



WakeMyPC Agent 5.2

Installation and Administration Guide

Release 5.2.0.326 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 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 Agent Overview | 5 |
| Agent Installation Prerequisites | 5 |
| Product Installation | 6 |
| Preparation | 6 |
| Microsoft Windows Group Policy Deployment Method | 7 |
| Alternative SMS / XCOPY Deployment Method | 17 |
| Deploying WakeMyPC Agent in a pre-built software image 'Ghost'-style deployment..... | 17 |
| Advanced Settings | 18 |
| How WakeMyPC Agent Works..... | 19 |
| Additional WakeMyPC Features | 19 |
| Windows Event Log | 19 |
| Troubleshooting | 20 |
| Problem: WakeMyPC Agent does not deploy correctly using the GPO method | 20 |
| Problem: WakeMyPC Agent is installed but the computers are not showing up on the server system..... | 22 |
| OR WakeMyPC Event Log entry reports Event #6015: Downloaded XML was corrupt | 22 |
| Problem: Application event log reports WakeMyPC error #2002 - Product key has expired. Please contact your sales representative to obtain an updated product key. The software will continue to function in reduced functionality mode. . | 23 |
| Problem: Some computers wake-up (resume) unexpectedly | 23 |
| Problem: Some computers fail to suspend / resume reliability and consistently | 24 |
| Problem: Unable to resume computer using selected input / button method | 24 |
| OR Unable to resume PC using a USB keyboard / mouse..... | 24 |
| OR Unable to resume PC using Wake-On-Lan (WOL)..... | 24 |
| OR Unable to configure Device Manager power management remotely | 24 |
| Problem: Network drive is disconnected after system has resumed..... | 29 |
| Other Deployment Resources..... | 29 |
| Appendix A – WakeMyPC Agent Command-line options..... | 30 |
| Appendix D – WakeMyPC Agent Policy Settings Reference | 31 |
| General Information | 31 |
| Product Licensing..... | 31 |
| WakeMyPC Server Configuration | 32 |
| Debugging / Advanced Settings..... | 33 |
| Appendix E - Alternative Configuration Method - Local Group Policy / Registry Settings | 34 |
| Example Registry File | 35 |

| | |
|-----------------------------------------------------|-----------|
| Appendix I – Common Event Log Messages | 36 |
|-----------------------------------------------------|-----------|

WakeMyPC Agent Overview

WakeMyPC Agent is an optional component of Data Synergy's WakeMyPC Server Enterprise software. 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 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 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.

Agent Installation Prerequisites

WakeMyPC Agent supports the following platforms:

- Windows Vista and Windows 7, Windows 8.x and Windows 10.0 (32-bit and 64-bit platforms)
- Windows 2008, 2012 and 2016 Server (64-bit platforms)

The WakeMyPC agent is a common executable (EXE) on all supported versions of Windows. The client software is available in both 32-bit and 64-bit formats. The 32-bit version may be used in mixed 32/64-bit workstations estates and offers identical features on 64-bit systems.

WakeMyPC Agent provides a common executable (EXE) on all supported versions of Windows. In most cases the product offers identical features on each version of Windows. There are some minor differences between operating systems due to operating system design. Where necessary these are highlighted in this guide. In all other circumstances features and configuration are identical.

WakeMyPC Agent is designed to integrate seamlessly with a **Windows Active Directory / Group Policy (GPO)** infrastructure and can, in many cases, be configured and deployed in less than one hour.

Alternatively, WakeMyPC Agent may be installed with a variety of alternative deployment and configuration methods. Common examples are:

- ZENworks
- LANDesk
- RM Community Connect
- Altiris
- HP OpenView
- SMS
- SCCM
- XCOPY style installation (single self-installing EXE)

The following sections explain the two most common deployment methods using Windows GPO and an SMS/XCOPY style installation. It also explains how the configuration Registry settings may be created, without an Active Directory infrastructure, using a standard Windows Vista or later client computer.

Product Installation

Preparation

Before starting on a WakeMyPC Agent deployment there are a few essential steps to prepare:

1. **Confirm the WakeMyPC Enterprise Server** is installed and functioning correctly
2. **Obtain a unique WakeMyPC Agent 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 WakeMyPC Agent product key and the WakeMyPC Enterprise Server product keys are **different**.

WakeMyPC **evaluation product keys** are designed to expire. When this happens WakeMyPC ceases to function. There is **no user pop-up** when the product key expires and the process is transparent to the user.

3. **Identify a workstation grouping strategy.** The available options are:
 - **None** – Do not group workstations together (group wake-up will be unavailable)
 - **SiteGUID** – Register a unique SiteGUID on the WakeMyPC Server for each group of computers and assign this SiteGUID using the available policy setting to each group of computers. There is further information on this topic in the WakeMyPC Enterprise Server manual.
 - **PowerMAN Integrated (Default)** – Inherit workstation grouping from an existing Data Synergy PowerMAN software installation. The SiteGUID used for PowerMAN will automatically be used for WakeMyPC

Groups of workstations are known as 'Sites' within WakeMyPC and PowerMAN.

An **ideal site** is a group of similar PC's within a defined environment such as an office, department or computer room. A typical site can have from 20 to several hundred computers and will be **suitable for managing as a single entity**.

You can easily create additional sites to logically divide your estate of computers. There is no limit on the number of sites supported.

4. **Select a deployment method** – WakeMyPC Agent may be deployed using a variety of methods. The two most common, using Windows Group Policy and an SMS/XCOPY-style deployment are described in the following sections.

Microsoft Windows Group Policy Deployment Method

The most common way to deploy WakeMyPC Agent is using Windows Group Policy. This feature is available on any network running Windows 2000 Server or later. The example below uses the Group Policy Management Console (GPMC) which is available from Microsoft as a free download (this is built into later versions of Windows 2003 Server and later). If GPMC is not available then the older GPEDIT tool (which is built in to Windows) may also be used.

Group Policy Management Console (GPMC) is available from:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=0A6D4C24-8CBD-4B35-9272-DD3CBFC81887&displaylang=en>

WakeMyPC Agent is supplied with two core files. These are the only files you need to perform an installation:

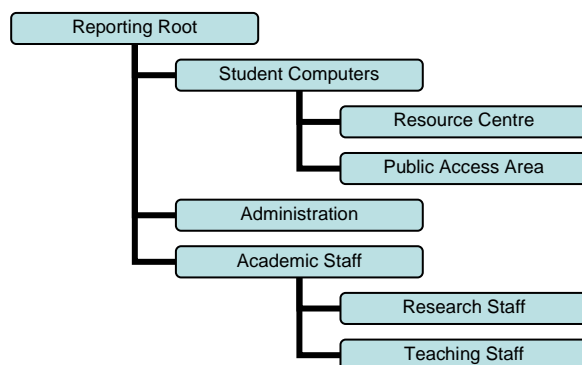


WMClientSetup.msi contains the WakeMyPC Agent program in a deployable form. This may be installed manually or via Windows GPO. This file also deploys the separate WOLMAN utility used for Wake-on-LAN debugging.



WMClient5.adm is an Administrative Template that is loaded onto the Windows Server and used to configure the WakeMyPC Agent software. An **ADMX** file is also provided for use on Windows 2008 and later servers. The policy features available are identical.

The supplied ADM/ADMX file can be used for both deployment and configuration. The basic example below assumes that there is only a single Organisation Unit (OU). However, WakeMyPC Agent fully supports operation in a diverse, multi-OU, network.



The ADM/ADMX file may be used to create several Group Policies to deploy settings at different OU levels.

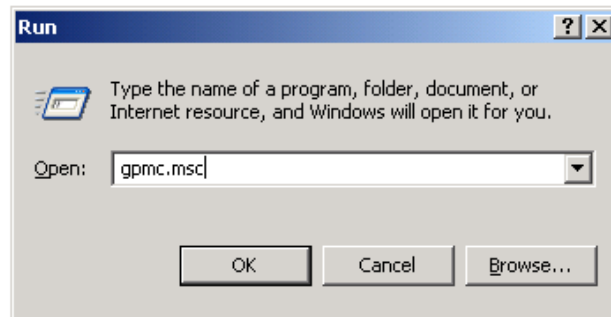
A common approach is to deploy the software and common settings (for instance the PID key) at the top level and separate reporting settings (SiteGUID) for child OUs.

Policies may be freely mixed in this way. **The only requirement is that a specific policy setting must only be applied once.**

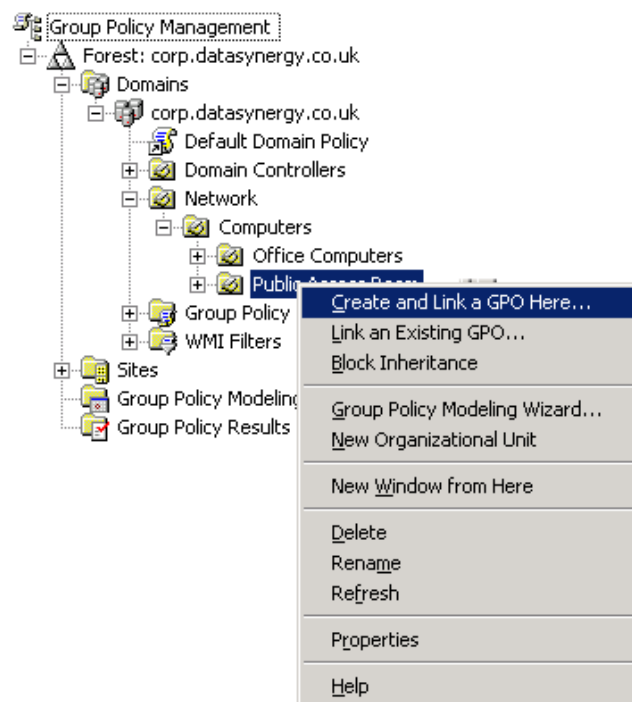
WakeMyPC Agent v5.2

To install WakeMyPC Agent using GPO on Server proceed as follows:

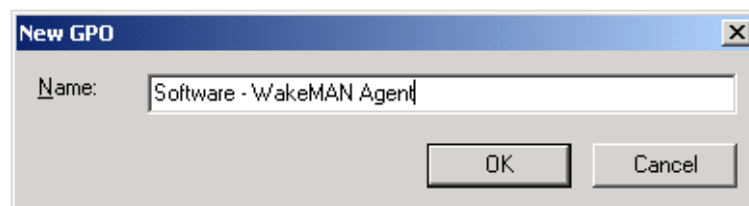
1. Open the Group Policy Management Console (GPMC.MSC):



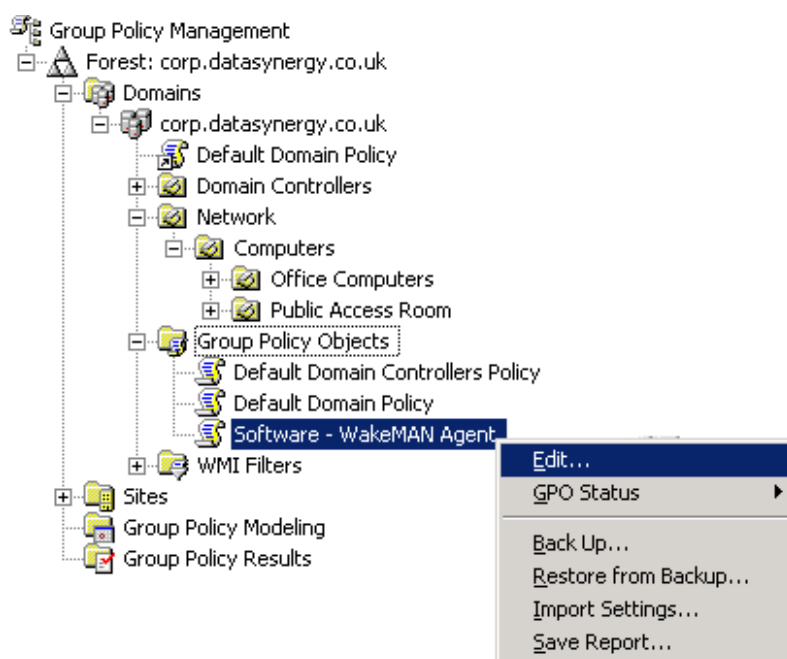
2. Locate the **Organizational Unit (OU)** that you wish to deploy the software to. The example deploys the software to a OU called **Public Access Room**



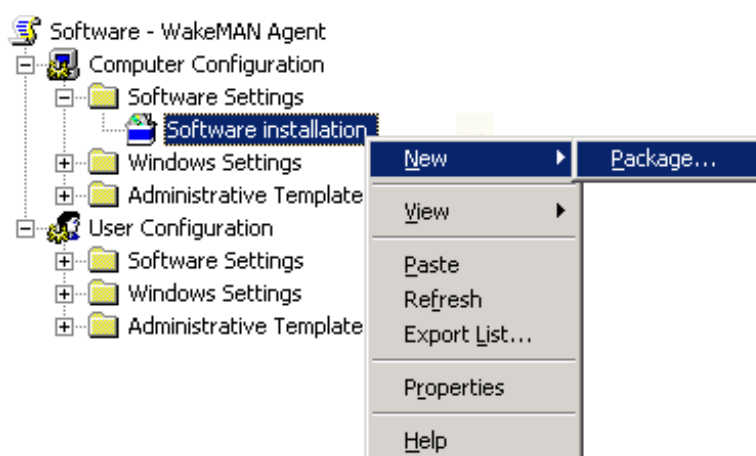
3. Right click the OU and select **Create and Link a GPO here**
4. Enter a name of the new policy and click **Ok**. The example creates a policy called **Software – WakeMyPC Agent**:



5. Select the newly created policy, right click and select **Edit**

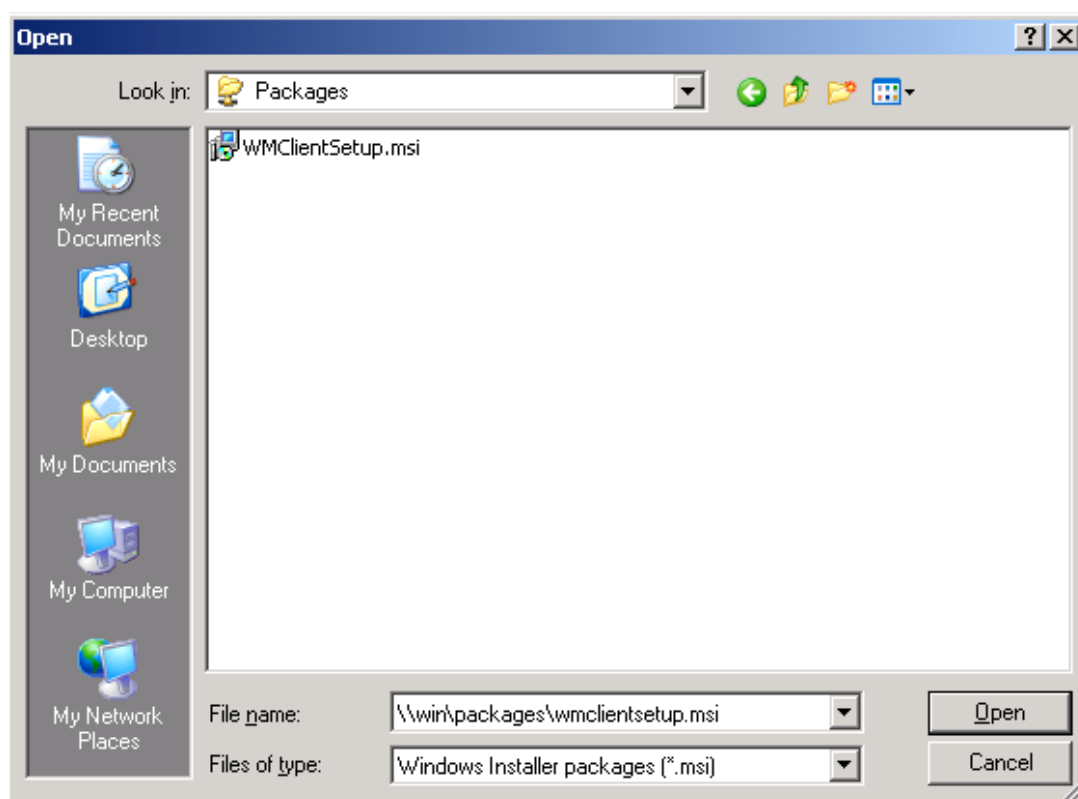


6. The **Group Policy Object Editor** should open. This is used to configure the deployment. Navigate to the **Computer Configuration** section and expand **Software Installation**. Right-click and select **New/Package**:



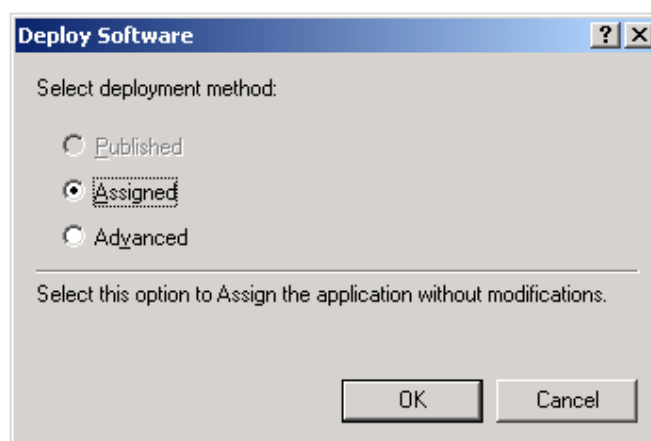
Remember: All WakeMyPC Agent settings are made in the Computer Configuration section of the Group Policy Editor. This is because the software must be deployed to a computer (and not a specific) user.

7. Browse to the network share that contains the **WMClientSetup.msi** file and press **Open**.

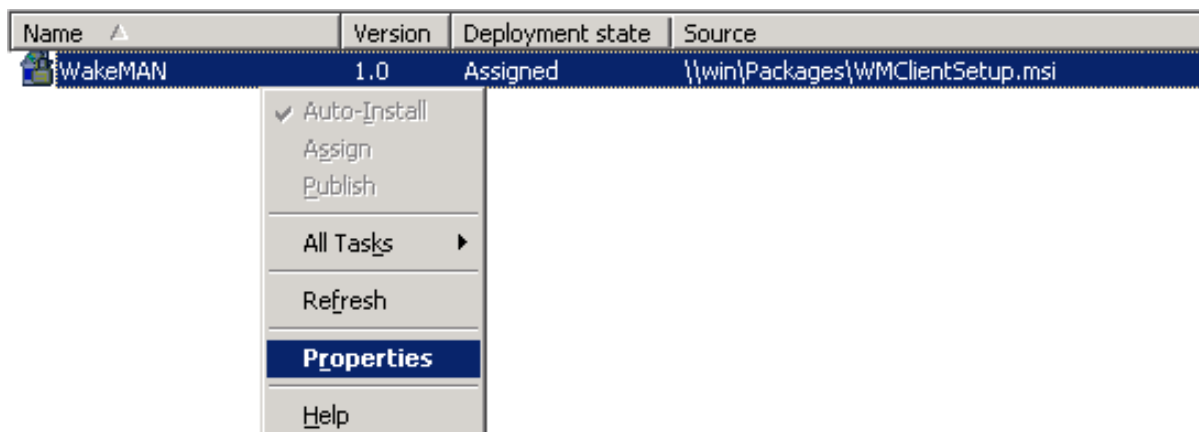


Remember: The MSI file should be placed in a **share** on the server that is accessible to the destination computers. A common technique is to grant **Domain Computers** read access of the share and underlying file system. This is explained further in the troubleshooting section below

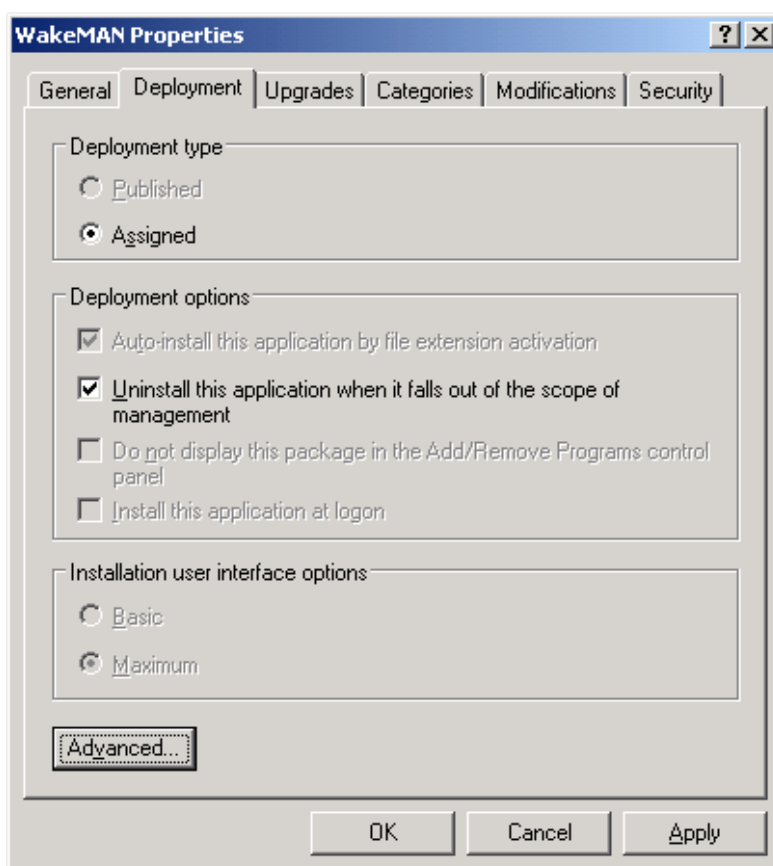
8. Select **Assigned** as the deployment method. WakeMyPC is a system application and therefore it is not appropriate to 'publish' it to users:



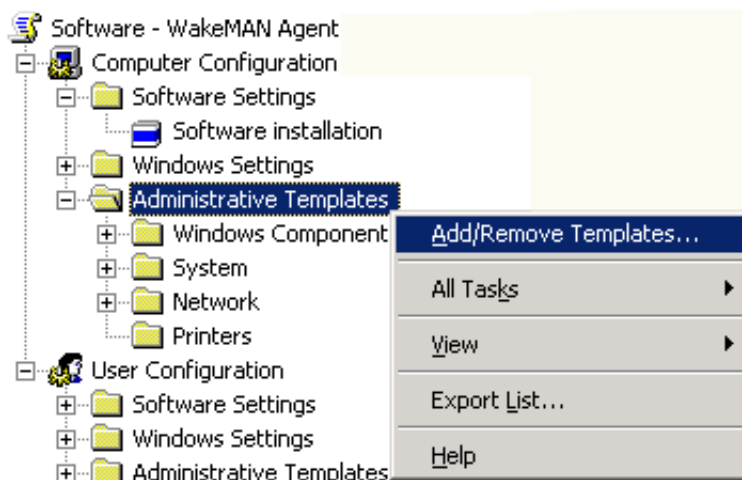
9. Right click on the newly created package and select **Properties**:



10. Select the **Deployment** tab (**Advanced** some earlier service pack revisions) and tick **Uninstall this application when it falls out of the scope of management**. This ensures that WakeMyPC Agent is deployed in a predictable way and then click **Ok**:



11. Navigate to the **Computer Configuration / Administered Templates**, right click and select **Add/Remote Templates**:

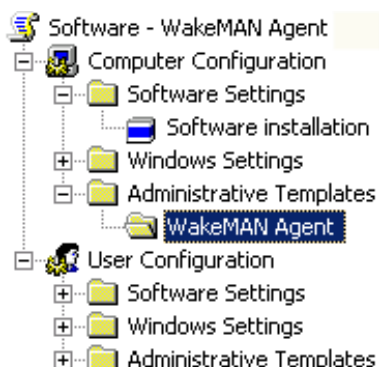


12. Click **Add** and locate the **WMClient5.adm** file supplied. When this is completed click **Close**. It may be helpful to remove the other administrative templates present using the **Remove** button. These are not required for WakeMyPC.




Tip: An ADMX file is provided for use on servers running Windows Server 2008 and later. It provides the same features as the ADM file. To install the policy files copy the **ADMX file** and **en-US** folder to the **Windows\PolicyDefinitions** folder on the server and re-open the Group Policy editor. Please see the following microsoft documentation for further information:

<http://msdn.microsoft.com/en-us/library/bb530196.aspx>

13. The **Administrative Templates** section should now contain a section for **WakeMyPC Agent** (other sections may be present depending on server configuration). Select the **WakeMyPC Agent** section.



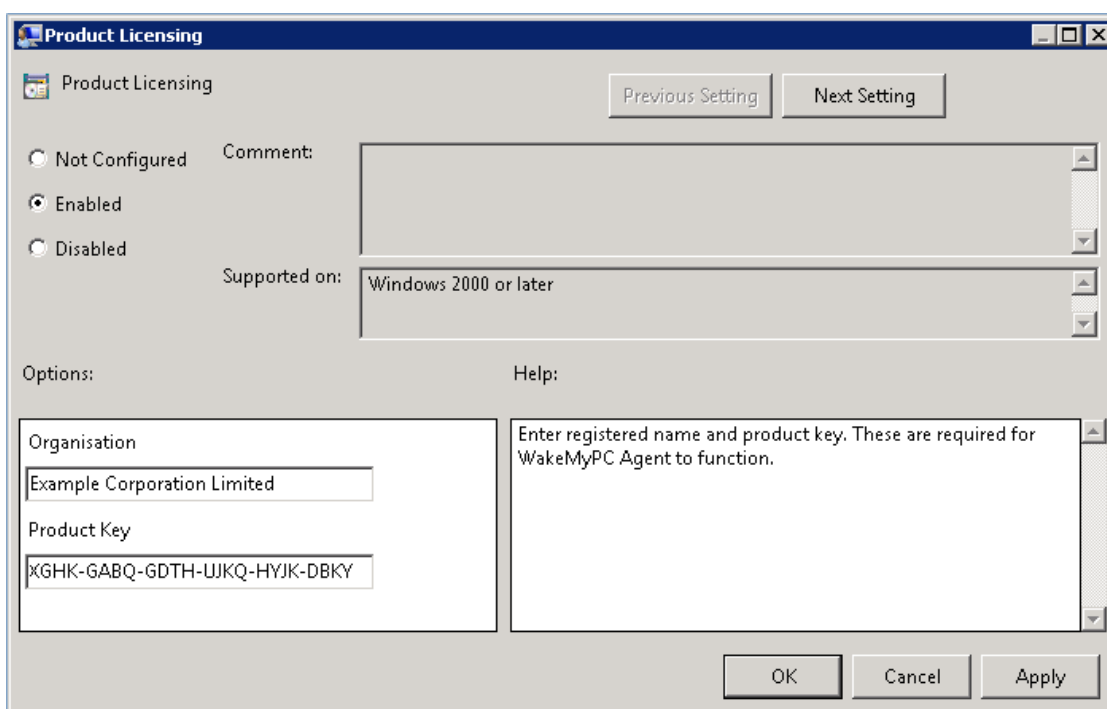
14. The right hand pane displays a list of the available policy settings:

| Setting | State |
|-------------------------------------------------------------------------------------------------------|----------------|
|  Product Licensing | Not configured |
|  WakeMAN Server | Not configured |
|  Advanced | Not configured |

| Section | Meaning |
|--------------------------|--------------------------------------------------------------------------------|
| Product Licensing | Product key settings. These are required for WakeMyPC Agent to fully function. |
| WakeMyPC Server | Site configuration and WakeMyPC Enterprise Server settings |
| Advanced | Advanced configuration and debug settings used for Technical Support |

15. Select **Product Licensing**, right click and select **Properties**

16. Select **Enabled**, carefully enter the product details supplied with the software, and click **OK**



Product Licensing

Product Licensing

Previous Setting Next Setting

☐ Not Configured Comment:
☒ Enabled
☐ Disabled

Supported on: Windows 2000 or later

Options:

Organisation: Example Corporation Limited

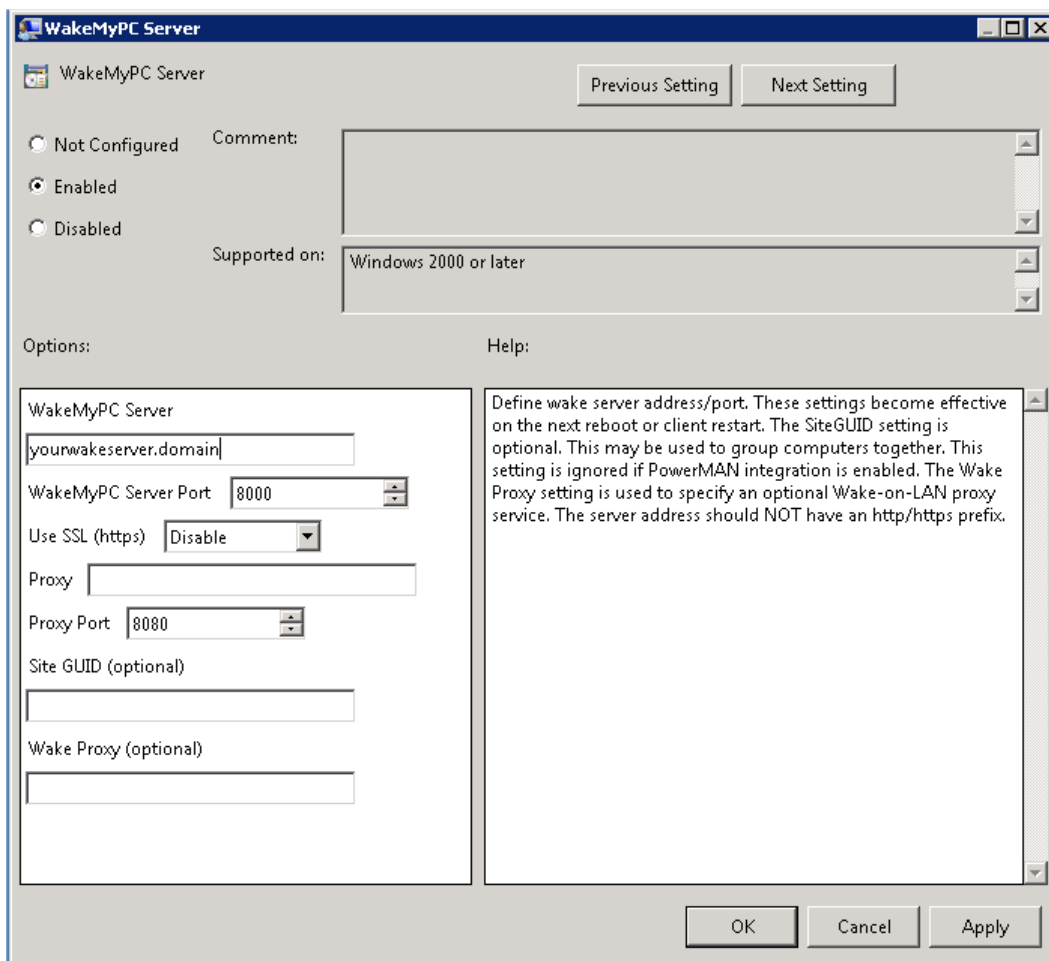
Product Key: XGHK-GABQ-GDTH-UJKQ-HYJK-DBKY

Help: Enter registered name and product key. These are required for WakeMyPC Agent to function.

OK Cancel Apply

17. Select **WakeMyPC Server**, right click and select **Properties**

18. Select **Enabled** and configure the basic site and reporting settings.



A basic WakeMyPC Agent installation requires **only five** settings:

- Registered organisation name
- Registered product identification key (PID key)
- WakeMyPC server name
- WakeMyPC server SSL support
- WakeMyPC server port – The standard server port is **8000** or **443 (SSL)**

If Data Synergy's PowerMAN product is also installed WakeMyPC will automatically use the site assigned for PowerMAN. In a non-PowerMAN integrated deployment the following additional setting is required to group workstations:

- SiteGUID – You can generate this on the WakeMyPC Enterprise Server

Some installations may require a proxy server to access the WakeMyPC Enterprise Server. In this situation the following additional settings are required:

- Proxy server name
- Proxy server port

These settings may be ignored if they are not required. Please remember to ensure that your site firewall / proxy server will allow **http protocol** traffic to the WakeMyPC Enterprise Server.

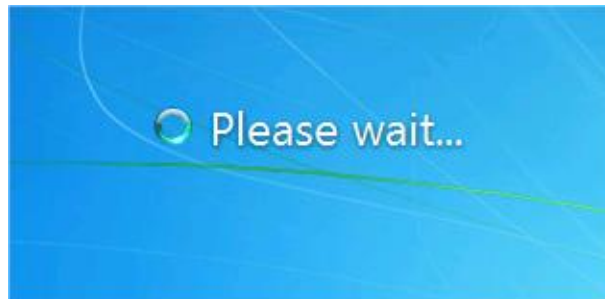
To complete the server configuration click **Ok**

WakeMyPC Agent v5.2

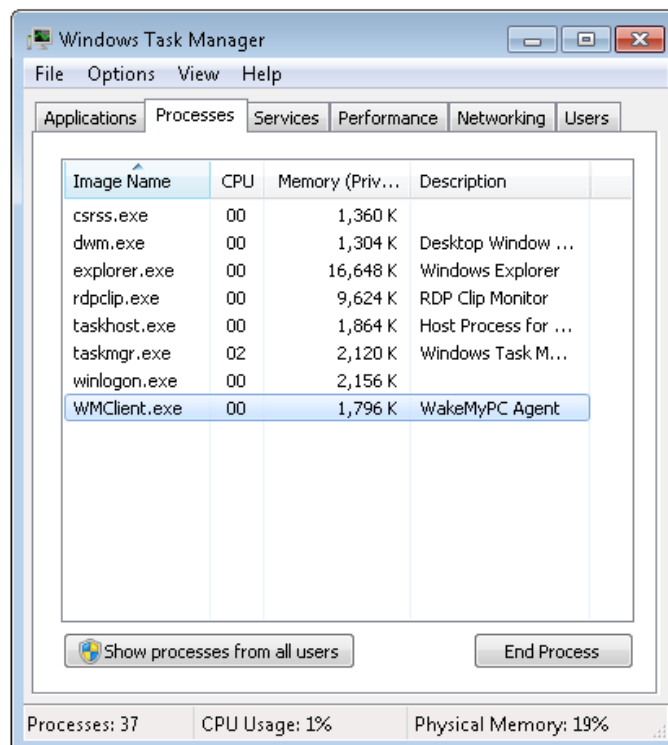
19. Close the Group Policy Object Editor and test the policy works by restarting a computer in the relevant Organisation Unit.
20. As the computer starts you should see the WakeMyPC Agent application install prior to the display of the logon prompt. If this does not happen please consult the troubleshooting section below.

Tip: Depending upon server configuration, timing and any other pending updates a second reboot may sometimes be necessary for the agent to complete installation. This is completely normal.

For instance, on Windows 7 the following dialogue is displayed during installation:

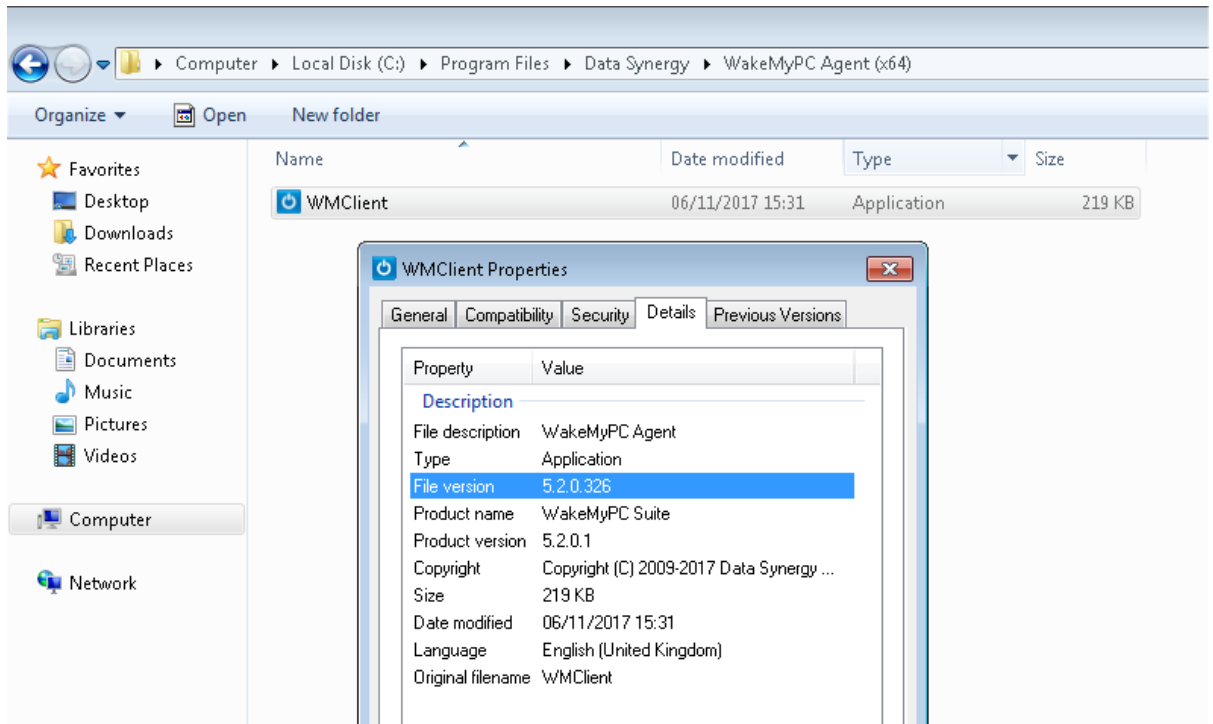


21. Logon and confirm that the WMClient process is running using Windows Task Manager.



WakeMyPC Agent v5.2

22. If necessary you can always verify the version of the WakeMyPC agent by locating the program in the **Program Files\Data Synergy** (or Program Files (x86) for 32-bit agent running on a 64-bit system) folder:



Alternative SMS / XCOPY Deployment Method

WakeMyPC Agent supports a variety of deployment methods. The so-called **XCOPY** method describes the most basic, manual, technique for installing the program. This may be adapted for environments such as SMS as required. This section explains the key features of such a deployment

1. Locate the WMClient.exe file in the '**standalone**' folder.
2. Copy this file to the target computer. The file may be located anywhere.
3. Install the agent with the following command:

WMCLIENT INSTALL

Remember: The WakeMyPC Agent must be installed by a user with local administrative rights. It is not possible to install WakeMyPC Agent using a logon script (which runs as a user). It is possible to install the software with a computer start-up script. See the following web page for an example:

[http://technet.microsoft.com/en-us/library/cc779329\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc779329(WS.10).aspx)

Deploy the required configuration settings using the Windows **Local Group Policy**, **REG.EXE** or **REGEDIT** tools. The section 'Alternative Configuration Method - Local Group Policy / Registry Settings' at the end of this document explains how this may be done. As noted above the minimal settings are:

- Registered organisation name
- Registered product identification key (PID key)
- WakeMyPC server name
- WakeMyPC server port – The standard port is **8000**

Deploying WakeMyPC Agent in a pre-built software image 'Ghost'-style deployment

WakeMyPC Agent fully supports deployment in a pre-built software image. This is sometimes known as a 'Ghost'-style deployment. Typically, in this scenario, WakeMyPC Agent is manually installed on a master computer and configured with the desired settings. This computer is then cloned on to multiple destination computers.

Advanced Settings

WakeMyPC Agent supports the following **Advanced Options**. These are intended for resolving configuration options and should normally be used only under the supervision of Technical Support.

| Advanced Settings | Meaning |
|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Upload Interval (Hours) | How often WakeMyPC Agent will attempt to upload information to the server. The default setting is 24 hours. An automatic upload also occurs whenever a new user logs onto the workstation |
| Force full updates every cycle | Force WakeMyPC Agent to send all information every upload cycle. Normally WakeMyPC Agent will only upload information that has changed since the last upload. This feature is designed to minimize use of network bandwidth and server resources. When enabled this feature forces a full update every time. This reduces server performance and should only be used under the guidance of Technical Support |
| Host polling interval ms Note: This value is in milliseconds | How often WakeMyPC Agent checks the current workstation status. This should happen at least once per minute. The default setting is 60 seconds. |
| Upload Timeout ms Note: This value is in milliseconds | How long WakeMyPC Agent will wait for the server before terminating an upload attempt. The default is 10 seconds |
| Event Logging | The amount of information reported in the Event Log. This setting may be changed to increase or reduce the amount of information reported. |
| PowerMAN Integration | This setting may be used to disable the default PowerMAN integration feature. When disabled WakeMyPC Agent will automatically use the PowerMAN SiteGUID when one is defined AND no WakeMyPC SiteGUID setting is also defined. Disabling this feature will result in WakeMyPC Agent ignoring PowerMAN completely. |

How WakeMyPC Agent Works

The WakeMyPC Agent is a small program that runs at user logon. It records information required for effective Wake-on-LAN and periodically uploads it to the WakeMyPC Enterprise Server. The software has a small system footprint and generally only uploads information that has changed since the last upload.



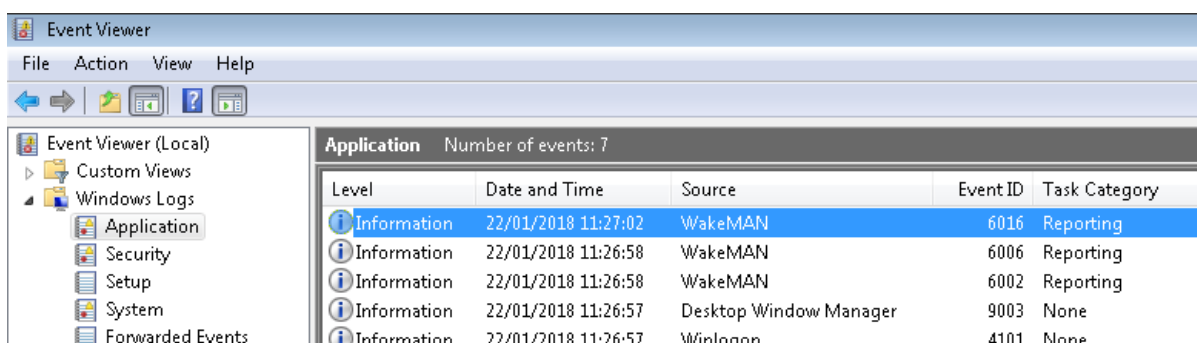
DMCMOS32.EXE
Application

Data Synergy also supplies an enterprise tool for deploying BIOS settings. If you require this utility to quickly deploy hardware settings to multiple computers please contact your sales representative.

Additional WakeMyPC Features

Windows Event Log

WakeMyPC records significant information in the Windows **'Application' event log**. This can be accessed with the standard Windows event viewer tool **Eventvwr.exe**. This information can be extremely useful when investigating power management problems or fine tuning settings. There is a summary of the most commonly logged events in an appendix at the end of this document.



| Application Number of events: 7 | | | | |
|---------------------------------|---------------------|------------------------|----------|---------------|
| Level | Date and Time | Source | Event ID | Task Category |
| Information | 22/01/2018 11:27:02 | WakeMAN | 6016 | Reporting |
| Information | 22/01/2018 11:26:58 | WakeMAN | 6006 | Reporting |
| Information | 22/01/2018 11:26:58 | WakeMAN | 6002 | Reporting |
| Information | 22/01/2018 11:26:57 | Desktop Window Manager | 9003 | None |
| Information | 22/01/2018 11:26:57 | Winlogon | 4101 | None |

WakeMyPC Agent can be configured to log additional information using the appropriate option under Advanced/Event Logging. The WakeMyPC Agent must be restarted with the `WMCLIENT RESTART` command or via user logout and then logon for this change to become effective.

Troubleshooting

WakeMyPC Agent is a very reliable program but problems do sometimes happen. Most issues arise during installation and can normally be solved quickly. The following section details some of the most common issues and explains possible solutions for them:

Problem: WakeMyPC Agent does not deploy correctly using the GPO method

This can occur for a number of reasons. The following should be considered:

1. Do other programs deploy correct via Group Policy?
2. Is the client computer within the correct Organizational Unit (OU)?
3. Are there any errors in Event Log?

If WakeMyPC is the first program to be deployed via GPO there may be an underlying problem with the domain or active directory configuration. The following should be checked:

- Do other applications deploy successfully using the group policy mechanism from the same file-share? Sometimes applications are inadvertently configured to deploy from a local drive letter (on the server) and not a publically available share.
- The client computer is within the correct Organisational Unit (OU). This can be checked with the **Active Directory Users and Computers** snap-in (dsa.msc)
- The MSI file is in share accessible (read access) to the **computer account** of the client PC. Sometimes there may be NTFS access restrictions that are stricter than the share permissions. Both types of permission should be checked. The easiest way to achieve this is to grant a Read Access to the group **Domain Computers**.

Remember: The Windows group policy engine runs in the security context of the computer account. Therefore the share and underlying NTFS permissions must grant access to this account. The effective permissions are the lowest common denominator of the share and NTFS permissions.

- Another policy or application may be preventing installation. This can be checked with the Resultant Set of Policy (RSOP.MSC) tool provided with Windows. The error tab contains information about policy deployment problems.
- Is the problem resolved by disabling Asynchronous policy deployment (see **Computer Configuration\Administrative Templates\System\Logon** in the Group Policy Object Editor)?
- Is the problem resolved by restarting the computer twice? Depending upon other group policies scheduled for installation and removal it can take up to two additional reboots for WakeMyPC to install. This situation can also happen if the MSI and license settings are deployed separately because WakeMyPC will not start until the product license key is present.

Microsoft also provides some advice on debugging GPO based deployment issues:

[http://technet.microsoft.com/en-us/library/cc787386\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc787386(WS.10).aspx)

[http://technet.microsoft.com/en-us/library/cc775679\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc775679(WS.10).aspx)

Microsoft also documents a scenario where a network timeout problem can prevent effective Group Policy application. The following document explains this and provides links to the necessary Windows hotfix:

<http://support.microsoft.com/kb/840669>

In some cases it may be necessary to investigate further by enabling 'verbose' MSI logging. This can be enabled on the client computer by creating the following Registry value:

Key: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer

REG_SZ: Logging

Value: voicewarmup

This will create log files in the %temp% folder (\Windows\Temp for standard Group Policy MSI deployment. The users' own temporary folder for manual MSI deployment). This following document explains this in detail:

<http://support.microsoft.com/kb/223300>

After this setting has been enabled, reboot the PC, and allow Windows to attempt the MSI installation again. When this process has completed (or nothing has happened) log into the machine and check the log files created in the \Windows\Temp folder.

If this technique does not reveal the cause of the problem it may also be useful to enable 'verbose' logging for the Windows Group Policy engine. Please remember that this is an advanced technique and it may take some time to decipher the log files. You can enable this logging by creating the following registry value. It may also be necessary to create the Diagnostics key if one is not already present.

Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics

REG_DWORD: AppMgmtDebugLevel

Value: 0x4b

After this setting has been enabled, reboot the PC, and repeat the installation process described above. The Group Policy engine will create a file called Appmgmt.log in the C:\Windows\Debug\Usermode folder. This is further explained here:

<http://support.microsoft.com/kb/246509/>

NB: You may also need to create the Usermode folder if it does not already exist.

Problem: WakeMyPC Agent is installed but the computers are not showing up on the server system**OR WakeMyPC Event Log entry reports Event #6015: Downloaded XML was corrupt**

WakeMyPC Agent records and transfers log data on a periodic basis. Uploads happen whenever a new user logs on, whenever the computer's network address changes or every 24 hours. In situations where nothing has changed the agent may delay any data upload for a period of time to conserve network bandwidth and server resources.

If computers do not register promptly with the WakeMyPC Enterprise Server then there may be a configuration problem. The following should be checked:

1. The SiteGUID setting is correctly configured and registered on the WakeMyPC Enterprise Server. The SiteGUID should always contain the {brace} characters.

NB: This setting may be blank if PowerMAN Integration is enabled (the default) and PowerMAN is installed on the workstation.

2. The WakeMyPC Enterprise Server address. There is no need to prefix this with http:// or www.
3. The server port. This is normally 8000 but may be any port assigned by the WakeMyPC Enterprise Server system administrator.

NB: Please remember that the server firewall (and any intermediate proxy / firewall) must allow standard incoming HTTP traffic on this port.

4. The proxy address and port setting. If you are using a proxy server please check that server address and port are correctly configured. The proxy should permit unauthenticated HTTP traffic to the reporting server. The proxy server logs may also indicate the cause of the problem.
5. The Application Event Log. This will probably explain the cause of the problem. Some upload problems are reported using a standard Winsock error code. These are explained in the following Microsoft document:

[http://msdn.microsoft.com/en-us/library/ms740668\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/ms740668(VS.85).aspx)

It some cases it may be helpful to enable additional event logging (located in the Advanced configuration section) and restart the computer. This may be combined with the FORCEUPLOAD command (see below).

Event #6015: 'Downloaded XML was corrupt' indicates that there was a problem with the response data from the WakeMyPC server. This can happen when an intermediate proxy server blocks the traffic and returns a human-readable error page.

In some circumstances it can be useful to force an immediate data upload. To force an upload use the following command:

```
WMCLIENT FORCEUPLOAD
```

The WakeMyPC Agent will attempt an immediate upload using the current settings. After a brief pause the agent will display the result of the upload attempt.

WakeMyPC Agent v5.2

If the above steps do not resolve the problem it may be necessary to investigate the network communication between the computer running WakeMyPC Agent and the WakeMyPC server. This advanced technique may be especially useful when using an intermediate proxy server. WakeMyPC Agent uses a standard Windows supplied component called WinHTTP to perform network communication. This is the same library used by most of Windows including Internet Explorer. Microsoft has incorporated a logging system into WinHTTP that can be used to examine the network traffic.

To use this technique proceed as follows:

1. Obtain the WinHTTPTraceCfg tool. This is in the Windows Server Resource Kit
2. Enable WinHTTP tracing with the following command:

```
winhttptracecfg -e 1 -d 0 -s 2 -t 1 -l c:\winhttplog
```

This will create a series of files in the C:\ folder prefixed 'winhttplog'

3. Force an upload using the above technique:

```
WMCLIENT FORCEUPLOAD
```

Check the C:\ folder for a log file (there may be several). These show the network transaction with the (proxy) server

4. Remember to disable logging with the command:

```
winhttptracecfg -e 0
```

The most common proxy server communication issues are:

- Incorrect proxy server address / port setting
- Proxy server requires authentication – WakeMyPC Agent does not support proxy authentication. You can work around this behaviour by creating a proxy server exception.
- The WakeMyPC Enterprise Server address is missing from the proxy 'white-list'

Problem: Application event log reports WakeMyPC error #2002 - Product key has expired. Please contact your sales representative to obtain an updated product key. The software will continue to function in reduced functionality mode.

This indicates that the WakeMyPC PID key has expired. This can happen during product evaluations when a time limited PID key is used. Non-evaluation PID keys are perpetual and do not expire. Please contact your Sales Representative to obtain an updated PID key.

Problem: Some computers wake-up (resume) unexpectedly

There are several reasons a PC may automatically resume from a low-power state. The following steps will help isolate the cause of the problem:

1. Unplug the mouse and the keyboard and determine if the problem is resolved. Sometimes a faulty input device (especially an optical mouse) may be the cause of the problem

WakeMyPC Agent v5.2

2. Unplug the network cable and determine if the problem is resolved. If the Wake-On-LAN (WOL) feature is not required disable it. If the network card supports wake on 'directed packet' (using IP address) and this feature is not actually required try disabling it
3. If PowerMAN is also installed: Study the power management event log. Is there a pattern? Does the automatic resume happen at set times or regular intervals?
4. Try a minimal software image removing all non-essential applications. The automatic resume maybe caused by another application

Problem: Some computers fail to suspend / resume reliability and consistently

Successful power management implementations often make extensive use the suspend (sometimes called sleep) and resume functionality present in modern computers. In most situations these functions work very well and require no specific configuration to be effective. Occasionally, however, some computers may have problems either successfully suspending or resuming to an operational state.

There are many potential reasons why this may happen and it may require some experimentation to fully diagnose. The following sections explain the basic steps that you can take to isolate the cause of such a problem. A separate troubleshooting section explains the steps that may be required on some systems to allow the computer to wake from a specific input (such as a USB keyboard or via Wake-On-Lan).

Please see the Data Synergy PowerMAN Troubleshooting guide for further information.

Problem: Unable to resume computer using selected input / button method

OR Unable to resume PC using a USB keyboard / mouse

OR Unable to resume PC using Wake-On-Lan (WOL)

OR Unable to configure Device Manager power management remotely

Most computers can be configured to suspend / resume with little difficulty.

However, sometimes, it can be difficult to initiate a 'resume' from suspend (S1, S2 or S3) or hibernate (S4) using the desired method. This is a distinct problem and should not be confused with systems that are unable to suspend or resume reliably. The most common scenario is that the PC can resume but not using the desired keyboard, mouse or Wake-On-Lan (WOL) method. This may cause user experience problems and potentially cause a power saving initiative to fail.

This troubleshooting section explains the most common scenarios and how they may be resolved.

There are four stages to this process:

1. Confirm the system can suspend and resume reliably (using ANY method)
2. Check the appropriate BIOS settings
3. Check the related Windows Device Manager settings
4. Check and configure the Power Management settings (this can be done with PowerMAN if installed)

WakeMyPC Agent v5.2

First, confirm that system can actually suspend and resume reliably using **any method**. The simplest approach is as follows:

1. Manually sleep the workstation. If PowerMAN is also installed you can use the following command:

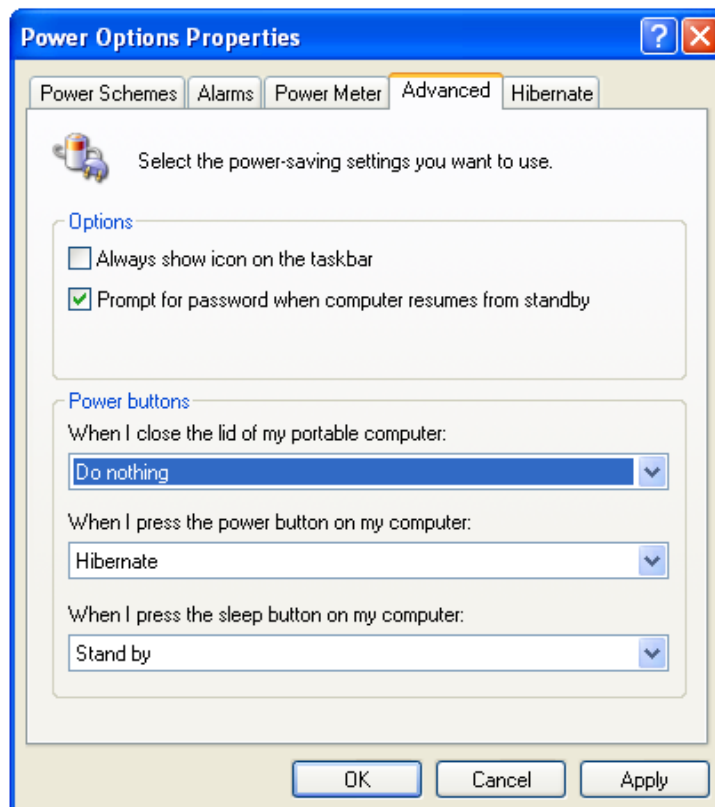
```
POWERMAN SLEEPCHECK
```

2. Wait two minutes. The system should resume automatically within this time
3. If this does not happen this may indicate the PC does not (currently) support automatic resume. Follow the following sections to resolve this.

The most simple resume method is a dedicated hardware button. Some systems include such buttons (although they are not always connected). Such buttons may normally be configured via a BIOS setting. It is not possible to configure this behaviour from Windows. Please check the BIOS configuration to determine if this is supported on your specific PC.

A second, related, approach is to initiate system resume using a legacy PS/2 keyboard (not a USB keyboard). As above, these are configured using only BIOS settings and do not require any configuration of the related Windows Device Manager entry. In some cases pressing any key will resume the system whilst in others a specific key must be pressed. Some systems also support resume via PS/2 mouse buttons. Please check the PC BIOS configuration to determine if this is supported on your specific PC.

Dedicated hardware sleep/resume buttons (including those on some legacy keyboards) may be configured using the PowerMAN 'Global Power Settings' feature. This is similar to the Power Options dialog in Windows 2000/XP/2003 Control Panel Power applet:



When investigating suspend / resume issues it can often be helpful to configure the hardware 'Power' button as the 'Sleep' button. This is especially useful on systems that do not have a dedicated sleep

WakeMyPC Agent v5.2

button or where this is not connected or appears to not function correctly. Please consider re-configuring the 'Power' button temporarily to check this.

Configuring the system to resume from a USB keyboard or mouse is considerably more complex than in the legacy cases above. This is because the functionality must be configured in the BIOS, Windows Device Manager and sometimes the related USB Hub devices. To configure resume from for USB keyboard please check the following:

1. The BIOS supports USB resume and this is enabled (often there is a dedicated setting called 'Resume on USB' or similar)
2. The Device Manager entry for the keyboard has the 'Allow this device to bring the computer out of standby' option ticked:



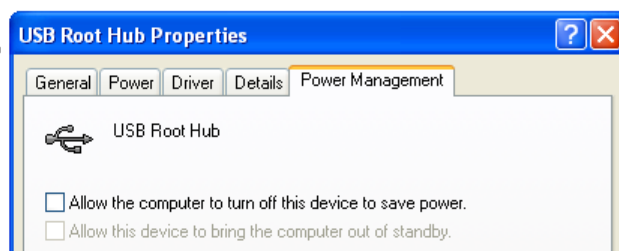
3. If this option is unavailable (greyed out) then this may indicate that the related BIOS feature is not enabled.
4. In some case this may also indicate that Windows has disabled resume for this device because the system is using the S3 suspend mode. This is only applicable to Windows XP.

To restore the functionality create a 'USBBIOSx' value in the Registry. This is described in the Microsoft KB article 'Description of how to enable the S3 system power state for standby when USB devices are armed for wake':

<http://support.microsoft.com/kb/841858>

NB: Very rarely enabling this feature may result in increased system instability or poor suspend/resume consistency. Please test this thoroughly prior to live deployment.

5. If the USB keyboard is connected via a USB Hub then this device must be configured to remain powered and not standby. This is because the hub must remain powered for the keyboard to operate. Please remember that in some cases the USB hub may be internal to the PC. To prevent a USB hub from entering the standby state un-tick the 'Allow the computer to turn off this device to save power' option in Device Manager.



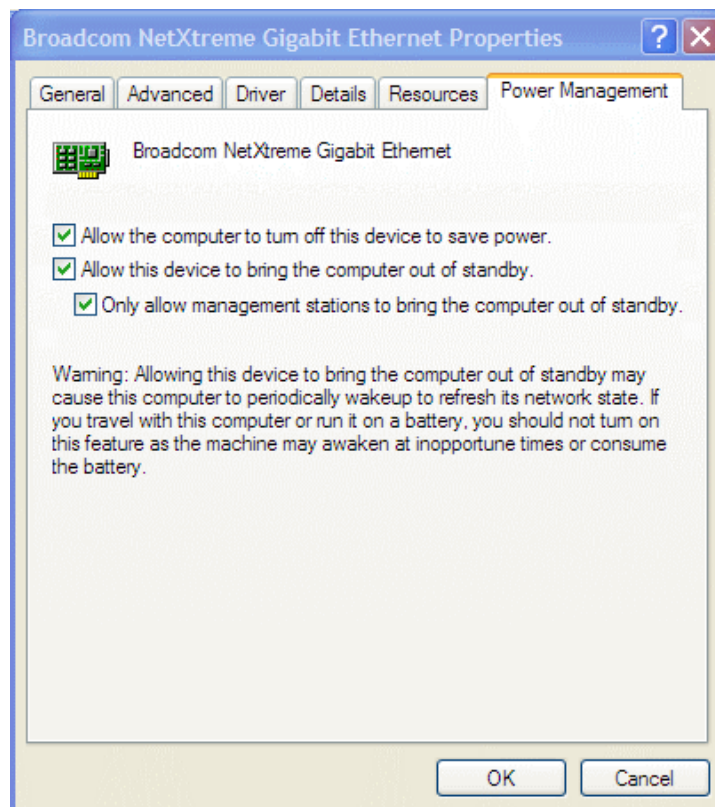
WakeMyPC Agent v5.2

Some system administrators use the Wake-On-LAN (WOL) feature to initiate system power-on or resume from a remote location. This is commonly used for patch management and remote support. WOL is a complex topic requiring specific hardware and network support. To allow WOL to operate the following must be correctly configured on the client PC:

1. WOL must be enabled in the system BIOS (if present)
2. The following options must be selected (ticked) in Device Manager:
 - Allow the computer to turn off this device to save power
 - Allow this device to bring the computer out of standby / wake the computer
 - Only allow management stations to bring the computer out of standby

NB: Some systems are unable to resume from S5 (full power-off) using WOL. Please check your system BIOS – in many cases there is a specific setting related to S5 WOL. A 'management station' means a true WOL 'magic' packet and not more general network traffic.

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



Sometimes it may be necessary to automate the deployment of these settings. This can be done using a script or batch file at deployment time. The following Microsoft documentation may also be useful:

| Article / Title | Notes |
|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| http://support.microsoft.com/kb/837058 How to disable power | This document explains the PnPCapabilities Registry setting. This is a DWORD value where the network device wake-up configuration is stored: HKLM\SYSTEM\CurrentControlSet\Control\Class\ |

| | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| management for a network adapter when you deploy Windows XP. | <p>[DriverKey]</p> <p>The following (hexadecimal) values are commonly used:</p> <p>No options ticked = dword:00000038 Allow device power saving = dword:00000030 Allow device to wake PC = dword:00000020 Management stations only = dword:00000120</p> <p>The system must be rebooted for a change in this setting to become active and be reflected in Device Manager.</p> |
| http://msdn.microsoft.com/en-us/library/ms793220.aspx Enabling Selective Suspend | <p>This document explains the HcDisableSelectiveSuspend Registry setting. This is a DWORD value that is linked to the 'Allow the computer to turn off this device to save power' option in Device Manager. It may be necessary to change this setting to prevent a USB hub from entering standby:</p> <p>HKLM\SYSTEM\CurrentControlSet\Control\Class\[DriverKey]</p> <p>The following (hexadecimal) values are commonly used:</p> <p>Disabled = dword:00000000 Enabled = dword:00000001</p> <p>The system must be rebooted for a change in this setting to become active and be reflected in Device Manager.</p> |
| Undocumented by Microsoft | <p>The WaitWakeEnabled Registry setting is a DWORD value that is linked to the 'Allow this device to bring the computer out of standby' option in Device Manager. It may be necessary to change this setting to allow a USB keyboard / mouse to wake the system:</p> <p>HKLM\CurrentControlSet\Enum\[DeviceInstancePath]\Device Parameters</p> <p>The following (hexadecimal) values are commonly used</p> <p>Disabled = dword:00000000 Enabled = dword:00000001</p> <p>The system must be rebooted for a change in this setting to become active and be reflected in Device Manager.</p> |
| http://support.microsoft.com/kb/841858 Description of how to enable the S3 system power state for standby when USB devices are armed for wake | <p>This article explains how to allow S3 suspend / resume on Windows XP when using USB devices.</p> <p>The system must be rebooted for a change in this setting to become effective.</p> |
| http://support.microsoft.com/kb/878467 Your Windows XP-based | <p>This article explains a problem in Windows XP that can prevent a USB mouse from being used to wake the system if the mouse is moved whilst the system is suspending. This problem is not currently fixed by Microsoft.</p> |

| | |
|--------------------------------------------------------------------------------------------------------|--|
| computer does not resume from standby when you move your USB mouse or press a key on your USB keyboard | |
|--------------------------------------------------------------------------------------------------------|--|

Problem: Network drive is disconnected after system has resumed

This problem can happen on some systems if the server connection has timed out. This following Microsoft article explains how to resolve this problem:

<http://support.microsoft.com/kb/297684>

Other Deployment Resources

The following Microsoft resources may also be useful:

[302430](#) How to assign software to a specific group by using Group Policy

[224330](#) Assigning a Windows Installer Package with minimal interaction

[257718](#) How to create a third-party Microsoft Installer package (MSI)

[278472](#) Packages assigned to computers with Group Policy are not installed

Appendix A – WakeMyPC Agent Command-line options

The WakeMyPC Agent supports the following command-line options. These may be used by an administrator to manually configure the service and report on the current installation status. Some of the supported commands require administrator level rights:

| Command | Requires Admin rights | Meaning |
|--------------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Install | Yes | Install the WakeMyPC Agent. For example: <code>WMCLIENT INSTALL</code> |
| Remove | Yes | Remove (uninstall) the WakeMyPC Agent (also stops if already running) |
| Start | No | Start the WakeMyPC Agent (also installs if not already installed) |
| Stop | No | Stop the WakeMyPC Agent. It will start again the next time a user logs on. |
| Restart | No | Restart the WakeMyPC Agent (and upload if necessary) |
| Status | No | Report status of WakeMyPC Agent |
| License | No | Check the current WakeMyPC license key and expiry (if applicable) |
| Forceupload | No | Force an immediate full data upload and display result. For example: <code>WMCLIENT FORCEUPLOAD</code> |
| Forceuploadsilent | No | Force an immediate full data upload. The operation is silent even if it fails. For example: <code>WMCLIENT FORCEUPLOADSILENT</code> |

Appendix D – WakeMyPC Agent Policy Settings Reference

The WakeMyPC Agent is designed, primarily, for configuration with the Microsoft Windows group policy tools supplied with all recent versions of Windows Server. An administrative template (ADM/ADMX) file is supplied to simplify this process.

The WakeMyPC Agent may also be configured by manually creating a suitable settings and importing them into the system registry of the deployed workstation computers. This section documents the supported policy settings and their default values. In a few cases options are available via the registry are deliberately omitted from the associated ADM/ADMX file. These options are intended for advanced configuration and troubleshooting.

General Information

Unless otherwise noted all settings are of type REG_DWORD. True is indicated by 1. False is indicated by 0. Where no value is specified for a setting (it is missing) a sensible default value is assumed.

The following table may be useful for calculating values expressed in seconds:

| Time in seconds | REG_DWORD Value (Decimal) |
|-----------------|---------------------------|
| Disabled | 0 |
| 1 Minute | 60 |
| 5 Minutes | 300 |
| 60 Minutes | 3600 etc |

Product Licensing

The product license settings are stored in **HKLM\SOFTWARE\Policies\WakeMAN:**

| Registry Setting Name / Type | Meaning |
|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| RegisteredOrganisation REG_SZ e.g. Example Corporation Limited | Organisation name supplied with the WakeMyPC product key. This forms part of the product key and must be entered exactly. |
| RegisteredProductKey REG_SZ e.g. XGHK-GABQ-GDTH-UJKQ-HYJK-DBKY | The product key supplied with WakeMyPC. This is exactly six groups of four characters separated by five dashes. |

WakeMyPC Server Configuration

The server configuration settings are stored in **HKLM\SOFTWARE\Policies\WakeMAN:**

| Registry Setting Name / Type | Meaning |
|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| WakeServer REG_SZ e.g. yourwakemypcserver.domain | The address of the WakeMyPC Server. This can be blank if management reporting information is not required. |
| WakeServerPort REG_DWORD e.g. 8000 | The port number of the WakeMyPC Server. This is usually either 80 or 8000. |
| WakeServerSSL REG_DWORD e.g. 0 | Use secure sockets layer (SSL) for data upload. The server must be configured to accept SSL traffic. 0 = Disabled 1 = Enabled |
| WakeServerProxy REG_SZ e.g. 192.168.1.1 | The address of the local proxy server that WakeMyPC Agent must use to send management information to the WakeMyPC Server. This can be blank if a proxy server is not required. |
| WakeServerProxyPort REG_DWORD e.g. 8080 | The port number of the proxy server. This is typically 8080. This value has no effect if a proxy server address is not defined. |
| SiteGUID REG_SZ e.g. {09ab90ee-98fe-4383-a17d-b7ccdb7da5f9} | Unique site identity used to track a group of computers that are managed as a single entity. This value can be generated on the WakeMyPC Server or using any other standard GUID generator. This setting may be blank if workstation grouping is not required or Data Synergy PowerMAN is also installed. In this case WakeMyPC will share the SiteGUID used by PowerMAN. |
| WakeProxy REG_SZ e.g. yourwakeproxy.domain | The address of the WakeMyPC Proxy Server used for this workstation. |

Debugging / Advanced Settings

The following debugging settings are supported. These settings are located in **HKLM\SOFTWARE\Policies\WakeMAN**. These are intended primarily for resolving problems under the instruction of Technical Support.

| Setting | Meaning / Supported Values |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UploadIntervalHours REG_DWORD e.g. 24 | How often WakeMyPC Agent should wait between uploads of unchanged system information. Typically WakeMyPC is configured to only upload when a system configuration change is detected or every 24 hours whichever happens first. The default setting is 24 hours. |
| ForceSendAll REG_DWORD 0=Disable (default) 1=Enable | When enabled this setting forces WakeMyPC Agent to upload all information on every upload check cycle. This feature is intended for Technical Support use and should not be enabled on a live deployment unless instructed by Technical Support. Enabling this feature will result in reduced client and server performance. |
| HostPollMS REG_DWORD e.g. 300000 | How often WakeMyPC Agent checks the current system status. This should happen at least once per hour. The default setting is 30 minutes. |
| UploadTimeoutMS REG_DWORD e.g. 10000 | How long WakeMyPC Agent should wait for a response from the WakeMyPC Server. The default setting is 10 seconds (10,000ms) |
| EventLoggingLevel REG_DWORD 0 = Default information 1 = Additional information 2 = All information (maximum verbosity) | <p>The level of event logging detail required. This may be one of the supported values shown.</p> <p>Logging additional information may fill the event log and cause other events to be lost. This option should therefore only be enabled when required.</p> |
| PowerManIntegration REG_DWORD 0=Disable 1=Enable (default) | When Data Synergy PowerMAN is installed WakeMyPC Agent will, by default, share the SiteGUID used by PowerMAN. This feature may be disabled using this setting. The default setting is enabled. |

Appendix E - Alternative Configuration Method - Local Group Policy / Registry Settings

It can be time consuming and potentially error prone to manually create the required settings. It is recommended that the Group Policy / ADM / ADMX method is used wherever possible. However, if this approach is not practical it is possible to use the ADM/ADMX file on a **local computer** to generate a master configuration and then deploy this using the built-in Windows Registry tools. This **Local Group Policy** approach has the advantage that it will create a consistent and reliable configuration with less likelihood of errors.

To use the ADM file on a local PC proceed as follows:

1. Install Windows on a computer that is **not** a member of a domain. It is not necessary for the WakeMyPC agent to be installed on the computer.
2. Create a folder, for example C:\WakeMAN and place a copy of the WMClient5.adm file within the folder.
3. Launch the Microsoft Management Console (MMC.EXE)
4. Navigate to the File menu and select Add/Remove Snap-in
5. Click Add
6. Select Group Policy Object Editor and click Add
7. The snap-in will default to Local Computer mode. This is correct. Click Finish
8. Click Close and then Ok to return to the main MMC window
9. Expand Local Computer Policy
10. Select Administrative Templates
11. Right click and select Add/Remote Templates
12. Click Add and locate the WMClient5.adm file. When finished click Close
13. Configure the desired power settings as per the GPO method instructions
14. Save the snap-in for later reuse (this avoids repeating steps 4-12 again) by selecting File/Save As and selecting the filename WakeMyPC.msc
15. Exit the management console
16. Export the generated registry settings for deployment on other computers by using the following command to create a file called WM.REG:

```
REG EXPORT HKEY_LOCAL_MACHINE\SOFTWARE\Policies\WakeMAN WM.REG
```

17. Deploy the settings to the required computers using your chosen deployment method. This could be one of the following:

i. REG IMPORT WM.REG

ii. REGEDIT /S WM.REG

iii. Third party deployment tool

18. If you need to create additional settings the following small batch file may be helpful. This overwrites the locally cached copy of the WMClient5.adm file and launches the previously saved snap-in. This process is particularly necessary if a new version of the ADM file has been released (it is normally only copied to the %windir%\system32\grouppolicy\adm\ folder when the snap-in is first configured):

```
COPY WMClient5.adm %windir%\system32\grouppolicy\adm\WMClient5.adm
```

```
MMC WakeMyPC.msc
```

Example Registry File

The following registry example contains the settings for a basic installation with the following properties:

1. Product key for 'Example Corporation Limited' is configured
2. No SiteGUID – PowerMAN integration is being used
3. WakeMyPC server is **yourwakemypcserver.domain:8000** (0x1F40 in hexadecimal)
4. No proxy server is required

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\WakeMan]
"RegisteredOrganisation"="Example Corporation Limited"
"RegisteredProductKey"="XGHK-GABQ-GDTH-UJKQ-HYJK-DBKY"
"WakeServer"="yourwakemypcserver.domain"
"WakeServerPort"=dword:00001f40
"WakeServerProxy"=""
"WakeServerProxyPort"=dword:00001f90
"WakeGateway"=""
"SiteGUID"=""
"WakeProxy"=""
```

Appendix I – Common Event Log Messages

WakeMyPC includes a comprehensive event logging feature. This section explains the most common logged events. The exact wording of some events may change from one WakeMyPC release to another. However, the general meaning of a specific event number will always be the same. Some events include parameters such as times, program or user names. The first parameter is shown as %1. The second parameter, if present, is marked %2 and so on.

| Event | Meaning |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2000 | Operating system not supported The current operating system is not supported. Please check the software documentation for a list of supported platforms. |
| 2001 | No valid product key was found. Check product key and registered organisation name. The product key was missing or invalid. Please check it. The WMCLIENT LICENSE command will report additional information. |
| 2002 | Product key has expired. Please contact your sales representative to obtain an updated product key. The software will continue to function in reduced functionality mode. %1 Some types of product key are designed to expire after a certain time. Please obtain an updated product key. |
| 2003 | WakeMAN client is initializing. |
| 2004 | WakeMAN client running. |
| 2005 | WakeMAN client stopped. |
| 6013 | Failed to upload XML (Error %1): %2 There was a problem transferring the power log data to the WakeMyPC server. The error number is normally a Windows Winsock error code indicating the cause of the problem. See http://msdn.microsoft.com/en-us/library/ms740668(VS.85).aspx for an explanation of these codes. |
| 6014 | Uploaded XML: %1 Data was upload to a WakeMyPC server. The upload data is attached to the log. |
| 6015 | Downloaded XML was corrupt: %1 The response from the WakeMyPC server was incomplete. This may indicate a network or proxy server problem. The failed data is attached to the log. |