enabled on such systems. This problem does not generally happen on later operating systems or when ASP.NET is installed after IIS.

To resolve this problem please follow the instructions in the following Microsoft article:

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

Problem: Unrecognized attribute "targetFramework" reported when you request an ASPX page

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.

Problem: Website reports - Could not load file or assembly 'PowerLib' or one of its dependencies. An attempt was made to load a program with an incorrect format

This error is reported when there is a mismatch between the installed website and the server hardware. Please check that the installed website platform (x86 or x86-64) matches your server hardware. If necessary replace the website with the correct version. This error can also occur if the Microsoft Visual C++ 2010 Redistributable Package is not installed. See related troubleshooting section below.

Problem: "The application has failed to start because its side-by-side configuration is incorrect. Please see the application event log or use the command-line sxstrace.exe tool for more detail. Exception from HRESULT: 0x800736B1" error message when you request an ASPX page**OR Could not load file or assembly 'PowerLib.dll' or one of its dependencies. The specified module could not be found.**

This problem can when the Microsoft Visual C++ Runtime is missing from the server. This is normally present on most systems and may indicate that the .NET 4.0 Framework is not installed. Please see above for instructions on how to install this Windows component.

If the .NET Framework is installed then it may be necessary to download and manually install the runtime appropriate for your platform:

Microsoft Visual C++ 2010 Redistributable Package (x86 32-bit):

<http://www.microsoft.com/download/en/details.aspx?id=5555>

Microsoft Visual C++ 2010 Redistributable Package (x64 64-bit):

<http://www.microsoft.com/download/en/details.aspx?id=14632>

If the problem continues after installing the appropriate runtime package Data Synergy Technical Support will be able to help you diagnosis the problem further. Please contact Technical Support with a SxSTrace log file. This may be generated as follows:

1. Start an command prompt (elevated on Windows Server 2008)
2. Enter the command:

```
SXSTRACE trace -logfile:sxstrace.etc
```

NB: This will leave a prompt on-screen reminding you to press [Enter] to stop the logging. Please do not shut this window.

3. Refresh the browser and confirm the error is still present
4. Return to the command prompt window and press [Enter] to stop the SXSTRACE trace
5. Enter the command:

```
SXSTRACE parse -logfile:sxstrace.etl -outfile:sxstrace.txt
```
6. The 'sxstrace.txt' file now contains readable log file. Please send this to technical Support.

Problem: Website generated URLs fail to work correctly.

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.

Appendix A – Data Synergy Remote Desktop Launcher

Overview

The 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 Terminal 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://$computername$.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. WakeMyPC Agent is not available with WakeMyPC Lite Server

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 webpage parameters

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 majority of pages are only available in WakeMyPC Enterprise Server edition. The WakeManual.aspx page is available in all editions.

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 parameter: ClientGUID</p> <p>Example: WakeComputer?ClientGUID={5fff352d-413a-4510-ba28-ebd4488df735}</p>
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 parameter: SiteGUID</p> <p>Example: WakeSite?SiteGUID={8a63b6b9-f031-4f6e-a3f8-2c7f409c747f}</p>
AdminWakeAll.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 provide enhanced security.</p> <p>Supported parameter: None required</p>
User\ComputerSetup.aspx	<p>Add or update an existing workstation</p> <p>Supported parameters: ComputerName IPAddress SubnetMask MacAddress Username (optional) ClientGUID (optional)</p> <p>Example: ComputerSetup.aspx ?ClientGUID={3ad36a85-1d48-4f58-9d61-d346f0977d00} &ComputerName=Accounts&UserName=Brenda &IPAddress=192.168.100.67&SubnetMask=255.255.255.0 &MacAddress=0026C7561234</p>
UserWakeManual.aspx	<p>Wake a specific workstation using known network information. This page is available in WakeMyPC Lite Server edition.</p> <p>Supported parameters: ComputerName MacAddress WoIMode IPAddress (required for subnet directed and direct modes)</p>

	SubnetMask (required for subnet directed and direct modes) Example: Wakemanager.aspx?ComputerName=Accounts &IPAddress=192.168.100.67&SubnetMask=255.255.255.0 &MacAddress=0026C7561234&WolMode=2
User\WakeSearch.aspx	Find and then wake a workstation Supported parameter: ComputerName Example: WakeSearch.aspx?ComputerName=Accounts

Appendix D – Authenticating Workstation Wake-up

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

- No authentication required (Default)
- IIS Integrated Windows Authentication (NTLM)
- 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. For instance to secure this folder on a Windows 2008 Server proceed as follows:

1. Open the Server Manager
2. Locate the **Internet Information Services (IIS)** Management snap-in (INETMGR.EXE)
3. Navigate to **Sites**
4. Locate the **WakeMAN5** site
5. Select **Content View**
6. Locate the **User** folder
7. Right click and select **Edit Permissions**
8. Navigate to the **Security** tab and press **Edit**
9. Click **Advanced**
10. Click **Changed Permissions** (if necessary)
11. Un-tick '**Include inheritable permissions from this objects parent**'
12. Click **Remove** and then click **OK** (if prompted by a warning click **Yes**)

WakeMyPC Server Installation and Administration Guide

13. Click **Add** and select the users or groups who will be allowed access to the wake-up website pages. For instance **Network Service** and **WakeUpUsers**.
14. Click **OK**
15. Confirm the selected users have **Read access** (you can deselect Read & Execute and List Folder Contents) and click **OK**

NB: Please remember the Network Service **MUST** be included in the user list for the website to function correctly.

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. All of the pages in the /User folder support this feature.

This feature maybe used in either of the following ways:

1. 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 – Upgrading existing WakeMyPC / WakeMAN Servers

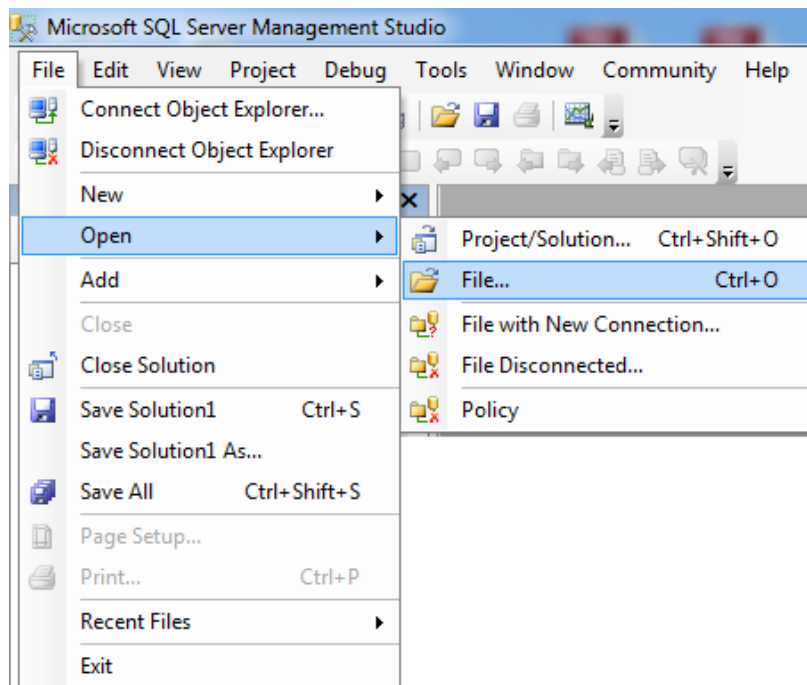
Existing WakeMyPC (formally WakeMAN) Server deployments may be updated to the current software release by using the following quick procedure:

1. Backup the existing web.config file
2. Delete the existing WakeMyPC / WakeMAN website
3. Follow the installation procedure above to install the new website
4. If using Enterprise Server and upgrading from v5.1.x to v5.1.3 follow the procedure below to update the existing SQL database

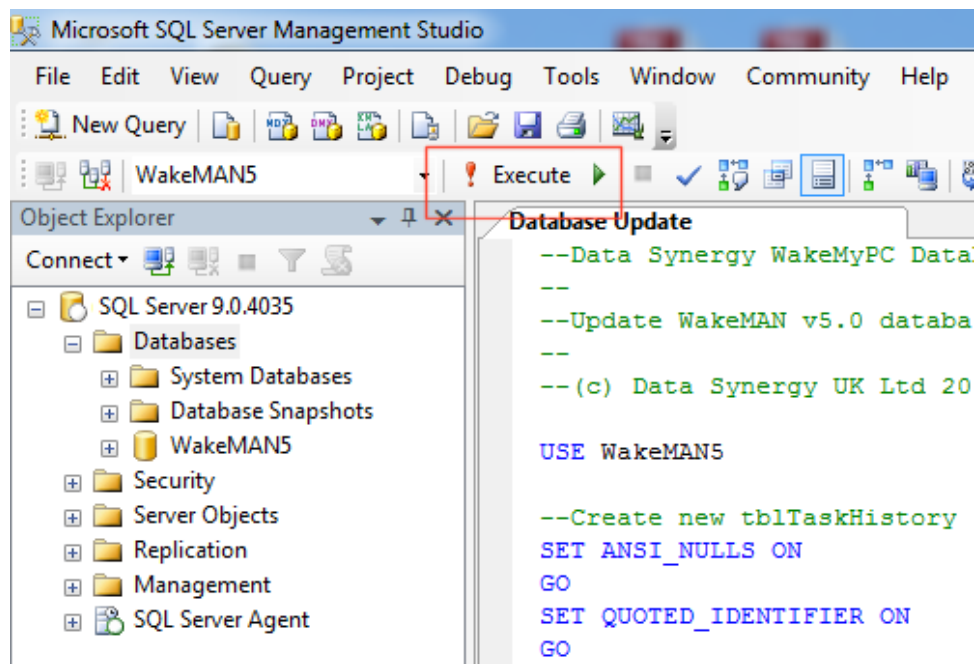
Appendix F – WakeMyPC Database v5.1.x Update Procedure

Existing WakeMyPC (formally WakeMAN) Enterprise Server deployments require a SQL database upgrade to function with the v5.1.3 software release. This procedure is not applicable to Lite Edition. To update the database proceed as follows:

1. Open SQL Server Management Studio
2. Select the File menu and then Open/File:



3. Locate the database update script. This is located in the **Enterprise Server\Existing Database Update** folder of the WakeMyPC distribution
4. Click **Execute**. The database update should only take a second:



5. Confirm that the update has installed successfully:

