Universal Management Service 2011

UMS 2011 Help

Printed: September 2011

Disclaimer:

This document is a reference guide for administrators of UMS. An administrator of UMS is someone responsible for the creation and maintenance of the UMS solution not the person managing the customer's use of UMS. This person is referred to as a User of UMS. A User Guide is provided within the product using F1, with a copy provided on the installation media.

Table of Contents

Part I Introduction 7

Part II Installation 10

1 Installation Requirements ... 10
2 Installing UMS Server ... 11
3 Licensing and Activation ... 13
4 Installing UMS Agent and Client ... 14
5 Enabling Intel vPro ... 16
6 Managing connections via Group Policy ... 17

Part III Server Manager 20

1 Managing Components ... 20
- Properties ... 21
- Security ... 22
- Upgrading Components ... 24

2 Managing Connections ... 24
- Connection Properties ... 25
- Terminating a Connection ... 26
- Reloading Client data ... 26

3 Managing Licenses ... 27
- License Status ... 28
- Server Product Key ... 29

4 Servers ... 30
- Description ... 30
- Server Setup ... 31
- Event Logging Options ... 33

5 General ... 33
6 Server Log ... 35

Part IV Client 37

1 Configuration ... 37

Part V Management Console 40

1 Using the Management Console ... 40
2 Add Computer Wizard ... 42
3 Find Computers ... 45
4 Computer Properties ... 45
- General ... 46
- System ... 47
- Tasks ... 47
- Events ... 48
- Options ... 49
- Member of ... 50
- Comments ... 50

DirectDrivers ... **50**
DirectTools ... **51**
Processes ... 51
Command Prompt ... 52
Remote Assistance ... 53
View ... 53
Intelligent Install ... **53**
Power Status ... **54**
5 Group Properties ... **56**
6 Tasks ... **56**
Add Task Wizard ... **57**
Task Properties ... **57**
Open Task ... **58**
7 Alert History ... **58**
8 vPro Authentication ... **58**

Part VI Components 60

1 DirectDrivers ... **60**
Navigating the Console ... **60**
View by Drivers ... 62
View by Devices ... 62
View by Computers ... 63
Adding New Drivers ... **63**
Manually adding drivers ... 63
Add Driver Wizard ... 63
Driver extraction ... 64
Managing Drivers ... **65**
Versions ... 67
Digital Signatures ... 67
Using Conditions ... 68
Missing files ... 69
Using DirectEngine Management Console ... 69
Integration with other Components ... **69**
DirectPXE ... 69
DirectEngine ... 71
2 DirectEngine ... **72**
Types ... **73**
Setup Components ... **73**
Binary Files ... 74
Config Files ... 74
OS Commands ... 74
OS Scripts ... 76
Pre OS Scripts ... 78
Registry ... 78
vPro ... **80**
Collections ... **81**
Options ... **82**
Tasks ... **84**
Pre Defined Script Items ... 87
Roles ... **88**
General ... **91**
Advanced Configuration ... **92**
Setup Import and Export ... 92
Script Triggers ... 92
Pre-Defined Options ... 93
Option Value Resolution ... 95

Task Script Properties ... 97
3 DirectPXE ... 99
Menus ... 100
Menu Items ... 101
Boot Images ... 103
Floppy Disk ... 104
Boot Program / Dynamic CD ... 104
Devices ... 105
General ... 107
Ports ... 107
Running on a DHCP server ... 107
DirectEngine macros ... 107
Make CD Image ... 108
Importing and Exporting ... 108
4 DirectReports ... 108
Computer Details ... 108
Daily Usage by Group ... 109
Monthly Power Reports ... 109
5 Intelligent Install ... 110
6 Powerwise ... 110
Costs ... 110
Profiles ... 111
Profile Properties ... 112
General ... 112
Schedule ... 113
User Notifications ... 116
Idle Options ... 117
Web Wakeup ... 117
Part VII Advanced Configuration 120
1 Upgrading UMS ... 120
2 Advanced Client Installation Options ... 121
3 Advanced Server Installation Options ... 122

Part I

Introduction

1 Introduction

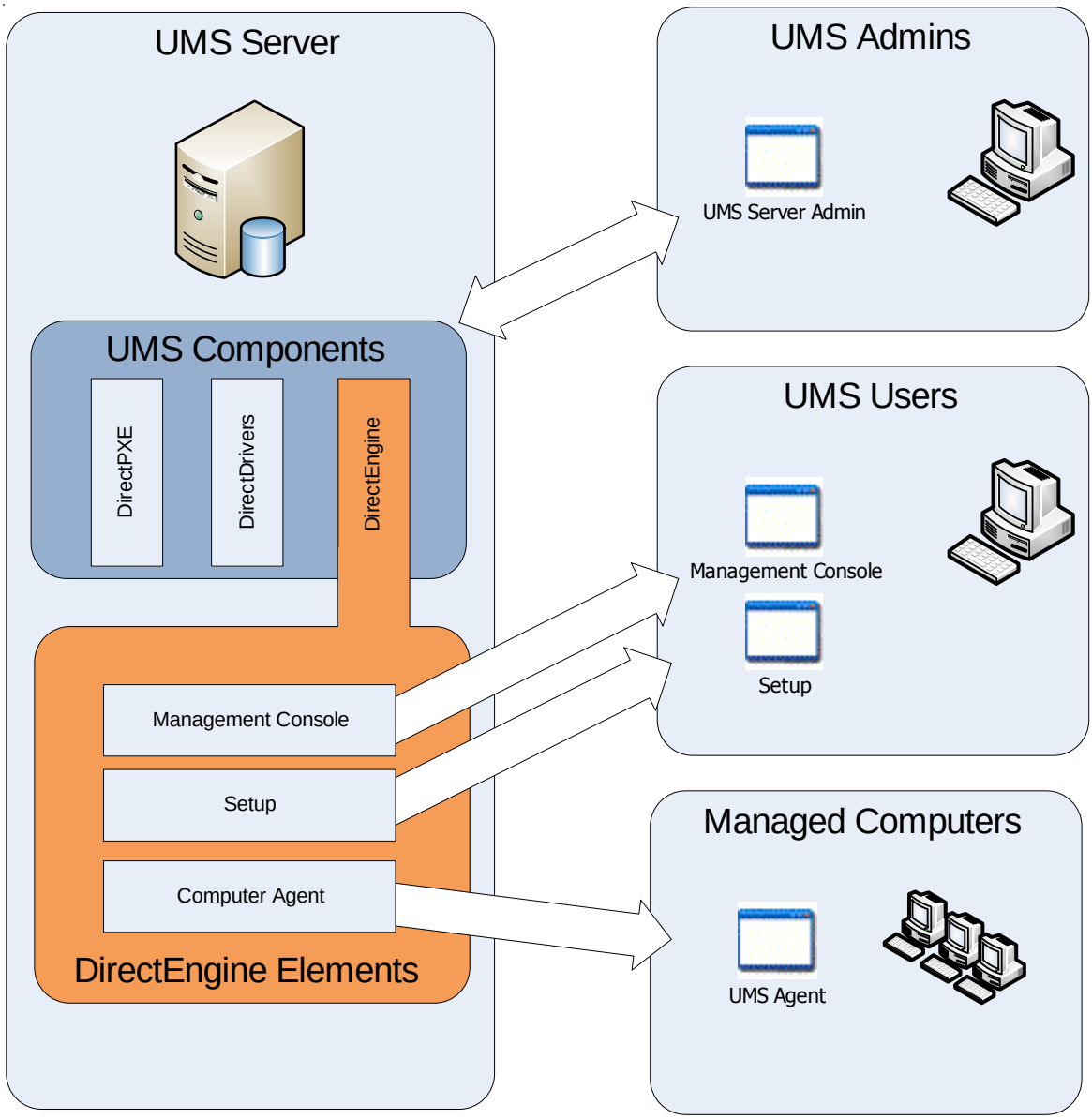
UMS (Universal Management Service) is a framework that allows the deployment of operating systems and applications to the desktop. Whether in place refresh, or 'bare metal' build, UMS can carry out zero touch deployment. The UMS framework has been designed from the start with extensibility at the core.

A UMS **Component** is an application which has been designed to run using the facilities provided by the UMS framework. A single Component is equivalent to an application.

A UMS **Element** is a sub-Component and provides a discrete piece of functionality to the other Elements of the same Component. Having elements enables control over which users use parts of the component by applying security.

The framework consists of server and Clients parts, with the Client being of three types; UMS Server Manager, UMS Client, and UMS Agent.

- UMS Server – Provides the central repository for the UMS framework, enabling centralised management of computers and processes. The server provides the framework for each component to run in, providing common services to each component (e.g. authentication, distributed database and network communication).
- UMS Agent – Runs as a service on a Client, enabling it to be managed. Managed Clients allow components to run component processes on the computer.
- UMS Admin – provides UMS administrators with a single method of managing components both for security and licensing. It also centrally manages connected UMS Client properties.
- UMS Client – Allows user interface elements to be presented in a consistent manner for all components. Computers running the UMS Client do not require the UMS Agent to be installed.



Part II

Installation

2 Installation

This chapter provides information on installing and licensing Universal Management Service.

2.1 Installation Requirements

UMS Hardware Requirements

UMS Server has no specific server hardware requirements. The server should be on a switched network, minimum 100Mbps and if using DirectPXE (a PXE server for 'zero touch' deployments) you should ensure that you network infrastructure is set up to support the PXE packet type.

UMS Software Requirements

The table below shows the operating system versions that are supported for use with UMS.

	UMS Server	UMSServer Manager	UMSClient	UMSAgent
Windows 2008 Server (any version)	■	■	■	■
Windows 2003 Server (any version)	■	■	■	■
Windows 2000 Server (any version)	■	■	■	■
Windows 7	☐	■	■	■
Windows Vista	☐	■	■	■
Windows XP Professional	☐	■	■	■
Windows 2000 Professional	☐	■	■	■

Key

■ Supported

☐ Supported, however this is the Microsoft restrictions for these platforms, notably 10 concurrent file share connections.

Other Requirements

Other PXE server(s) on the network should be configured to ignore requests from the Clients to be managed. Using DirectPXE also requires a DHCP server on the network.

If the server is to run on the same server as DHCP please see the section 'Running DirectPXE on a DHCP server'

To complete this example installation to deploy Operating Systems and Applications, you will need:

- A License Key. Evaluation license keys are available. Contact info@modus-interactive.co.uk for more information.
- Microsoft Volume Licence installation media (typically Windows Vista, Windows XP or Windows Server 2003) in ISO format.
- Application Source media in Windows Installer (MSI) format.

UMS Security Considerations

The UMS server integrates with the Microsoft security model and a service account is created for the server at installation time. Therefore the decision to build the server as a workgroup server or a member of an Active Directory domain should be taken before the server is installed.

During installation an account will automatically be created depending on the status of the server platform, therefore if the server is a member of a domain you must be logged onto the server with privileges to create accounts within the domain. The account has the following format:

UUSR<computername>

Where <computername> is the name of the server platform at installation time.

2.2 Installing UMS Server

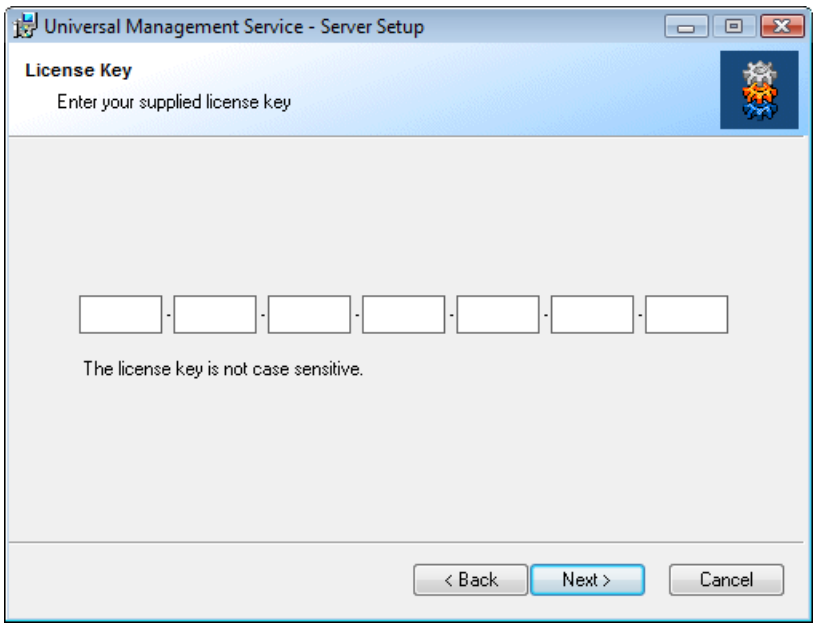
1. Insert the CD or locate the directory where you have the UMS source expanded. Click on Autorun if you are not using a CD.

2. Click on Install UMS Server at Splash screen

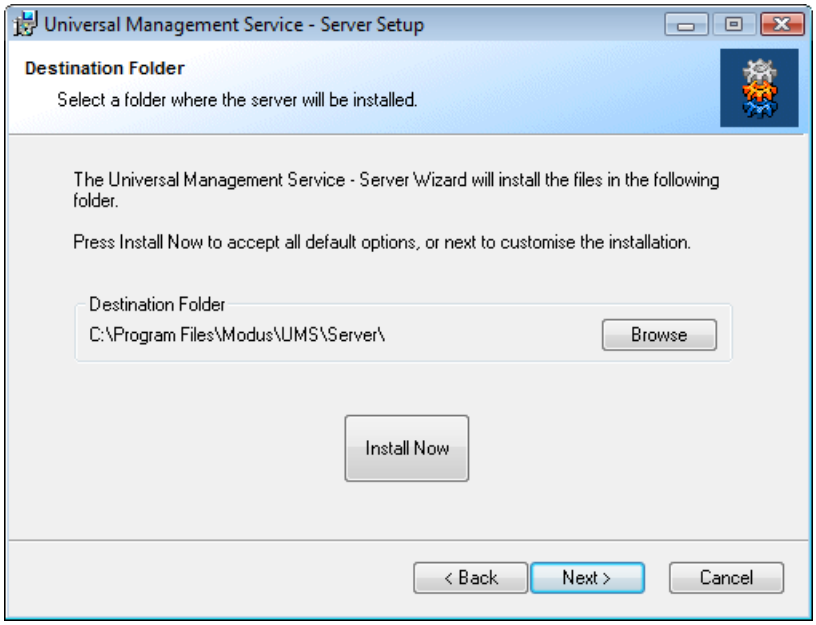
3. On the Installation Wizard click Next>

4. Read and accept the license and then click Next>

5. Now enter the license key that was provided. By default, the license will be activated at the end of the installation procedure.



6. You can now amend the destination folder if you wish.



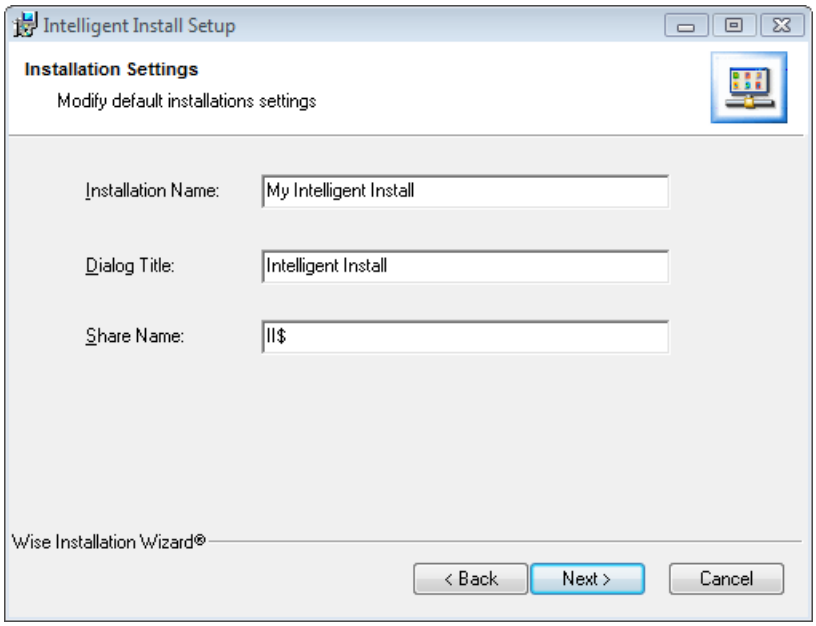
7. After clicking Install Now the installation wizard will install the UMS components and start the Server. You will see the UMS Server start and the Component elements available to the Client start to be listed as each component is started by the Server. You can minimise the Client at this time.

8. Now go back to the CD splash screen and click on Install Intelligent Install

9. Welcome to II Installation Wizard Next >

10. You now have the option to amend the Destination Folder. If you changed the destination folder of UMS we recommend you do the same for II and keep it at the same path relative to the change you made for UMS

11. Unless it is absolutely necessary we would recommend you leave the Share Name as is in the default Installation Settings, however if you wish to change the Installation Name and/or the Dialog Title, change it now.



12. Click Next > and then Next > again and Intelligent Install will complete its installation

13. The wizard will now inform you of a successful installation and you can click on Finish> to complete the installation. You will now need to add a license key for Intelligent Install.

2.3 Licensing and Activation

A default installation requires a license key, and will be activated at the end installation. This activation requires internet access. If this process fails during installation you complete the activation process manually.

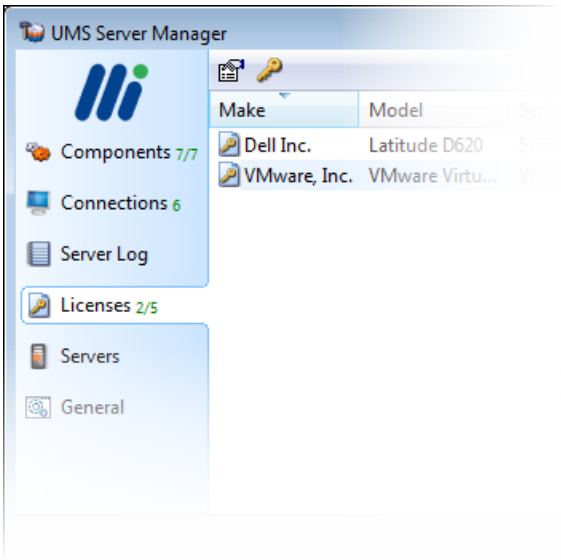
Universal Management Service

You will have a 28 character license key for UMS, that was entered during the installation. If activation was disabled or failed, you will need to activate the key. You have three days to activate the key. After activation, the license is tied to the server you installed UMS on.

To move this installation to another server you will need to contact support (enter value) to activate the license key for a different server.

To activate the UMS license:

Run the UMS Server Manager on a workstation with internet access.



Ensure that Server Manager is connected to UMS and click the Licenses tab. Click the Product key  in the toolbar to open the license key properties page.

Click "Activate..."

If further registration details are required you will be prompted to complete the fields.

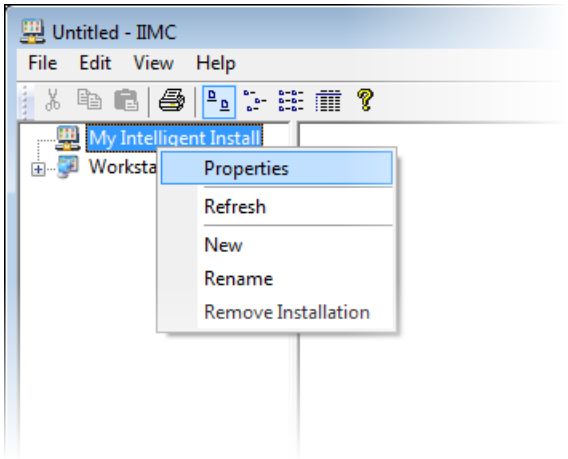
See License for more information on License status.

Intelligent Install

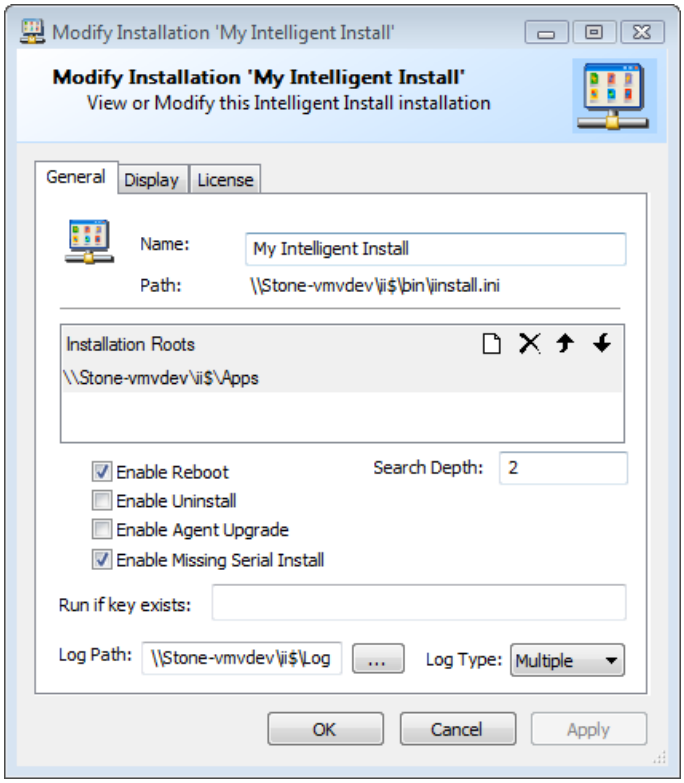
You also need to add a license key for Intelligent Install, and this is done via the Intelligent Install Management Console (IIMC).

1. Load the IIMC from the Start Menu. You should see a clean empty IIMC console load like the one

below.



2. Now right click on My Intelligent Install in the left hand pane and select Properties from the context menu. This will load the Properties window similar to the one below.



3. Click on the License tab and input the Intelligent Install license that you have.

2.4 Installing UMS Agent and Client

By default, the server installation will also install the Client on the same computer as the server. However, it is normal to install the Client on an administrator's computer. The Agent will need to be installed on all computers to be managed by UMS.

Installation Technique	Recommended use
Add Computer Wizard	For small numbers of devices within an Active Directory domain where there is

	no automated deployment tool.
Web page	Ad hoc installation onto small numbers of devices, where getting access to the device is simple.
MSI windows installer package	For medium to large deployments where the software distribution tool can reliably roll out the Agent, minimising the need for technical staff involvement.

➔ We recommend deploying the UMS Agent via a software distribution system using an installer package (MSI). It provides a reliable method for ensuring the Agent is installed on all computers including when new machines are added, or when existing machines are rebuilt.

Install the Agent using the Add Computer Wizard

If the network meets the following criteria, the 'Add Computer Wizard' can be used to remotely install the Agent.

- File sharing enabled at target computer, and 'Simple File Sharing' disabled
- No firewall, or firewall that allows remote file sharing
- Target computers are member of Active Directory domain, or the local Administrator password is known

See Add Computer Wizard for more information.

Install the Client or Agent locally

The UMS Client or Agent can be installed from the UMS Server web page. On the machine you want to install the UMS Client or Agent, open Internet Explorer and type in the following URL:

http://<servername>:2248

If the UMS server is set to respond on HTTP port (80) (see Server Properties for details on setting this parameter) then the following URL can be used instead:

http://<servername>

This will load the web page or web console from which you can install, or Quick Run both the UMS Client and UMS Server admin programs. The Quick Run option allows you to run the program without installing it on the current machine. The facility to quick run the UMS Client without installing it can be extremely useful, especially when it is either not possible (e.g. insufficient permissions) or not necessary to install the software locally. There is no loss of functionality by running the Client without installing it.

Install the Agent using Software Distribution

Software Distribution systems automatically install software for a group of computers. As the Agent is provided as an industry standard Windows Installer package, it can easily be configured and deployed by all leading software distribution systems.

Example compatible software distribution systems:

- Modus Interactive Intelligent Install

- Microsoft Active Directory Group Policies
- Microsoft System Center Configuration Manager

The Agent packages can be generated and placed in a temporary folder of your choosing. See Client Package within the server advanced settings. This technique allows you to configure default Agent installation properties without requiring installer properties to be set via the command line.

Alternatively, the Agent package can be found in a sub folder of the server installation. By default this is located at the following path:

```
C:\Program Files\modus\UMS\Server\Default\Clients\x86
```

The files required to install the Agent are:

```
UMSAgent.MSI
```

The default installation options can be modified using Windows Installer properties. The method for modifying these depends on the distribution tool chosen. These properties are detailed under Advanced Client Installation Options.

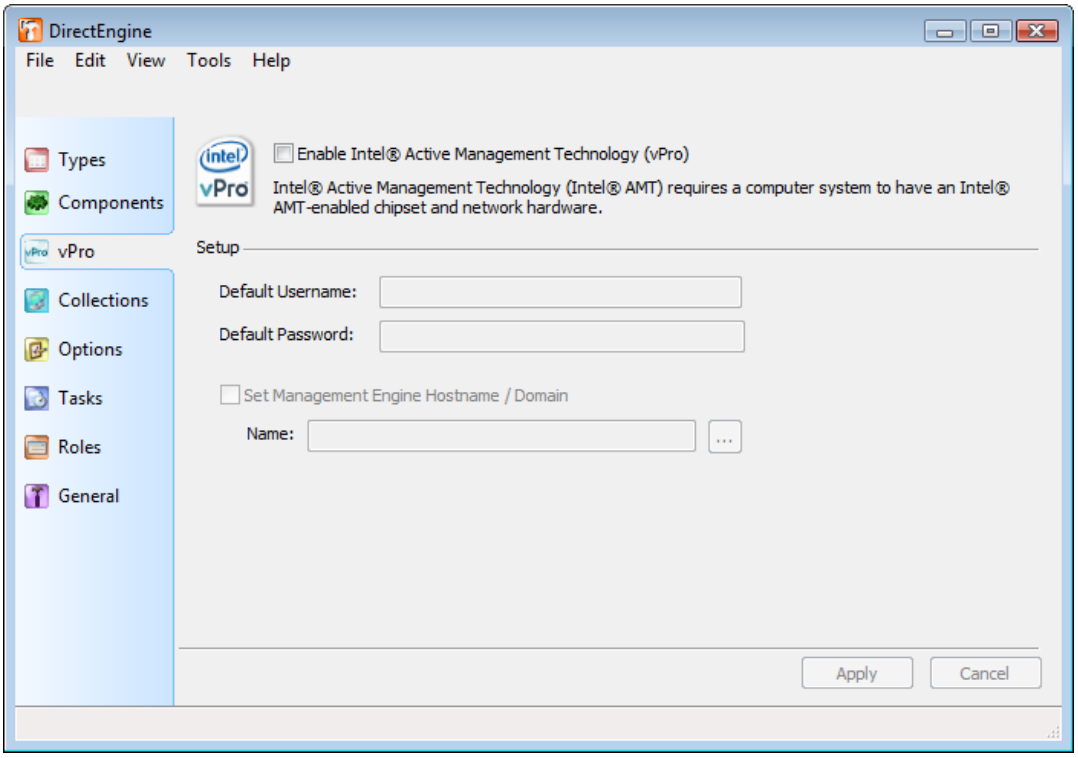
➔ When used in an Active Directory managed network, connection parameters can be set via Group Policy using an administrative template. See Managing Connections via group policy.

2.5 Enabling Intel vPro

Intel Active Management Technology (vPro) allows remote management of devices even when the device is turned off.

In order for a device to be issued a wakeup via vPro the following conditions must be met:

- Computers need to have an Intel AMT enabled chipset and network hardware
- The computer must have been provisioned (Intel configured)
- UMS must have been configured with the correct vPro credentials



2.6 Managing connections via Group Policy

When managing devices in an Active Directory domain, an Administrative Template is available to manage settings.

Installing the Administrative Template

The Administrative Templates are not installed by default. Locate the UMS.adm administrative template on your UMS installation and import it into Group Policy.

The template is a computer template.

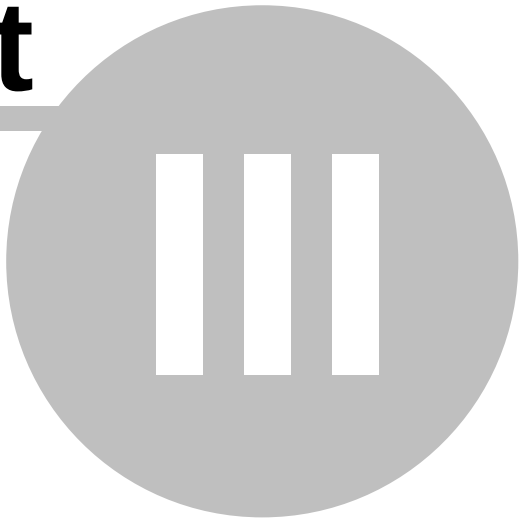
Group Policy managed parameters

The administrative template allows the management of the following properties :

Parameter	Values	Purpose
Server Name	DNS Name or IP Address	Sets the address of the of the UMS server the Agent will connect to.
Discover Server	1= true, 0 = false	If on, Agent will broadcast to find the nearest UMS Server which it will then connect to.
Profile Name	Defined Profile Name	Sets the UMS Profile that the computer will use. Allows the profile to be set via Group Policy which may be more familiar to IT administrators. Profile name must match Profile available on UMS Management Console
Type Name	Defined Type Names	For UMS Computers have a type which can be set via Group Policy.

➔ For an organisation managing large numbers of computers using the Administrative template can help ensure that the right UMS Profile is being used. The Group Policy can set Agent connection details and Profile to use, simply and effectively.

Part



Server Manager

3 Server Manager

UMS Server Manager is installed on the server during the installation of UMS. It can also be installed on any computer if required. It is also possible to 'Quick Run' UMS Server Manager from the UMS Client Installation web page (http://UMS_server_name:2248).

Launching UMS Server Manager will automatically connect you to the server you installed it from . You can change the options to allow you to select a server to connect to at start up which allows you to pick and chose the server to manage in a multi-server environment. When using this option the Server field will have the last connected server already populated. You can edit this field or use the drop down arrow to see a list of detected servers. To change the default connection options for future use, go to Options on the toolbar where you can set the default server name and details of the connection. This will allow you to configure your preferred connection settings.

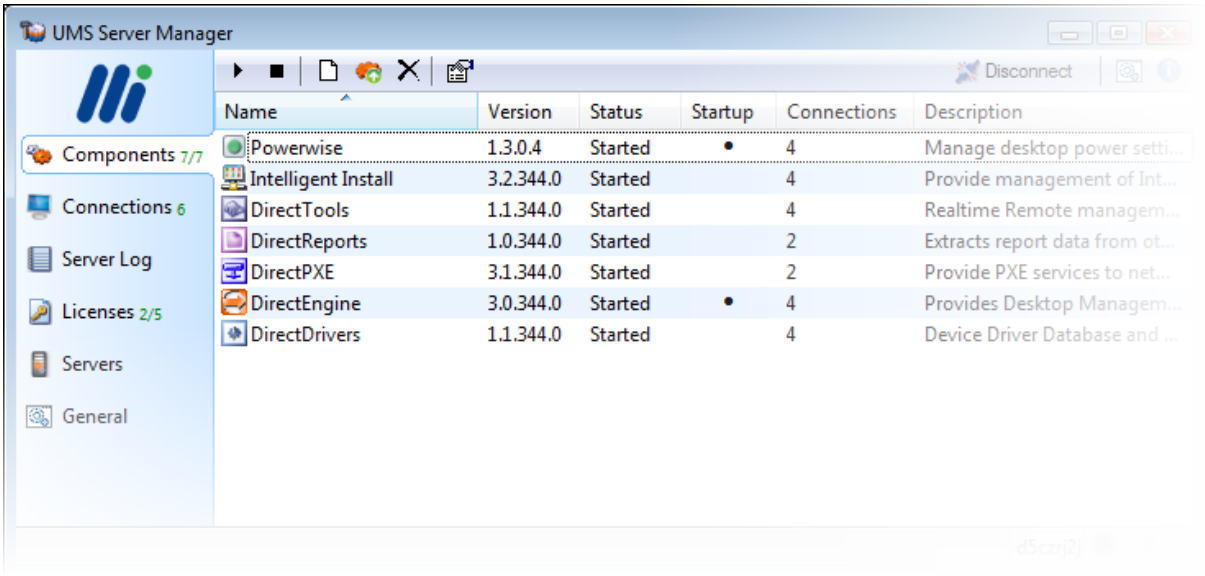
➔Server Manager is for managing UMS configuration which includes security, licenses and components. Once configured little active management is usually required.

By default the UMS Server Manager console will launch with the Connections tab selected, displaying all current connections to the server in the right pane.

Server Manager tab	Description
Components	Shows the state and version of installed components that provide specific UMS functionality
Connections	Shows active connections to the server
Server Log	Provides a log of server activity
Licenses	Shows allocated licenses and provides an interface for them to be managed. Licenses can be activated and refreshed from here.
Servers	Provides details of installed servers
General	Allows the configuration of a number of settings

3.1 Managing Components

Click Components in the UMS Server Manager console to display which Components that are installed on the server, along with information about them. To customise which columns are displayed in the right hand pane click on Customise on the View menu. You can then unlock the columns and select which columns to add or remove.



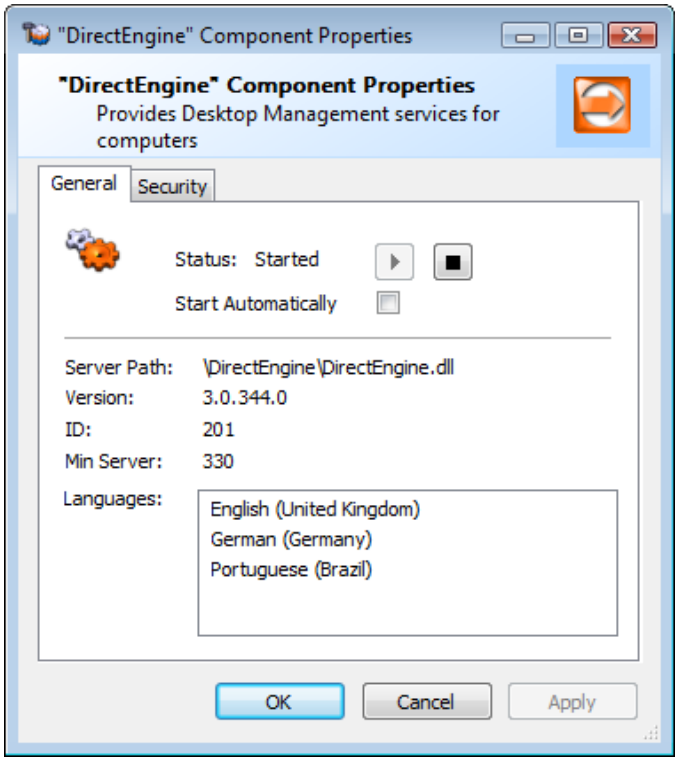
Right click on a Component in the right pane to show the Component context menu. From the context menu you can:

- Start the Component
- Stop the Component
- Add a new Component using the New Component Wizard
- Remove the Component
- Upgrade the Component
- Open the Properties window

➔We recommend that components are set to automatically start. If the server is rebooted then the UMS components are started automatically.

3.1.1 Properties

Each Component Properties window has two tabs; General and Security.



.

Component Property – General

This tab allows you to stop and start the Component. You can also specify if the Component starts automatically when the server starts. Detected language files are shown as well as the Component installation path and Component version information. If a supported language is available for the local language of the device launching the UMS Component then language is shown automatically. Min server shows the minimum UMS server installation required to support this Component.

Component Property – Security

This allows security to be applied to the Elements of the Component. Elements can be User (UMS Client) or Agent Elements however it is only User Elements that can have security applied. Double click an Element to apply security.

An example of how security should be set up for a typical desktop deployment scenario is detailed in the Security topic.

3.1.2 Security

Security of UMS is tackled at a number of levels:

- Framework
- Component Element
- Within an Element

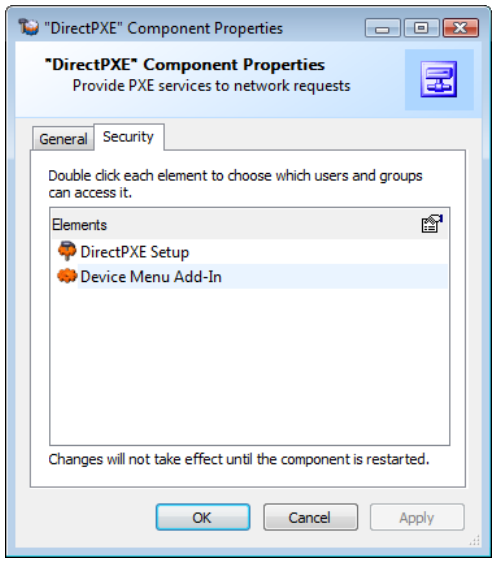
Whether using local security or Domain security we suggest you first setup a minimum of two user groups to control security of the UMS environment. One for 'UMS Administrators', and one for 'UMS Users'. See the Server properties topic on Security for how to secure the Framework, and an explanation of what determines a UMS Administrator and a UMS User.

This section provides example Component Security setup information for desktop deployments. The two main Components benefiting from this level of security are DirectPXE and DirectEngine. Component Security is set within the Properties of each Component using UMS Admin.

DirectPXE

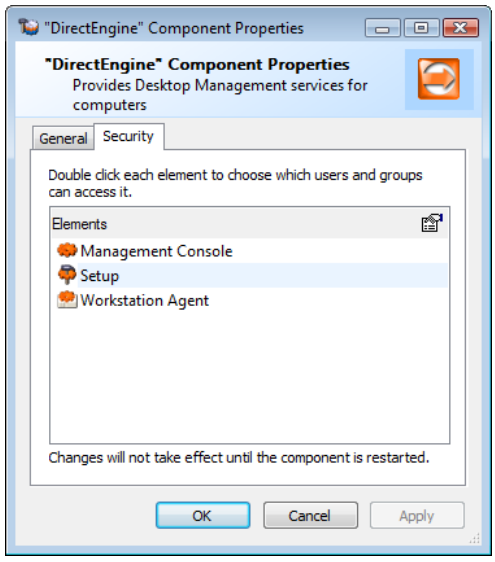
DirectPXE has two Elements which should both be secured. **DirectPXE Setup** is a UMS Client Element which allows the configuration of the DirectPXE server and as such should typically be configured for Administrators and not Users. **Device Menu Add-in** is a DirectEngine Management Console plug-in that enables the PXE Menu properties for a Device to be set from within the Computer properties, within DirectEngine Management Console. As this is a plug-in that links to DirectPXE Setup this should also typically be configured for Administrators and not Users.

Double click on each Element to assign security.



DirectEngine

DirectEngine has three Elements which should be secured and one which does not have security settings



Management Console sets the access control list for access to the DirectEngine Management Console Element. Typically this Element is configured for Users as by definition they are the main users of the Management Console, however you would also add the Administrators too as you would not want to exclude them from using the Management Console.

Securing this Element also secures access to the Management Console and Tasks from the WinPE environment and therefore provides security at the initiation of a build process.

The management console can have the features further controlled by using DirectEngine roles.

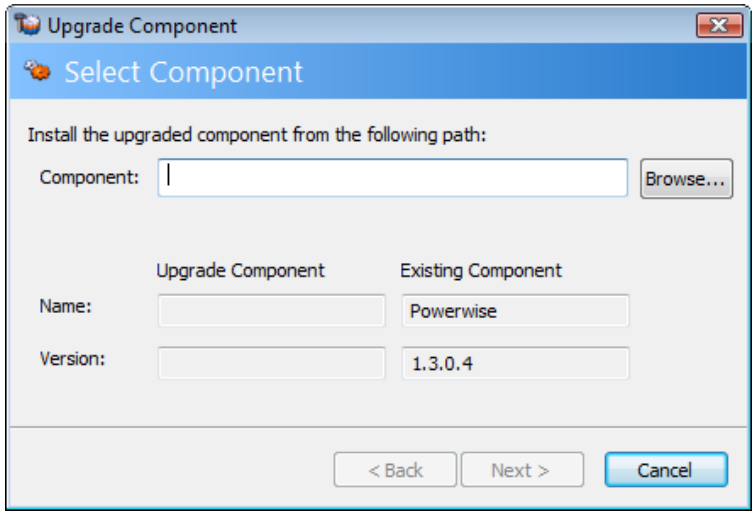
Setup sets the access control list for access to the DirectEngine Setup Element. You would typically limit this to Administrators as it is where all DirectEngine configuration is carried out which is not typically the role of the Users.

Workstation Agent does not have security settings.

3.1.3 Upgrading Components

It may be necessary to upgrade specific Components from time to time as new releases become available.

Components are upgraded individually. The Component wizard will allow you to select the new Component and upgrade the UMS Server installation. To start the upgrade wizard select the Component to upgrade and click the upgrade button  , or select **Upgrade** from the right click context menu.



➔ When browsing for the file, the upgraded Component file location is local to the UMS Server Manager program, not the UMS server. The file is automatically transferred to the server as part of the upgrade process.

The UMS Server will automatically ensure all Client connections are upgraded as soon as they connect and require the upgraded Component.

3.2 Managing Connections

Click the Connections tab in the UMS Server Manager console to display a list of all the current connections to the server.

Each connection shown is one of three possible types as defined below.

Connection Type	Description

Agent	Shows all active UMS computer Agentconnections
User	Shows all active UMS Management Console connections
Administrator	Shows all UMS Server Manager connections

➔ Only Agent connections require a license, User and Administrator connections do not consume licenses.

Right click a Connection in the right pane to show the Connection Context menu where you can:

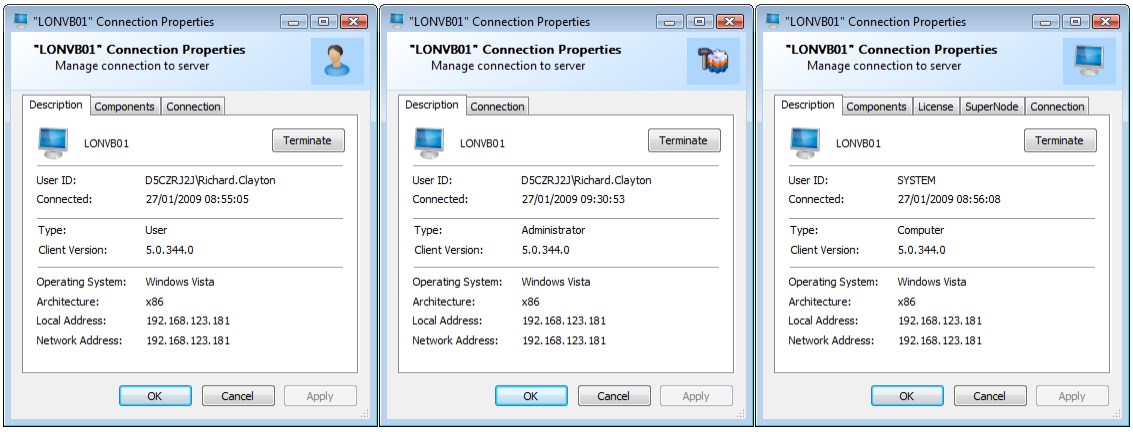
- Load the Properties window
- Terminate a connection
- Clear the local cache

Custom connection view

It is possible to alter the columns displayed to simplify management tasks.To customise which columns are displayed in the right hand pane right click a column header. You can then unlock the columns and select which columns to add or remove

3.2.1 Connection Properties

The Connection Properties differs depending on whether the connection is an Administrator connection (i.e. from UMS Server Manager) or a User connection (i.e. from UMS Client). System connections (i.e UMS Agent connections) are also shown as a computer icon and behave in a similar manner to User connections.



User, Administrator and Computer connection property pages

Connection Property – Description

This tab shows information only; User of the connection, time and date of the connection, whether the connection if from UMS Server Manager or the UMS Client, and the version of the Client type.

Current connection can be immediately terminated by clicking the Terminate button. Connection can be re-established by the user concerned by reconnecting the UMS Server Manager or UMS Client.

Connection Property - Component

This allows the stopping and starting of the UMS user Component parts. If all Components are stopped then the local cache can be cleared of downloaded files by clicking "Clear Local Cache". See

Reloading Client data.

Please note: This page does not appear for Administrator connections, as they cannot host Components.

Connection Property – License

This page shows the license status of the connection. See License Status for more information.

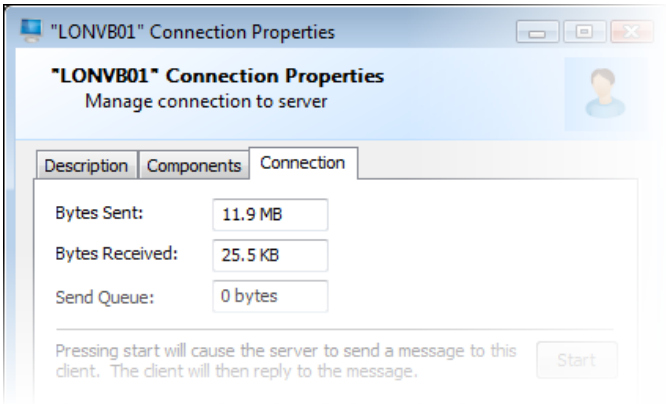
Please note: This page will only appear for connections that use a licensed Component.

Connection Property – SuperNode

This page determines if the Agent connection can participate as a SuperNode for the server. SuperNodes allow caching of files on a subnet to improve performance and reduce WAN traffic. SuperNode usage is defined within the general server installation settings.

Please note: This page will only appear for Computer (Agent) connections as they are the only connection type that support SuperNode functionality.

Connection Property – Connection



To help determine any connection issues, the connection tab shows the data traffic sent and received to the active connection by the UMS Server.

A "ping" test allows the connection to the Client to be tested by the sending of a message between server and Client. Note the ping is successful if the number field increases. A response time of 0 milliseconds is possible on fast networks.

3.2.2 Terminating a Connection

To terminate a Client connection, right click the relevant connection and select Terminate Connection from the context menu.

Terminating a Client connection closes the connection immediately. The connection can be re-established. Agents would reconnect once restarted and a user can reconnect the UMS Client or UMS Server Manager.

To permanently stop an Agent connecting revoke the license as this will stop the Agent connecting again unless the license is explicitly granted. See Managing Licenses for more information on license management.

3.2.3 Reloading Client data

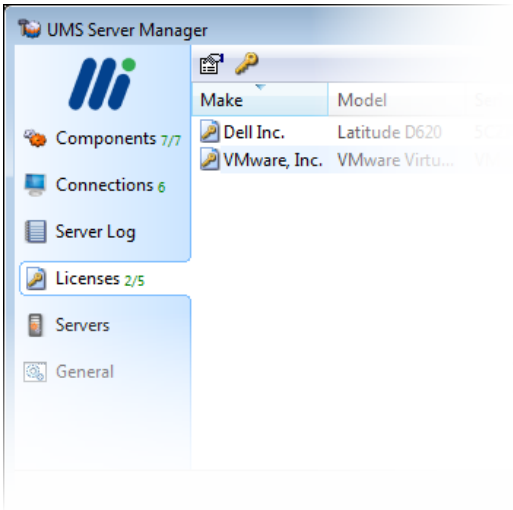
When the Client is first run various application data is cached to the local workstation. Whenever the Client reconnects it verifies the local data against the server and only reloads as necessary.

To force the reloading of all local data you must first open the connection properties window and from the Components tab stop all the Components that are running. You can then click Clear Local Cache on the context menu of the connection.

3.3 Managing Licenses

Licenses come in two forms. The UMS Server Product key controls the total number of computers which may be managed by the server. Once activated this key ensures the UMS Server can run. In addition each Agent requires a Client access license in order to be managed by the UMS Server. The number of these Client access licenses is determined by the activated server Product Key.

The licenses tab shows the number of Client licenses used by the UMS server.



Allocated Client access licenses

Licenses are allocated when the computer first attempts to connect to the server. Once a license has been allocated its considered to be **managed**.

When removing old computers, the license needs to be removed so the license is available for new computers.
The icon in the list shows if the license is currently active or not. See License Status for details of possible license states.

➔ Only Agents managed by UMS count towards the total license count. UMS Server Manager and Console connections don't require a separate license.

An activated server license includes a preset number of Client access licenses. These are allocated to connections on a first-come-first-serve basis. This allocation process can be disabled by removing the 'Auto Grant Licenses' option on the Server Manager Servers tab, and selecting properties for the required server.

Licensing and Activation gives an overview of activating a UMS server license key.

This topic discusses managing individual Client license allocations.

3.3.1 License Status

The UMS 'Workstation Agent' Component requires a license to be allocated before it will start at a connected Agent. When 'Auto Grant' is enabled, all connections within the total license limit will have a status of Active.

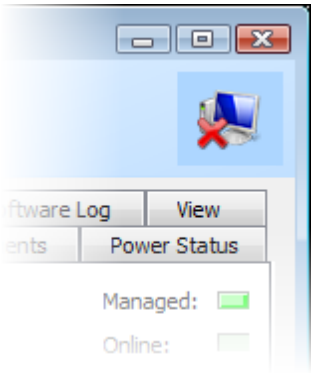
If manual license granting is selected, the licenses can be one of the following states:

Status	Icon	Possible Options	Description
Active		Revoke	This connection is using a license. The license can be revoked if the license is no longer required.
Revoked		Grant	This connection has been refused a license. Pressing grant will allocate a license. The computer is not managed by UMS.
Pending		Grant/Revoke	The 'Auto Grant' option is not set and this connection is waiting for a licence to be either revoked or granted. The computer is not being managed.
Pending Granted		Revoke	This connection has had a license granted, but is not connected or the component requiring a license is not running. When the component connects the license will be set to Active.

If the number of licenses has been exceeded then any additional license requests will result in a Pending status. The computers will not be managed until they have been allocated a license.

UMS Management Console License

If a previously licensed computer has its license revoked then the entry will remain in the UMS Management Console. The icon will change and will be shown disabled, both in the console and computer properties page .



Revoked License Computer icon

➔ Computers which have never had an active license won't be shown in the management console as managed. Only computers which have an active license (or one which has since been revoked) will be shown in the management console unless added via a network scan.

Computers which have been added to the console via a scan now, or added manually will not activate a license until the agent connects to the server for the first time. These computers will be in the management console but will not be managed.

3.3.2 Server Product Key

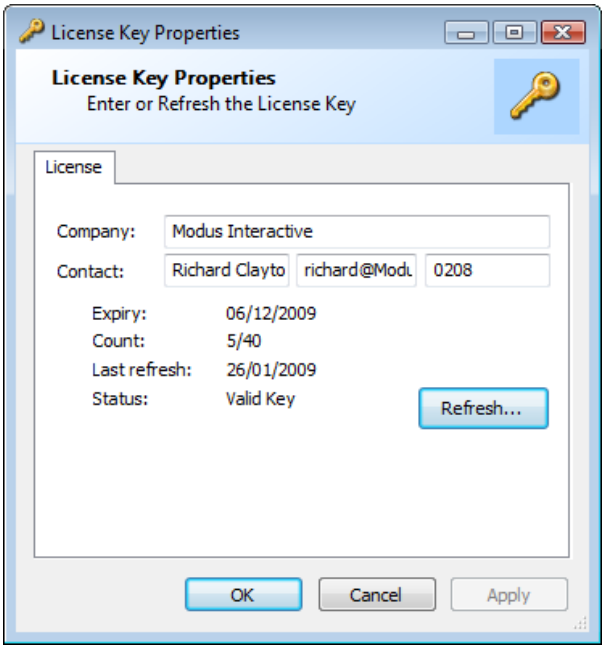
Product Key

Your product key is not displayed in the UMS Server Manager program. Your Product key is either the product media if you purchased a physical copy, or was emailed to you. the product key is required when installing the UMS Server.

In the case of a lost UMS Product Key please contact enter value.

Key Properties

The License page shows the current state of the UMS Server product key.



The number of computers which can be managed by UMS is determined by the Count parameter. For multi-activate licenses the number of licenses for this server is shown, compared to the total number of licenses the product key has. e.g. 50/400 means that only 50 licenses are available from a total pool of 400 Licenses. For single server installations the license always equals the total number of licenses available. e.g. 100/100.

This key can be one of the following states:

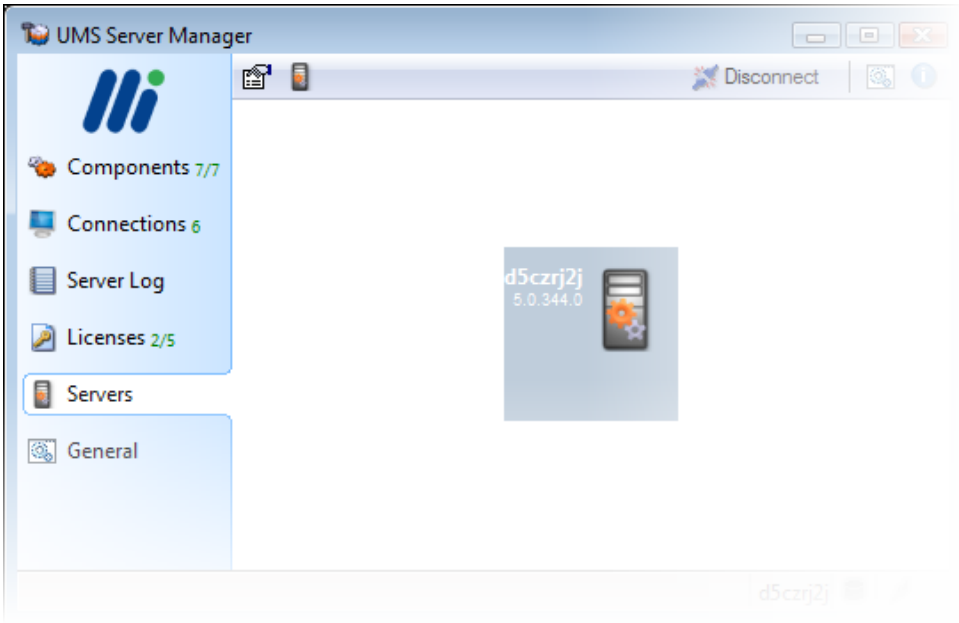
Status	Server active	Description
Valid	Yes	Key has been activated successfully. If new licenses have been purchased then the key can be "refreshed" which will re-apply values from the activation server.
Invalid Key	No	There is no key, or the key is invalid. Click **'Add Key'** to enter a license key. When no license key is present the server will not be able to start components.
Not Activated	Yes - temporarily	The key has not yet been activated and the server will run normally during its 3 days grace period. Click **'Activate'** to launch the Activation wizard. After 3 days the components will stop automatically and the License will need to be activated.

Expired	No	If the key Expired, clicking the **'Refresh'** button updates to the key.

For expiring keys, any Client connections (UMS Server Manager or Client) will receive a warning about the license expiring, three days prior to the keys expiry.

3.4 Servers

Server Management provides details of servers in installation.

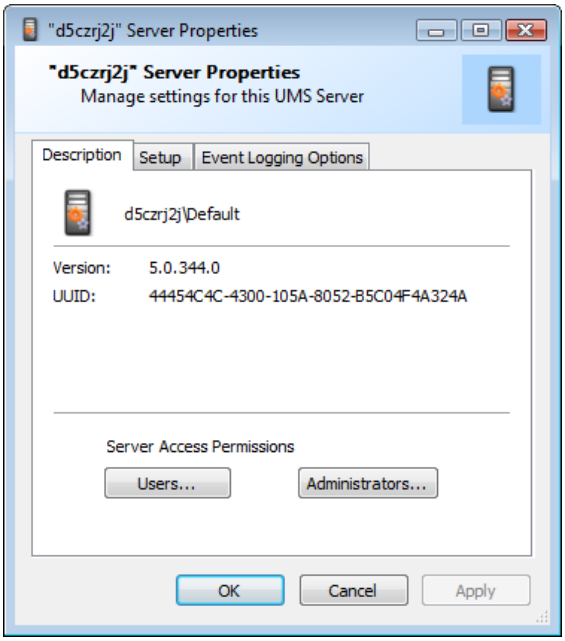


A server has a set of advanced installation options which control the behaviour of the server.

Description - Server version and Server Access Permissions
Setup - Advanced server installation options plus generate Agent Client Packages (MSI install files)
Event Logging Options - Determine what server events to monitor

3.4.1 Description

Identifies the specific server and allows you to define permissions for access to the server.



Server Instance

Shows the installation instance of the UMS installation.

Server Version

Identifies the full version of the UMS installation.

UUID

States the unique id for the server installation.

Server Access Permissions

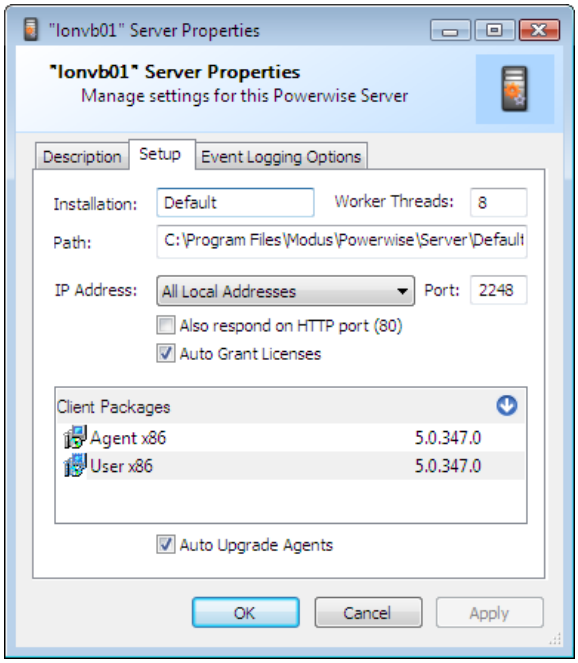
Users... designates people who can connect to the server using the UMS Client, and **Administrators...** designates which users can connect to the server using UMS Server Manager component of the Client.

Please note: All UMS Agents can connect to the server.

Further security can be set on individual UMS Components and their Elements. This is set on the properties of each relevant Component. See the Managing Components topic.

3.4.2 Server Setup

The server page shows advanced installation settings of this server.



Installation

The server installation name is set during installation and cannot be changed.

Worker Threads

This setting is used to tune how the server responds to many connected Clients, and is dependent on the number of processors available. Unless you are running a UMS Server with more than two processors this value should not be changed.

IP Address

By default UMS Server is operating across all IP Addresses known on the server. You can restrict the server to being available on a single IP address assigned to the server. If you select this and the address is removed at a later date, the server will revert to listening on all IP Addresses.

Port

Port 2248 has been registered with the Internet Assigned Numbers Authority (IANA) as the UMS Service port. Changing the port number is not recommended and should be used by advanced users only.

Also respond on HTTP port (80)

The server can also optionally respond on the standard HTTP port (80). This makes it simpler for users who access features via the built in web server, who would otherwise have to remember the preset port (2248).

Auto Grant Licenses

When a Component connects to the server that requires a free license to be allocated, this is done automatically without requiring an operator to grant the license. See License Status for more information.

Path to Data files

This shows the path chosen during the UMS Server Installation.

Client Packages

By selecting a Client package and clicking the download icon a download package can be created into the specified directory. The Client installation windows installer package (MSI) and associated transform file are created in the specifed directory. The created files can then be installed onto target

devices using the customer's preferred software distribution technology.

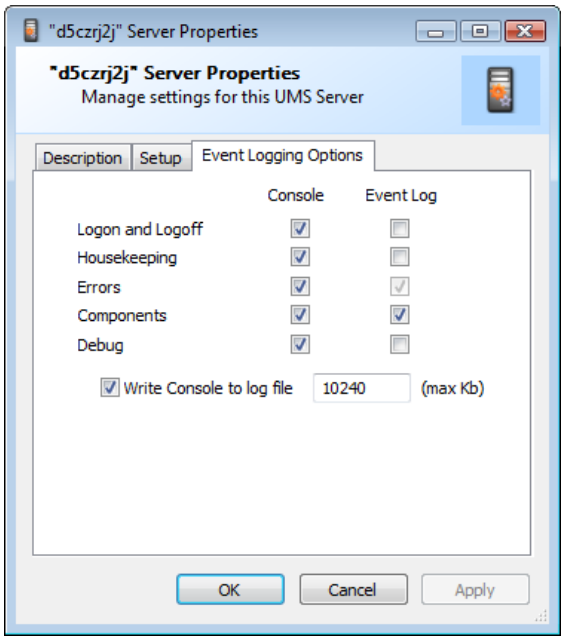
Auto Upgrade Agents

When an Agent from a previous version of UMS connects to a server, this automates the upgrade to the current version. This option is only available for the UMS Agent, as elevated privileges may not be available to upgrade other Clients.

Please note: UMS Auto Upgrade only enables UMS Agent 2008 or newer Agents to upgrade. Older Agents will need to be upgraded using other methods.

3.4.3 Event Logging Options

Different types of events can be monitored by the Server and these can be configured to report in two different locations; the UMS Server Manager console, and the Windows event log.



Components can be customised to produce various events, and it is recommended that these should be enabled. The console log can be viewed in real time from the UMS Server Manager console window. If Event Log is enabled, the entry is written to the server's event log.

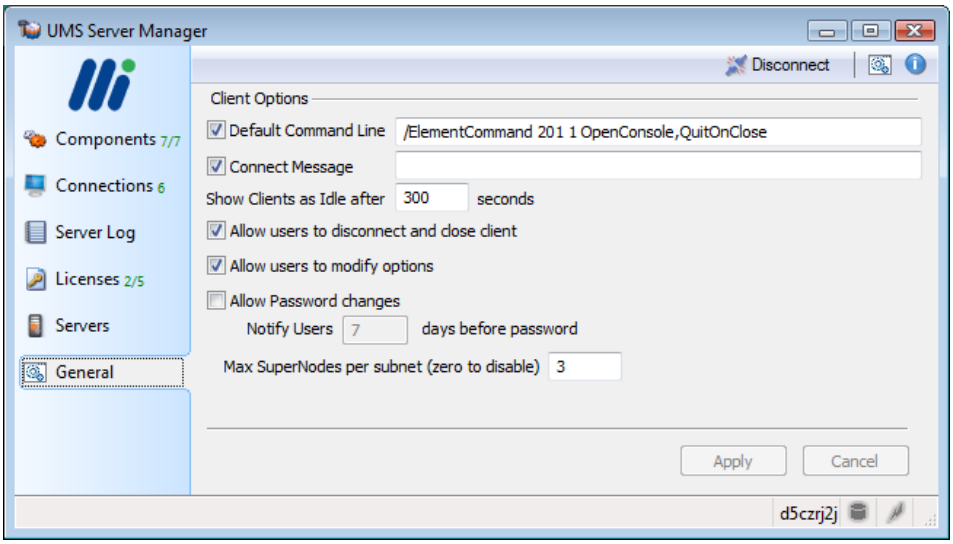
Event Types

- Logon and Logoff – monitors agent and user connections to server
- Housekeeping – captures UMS server housekeeping events
- Errors – Any system errors are logged, event log is always on
- Components – logs component specific events, which may be user defined.
- Debug – Captures detailed debugging information. When 'Console' debug is selected, debug files are cached on every Client.

Select the Write Console to log file to output the console log to a file within a log directory which is located in the same directory as the path to the server files root (e.g. for Path of "C:\modus\UMS\Server\Default" the log directory is "C:\modus\UMS\Server\Log". Each log file is limited to the maximum size specified, and a new log file is automatically created when the log size is exceeded.

3.5 General

Client Options are applied each time the UMS Client application runs and connects to the server. The default settings are sufficient for nearly all scenarios.



Check for Updates

Checks with the activation server to determine if there are any software updates available online. If updates are available then the wizard will guide you through the upgrade process.

Default Command Line

This allows the default action on loading the Client to be customised. The default command line is to load the Direct Engine Management Console.

Unless instructed to do so, we strongly recommend that the default command line is left unchanged.

Connect Message

When the UMS Client connects to the server it can display a Connect Message. With this option checked you can also customise the Connect Message. By default the message informs the user of the user credentials used to connect, and the server name and UMS Server name it has connected to.

Show Clients as idle after <> seconds

Certain UMS Components may be configured to perform tasks when the UMS Client is detected as idle. The amount of time of no mouse/keyboard activity before the status of the UMS Client is set to idle is set in seconds.

Allow users to disconnect and close Client

Select whether you want users to be able to disconnect and close the UMS Client.

Allow users to modify options

Select whether you want users to be able to modify the UMS Client options. The options available from the Options button on the Client are shown in the UMS Client Configuration topic.

Allow password changes

Select whether you want to allow users to change their password and set the number of days prior to

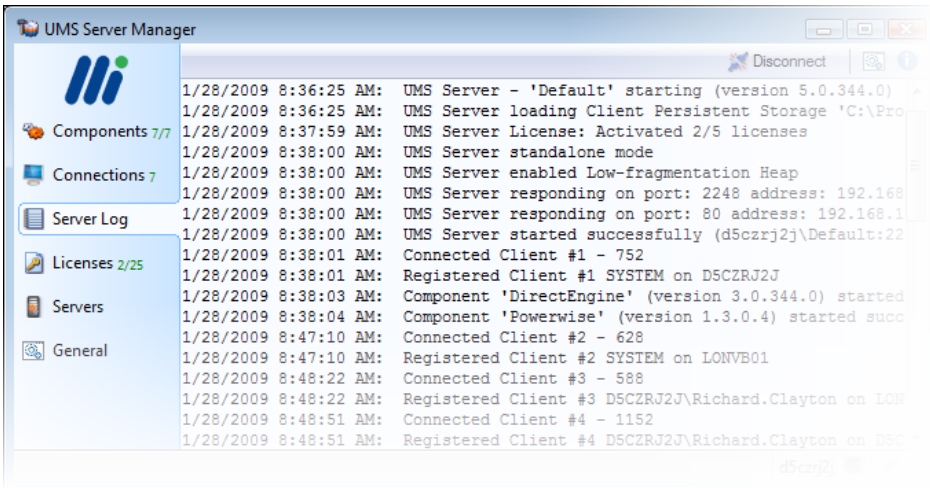
expiration they are notified.

Max SuperNodes per subnet (zero to disable)

A SuperNode allows UMS to cache information from the server and pass it to other Agents in the same subnet, instead of transferring it directly from the server. This process enables more efficient use of network bandwidth.

3.6 Server Log

The server log can be used to monitor server activity and identify unusual events or errors.



The contents of the log are determined by the Event Logging Options defined within the UMS server.

Console updates in real time as events occur.

Part IV

Client

4 Client

The UMS Client is used to provide a consistent interface to UMS Components, enabling users to access Components from a common location, while ensuring authentication is performed once for all UMS Components, rather than once per Component. By default the Management Console is loaded when you login to the Client, and from the Management Console all available Component Elements (subject security and roles) will be available.

The UMS Client provides:-

- Authentication services with UMS Server
- Communication services with UMS Server
- Common Alert mechanism and Alert history

In this section

Configuration

4.1 Configuration

The UMS Client configuration Options are accessible from the Options button on the UMS Client login dialog box. If you have installed the UMS Client, launch it by selecting the UMS icon on the start menu. Alternatively you can Quick Run the UMS Client.

➔ Access Client options from either the management console tools menu, or if at the UMS login dialog, click the tools button which will allow you to select options.

Click on the Options button to configure the Client Options. The Options dialogue has two tabs; Preferences and Connection.

Preferences

Run this program when Windows starts

If checked, then the Client will start as soon as the user logs on. This will also place an icon in the system tray which can be used to control the UMS Client.

Play a sound when a new Alert arrives

If checked, whenever an alert occurs the corresponding UMS new alert sound is played.

Connection

Server Name

Either the DNS name or IP address of the server to connect to. Clicking the drop-down arrow will browse for available UMS servers on your network.

Attempt to connect to the first discovered server

During connection the Client will broadcast a request to all UMS servers (this will be restricted to the local subnet unless appropriate port forwarding is enabled). By default, this broadcast will be on UDP port 2248.

Note: *Where both the* ***Server name*** *and* ***Attempt to connect to first discovered server*** *checkbox is set, the Client first sends a broadcast packet and connects to the first server that responds. If no server responds after 20 seconds, the Client will then attempt to connect to the server name specified.*

Automatically connect when Program starts

UMS Client will attempt to connect to a UMS server as soon as the program starts. Either the server name or “Attempt to connect to first discovered server” checkbox must be set for a connection attempt to be made.

➔ If you always connect to the same UMS server then you can specify both the server name and then tick the box to automatically connect. You will then automatically launch straight into the management console

Type

Select whether to use the current user credentials or to provide a user name and password.

Part V

Management Console

5 Management Console

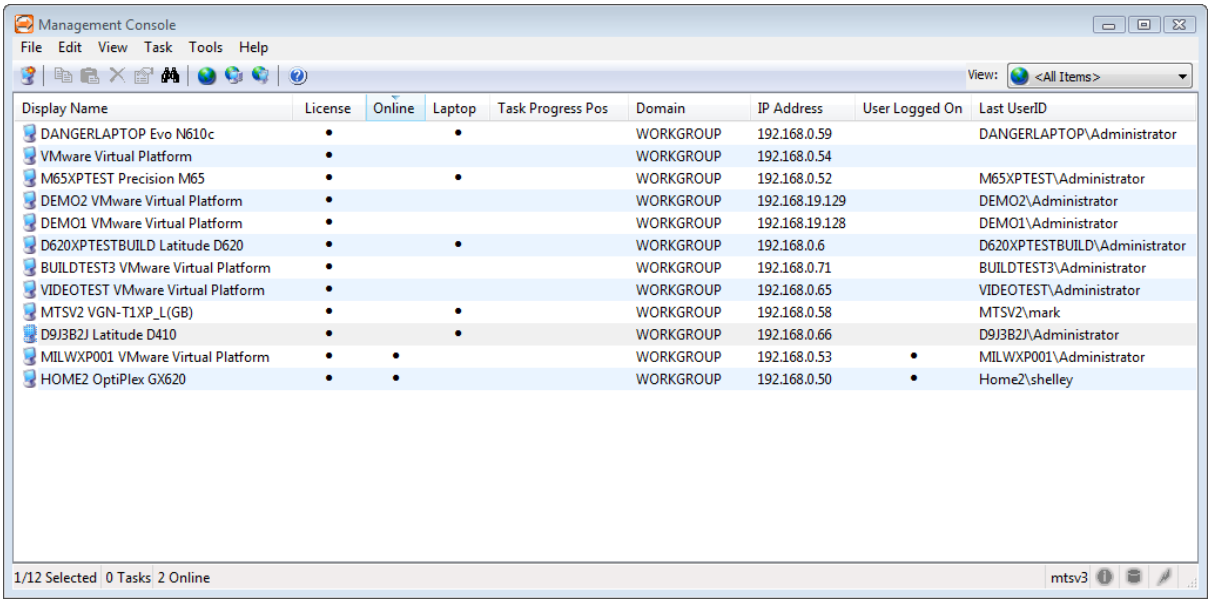
The UMS Management Console is the default element loaded after UMS Client login. The Management Console provides both a tool for monitoring and managing all the computers connected to the server, and also a tool which provides access to any of the other Component Elements a user has access to (dependant on security and role).

In this section

Navigating the Management Console
Add Computer Wizard
Find Computers
Computer Properties
Group Properties
Tasks
Alert History

5.1 Using the Management Console

An example UMS Management Console is shown below. Move your mouse over the image and click on additional information about navigating the console. What a user can and cannot do in the Management Console is controlled via UMS Roles.



Menu Toolbar

The menu toolbar provides a shortcut to the following functions:

Icon name	Description
New Computer	Launch the Add Computer wizard
Copy	Copy the selected item. You cannot copy computers
Paste	Paste the selected item
Delete	Delete the computer or group
Properties	Show the properties of the selected item
Find	Launch the Find Computers dialog

All Items view	Change the view to All Items
All Computers view	Change the view to All Computers
All Groups view	Change the view to All Computer Groups Dynamic groups are only listed in the drop down view
About	Launch the About dialog

Changing the view

Use this dropdown list to change the default view in the console between All Items, All Computers, All Groups, and Search Filters. Console will by default show 'All Items' including both computers and groups. Standard filters allow viewing of either computers or groups. Once a group has been created, the group can be selected in the filter and then all the member computers are shown in the console. Dynamic groups (collections) have been configured and computer membership of these groups is automatically maintained.

Dynamic Group	Description
Managed	Computer has had the Agent installed
Online	Computer is connected to the server
Model	A group is created for each distinct computer Model
User Logged On	Group of computers where a user is currently logged on
Task Running	Shows all computers where is task is currently running

➔Dynamic collections are a powerful tool to show all computers with a given property. For example, a collection can show you all online computers, or all computers with a user currently logged on.

Computer groups are a convenient way of managing a collection of computers together. Tasks may be submitted for both computers and groups. Use the view drop down list to change the view. As computer groups and filters are created they are added to the list of available views.

Customising the columns

By right clicking on the column header it is possible to lock and unlock the columns, as well as select from a comprehensive list of other columns.

Column	Description
Display Name	Computer or Computer group name. Display name intelligently provides name of computer and model if available. Where name is not available the MAC Address is used.
License	Indicates whether computer has had a license allocated to it and can therefore be managed
Online	shows if a client Agent is currently connected (computers only)
Laptop	shows if a managed computer has been detected to be a laptop
Task Progress	
Domain	Domain or Workgroup of computer
IP Address	Last detected TCPIP address
User Logged On	Indicates whether an account is currently logged on to the console of this computer
Last UserID	The UserID of the account to be logged on to the console of this computer

The console can be customised either by the user (or administrator) so that the any number of columns can be displayed according to the users needs.

Tasks may be submitted against multiple computers and groups by selecting the required rows and then using the context menu to select a task to submit.

The console updates in real time allowing the user to see the exact status of the system at any point in time.

Status bar

As well as showing the number of selected items, the number of running tasks, and the number of online devices, the Status bar also shows:

Icon	Description
<name>	This shows the name of server the console is connected to
	This icon will be highlighted when there is task Alert History to be viewed. Double click on this icon to open the Alert History window
	This icon will be highlighted when there is a file transfer in progress. Hover over the icon to see the current activity
	This icon will be highlighted when there is network activity between the server and any Agents. Hover over the icon to see the current activity

5.2 Add Computer Wizard

There are a number of ways to add a computer to UMS. Computers automatically appear in the Console as soon as the Agent is installed (see Installing the Powerwise Agent) and it connects for the first time. This is probably the standard and most common way of adding computers to the Console. Alternatively, using the Add Computer Wizard allows computers from Active Directory, or the current network browse list to be imported into the Management Console. Two methods of adding computers are available through the wizard.

Import Computers

Import Computers allows a list of computers to be built that can then be added to the console. The list can be built from 3 sources:

1. Enter computer details manually. Computer Name, PXE GUID and MAC address can be entered to define the new computer.
2. If the computer is a member of an Active Directory domain, the domain structure can be browsed and computers added to the list
3. Contents of the network browse list can be added to the list.

Once a list of computers is created, a task can be automatically launched once the computers have been added to the console. This can be used to install the Agent.

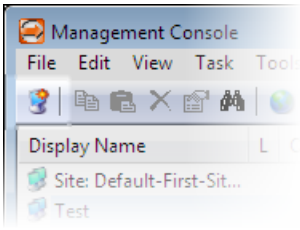
Scan Network

Scan the network will discover computers on available subnets and immediately add them to the console.

Using the Wizard

The following guide shows the steps required to use the Wizard.

1. Click on the 'Add Computer Wizard' icon on the toolbar or select File/New Computer.



Choose either 'Import Computers' or 'Scan the network'

2. Click Next >

Scan the network

Click the 'Scan Now' button to add detected computers to the console.

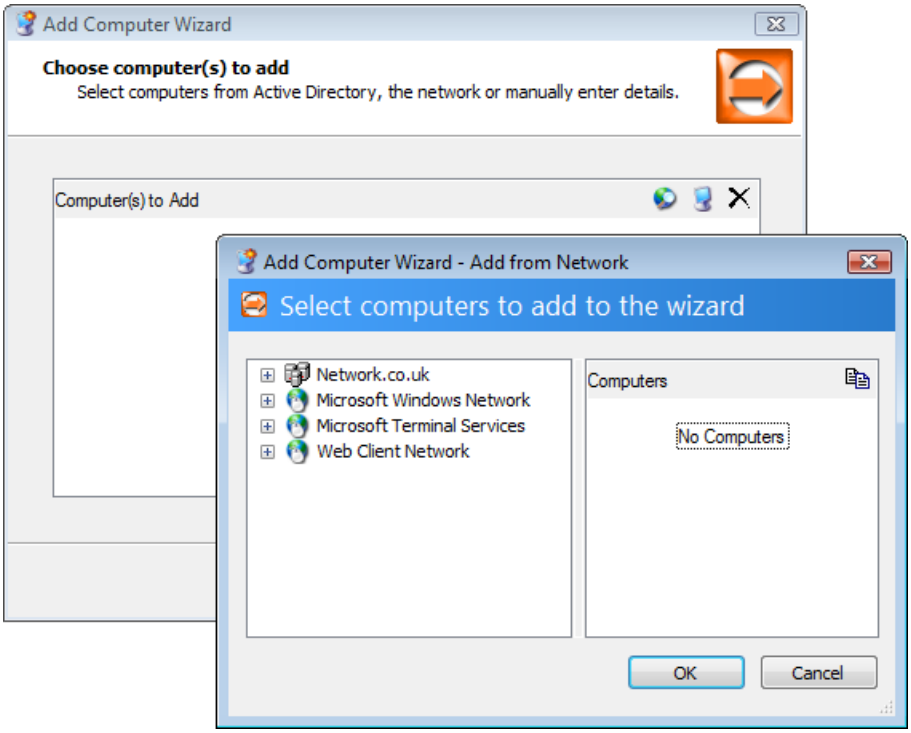
Computers responding to the scan will be added directly into the console and will not be able to have any Add Computer task run against them. This task can be run after the wizard is closed by selecting the new computers in the console.

Scanning uses the NetBIOS protocol to detect computers. With Windows XP SP2, Microsoft prevents the workstation from responding to these scan requests. Currently only Microsoft Windows Server family, Windows XP SP1 and prior, and Linux servers will respond to the scan request. Also, if a firewall is enabled on the computers, they may not be detected.

3. Click Next >

Import Computers

Computers can be manually entered or selected from the Network or Active Directory. Click on the Add from Network icon and browse and select computers



Browse the Active Directory OU, or select from the Network. Available computers will be listed in the left panel. Multiple computers can be selected.

4. Once selected computer(s) from the 'Add from Network' dialog, click OK.

   For each computer selected you will either see a 'Responding' or 'Not Responding' status in the window, to show if the computer is active.

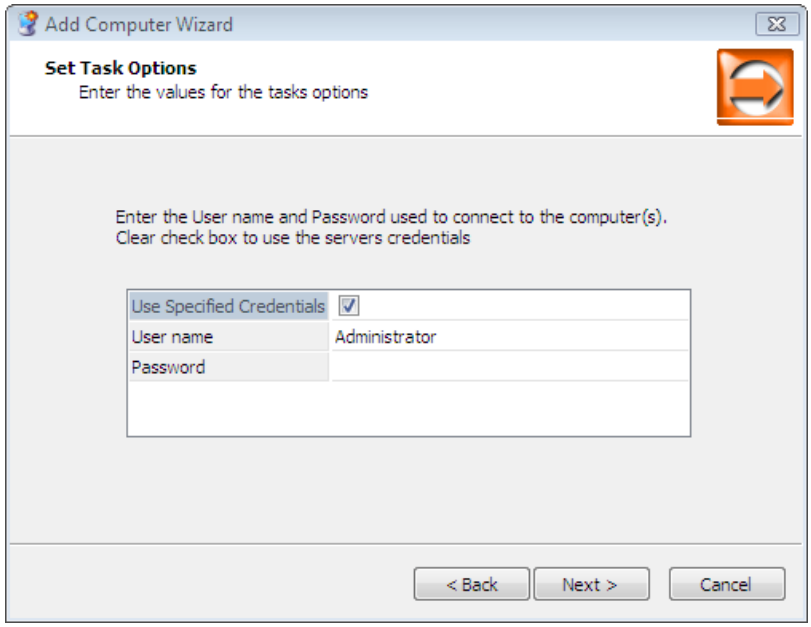
> ➔ Responding uses ICMP ping to query the computer. If a firewall is enabled on the computer that prevents response to ICMP requests, the computer may show as 'Not Responding' even if it is online.

5. Once you have selected the computers click Next >

   By default, the option to install the Agent to the computers will be enabled.

6. Click Next >

   If the 'Install Agent' option was chosen, you will be prompted to enter credentials.



   If the network is configured to use Active Directory, specific credentials will not be required. Uncheck the 'Use Specified Credentials' option, the other options will be ignored. The Install Agent task will be launched under the context of the Server service account, which will need appropriate rights (local admin) to install the software on the computer.

   Other scenarios will require the username and password of an Administrator account for the target computer(s).

> ➔ To install the Agent using this method, 'File Sharing' must be enabled on the computer, 'Simple File Sharing' must be disabled and, if a firewall is enabled, file sharing must be a configured exception. Also, the Admin$ share must exist on the computer. You may also find your anti-virus products are configured to stop the process used to push the Agent in this manner.

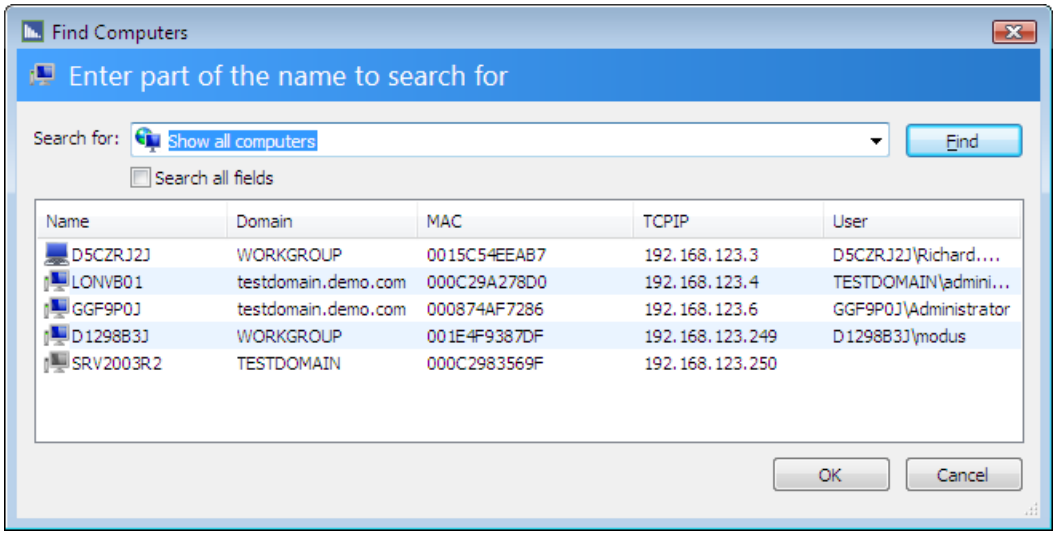
7. The computers will be added to the console.

   If 'Install Agent' was selected a task schedule will open showing the progress for every computer.

Check the summary screen at the end of the wizard and click Finish to start the process.

5.3 Find Computers

Pressing F3 at the Management Console will present the search dialog:



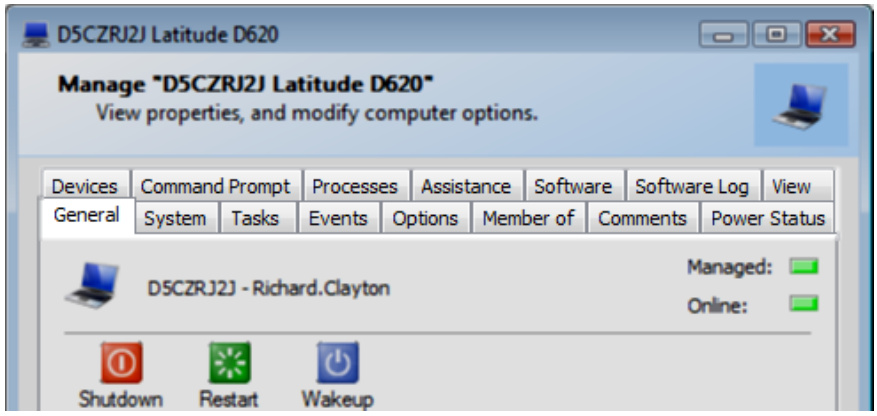
By default the dialog will search for any computer names matching all or part of the search text. To search any of the columns shown, click the 'search all fields' checkbox.

Selecting one or more computers and clicking 'OK' will open each of the selected computers.

5.4 Computer Properties

The computer properties window provides detailed information for the selected computer. Access this window by selecting properties from context menu for the desired computer from the management console window, or double clicking on the computer listed in the window.

The tabs available will vary according to the role you have been assigned by the UMS administrator.



Automatic synchronisation

All changes to the computer while the properties window is open are automatically updated without user intervention. Changes made by the user unless otherwise indicated are not made until the user presses either OK or Apply. Some specific changes are made immediately (submitting of new task for example). While a change is outstanding (e.g. Option type has been changed but not applied) it is not possible to add a task via the Tasks tab until the changes have either been applied or cancelled.

If a computer is updated which has an outstanding change then that outstanding change is lost. This functionality ensures the objects remain in a consistent state.

5.4.1 General

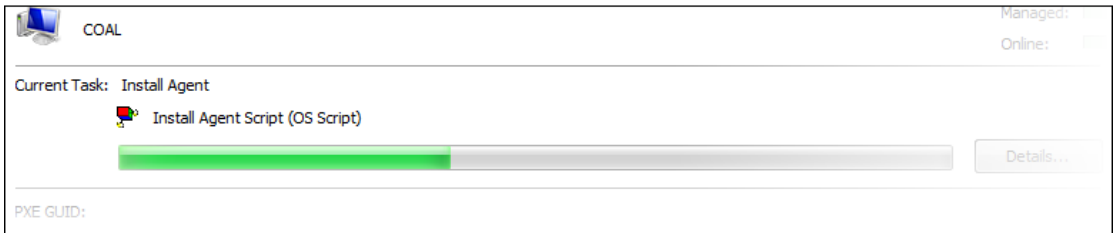
The General tab shows the standard headline information about the computer. This includes the computer name, whether it is online and managed, information about any current task running, as well as summary network information.

➔**Managed** simply means the Agent has connected successfully to the server at least once. **Online** means that the Agent is currently connected to the server.

Attribute	Description
Managed	A device is identified as managed if it has the Direct Engine Agent software installed on it and the Agent has connected at least once to the server. A device which is managed can be controlled via the management console.Control features include items such as remote takeover.
Online	An online device is one that is managed and is connected to the UMS server. A device without the Agent installed is never shown as online. This indicator shows orange is the connection is from a PreOS computer.
Task Detail	If a task is executing then this dialog will show the progress of the task and the current step the task is running. The progress bar indicates the status of the task. This progress bar is indicative as each component which makes up the complete task can differ in duration. When a task is running additional options are available. See executing tasks below.
PXE GUID	The PXE Globally Unique Identifier (GUID) is the unique identifier passed by the PXE Client device while performing a PXE boot. The PXE Guid is shown once it has been captured by the console. The most common way to discover the GUID is for the computer in question to boot and perform a PXE broadcast. If a computer has been added manually then the GUID can be set through the Add Computer Wizard. The PXE GUID can be considered unique although using a docking station for a notebook will pass the same PXE Guid irrespective of the notebook attached.
IP Address	The last known IP address on which the machine connected to the console. This is automatically updated each time the device changes IP address.
MAC Address	The unique network address of a node on the network. The MAC address is a hardware address of a particular network device.
Version	This shows the version of the Agent as of the last time connected.

Executing Tasks

When a task is running the general tab will change to show the task progress bar.



Clicking on the **Details...** button opens the manage task schedule window. Once the task is complete the dialog reverts to showing available tasks. To show details of a completed task click the Tasks tab, before selecting the properties of the task of interest.

Icon Display

The icon shown in the general tab changes depending on the hardware shown. Laptop and Desktop computers are shown with different icons. Revoked connections where the license has been revoked have a big cross through them. Computers with revoked licenses will never come online, though they are still shown as managed in the console.

Revoked desktop icon

5.4.2 System

The System tab shows a summary of operating system and hardware information. This tab will only show data if the computer is Managed.

Operating System information

When a task is running the computer is managed then this information is populated with the fields shown. It can be useful to see the OS, User and computer AD information.

➔**Previous User** simply shows who the last user logged on was. Useful when no-one is currently logged on.

Hardware information

Shows general hardware information, plus the last IP address the device connected with. This will be accurate for online devices but may be incorrect where a computer uses DHCP and isn't online.

5.4.3 Tasks

The Task tab shows any tasks which have been scheduled against the selected computer. This tab can be used to see what tasks have run previously as well as any tasks which have yet to run or are currently running. Icons clearly show the task status, allowing for fast identification of failures and problems.

Tasks can be added from with the task window. Simply click Add Task to see what tasks are available. Task Filters allow you to show tasks with a specific status.

Add Task

Click on this button to see a select from a list of tasks to run against the computer. The list that you

see is controlled by the UMS administrator. In some cases the add task button is disabled and it is not possible to add tasks for that computer. This is because another change has been made to that computer object which has yet to be applied. The most common cause for this is a change to a computer option which hasn't been applied yet. Once the change has been applied the new task button is enabled. This feature prevents unexpected behaviour when running tasks.

Immediate execution / Scheduled execution Tasks may either be defined to run immediately or can be scheduled to run at some point in the future (and the task may be scheduled to repeat at regular intervals). Your administrator will configure which tasks are immediate and which are scheduled. By default any task which has a high impact on the target computer will not be marked for immediate execution so that the user may review and amend the task before submitting the task. The task may be scheduled to execute immediately if necessary

Cancel Task

Click on this button to cancel the currently selected task.

Delete Task

Click on this button to delete the currently selected task from the task history. A warning dialog asks the user to confirm that the task should be deleted as it will delete the task for all computers it is assigned to, not just the current computer. When deleted the task is deleted for all computers it was assigned to. Once deleted the information cannot be retrieved. Some users may not be able to delete tasks depending on their role.

Task Property

Click on this button to view the Task Properties of the currently selected task.

Task Filters

The filter toggle push buttons on the dialog toolbar allow the user to select which tasks they wish to view. The buttons states :-

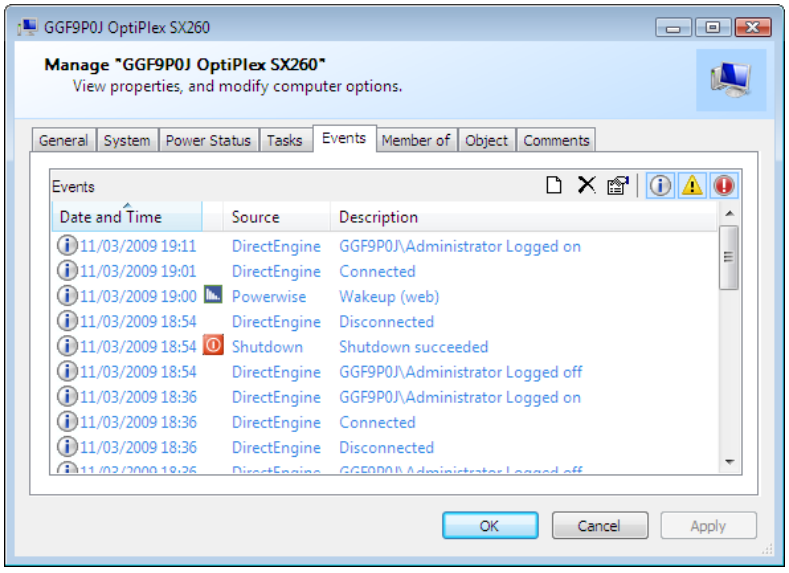
- Scheduled - Tasks scheduled to run in the future
- Executing - Task currently executing, or execution is pending
- Completed - Tasks which have completed

The buttons can be toggled in any combination to suit the user. Only one task can be executing at a point in time but several tasks can be queued for execution.

Note: Tasks can also be assigned to groups.

5.4.4 Events

The Events tab shows a log of events that have occurred against the computer.



Events show connection and disconnection activity, logon/logoff activity, plus any hibernate/shutdown/wakeup actions. When an event of type 'Warning' or type 'Error' occurs, the Alert Status of the computer is set to the corresponding value. This status will remain set until it is manually cleared by a console user.

A console user may also add events to the log for administration purposes. Pressing the 'New' button will show the event entry dialog.

Clicking the 'Delete' button will reset all events for the computer by clearing the log. Once 'Apply' or 'OK' is clicked to save the dialog, the event history will be cleared and a new event will be entered to detail the user who cleared the log.

Some tasks may add corresponding events to show their completion status. but the complete list of tasks appears in the **Tasks** tab.

Clock Skew

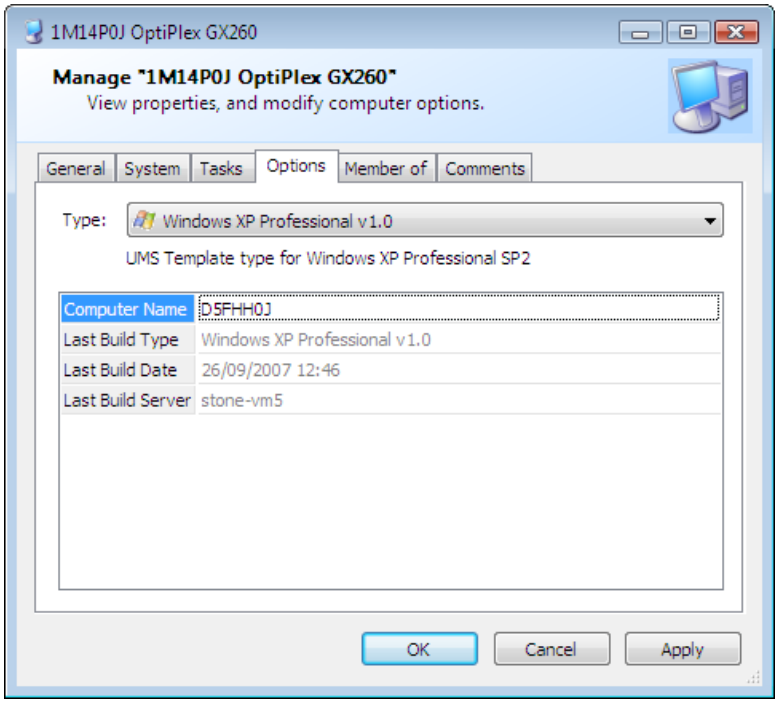
For computers which aren't in a domain its possible for the server and Agent computers to be out of sync. These are shown as warning in the event tab as clock skew. Scheme changes etc will take place at the Agent computers time, rather than the server time.

This should not affect computers which are in a domain. The clock is set from the domain controller.

➔UMS is timezone aware. Changes take place at the client's local time, which can be different to the server time.

5.4.5 Options

The Options tab allows the user to select the most appropriate options for the device.



Type

The type is used to select one of the pre-defined build types for the individual computer in question. Each type defines a specific build of interest to the organisation. Each type has its own set of features and options.

Types should be defined to best reflect your organisation and the different builds available to your user base.

Selecting a different type shows the individual build options associated with that type. An option can be available to any number of types.

Note: Types can also be changed from the computer context menu on the Management Console.

Options

The values chosen can have a dramatic effect on tasks when executing. Options allow users to specify values which can be utilised by tasks. After making changes, the changes need to be applied before the system will utilise the new values. Options are created through the Direct Engine setup program and are associated to particular build types. Each option is defined as being one of the following types:-

- Text Line - Free format text line, can be limited in length and valid characters
- Drop Down List of options - To select single predefined option from list of choices
- Checkbox - used to indicate true/false selection

Some options may be read-only and cannot be edited by the user.

Option values can be set to other build option values, or other system defined variables. For example the value $(ComputerName) will be replaced by the task with the detected computer name of the computer the task is running against.

5.4.6 Member of

Computers can be placed in groups to assist with management, however tasks can also be run against groups. This tab allows you to see which groups the computer is a member of, as well as add or remove the computer from groups.

Groups are static in nature, you add and remove computers manually. UMS also has dynamic groups which have membership controlled automatically depending on the properties of the computer.

Group Membership

Computers can be members of more than one group. You cannot add the computer manually to a dynamic collection.

➔ To see all computers in a group change the view in the management console to show the required group.

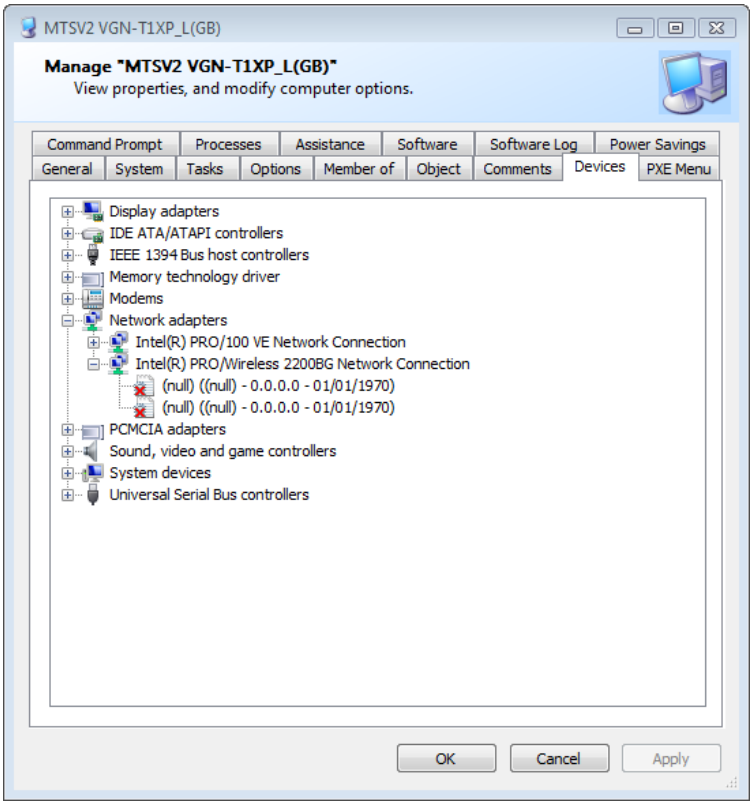
5.4.7 Comments

The comments tab provides a free text box where comments about the computer can be recorded. This can be especially useful if the comments column is visible at the Management Console.

5.4.8 DirectDrivers

DirectDrivers can add a 'Devices' page to the Computer Properties window of the Management Console. This page shows all the detected devices for the computer, and whether that device has any matching drivers in the database.

The computer will need the agent installed for this list to be populated. The list identifies the drivers which will be injected when deploying the computer.



Addin pages, such as the Devices tab shown above, are enabled/disabled in DirectEngine by modifying Roles, and therefore may not be available to all users.

5.4.9 DirectTools

DirectTools enables access to real-time remote diagnostics utilities to computers from within the DirectEngine management console.

DirectTools provide three additional computer page add-ins to DirectEngine. The available pages and privileges are modified by editing a users Role in DirectEngine setup.

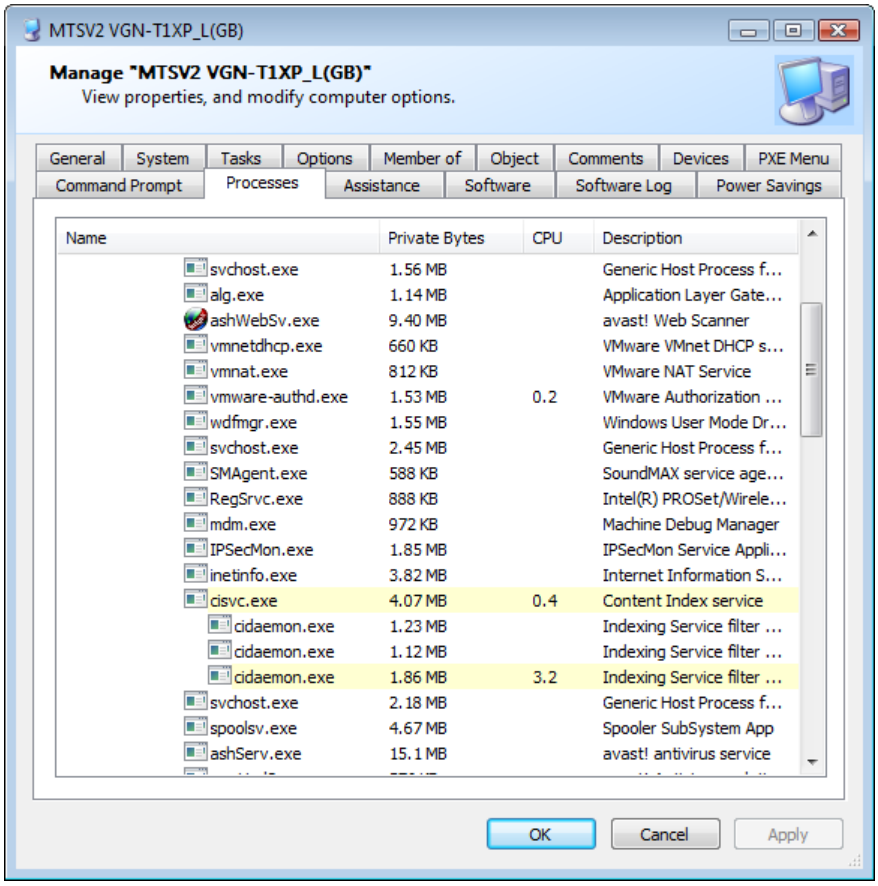
In this section

Processes
Command Prompt
Remote Assistance
View

5.4.9.1 Processes

Processes shows a real-time view of the processes, or tasks executing on the remote computer. Many process details such as CPU utilisation and memory usage can be shown. Using UMS roles, the user may have access to terminate remote processes and related child processes. Additional columns can be added/ removed by right-clicking on the column header

Viewing currently executing processes is a useful first stop when diagnosing problems on remote computers.

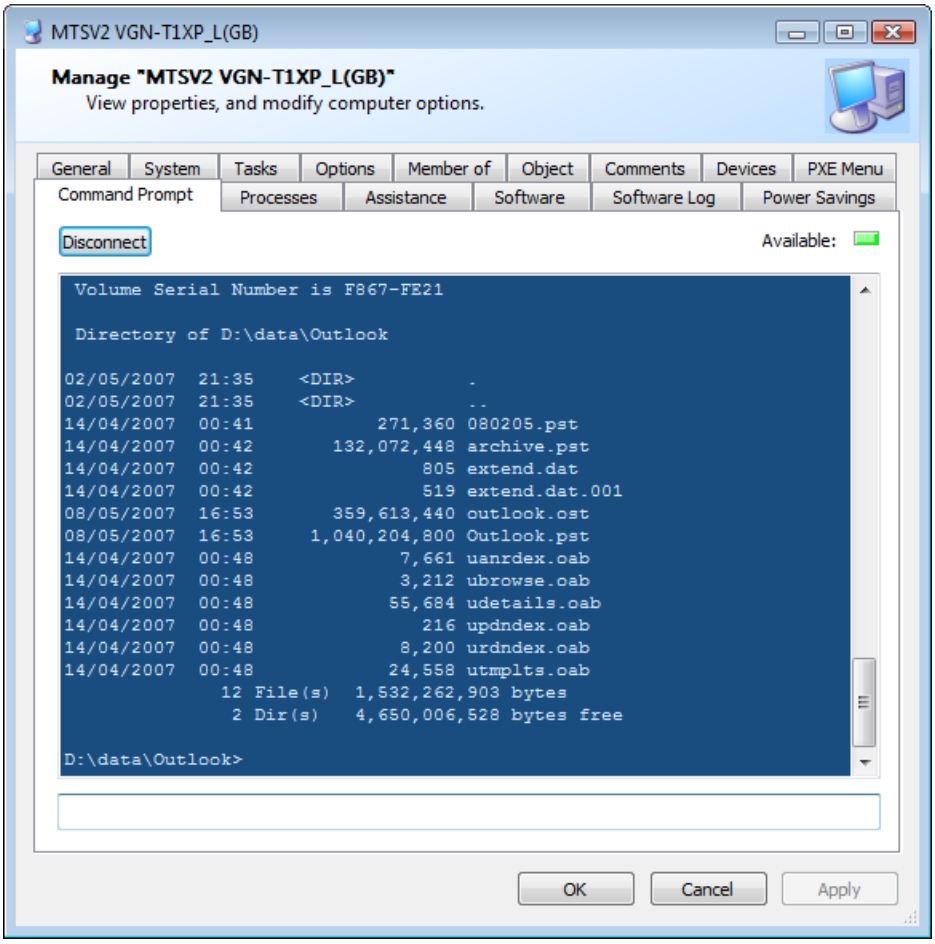


More details of a process can be viewed by double-clicking on the process.

Additional columns can be added/removed by right-clicking on the column header. Right-Clicking a process allows an operator to terminate that process. This privilege can be controlled through the DirectEngine role.

5.4.9.2 Command Prompt

Command Prompt allows the UMS user to run a console session on the remote computer. A remote console session can be used to fix identified problems on the remote computer, by stopping or starting services and copying or deleting files. Through UMS roles, users can be given access to a computer when they would otherwise not have appropriate privileges.



5.4.9.3 Remote Assistance

Remote Assistance allows a helpdesk expert to view a users screen, chat online with the user and take control of the users screen with their permission. As this feature uses the 'Offer Assistance' feature the following conditions must be true for it to work:

- Both the novice and expert computers must be running Windows XP, or better.
- The novice and expert users are members of the same domain, or are members of trusting domains.
- Both the novice and expert computers must be connected to the Internet, or the same LAN or WAN.

See Microsoft knowledge base article 301527 for more information about How to configure a computer to receive Remote Assistance offers.

5.4.9.4 View

The view tab shows a snapshot of the screen of the current logged on user. Note that if no-one is logged onto the remote computer, or their desktop is locked the remote view will be unavailable.

The view is refreshed approximately every 5 seconds.

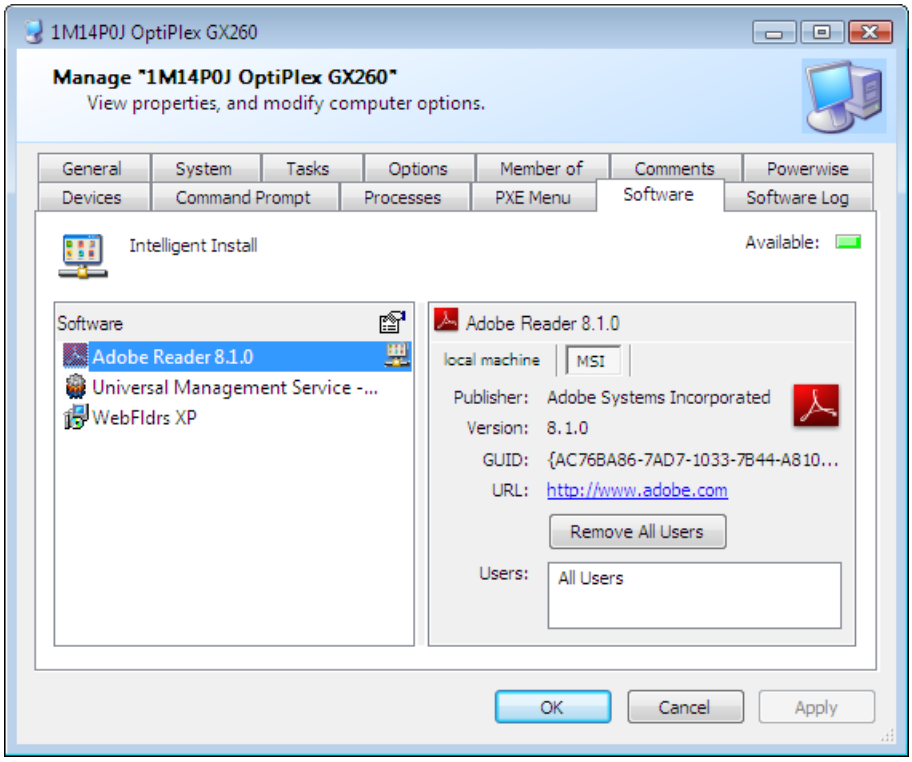
5.4.10 Intelligent Install

The Intelligent Install component shows software that has been installed on a computer, and the history of installation activity on the Log page.

Software Page

The software page shows all software installed by Intelligent Install, and other Windows Installer application installed at the computer. Each application has a detail page.

The II icon on the left hand side of the software list designates the application as having been installed by Intelligent Install.



If the computer is currently connected to the server, the **Available** option will be lit, and the console user will be able to remove applications. This is available for all Windows Installer applications.

Software Log Page

The Software Log page shows the history of installation attempts by Intelligent Install. Logging options are configured by the Intelligent Install Management Console.

5.4.11 Power Status

The Power Status tab shows the current status of the computers power related items.

Profile

The computer can opt-out of Powerwise power saving features, enabled by the corresponding check-box. Profiles can also be enabled or disabled, allowing administrators to opt-out groups of computers.

Each computer can only use a single Powerwise profile. If the <Use Default> option is set, the computer will use which ever profile the administrator sets to be the default. If the administrator changes which profile is the default, all computers set to <Use Default> will switch to using the new profile.

Multiple computers can have their current profile switched by selecting the multiple computers in the management console, and using the Powerwise context menu.

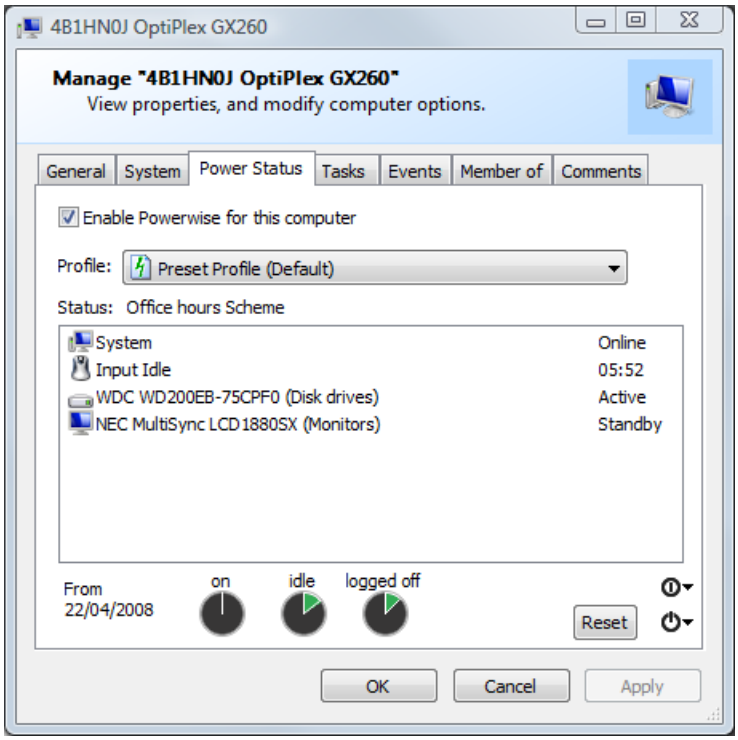
Profile changes take immediate effect.

Enable Powerwise for this computer

If this checkbox is ticked then the active Profile will be applied. If unchecked then the Profile is not applied to this computer.

Status

The Status area shows the name of the Profile Scheme (if active), along with the status of each power management element. There are also three pie charts displaying the current metrics of Powerwise. Hovering over the pie charts will show the actual figures.



Each part of the status information is described in the table below:

Part	Description
System	**Online/Offline.** Shows whether the computer is currently connected to the server.
Input Idle	Active/Time Idle. Shows whether keyboard or mouse activity has been detected at the console. If it has it will show 'Active'. If not, after the Client Idle timeout has been reached, the amount of time the console has been idle will be displayed.
(Disk drives)	**Active/Standby**. An entry for every Disk Drive with power management features will be listed. If it is in use and using power it will show Active. If it has been powered down to save power, it will show Standby.
(Monitors)	**Active/Standby**. An entry for every Disk Drive with power management features will be listed. If it is in use and using power it will show Active. If it has been powered down to save power, it will show Standby. Note that power management features cannot detect if a monitor is actually attached to the display adapter.
Monitor Standby Disabled	Software can prevent monitors from going into standby state. If any software is running that will prevent monitor standby, this warning will be

	shown.
System Standby Disabled	Software can prevent computers from shutting down or hibernating. If any software is running that will prevent the system from entering standby, this warning will be shown.
On Pie chart	Shows the percentage of time the computer has been on, since Powerwise was installed.
Idle Pie chart	Shows the percentage of time the computer has been on and idle/ logged off, since Powerwise was installed.
Logged Off Pie chart	Shows the percentage of time the computer has been on and logged off, since Powerwise was installed.
Reset	Reset will erase all power status data for this computer.
 Away Mode	Away Mode allows the console user to hibernate immediately for a set amount of time, and then wakeup after the time interval. This can be used if it is known that the computer will not be used, for example when the user has a lunch break.
 Keep Awake	Keep Awake mode prevents any of the Powerwise idle functions from triggering for a set amount of time, and then returns to normal operation.

5.5 Group Properties

Computer groups simply group together devices which are logically related. They enable administrators to perform tasks to multiple machines without having to select each machine individually.

There is no restriction on computers being members of more than one computer group. Task membership is determined when the task starts executing, not at the time the task is submitted.

Computers can be bulk added to a group by highlighting them in the Management Console and selecting "Add to Group" from the context menu.

Note: Groups can be dynamically created and deleted by executing tasks.

5.6 Tasks

Tasks are the core management actions initiated against computers within Direct Engine. Except for a few special cases any action against one or more computers is performed by running tasks. Tasks are configured by administrators to perform one or more actions against a computer. This can be anything from initiating a remote takeover session to rebuilding the computer.

Each task is configured so it may only run on appropriate devices. Some tasks run immediately while others can be scheduled to run at a later date.

Tasks can be added and removed as required by the administrator. Commonly used tasks can be added to the shortcut (context) menu so that users can easily run them against computers and computer groups. If a task is not available for the selected entry then it is shown but disabled.

The tasks shown in your management console depend on your role and the tasks you have available to you. Administrators can limit who may run tasks to enable tasks to be assigned to job function. If you cannot find a task which you know should be available, ask your administrator to check you have the right permissions.

Some tasks may be scheduled to run repeatedly, if the management operation requires it. This is configured in the task wizard. Some tasks run immediately in which case they cannot be scheduled to run repeatedly. You can schedule the task from the task wizard (see below) to get around this limitation if necessary.

When a task is scheduled against a computer group (static or dynamic), the task runs against the computers which are members at the time of execution. Therefore a task can be scheduled in the future if computers are added or removed from the group then they will run the task if they are part of the group at execution time.

Tasks can be launched in the following ways:

- Add a task to a computer from its Task page
- Add a task to a group from its Task page
- From the Add Task Wizard accessed from the Task menu
- From the Management Console context menu

5.6.1 Add Task Wizard

Using the task wizard to add a task to the system allows all options of a task to be configured.

Select 'Add Task...' from the task menu on the Management Console. This will launch the wizard, and provide a walk through of the steps required to create a task and assign it to computers or groups.

5.6.2 Task Properties

The task properties dialog shows the status of a scheduled, running or completed task

General

The general tab shows the task name and description. The task name of scheduled tasks can be modified to something more meaningful.
Start: This shows the next time the task is scheduled to run. A run immediate task has already been launched and can only be run once.

Task Hold: Putting a task on hold stops the task from being scheduled. Tasks which have already been scheduled or are already running are unaffected by the hold status. All computers assigned in the task are held. It is not possible to hold a subset of the assigned computers, although the computers assigned to the task may be changed as necessary.

Assigned

Shows the computers and computer groups which have been assigned to run against this task. If the task has already started executing (scheduled for execution) then the list is readonly and cannot be altered.

Before the task starts executing the computers and computer groups can be amended as necessary. Any Changes need to be applied before coming effective. If a computer is referenced twice (e.g explicitly and as part of a group) then duplicates are removed before the task is submitted.

Executing

Shows the current execution status of each computer against which the job is running.

When a computer is selected from the list the individual status information is shown in the lower half of the dialog. The progress bar indicates total task progress. Duration is only shown on completion of the job. While the task is running the task may be cancelled by pressing the cancel button. This may leave the computer in an undefined state. The Cancel button will stop any further task steps from being executed, but the currently executing step will continue to completion, depending on the type of step currently being executed.

Completed

Once tasks have completed they are moved from the executing tab to the completed tab. Repeating Tasks Repeating tasks are likely to have have more than one entry in the progress panel, depending on if the task has been repeated yet. There is one entry for every time the task has been scheduled to run. The number of entries in the completed panel will continue to grow over time.

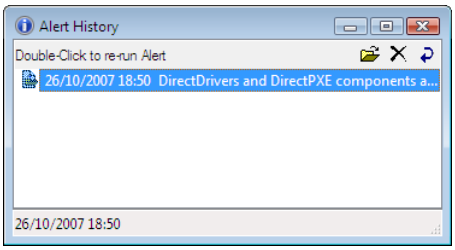
5.6.3 Open Task

The 'Open Task...' any task to be found which exists in the management console. The following describes the search types:

Search	Description
On Hold	All scheduled tasks with a current status of 'On Hold'.
Scheduled	Tasks that are scheduled. They may or may not have already executed.
Scheduled Successfully	Tasks that have been scheduled, and the execution was successfully launched. Not that a successful schedule, does not reflect a successful execution.
Failed	A task schedule that failed to launch.

5.7 Alert History

Alerts are used by UMS Components to bring something important to the attention of the user. How you see Alerts depends on how you run the UMS Client. The  icon will flash to indicate new Alerts, and to view the Alert history window click double click on the icon. Alternatively, if you configured the Client to load at Windows startup then you will have the Client system tray icon and this will present you with scrolled messages each time an Alert is generated. You can click on the scrolling Alert to see more details.



To replay alerts open the client alert history window and double click any alerts that you would like rerun. You can also highlight the required alert and press the Rerun alert icon  .

If you wish to open the appropriate Component window immediately, highlight the alert and press the Open folder icon  .

To delete alerts press the delete alert icon  .

5.8 vPro Authentication

vPro is enabled from the Tools Setup menu. When enabled, authentication needs to be established between the server and every vPro enabled computer. The server will attempt to connect to each detected vPro computer using the default userid and password. If this fails, the computer will get an entry in this window, allowing a computer specific userid and password to be entered. This should match the password entered at the computer's BIOS.

Part VI

Components

6 Components

A UMS Component is an application which has been designed to run using the facilities provided by the UMS framework. A single Component is equivalent to an application.

6.1 DirectDrivers

DirectDrivers is a UMS component that provides the following functions:

- A device driver repository
- A computer hardware scan database
- Matches all available drivers to a computer hardware scan
- Provide matched drivers for use by Windows OS builds and WinPE environment.

When used in conjunction with DirectPXE, a WinPE environment is created specifically for the connected device, every time that device boots. This removes the need to have static CD images with multiple network drivers. Once the network driver has been added to DirectDrivers it will then be automatically used when WinPE is loaded at workstations.

When workstations are built, all the available valid drivers are added to the build. By adding the latest drivers to DirectDrivers database, a workstation build will automatically select the most appropriate drivers.

Once a device has had a hardware scan (by installing the agent, or booting to WinPE) then its possible to see a list of all the PCI drivers required by the computer. You can also see which ones are available and which are missing.

DirectDrivers currently supports PCI devices only. However, DirectDrivers can still deliver non-PCI drivers, for more information see Using Conditions in the Reviewing Drivers section. Conditions allow you to inject any drivers you like, giving you the flexibility to present drivers wish to use.

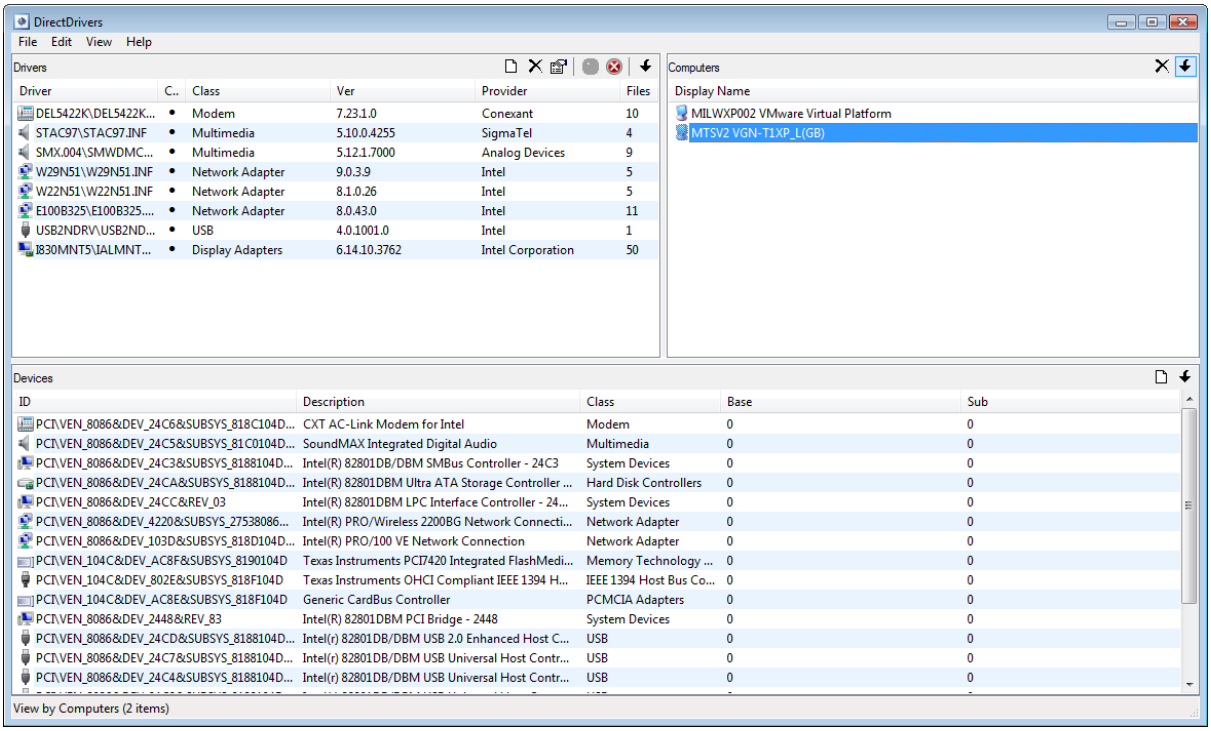
➔Direct Drivers removes the need to maintain an image with drivers for all devices. The required drivers are injected automatically..

In this section

Navigating the Console
Adding New Drivers
Managing Drivers
Integration with other Components

6.1.1 Navigating the Console

The DirectDrivers console uses a GUI interface to simplify the management of drivers. The console can show the relationships between Drivers, devices and computers, depending on the current view mode and item selection.



➔When opened for the first time, only the drivers pane is shown, add the Computers and Devices panes from the view menu.

The console is shown in three Lists, Drivers, Computers and Devices. By default, the Computers and Devices windows are hidden, and can be revealed by using the View menu. The position of the three lists may not be changed although they may be re-sized as necessary.

View	Shows
Drivers	Individual drivers which are available to Direct Drivers. Properties show the available information, and allow conditions to be defined to determine when a driver will be injected.
Computers	Lists all the devices which are available. This list is syncronised with the management console, allowing the selection of any of the available computers.
Devices	Lists the devices supported by the available drivers. Its possible that a device is supported by more than one driver, in which case when the device is selected both drivers are shown.

Any of the lists may be considered primary, and this is denoted by the highlighted "view all items" button [ ]. Whichever window has this button selected will be showing all the items of that type. The view is also shown in the status bar along with the number of items of that type.

➔When a view is primary, the other views then change to reflect relevant information, e.g. select a computer when its primary and all the device drivers it needs are shown in the devices list. Plus all the drivers which support those devices are shown in the drivers pane.

6.1.1.1 View by Drivers

The only mandatory list, it shows a list of the drivers features including the location of the .inf file, its class, version and manufacturer. The complete indicator shows whether all the associated files listed in the .inf file are stored in the driver database. The columns in this list may be altered to add the driver database or to remove any columns not required.

List contents with Drivers as primary view:

view	shows
Drivers	Shows all drivers in the database
Devices	For a selected device shows all drivers which support that device
Computers	For a selected computer show all drivers which will be provided to that computer when it is deployed (built)

Disabled Drivers

Whenever a driver is first added it is disabled by default – A disabled driver will not be provided to a computer until the driver has been enabled. Disabled drivers are shown by the device icon having a red cross through them: 

➔While a driver is disabled its not used for injection, even if a condition is specified. Disabling drivers can be useful when troubleshooting.

Drivers with Conditions

Drivers can have conditions set, to control when they are used. This can provide support for non-PCI drivers, by specifying the hardware types to deliver the driver to.

Drivers with conditions have a yellow explanation mark: 

➔If a device is included by condition, it won't be shown in the drivers list unless it happens to be a PCI device which would be included anyway by device matching. The condition is only checked during driver injection.

6.1.1.2 View by Devices

The devices list shows known devices and their properties. The primary column is the device ID along with the class and description of the device. The actual devices shown in this list are dependent on the “primary view”, which is always shown in the status bar.

List contents with Devices as primary View:

view	shows
Drivers	For the selected device shows drivers that support shows the current selection
Devices	Shows all the devices held in the driver database
Computers	Shows the known computers that have the selected device

If the devices list is not shown it may be enabled from the view menu.

It is possible for devices to be in the database but to be unrecognised by the database. In this case the device icon will be represented by a yellow question mark. 

6.1.1.3 View by Computers

Shows a list of computers name and optionally the model, manufacturer, serial number and UUID of the computer. The contents of the list depend on the primary view, which is shown in the status bar. If the Computers list is the primary view then the list contains all the computers known to the system.

List contents with Computers as primary view:

view	shows
Drivers	For a selected computer, shows all drivers that support the computers devices
Devices	Shows all PCI devices installed in currently selected computer
Computers	Shows all computers in the system

If the computers list is not shown it may be enabled from the view menu.

6.1.2 Adding New Drivers

Drivers can be added in one of any 2 ways:

- Manually adding drivers
- Add Driver Wizard

When adding drivers for OS installation you do not need to add drivers which are already part of the Microsoft installation CD, however you will need to add network drivers for use in the PreOS (WinPE) dynamic CD

The driver database is a single source, so you do not need to add the same drivers for WinPE and again for the OS installation. This is relevant as WinPE drivers are installed uncompressed, while OS drivers can be injected compressed and the OS installation will automatically uncompress them.

6.1.2.1 Manually adding drivers

If you already have a driver database then this can be copied directly into the DirectDrivers\DRIVERS folder. The drivers will automatically be identified and added to the database list. Note that drivers will always be added in a disabled state, and will need to be enabled prior to them being used.

Duplicate drivers added will be automatically removed.

This technique is not recommended, as unnecessary files that are part of the driver delivery package, not the actual driver may be deposited in the database. To ensure a clean database, use the Add Driver Wizard.

6.1.2.2 Add Driver Wizard

The Add Driver Wizard allows you to install one or more driver(s) into the database. The Add Driver Wizard can be launched from the File\New menu, the New icon on the toolbar, or by right clicking the Drivers list pane and selecting New. Selecting New on the Devices window will automatically set the 'Must support device' option with the device id for that device.

➔Using the **Add Driver Wizard** is the recommended technique to add drivers.

If you want to import a single driver select "Add single device driver" from the Add Driver wizard. This will allow you to add a single
driver into the database. You will need to locate the .inf file in order to import the driver.

To add multiple drivers select the "select multiple drivers from directory" option which will scan through a directory (and optionally sub folders) identifying drivers which you may then import as you require.

- **Search Directories:** All Subdirectories of the selected directory will be searched for valid device drivers.
- **Ignore drivers with Windows 9x signatures:** Older drivers are flagged as being compatible with all versions of Windows. These drivers can be ignored to reduce the number of drivers matching the search.
- **Include only complete drivers:** If a driver has a listed file or digital signature missing it can be ignored.
- **Must support device:** Search for a driver that matches the entered PCI Vendor id. This option is automatically set when the wizard is launched from the Devices context menu.

Pressing next will perform the device driver search and display the matching drivers. All imported drivers are disabled by default and will need to be enabled before they will be used, by right clicking and selecting enable.

6.1.2.2.1 Driver extraction

If a computer has already been configured with the correct drivers, the extraction (ripping) option will allow you to lift the driver from the computer and place it in the DirectDrivers database.

➔Driver extraction is useful when you don't have access to the original driver files.

Some caveats to this extraction exist as complete drivers files are not always available on computers; however it still provides a powerful tool in the management of device drivers. The ripping process is likely to find incomplete drivers if:

- the original driver used CAB files to compress the driver files
- the original driver contained files for more than one target OS

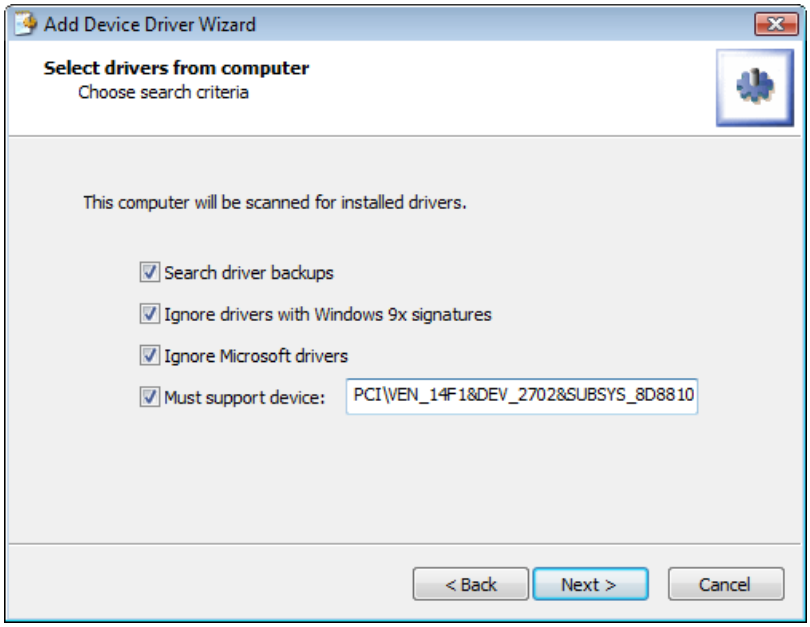
However, having access to the appropriate setup file will often enable the administrator to locate the complete driver from the manufacturers web site, and often the incomplete driver will still function correctly.

➔You must run the management console from the computer you wish to extract the driver from.

Extracting a driver

The driver wizard allows you to select only drivers which support a specific device entered. Launching the driver wizard:

1. Launch the DirectDrivers console from the computer with the driver installed on it
2. Select the device you wish to rip the driver for in the Devices list
3. Select **Add Driver** from the context menu
4. Choose "**Add Drivers from current computer**" option and click Next.
5. The must support device checkbox will be automatically ticked with the device ID of the device you selected in step 2
6. Press Next to show the driver which supports this device.
7. Complete the wizard to import the driver into the driver database

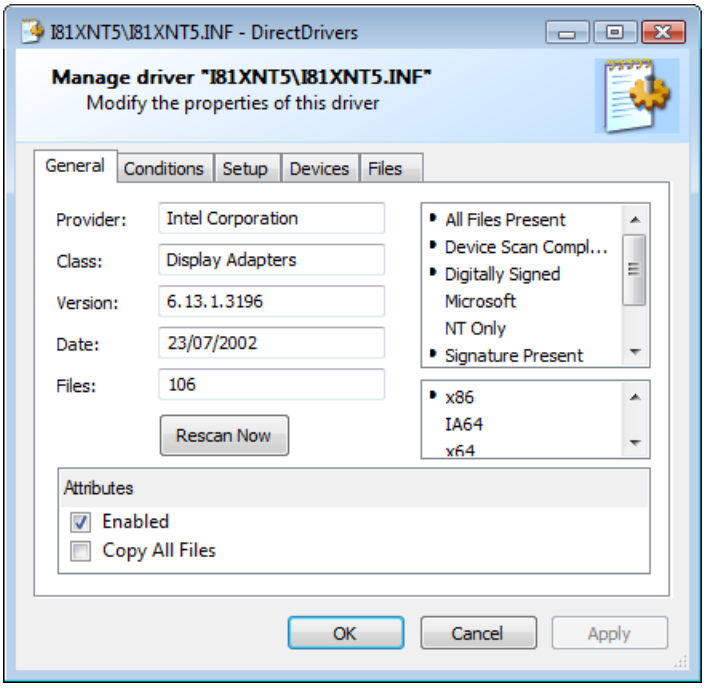


The available options for the driver extraction wizard are similar to the standard options, apart from the following:

- **Search driver backups:** When a Update Driver is installed on a computer, the previous driver is stored in a backup folder. This folder can also be searched for valid drivers.

6.1.3 Managing Drivers

The management console provides features to allow for driver review. Selecting **Properties...** from the context menu on a driver will open the drivers management window, showing the attributes of the driver.



Attribute	Purpose
All Files Present	All files as defined with the driver file,
Device scan complete	
Digitally Signed	The device was authored with a digital signature
Microsoft	Driver was authored by Microsoft
NT Only	Will only work on Windows NT Operating system
Signature Present	The device was authored with a digital signature, and the signature is present
Textmode Setup	Driver is a specifically for use within text portion of OS installation (and also WinPE) to add hardware support for disk drives not natively supported by Windows installation. e.g. Windows XP SATA drive support.

DirectDrivers caches information from the driver in its database. It also detects changes to the driver and automatically re-caches the information. To force a re-cache, press the **Rescan Now** button.

➔Its not normally required to Rescan drivers. If you adjust driver files directly rather than through the Direct Drivers GUI, then you should Rescan the driver.

As the driver caching can take some time, there is a caching queue. While a driver is waiting the be cached, the **Device Scan Complete** attribute will be cleared.

The most common use is when adding a new computer into enterprise and you need to check that you have the appropriate drivers to support the device.

The simplest method is to add the device to the network and boot the device. If you initiate a boot into the PreOS environment, then the device list is automatically added to the Driver console. Any devices that are of an unknown type by the system are automatically shown with a yellow question mark.

Note that the boot into WinPE will not succeed if the network card is not in the DirectDriver database, but we will have identified the drivers that need to be added, without making any physical changes to the new computer. A computer booted into WinPE without a valid network card driver will get a WINBOM error displayed on the client.

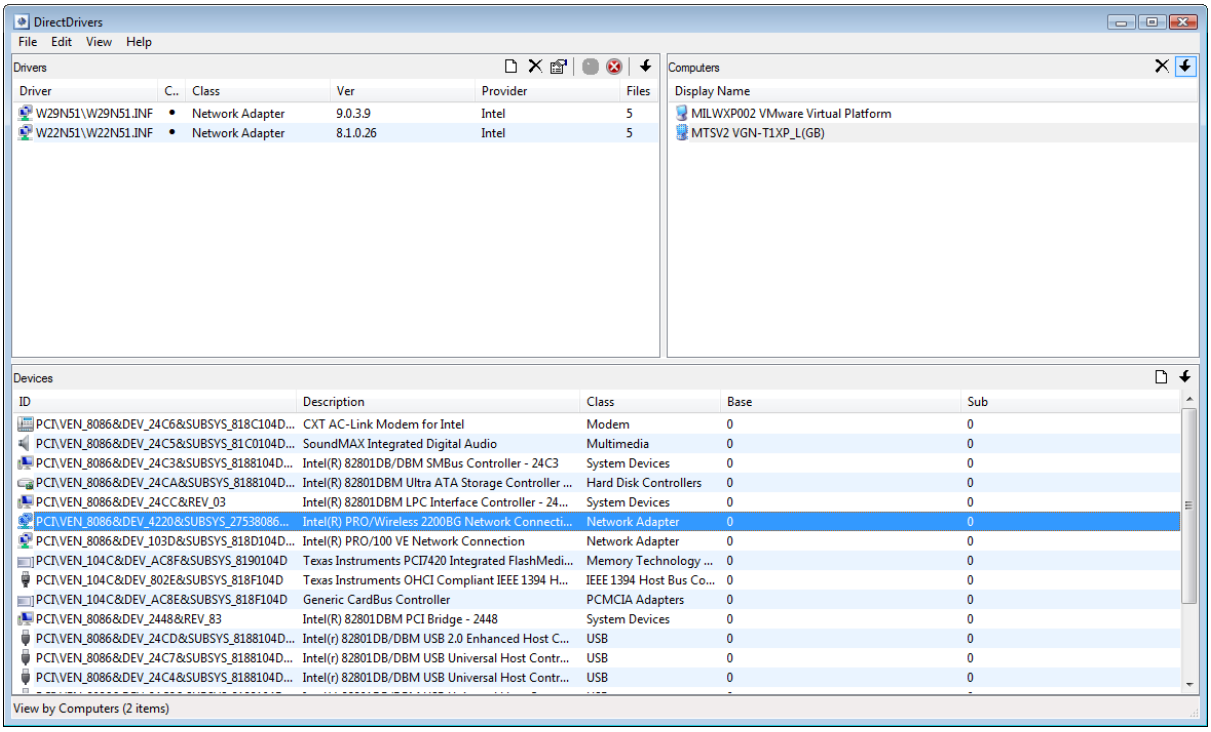
If the new workstation already has a version of windows installed then by installing the UMS Agent onto the device will also provide a list of the hardware devices. Installing the UMS client onto the workstation would allow the drivers to be ripped from the existing device into the driver database.

The majority of new computers will come with a CD containing drivers for the OS you wish to install, and these drivers can be extracted from this CD as necessary and installed.

Once the computer devices have supporting drivers in the driver database then the computer can be built in the same manner as your existing devices and Direct Driver will inject the appropriate drivers.

6.1.3.1 Versions

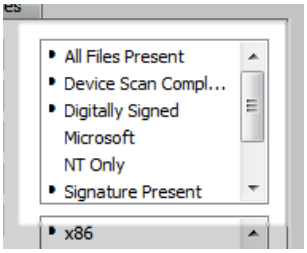
DirectDrivers carries out automatic version control. This will only happen when you need to load a driver for a second time, due to incomplete files for example. The console screen shot below shows two copies of the same Intel Pro Wireless adapter, W29N51. They are both version 9.0.3.9 of the driver itself but DirectDrivers has applied its own version control using the Driver path. This second copy had to be loaded as the first one shows as incomplete.



In the above example there is an extra driver in the drivers window for the selected Intel Pro Wireless adapter; W22N51. This occurs as you are likely over time to build up a library of multiple drivers that support the same device. The operating system will determine which driver to use at the time of installation.

6.1.3.2 Digital Signatures

Drivers can be signed by the vendor by a digital signature. Two attributes show a drivers signature state:



Digitally Signed: The driver was authored with a digital signature

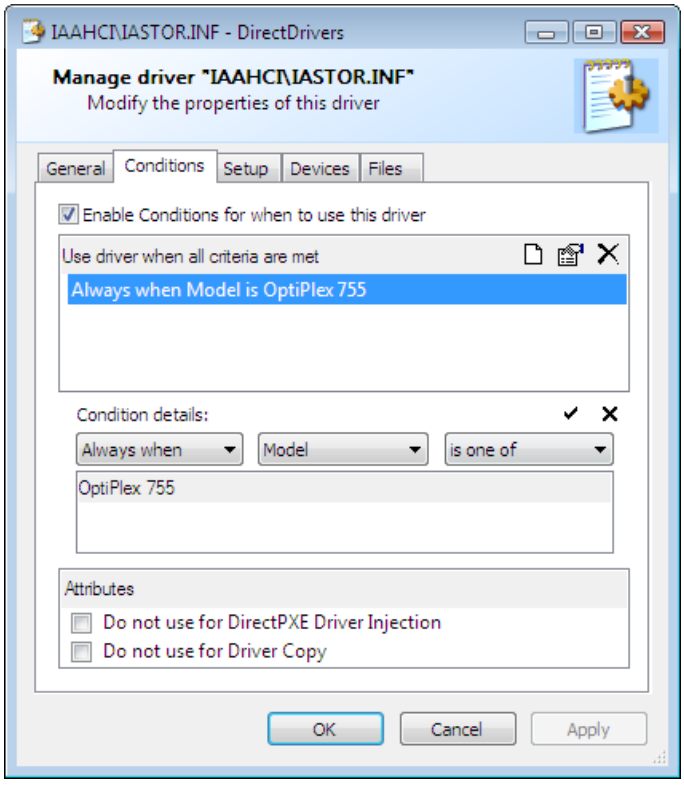
Signature Present: The driver was authored with a digital signature, and the signature is present

Signed Drivers will gain a higher priority when multiple drivers for the same device exist during the Microsoft OS Installation process. Microsoft is encouraging all device driver vendors to sign their drivers, and by default some Operating Systems will only install signed drivers.

6.1.3.3 Using Conditions

Conditions can be used to deliver drivers when the PCI device matching fails. This can be used to support non-PCI devices, by always delivering a driver when a matching hardware model is detected.

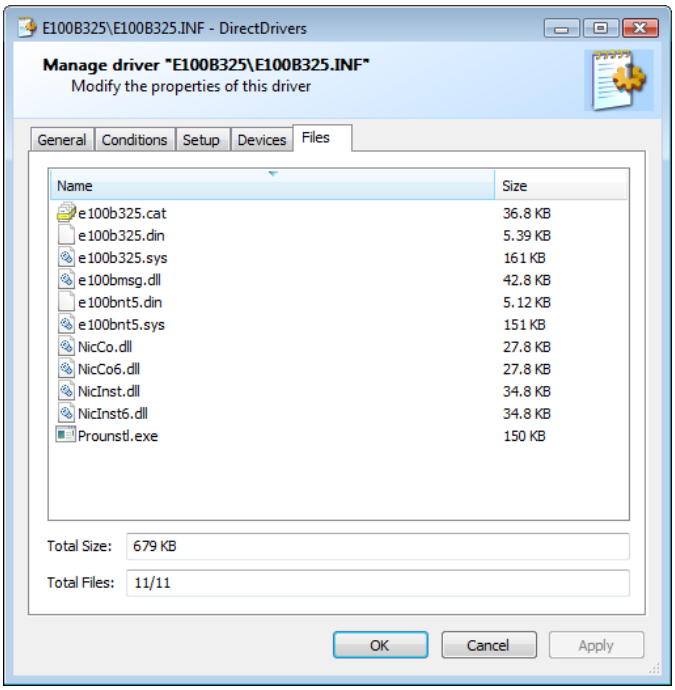
The following steps walk through the process of adding a condition to a driver:



1. Select **'Enable Conditions for when to use this driver'** on the Conditions page.
2. Press new button to open a new Condition details item
3. Change the selection criteria boxes so they read: **'Always when : Model : is one of'**
4. In the window below, insert a new item by selecting **'New'** from the context menu or pressing the Insert button.
5. Press the more button to display available models. This list will show all models that have connected to the DirectDrivers database. Choose a model
6. Press the ok button (tick) to add the condition to this drivers criteria

6.1.3.4 Missing files

For each device you should check that the drivers are marked as “complete”. Any incomplete drivers may work, but one or more files are missing. The dialogue below shows an incomplete Intel Wireless driver W29N51; the w29n51.cat file is missing from the driver database.



The driver properties also show whether a driver is digitally signed, which will increase the chances that the driver will be selected, rather than an unsigned one.

The file with extension .CAT is part of the digital signature. If this file is missing, the driver will be flagged as incomplete and a missing file item will be shown in this dialog.

6.1.3.5 Using DirectEngine Management Console

DirectDrivers can add a Devices page to the Computer Properties window of the Management Console. This page shows all the detected devices for the computer, and whether that device has any matching drivers in the database.

6.1.4 Integration with other Components

The framework nature of UMS means that as well as providing a set of features a component can be integrated with other components. Whilst providing a library of device drivers DirectDrivers also provides integration with other components such as DirectPXE and DirectEngine to allow the drivers to be used as part of tasks and scripts within these other components.

In this section

DirectPXE
DirectEngine

6.1.4.1 DirectPXE

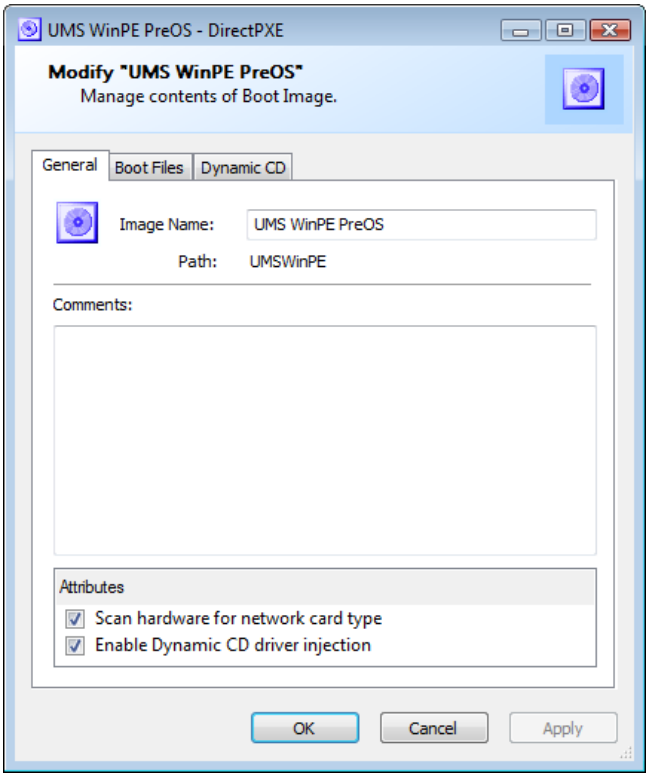
The drivers from DirectDrivers can be used in DirectPXE to dynamically add the correct hardware drivers to a boot image.

Boot Image General Attributes

In order for drivers to be automatically identified and selected the appropriate Boot Image attributes must be enabled in DirectPXE setup. Shown below is the dynamic CD boot image "UMS WinPE 40", General tab.

Scan hardware for network card type must be enabled to allow PXE to return the network card type to Direct Drivers so the correct driver may be selected for injection into WinPE.

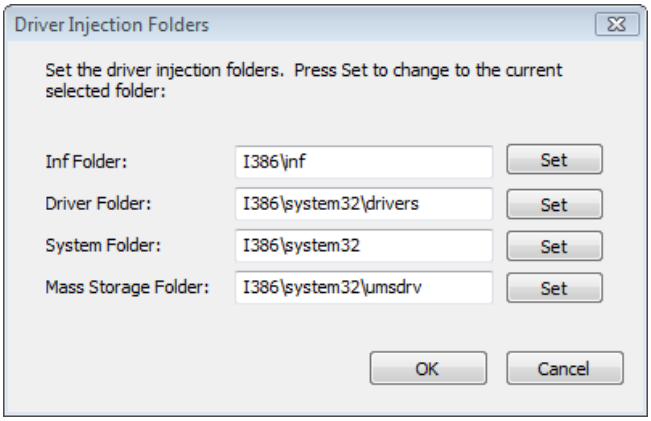
Enable Dynamic CD driver injection must be selected to enable dynamic driver injection from the DirectDriver library into the Dynamic CD.



Boot Image Dynamic CD

For WinPE to work the drivers must be injected into the right location on the Dynamic CD. The available driver injection folders can be shown from the Dynamic CD tab of the WinPE image by pressing the following icon labelled 'Set driver injection folders..."

Click on the icon to open the dialogue shown below.



By pressing set against a Folder the folder location will be set to the current location in the Dynamic CD. This is provided to avoid typing errors when setting the driver locations manually.

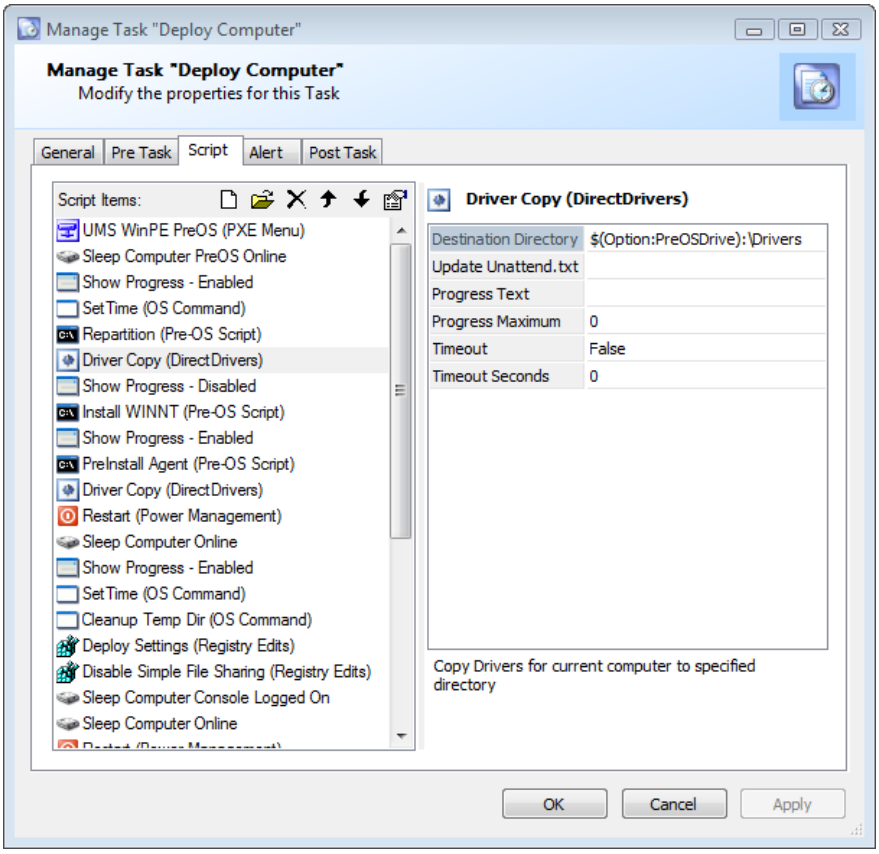
Mass Storage Drivers

When installing an OS which requires mass storage drivers to be added (e.g. computers with SATA hard drives) WinPE will configure the driver so all of the devices supported by the mass storage driver are available. Traditionally the Mass Storage driver file would have required modification to select the specific Mass Storage device needed. This is no longer necessary as DirectPXE handles the required configuration.

6.1.4.2 DirectEngine

To enable drivers to be dynamically added to deployments the DirectDrivers component exposes an add-in script item to DirectEngine setup. The Driver Copy script item specifies where to inject the drivers and also provides the location of the “unattend.txt” or "unattend.xml" file to edit.

The Deploy Computer task below shows how this script is used in a workstation build task.



Parameter	Description
Destination Directory	The subdirectory to copy the detected drivers too. If a second parameter exists (delimited by a comma), Mass Storage drivers will be copied to the appropriate directories, and is assumed to be the root of the System drive.
Update Unattend.txt	If this parameter is omitted, the command will update the Windows Driver search path to the newly copied directories. If this parameter exists, it will modify the Unattend.txt file to search for drivers at the second parameters location

6.2 DirectEngine

DirectEngine is the UMS Component that provides fully integrated desktop management. It has the ability to remotely deploy operating systems and applications to machines within the organisation. Tasks can be built from a variety of industry standard scripting techniques that allows DirectEngine to be customised to perform any management task. Once a new task has been added it can be utilised by all the Direct Engine users.

DirectEngine Setup is the UMS Client Element that stores the configuration of DirectEngine. By separating the setup and management console, the complexity can be hidden from console operators. As with DirectPXE setup DirectEngine Setup is launched from the Tools/Setup menu in the UMS Management Console.

In this section

Types
Setup Components
Collections
Options
Tasks
Roles
General
Advanced Configuration

6.2.1 Types

A Type is a named group of Option values, and whilst there can be many Types defined a computer can only have one Type associated with it. The 'default' Type is selected automatically when the computer is first discovered. A type is therefore used to group a set of computers that have something in common.

The grouping of Options to create a Type leads to the ability to create Types that can meet almost any build requirement. Common types chosen include:-

- Operating Systems (default template)
- Department Names
- Locations
- Hardware types
- Combination of the above

During the definition of a type, or during the development of a build it is often identified that devices will require distinct properties from one another. It is often the need to have more than one distinct property that multiple Types become useful.

Types are also used to control the options which the user may wish to alter (via the Options tab on a Computer properties window).

Versions

A new version of a type can be created by Copying/Pasting a type. The version of the type will be incremented, this is however a text field and can be overwritten with any version number scheme.

6.2.2 Setup Components

Setup Components are typically the script items that are used to create a Task. There are seven different Component types:-

- Binary Files
- Config Files
- OS Command
- OS Script
- Pre OS Script
- Registry Edit
- Registry Query

Components are typically the script items that make up a Task. Binary and Config files however do not fall into this category as they are used to link scripts and command lines to data files. Binary files are copied to the required location so they can be accessed by the required scripts. Registry Queries and Registry Edits read and set registry values on target machines respectively. Each Query or Edit can be used to process multiple registry keys at the same time.

There are four Pre-Defined script items defined internally and are not shown in the Setup Component list. These script items cannot be deleted and are available for use by tasks as required.

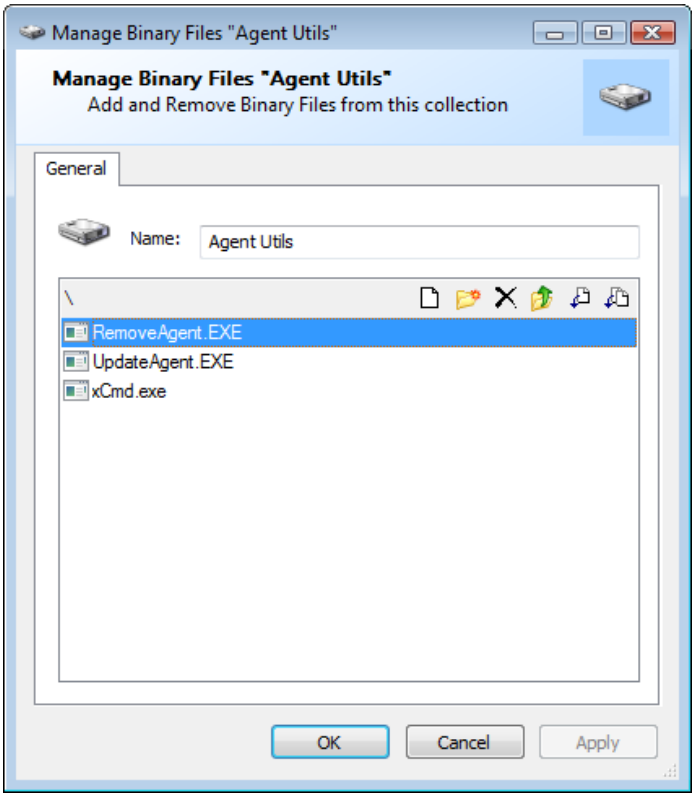
- Event
- Power Management

- Sleep
- Show Progress

6.2.2.1 Binary Files

Binary Files are managed as part of DirectEngine, meaning that all files associated with the desktop management process are stored within DirectEngine. This allows files to be copied to the correct location automatically thereby allowing the administrator to concentrate on the functionality of the process, rather than the logistics of copying files to the correct location.

Binary Files replicate a directory structure, so both folders and files are supported. Files and folders can be copied and referenced in a logical and consistent manner. Files can be downloaded from the server to a location specified by the administrator.



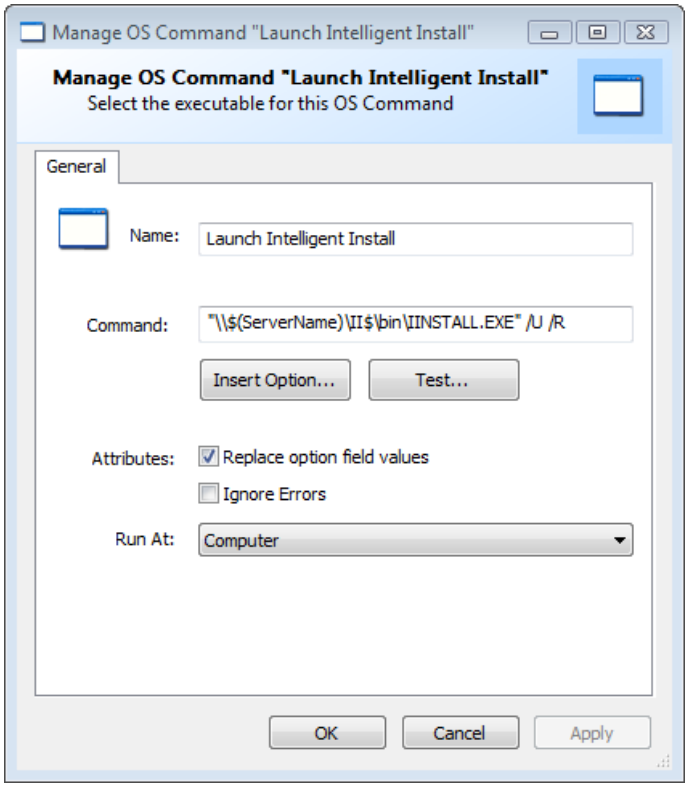
6.2.2.2 Config Files

Config files are typically used to provide text based configuration files to other components within DirectEngine, for example the unattend.txt file for the o/s installation. Config Files support the use of inserting other Option and Component values to provide variable commands and data. If a config file refers to another config file or binary file, those files will be made available when the task is run.

'Replace option field values' searches the text for the Direct Engine options to be replaced at runtime with the matching computer's values. Without this option the text would be used without modification. If you have a large amount of text that contains no option fields, then you would clear this option to increase performance.

6.2.2.3 OS Commands

OS commands like other scripts can be run at the server, the console or computers. OS commands are equivalent to running a command via the run command. Commands run under the system account so do not interact with the currently logged on user (if any).



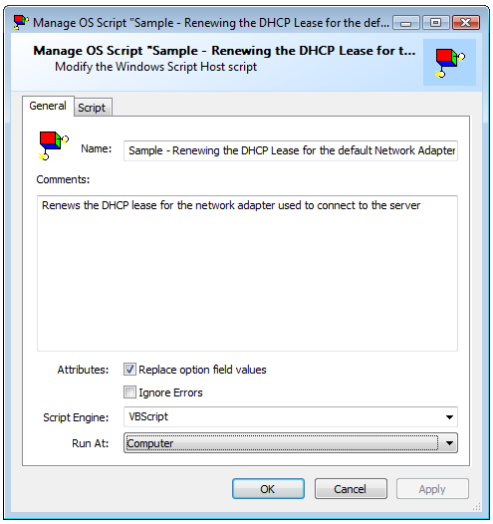
When running OS commands care should be taken that the command will behave in the expected manner on all the targeted operating system variants. OS commands and parameters do vary according to OS and need to be tested carefully.

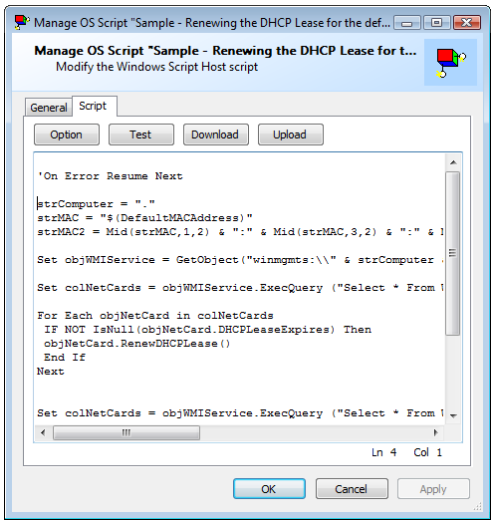
By referencing commands via Binary File Components Direct Engine will ensure that the binary file will be temporarily copied to a suitable location. Built in OS commands should not be copied into a binary Component.

Run At:	Description
Computer	The command will execute at the computer the task is launched against. The task will wait for the computer to be online to launch the task. The task will run under the System context.
Console	The command will execute at the management console computer. This will fail if the task was not launched by a management console (e.g. A scheduled task or an alert task). The task will run under the same context as the management console (typically the user context).
Console, with Computer online	Similar to RunAt Console, but will wait for the task's computer to be online before launching.
Server	The command will execute at the UMS server under the UMS server account.
Server, with Computer online	Similar to RunAt Server, but will wait for the task's computer to be online before launching.

6.2.2.4 OS Scripts

Scripts can be used extensively within Direct Engine to provide management functionality. OS Scripts can use any installed Windows Scripting Host Engine, or the command processor Batch files, selected by the Script Engine type.





The RunAt field functions in the same way as OS Commands RunAt.

Direct Engine takes responsibility for copying the scripts and other reference config files to suitable locations so the script can run.

As long as the **replace option field values** is checked on the general tab then any option values will be replaced by the value it represents. Along with the normal Option Value resolution, Scripts can also be used to set options of a computer.

Script Commands

Any script that writes to the console (@ECHO in a batch file or WScript.Echo in VBScript) can be used to execute script commands. Any text enclosed in <% … %> is parsed for commands by the UMS script engine.

Command	Parameters	Description
Computer	ComputerName:COMP SET Name = Value, PXEGUID:XXX Get Value = Name, SysID:Num Get Value = Name	Retrieves an Option Value from a different computer, or sets an Option Value for a different computer. The remote computer can be referenced by its Name, ID or PXE Guid. A value can either be 'SET' or 'GET'
Delete	Name	Remove an Option 'Name' from a computer
End	Num, Num = Error Text	Inform UMS the script has completed before it has, either returning success (0) or an error code with optional error text
Event	INFORMATION = Text WARNING = Text ERROR = Text	Add an event record for the computer.
Group	ADD = Value REMOVE = Value	ADD a computer to group 'Value', or REMOVE a computer from group 'Value'
Progress	TEXT = Value	Set the progress text or position for the current task

	POS = X,Y SHOW = X,Y,Z	script item. To enable accurate POS setting, the task script item 'Progress Maximum' will need to be increased. Show will turn/off the computers progress dialog: x=0 – disable, 1 – enable y= 1 – none, 2 – image, 3 – prev, 4 – desktop colour, 5 – desktop wallpaper z = image
Set	Name = Value	Set a computers Option 'Name' to 'Value'
Task	Add = Value	Schedule a task to execute against this computer when the current task has finished. Value is the TaskID number.
Trigger	Name	Trigger 'Name', allowing a script to synchronise with a task.
Type	Num	Set a computers type to 'Num', where num is the numeric value of the Types Unique ID

Script Command Examples

Set the current progress text in a Batch file to 'Please Wait…'

```
@Echo "<%% PROGRESS TEXT= Please Wait… %%>"
```

Note: Batch files need a double %%'s to represent a single %

Set the current progress to 75% for a task in a VBScript.

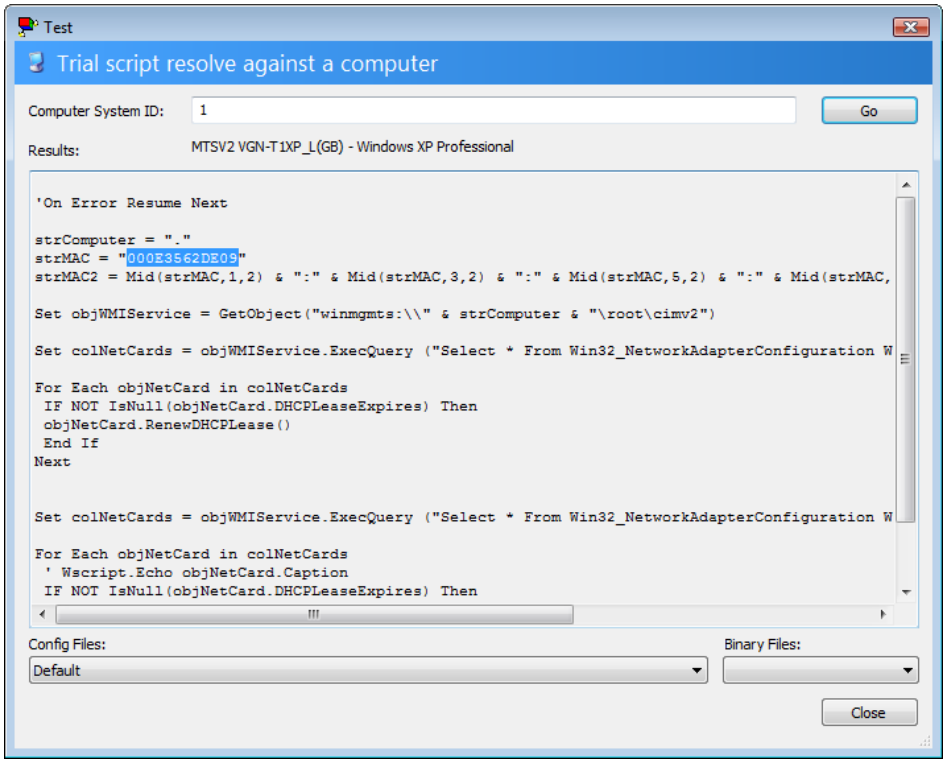
```
Wscript.Echo "<% SET PROGRESS POS = 75, 100 %>"
```

Set the current progress to 75% for a task in a VBScript, using a variable for the current position

```
nPos = 75
Wscript.Echo "<% SET PROGRESS POS = " & nPos & ", 100 %>"
```

Testing OS Scripts

It is possible to see how option values will be replaced by using the Test… button. This does not run the script and therefore no result will be processed, but it does show what the values would be resolved to, and any referenced files that would be made available to the script. In order to do this a Computer System ID needs to be specified for the values to be resolved against. To find a specific computer system ID see the computer properties object tab which is enabled by selecting "Advanced" from the management console view menu. If preferred the system ID column can be added to the management console window. The id is required as option values are always held against a computer.



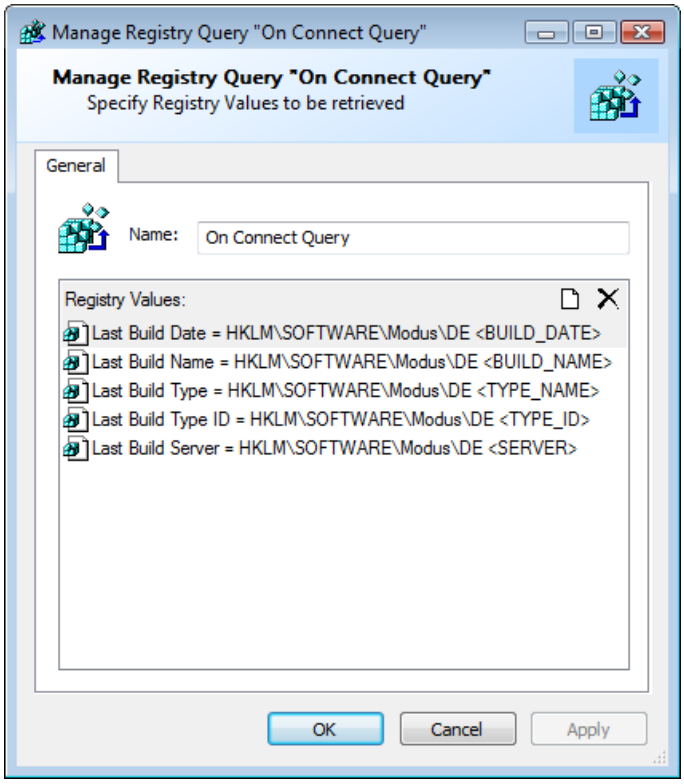
Note: All Option variables are resolved when the script is about to execute. As variables are replaced prior to execution, a variable that is updated by a script cannot be set, and the new value then referenced in the same script. The new value can be referenced by a second script.

6.2.2.5 Pre OS Scripts

Pre OS scripts can be used by either the UMS DOS Pre OS environment, or the UMS WinPE environment. They result in command processor batch files.

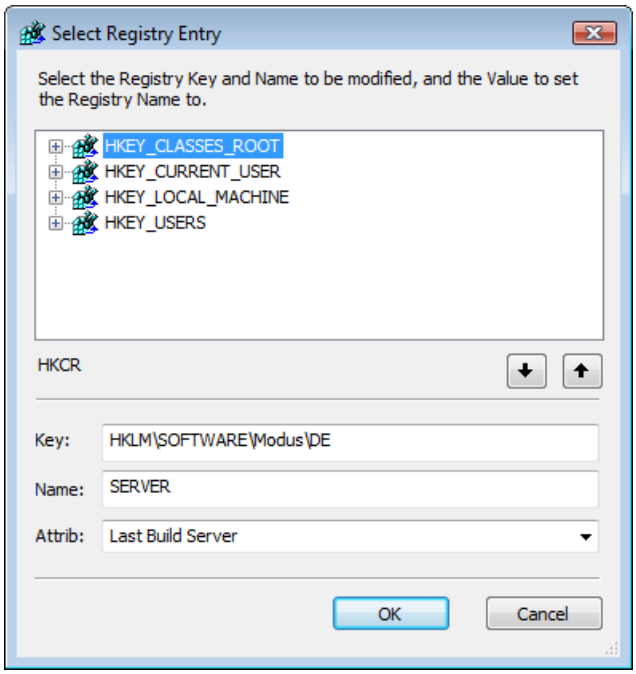
6.2.2.6 Registry

There are two supported registry Components, Query and Edit. Query reads the target registry and saves the value into an Option variable. Edit sets a specific registry key on the target device.

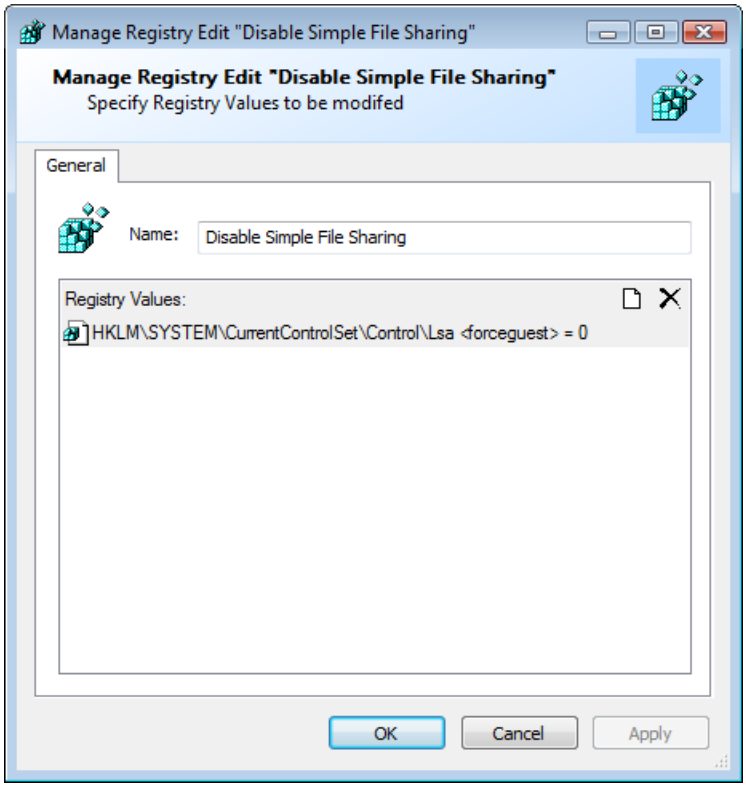


Multiple registry queries can be combined and executed together. If a key is not found then the Option variable is set to NULL (i.e. is empty).

The dialogue shows the selection of a key value from the registry. The local machine's registry is displayed to make the key selection easier; however the key can be typed in manually if required. The up / down buttons can be used to either copy the selected key to the text fields (down arrow button) or locate the key in the registry (up arrow).

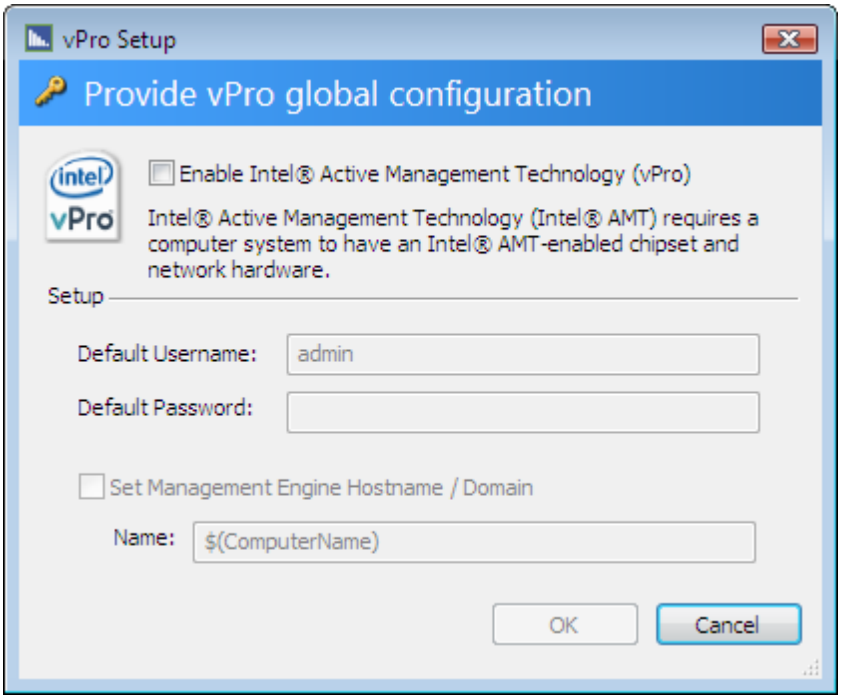


The Attrib: drop down list allows selection of any named option into which the registry value will be copied. This value can be added manually if required, allowing use of an unnamed option.



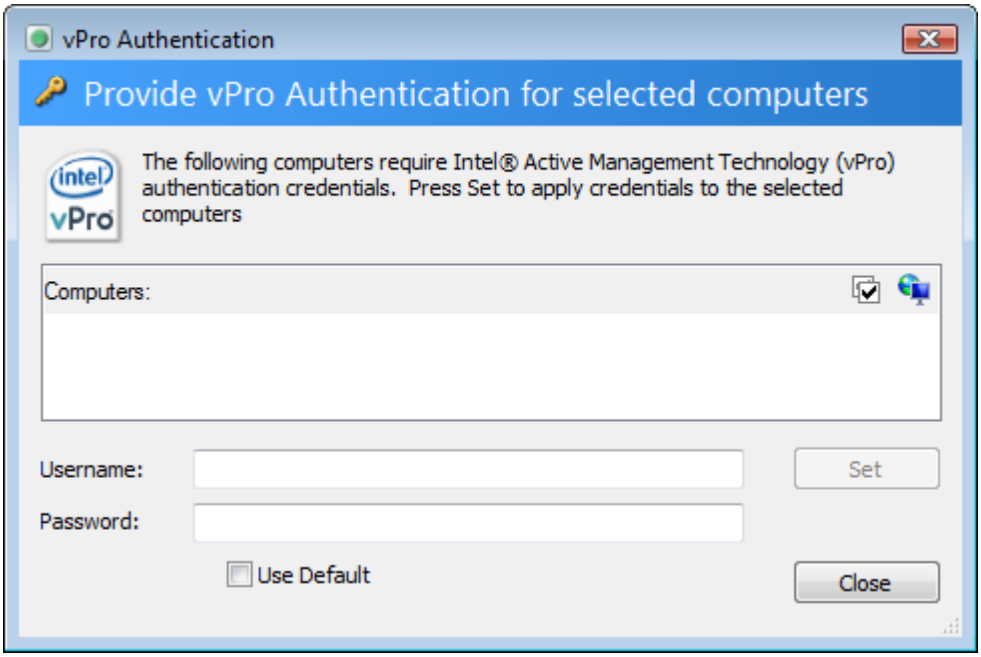
6.2.3 vPro

vPro allows computers to be managed without an Operating System installed or functioning at the computer. If the vPro option is enabled, and authentication is established between a computer and the server, the server will use vPro management to turn on (or wakeup) remote computers. This has the advantage of not relying on broadcast technologies and is more secure as the connection is authenticated.



Enable vPro support and set default connection credentials

A default userid and password can be set. This userid and password will be used to connect to remote computers, unless it is overridden by computer specific credentials entered at the management console.



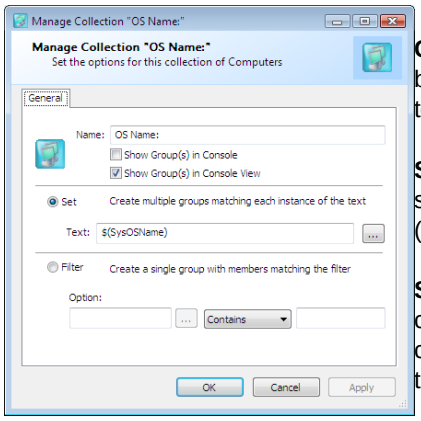
Specific devices can use a different credentials if necessary

When a server connects to the remote management engine, the server can optionally configure the remote hosts name and domain name, using options from the server.

6.2.4 Collections

Collections allow automatic group membership of computers. Used to identify computers which have similar characteristics, collections provide a convenient method of grouping computers. It makes it possible for users to manage devices as a group. The dynamic nature of collections allows scheduled tasks to include only computers which are members of a collection at task execution.

Collections are dynamic in that once defined collection membership is automatically maintained. Change a computers option value and its collection membership is modified appropriately. A user cannot add (or remove) a computer to a collection manually, the membership is determined solely by the collection definition.



Collection Name: Unique name of the collection. The name can be seen in the management console, so should be meaningful to the user.

Show Group(s) in Console: If ticked, allows the collection to be seen when viewing "All Items" in management console. *Default* (un-ticked) is not to show groups in Console.

Show Group(s) in Console View: when ticked allows the console user to view collection membership by selecting collection name from the view drop down list. If un-ticked then the collection membership cannot be viewed. *Default* is ticked.

Collection types

Collections come in two forms, either Set or Filter based.

Set: Creates a group for each unique value of the set definition. When a new value is set, a corresponding collection is created. When the collection has no members, the collection is automatically removed.

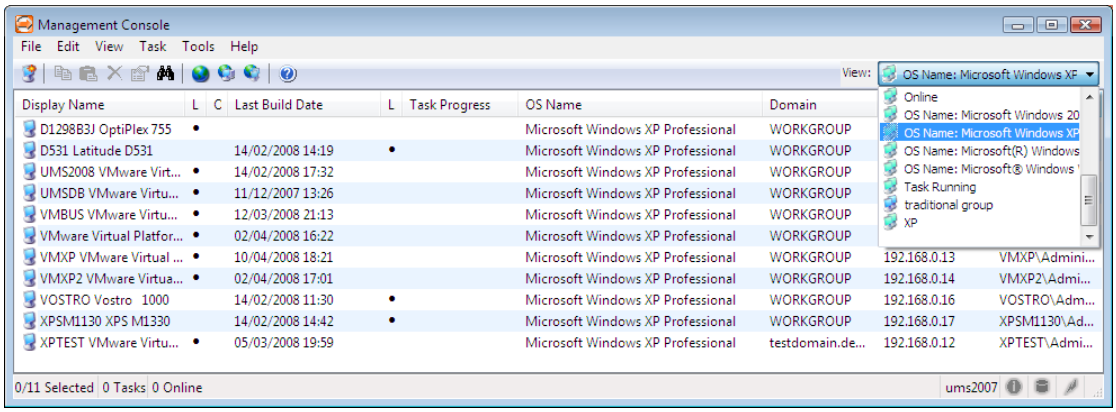
Example: We want a series of collections, one for each operating system installed. Create a set based on the pre-defined Option “OS Name” and a group will be created for each operating system.

Filter: Creates a single group and membership is determined by checking the filter, which is based on an Option. The filter provides parameters for testing the contents of an Option to restrict the collection membership. The collection always exists, even if the collection has no members.

Example: We want a collection to show us all the computers which have Windows XP installed. Create a filter collection based on predefined option “OS Name”, and set the parameters to check that it contains the text XP. This will create a single collection, where any computer with an installed OS containing XP will be included.

Collection Names in Management Console

Set Collections are always pre-fixed with the name of the collection, so that they can be identified (and grouped together) in the management console view. A filter collection is identified by its Name.



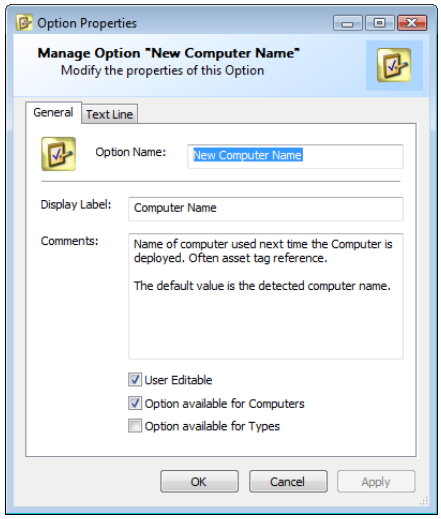
To manage groups of computers manually without dynamic membership, use “Computer Groups” which provide a simple method for grouping computers. Computer Groups are static and membership is manually maintained.

6.2.5 Options

Options hold individual values which are used throughout Direct Engine. The Options displayed in the console are defined as ‘User Defined Options’. When Options are deleted, any Option values stored for a Computer remain in the database. These Options then become classed as Unnamed Options. Options values can be set by types, option defaults, computer properties or scripts.

The following shows what is possible, using the 'New Computer Name' option as a guide.

General



Option Name is the name by which the Option is known within the system. It is possible to set the Display Label as different to that of the Option Name. This can be useful for the administrator in certain situations where using the Option Name would be confusing to the user.

If the Option is not **User Editable**, then the user may be able to see the Option, if it is entered in the appropriate type, but the user will not be able to amend the value.

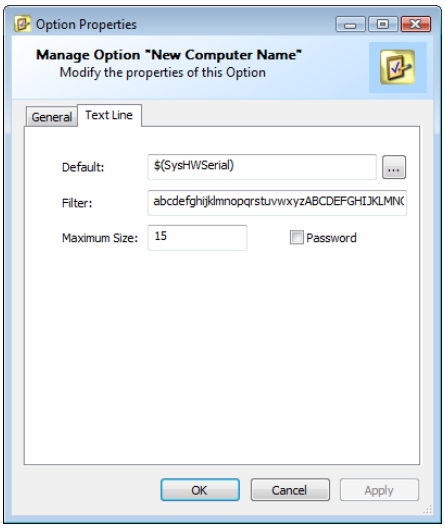
If the **Option available for Computers** checkbox is ticked then the Option will be available to Users within Computer Properties in the Management Console. If an Option is to be used internally, having this box un-ticked will ensure that the Option is not displayed in the Management Console.

Option available for Types indicates if a defined Type can set a default value for the given option.

Option available for Tasks allows the option to be assigned to a task, and have the value set when a task is scheduled.

There are a number of predefined system options which are always available. Predefined options are not listed in the Options tab in the setup window. They are available to scripts and can be accessed by using the select options dialog. Predefined options include many computer specific entries, date and time values in various formats and the server currently connected. The predefined options are detailed in the Advanced Configuration topic.

Text Line



The **Default** field determines the default value used for this Option if an actual value has not been recorded previously. Using the More Options button [...] allows another Option to be used as the Default Option Value (Recursive Resolution).

The **Filter** determines the valid set of characters available for the option. Characters are case sensitive so the 'a' and 'A' would be needed to allow both upper and lower case character sets. A blank filter indicates that any character is allowed.

Maximum Size limits the size of the option value.

If the **Password** box is checked then the console user will only see a password field (i.e. * characters rather than the actual characters) in place of the data value.

If the Option is user editable then the user may still alter the password as necessary.

6.2.6 Tasks

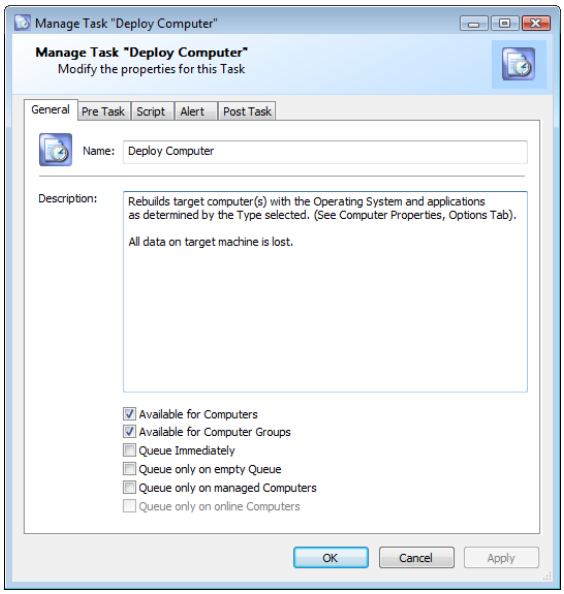
Tasks are formed of one or more Components and can be run by users of the management console. Tasks can run against one or more computers, or a group. Tasks which are submitted against Computer Groups are resolved to individual computers when the task is executed.

If a task has no valid computers to run against, the task will fail with an appropriate error message.

Task Properties

General Tab

It is recommended that a suitable description is entered as this text can be viewed by Users and helps them decide if the task is the correct one for the procedure they need to complete.



Use the **Available for Computers** and **Available for Computer Groups** to set whether a task is available to computers, computer groups, or both. Many tasks are available for both computers and computer groups although some tasks are inappropriate for computer groups (remote takeover for example).

Queue Immediately instructs the scheduler to run the task immediately without confirming the scheduled execution time.

Queue only on Empty Queue only allows the task to run if no other task is currently executing. Only one task can ever execute at a time for a given computer, so this option restricts a task from being scheduled if it is inappropriate to wait for the currently executing task to complete first.

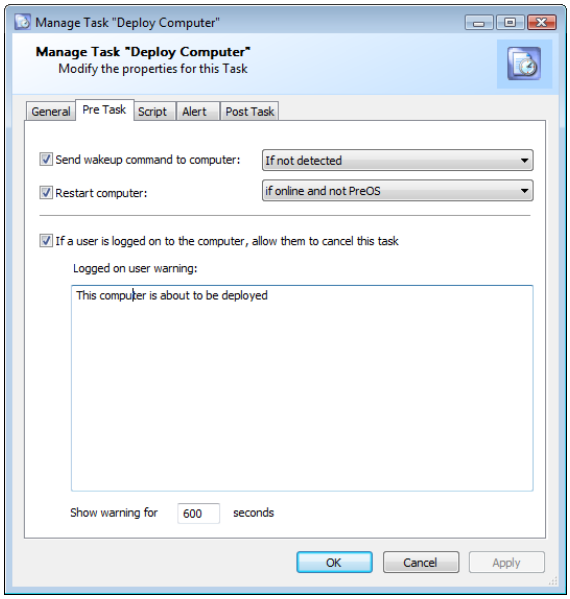
Queue only on managed Computers will only allow a task to run on a machine which has the Agent installed on it (i.e. Managed). If selected, this can be further defined to include only machines which are currently online. Some tasks would fail if the machine is not already managed and online so it provides mechanism where tasks cannot be submitted on computers which would never succeed in their currently known configuration.

Options tab

Add options on this tab to allow option values to be entered when the task is scheduled.

Pre Task tab

Pre task options are processed at the time the task is scheduled to start running.



You can select whether you want to **Send wakeup command to computer** based on its current state. This is not guaranteed to work as several other factors must be taken into consideration, including the power management settings in the BIOS the destination computer having to be configured to Wakeup on LAN.

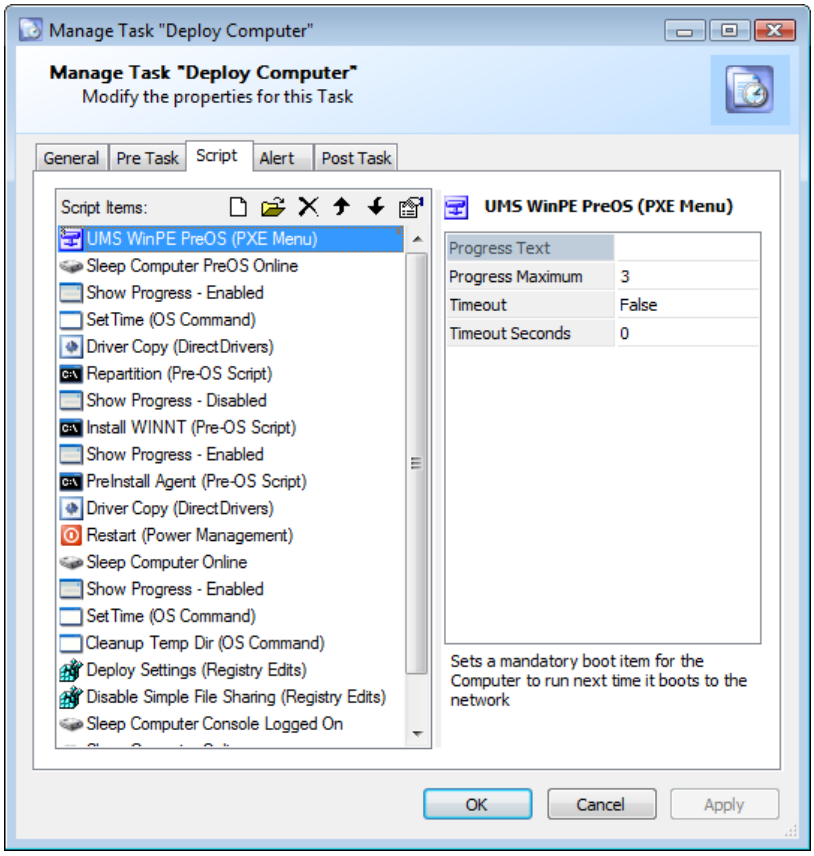
Selecting **Restart computer** if currently online will ensure a reboot prior to the task running if required. This is normally linked with the fact that the task will be initiated from a PXE boot as the machine restarts.

As a task can be executed whilst a user is logged on to the target computer you can select **If a user is logged on to the computer, allow them to cancel this task** to show the user a warning and allow them to cancel the tasks if you wish. This option is only available to managed computers, which are online. Where the computer is not online, the warning is not displayed.

Script tab

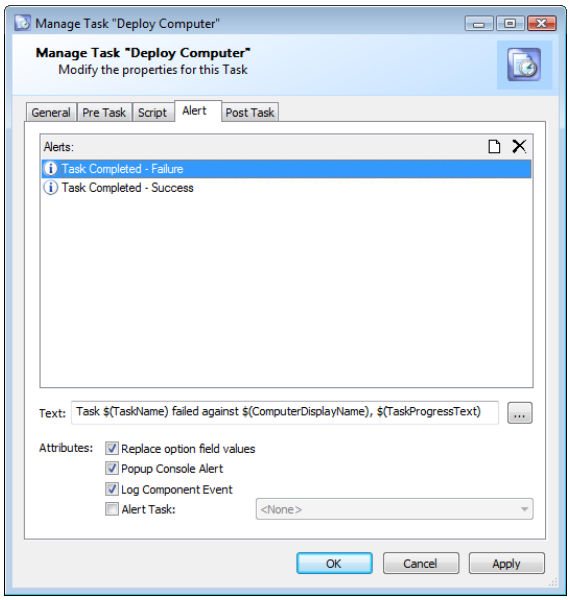
Task scripts can vary in their complexity and length. The Scripts are executed in the order the items appear in the list. Each list item has its own set of parameters available which vary according to the type item. See Appendix F - Task Script Properties on page 78 for descriptions of the Script Item properties.

Script Items are either Pre-Defined, provided by other UMS Components, or are defined in the Setup Components.



Alert tab

Tasks Alerts are used to report information on the status of tasks back to the users of the management console.



Task alerts provide feedback to the console depending on the outcome of tasks. By selecting the appropriate alert mechanism, valuable feedback can be provided to the console user. The text that is reported can include option variables to improve the alert meaning.

Select **Popup Console Alert** to have the report displayed by the Client. Selective console alerts provide useful feedback to the console user, without overloading them with

Select **Log Component Event** to have a report written to the event log of the server. Note:- In order to ensure the event is written to the server event log, the UMS server component event logging option, needs to have be enabled, which can be set from the UMS server Admin property pages.

Select **Alert Task:** to run another task on the alert. Whenever the alert is triggered, another task can be immediately scheduled to run. For example if a task failed, then a diagnostic task

can be scheduled to run automatically.

Post Task tab

Tasks can have a maximum timeout period set, after which time if the job has not yet completed the job will fail with a timeout error.

For tasks which are run repetitively, an execution purge can be scheduled which can remove the task from the database after a specified time. This can be useful, especially for frequently run tasks which after they have run, hold no useful information.

6.2.6.1 Pre Defined Script Items

Four Pre-Defined Script Items are available for use in tasks:

- Event
- Power Management
- Sleep
- Show Progress

Event

This script item will record an event against the computer.

Power Management

This script item enables the inclusion of power management features of the operating system to managed devices.

Command	Description
Wakeup	Issues wake on LAN (WOL) to be sent to device
Restart	Reboots the computer. If the computer is not online, script will continue. Will wait for computer to go offline before continuing.
Shutdown	Reboots the computer. If the computer is not online, script will continue. Will wait for computer to go offline before continuing.
Suspend	Suspend the computer. If the computer is not online, script will continue. Will wait for computer to go offline before continuing.
Hibernate	Hibernate the computer if supported. If the computer is not online, script will continue. Will wait for computer to go offline before continuing.
Logoff	Logoff the console user
Lock	Lock the console users session
Display On	Turn on the monitor
Display Off	Turn off the monitor

Sleep Component

The Sleep item allows the script to be suspended for a specified duration or until a specific event has occurred. The table below details the events that are valid for the Sleep item.

Command	Description
Trigger	Wait for the custom trigger specified by Param field.

Hours	Wait for Param hours
Minutes	Wait for Param minutes
Seconds	Wait for Param seconds
Console Logged On	Wait for anyone to be logged onto the computers console
Console Logged Off	Wait for no-one to be logged onto the computers console
Computer Online	Wait for the UMS agent to connect to the server
Computer Offline	Wait for the UMS agent to disconnect from the server
PreOS Online	Wait for the PreOS agent to connect to the server
Computer Responding	Wait for the computer to respond to an ICMP ping. Ping request is sent every 2 minutes +/- 20 sec random value. Each ping will wait up to 2 seconds for a response.
Computer Not Responding	Opposite to Computer Responding
Attribute Not Empty	Wait for the computers Param attribute to contain a value. This value can be populated by a script executing against another computer, using the COMPUTER SET command
Attribute Empty	Wait for the computers Param attribute to contain no value. This value can be removed by a script executing against another computer, using the COMPUTER SET command

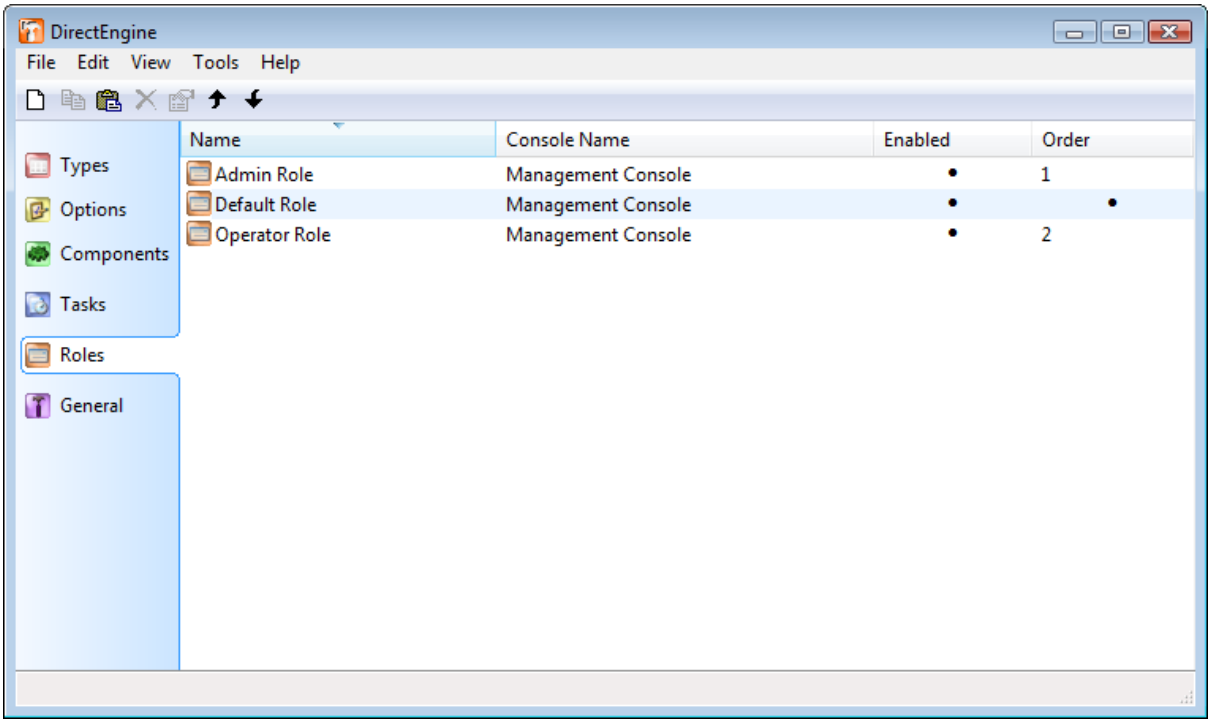
Show Progress

Show Progress component enables the task progress to be shown on the target device. Parameter settings determine the background displayed to the user.

6.2.7 Roles

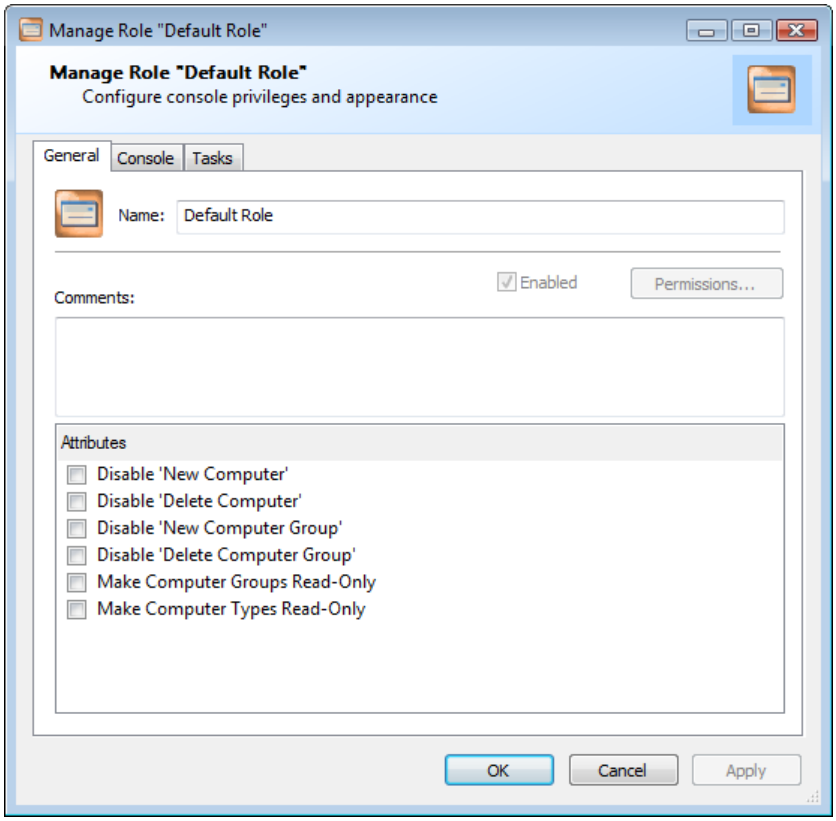
Roles allow the administrator to control the features available to differing groups of management console users.

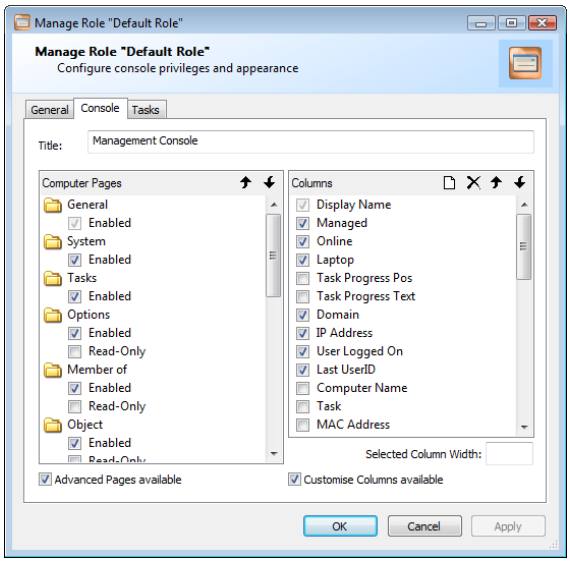
Access to the management console Component itself is controlled via the UMSAdmin program. Roles control the features of the management console available.



The default role is always available and cannot be deleted. All users have access to this role, so no permissions can be set to restrict access to it. Roles are only active once they have been enabled. When a user logs on to the client the role is selected by finding the first role to which the user has permission to use in descending numerical order. The default role is chosen if the user has no other valid role available.

Role Properties





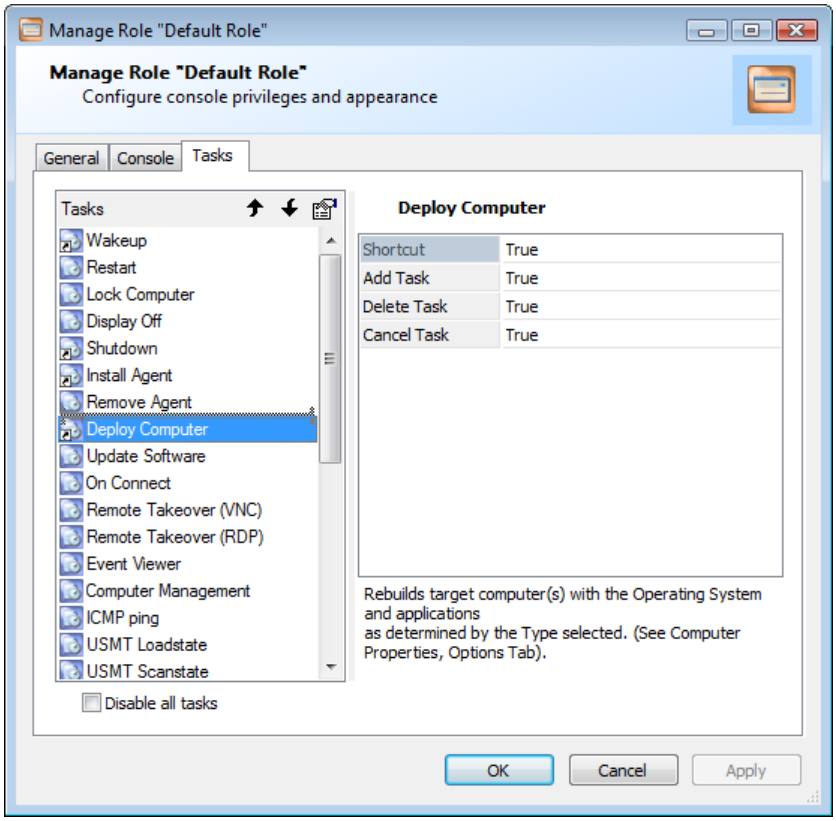
The console **Title** can be altered for each role as required. Different roles can share the same console title if required.

The console property page is used to control the data the given user has access to. The computer pages listbox allows both the choice of which pages are visible and which order they should be displayed in. Any available Direct Engine Add In Components are also included in this list.

Columns defines both which columns are displayed in the management console and the order of the columns. Columns also determines which columns can be selected by the user if they are allowed to customise the management console interface.

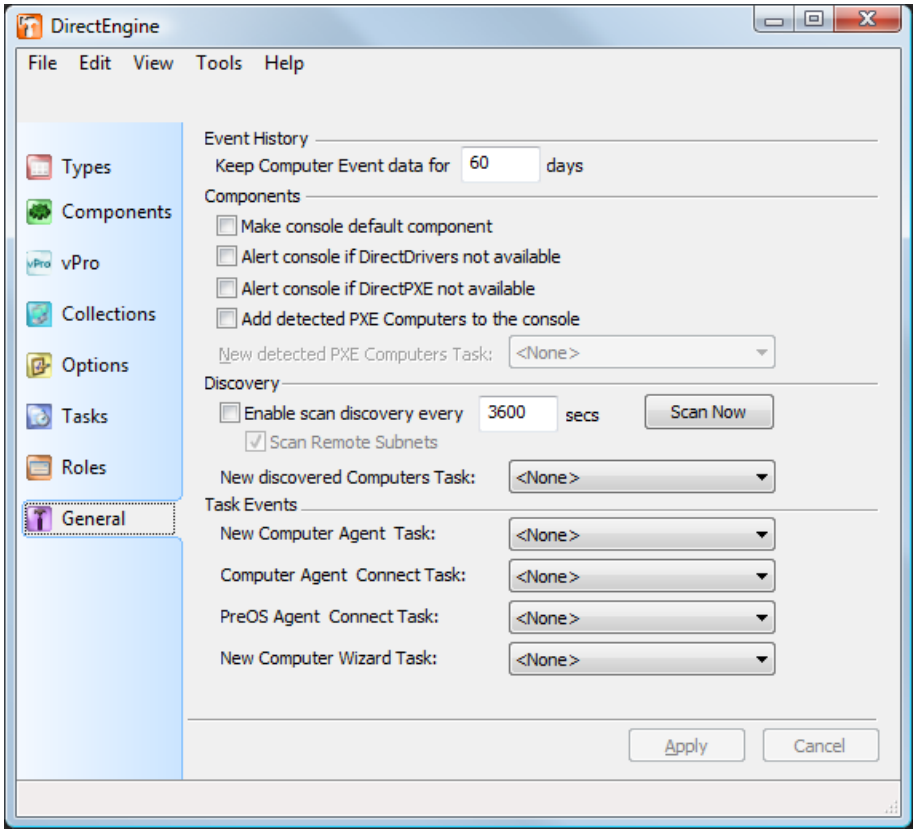
The advance pages checkbox determines whether the user can view the advanced object property pages for computers, computer groups and task schedules.

This Task tab allows control over tasks, both which tasks are available and which tasks can be submitted via the users shortcut menu.



6.2.8 General

The General tab provides general Direct Engine setup information. When making changes to the general settings, any changes need to be applied using the "Apply" button before they take effect



Event History

Events older than the specified number of days will be erased.

Components

Select **Make console default component** to make the Management Console load automatically after Client login. If this is de-selected the Client will present a list of available components to run.

You can select to be notified if DirectDrivers and/or DirectPXE are available.

You can select whether or not to automatically add Computers to the console when they first perform a PXE boot.

Event: You can set a Task to run when a new computer is detected from a PXE Boot.

Discovery

Select **Enable scan discovery** to allow the server to actively discover all computers on the network and add them to the console. You can also set a frequency this is repeated. If it is enabled you can also select **Scan Remote Subnets**. This feature uses Agents on remote subnets to proxy the scan on behalf of the server. This can only be performed only when a UMS Agent is installed on at least one computer on the remote subnet.

To scan manually use the Scan Now button.

Event: You can set a Task to run when a new computer is detected from a network scan.

Note: Scanning uses the NetBIOS protocol to detect computers. If a firewall is enabled on the computers, they may not be detected.

Events

Other tasks that can be launched when the following events occur:

Event	Description
New Computer Agent	This task is launched when a new computer is detected when the agent connects to the server for the first time.
Computer Agent Connect	A task is launched every time the agent connects to the server
PreOS Agent Connect	This task is launched when a new computer is detected when the agent connects to the server for the first time, from the WinPE PreOS environment
New Computer Wizard	This task is launched when a computer is added from the Add Computer Wizard

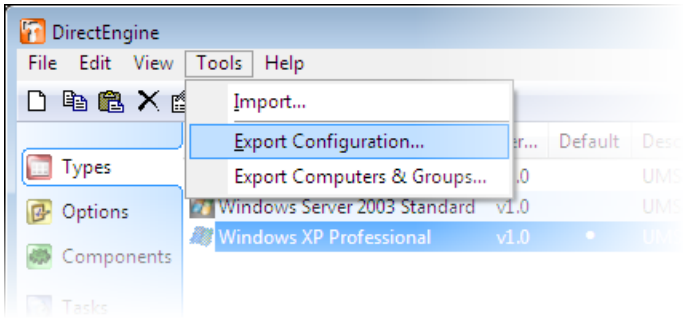
.

6.2.9 Advanced Configuration

6.2.9.1 Setup Import and Export

UMSprovides features to import and export its configuration. All or part of the configuration can be exported, as XML scripts which can be used to build servers.

This import/export wizards are accessed from the Tools menu:



Both the import and export wizards allow all or part of the configuration to be extracted. This allows scripts to be built that extend the configuration of the system.

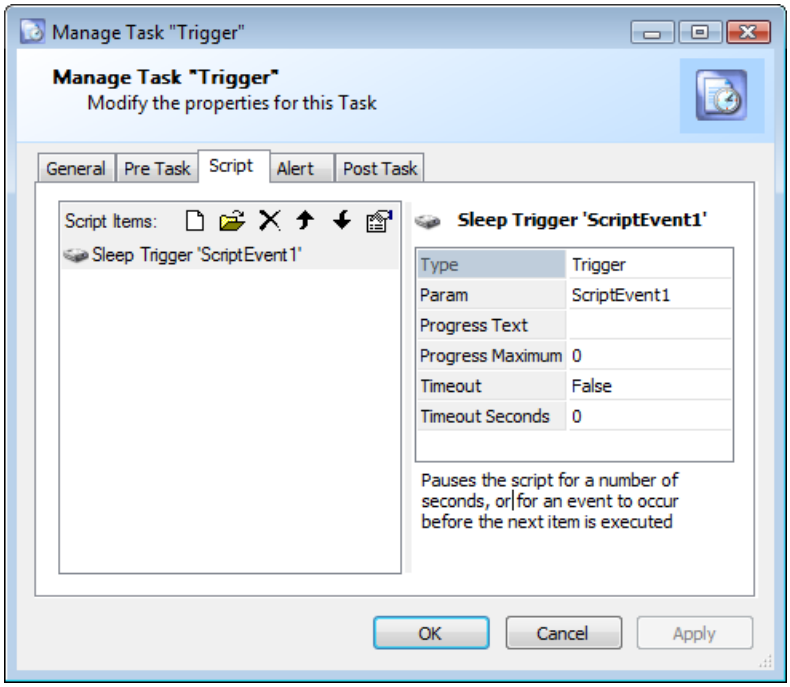
6.2.9.2 Script Triggers

Script triggers provide a method for synchronising UMS Tasks with external processes. A script author can specify that the UMS task pauses until a named event is triggered.

For a computer to successfully send a script trigger, the UMS Agent must already be connected to the server. It is then triggered as follows, be executing the agent with the trigger command line parameter as follows:

```
UMSAgent.exe /trigger:ScriptEvent1
```

The task would then have a matching Sleep event:



6.2.9.3 Pre-Defined Options

Name	Macro	Global	Description
AD OU	SysADOU		If a member of Active Directory, this option returns the OU that contains the computer.
AD OU Fully Qualified DN	SysADOUFQDN		If a member of Active Directory, this option returns the OU in FQDN format that contains the computer.
AD Site	SysADSite		If the computer is a member of Active Directory, this option will return the AD Site Name
Alert Status	SysAlertStatus		This value contains a numeric field. 0 indicates normal, 4 indicates warning, and 5 indicates error.
Comments	ComputerComments		The contents of a computers comments field
Computer Name	ComputerName		Current computer name
Current Date	DateCurrent	•	The current date, formatted using the servers current regional settings
Current Date As Name	DateCurrentAsName	•	The current date in reverse with no formatting, example: 20060328
Current Date As Number	DateCurrentAsNumber	•	The current date and time in seconds since midnight (00:00:00), January 1, 1970, coordinated universal time (UTC).
Current Time	TimeCurrent	•	The current time, formatted using the servers current regional settings
Date First	DateFirstDetected		The date the computer object was created,

Detected			formatted using the servers current regional settings
Date Last Detected	DateLastDetected		The date the computer was last updated by the computer, formatted using the servers current regional settings
Display Name	ComputerDisplay Name		A combination of 'Computer Name', 'Hardware Model' and 'MAC Address' – depending on information available
Domain	SysDomainName		The name of the Domain or Workgroup the computer belongs to
Hardware Model	SysHWModel		The computers BIOS model
Hardware Serial Number	SysHWSerial		The computers BIOS serial number
Hardware Server	SysHWServer		The computers OS is a Server edition
Hardware Vendor	SysHWVendor		The computers BIOS manufacturer
Hardware Virtual	SysHWVirtual		The computers hardware is running under VMWare or Virtual PC
Hardware vPro	SysHWvPro		If vPro is detected on the computer, this value is set to 1.
Hardware vPro Version	SysHWvProVersion		The detected version of vPro at the computer
IP Address	DefaultIPAddress		The IP Address of the network card connected to the UMS server
IP Gateway	DefaultIPGateway		The IP Gateway Address of the network card connected to the UMS server
IP Subnet	DefaultIPSubnet		The IP Subnet of the network card connected to the UMS server, in the form: X.X.X.X/Y
IP Subnet Mask	DefaultIPSubnetMask		The subnet mask of the network card connected to the UMS server
Laptop	SysHWLaptop		If the computer is a laptop this value will be set to 1.
Last UserID	SysLastUserID		The Domain and UserID of the last logged on user at the computer in the format DOMAIN\UserID
License	SysLicenseActive		If the connected computer has an active license, the value will be set to 1.
MAC Address	DefaultMACAddress		The MAC Address of the network card connected to the UMS server
Managed	ComputerManaged		If the Agent has connected to the server at least once, value will be set to 1.
Online	ComputerOnline		If the Agent (normal or PreOS) is currently connected to the server, value will be set to 1.
OS CSD Version	SysOSCSDVersion		The Operating System service pack level
OS Install Date	SysOSInstallDate		The Date the Operating System reports the system was installed
OS Name	SysOSName		The Operating System name
OS Time Zone Name	SysOSTimeZone Name		The current OS Time Zone name

Pre OS	SysPreOS		If the Agent is currently connected to the server in PreOS, value will be set to 1.
Preboot Password	PreBootPassword	•	Binary files held in DirectSetup components are access from the PreOS environment through a share on the server. This value represents the current password required to connect to the share
PXE Guid	PXEGUID		The computers BIOS unique GUID
Server	SysHWServer		The Operating System is a Server
Server FQDN	ServerFQDN	•	The full DNS name of the UMS server (Fully Qualified Domain Name)
Server IP Address	ServerIPAddress		The IP address of the UMS server as seen by the UMS Agent when it is connected to the server. If a computer is not connected, this value is empty.
Server Name	ServerName	•	The computer name of the UMS server
System ID	SysID		The unique number allocated to a computer by DirectEngine
Task	ComputerTask		If a task is currently executing against this computer, value will be set to 1.
Task Author	TaskAuthor		The User name of the account that submitted the task through the management console.
Task Comments	TaskComments		The currently executing tasks comments field
Task Execute ID	TaskExecutionID		Each instance of a task has a unique number per computer allocated
Task ID	TaskID		The currently executing tasks comments System ID
Task Name	TaskName		The currently executing tasks name
Task Progress Pos	TaskProgressPos		The percentage of the overall task progress
Task Progress Text	TaskProgressText		The current displayed progress text
Time First Detected	TimeFirstDetected		The time the computer object was created, formatted using the servers current regional settings
Time Last Detected	TimeLastDetected		The time the computer object was last detected, formatted using the servers current regional settings
Type Comments	TypeComments		A computers select type's comments field
Type ID	TypeID		A computers select type's unique ID
Type Name	TypeName		A computers select type's name
User Logged ON	SysUserLoggedOn		If a user is currently logged onto the console of this computer, value will be set to 1.
User Name	SysUserName		The UserID of the currently logged on user

6.2.9.4 Option Value Resolution

DirectEngine Options are values that can be used by tasks or displayed in the Management Console.

Five types of option are available:

- **User Defined:** A user defined option can be modified and displayed in the Computers “Options” tab. User defined options can be display as:

  - Checkbox
  - Single Text line
  - Drop down list box

- **Config files:** Reference to Config text file within DirectEngine Components. These values are global.
- **Binary files:** Reference to Binary file or folder within DirectEngine Components. These values are global.
- **Add-Ins**: Other UMS components can make Options available, that maybe specific to the computer the task script is executing, or the selected computer in the management console.
- **Pre-Defined:** The UMS server provides a list of useful global values

User Defined Option Values

The User Defined Option values can be set by (in order of precedence):

- **Type Value:** An option must be assigned to a type to have its value modified, either by the type or by a specific computer value. Setting an option to a specific value for a type is set in DirectSetup / Types page, and the option must have “Option available for Types” set.
- **Computer Value:** Once an option value has been assigned to a type, and that option value is has “Option available for Computers”, and that computer is set to the assigned type, the option will appear in the Computers “Options” tab. The value will be modifiable if “User Editable” is set for the option.
- **Default Value:** When an option is defined and it is not modified by any other part of the system, the default value is used. The default value is set in DirectSetup / Options page.
- **Task script output:** When a task is launched, the values for each option are resolved. A Computer can have a specific value set to an option by a task script, overwriting any previous value.

Scripts can store option values against a computer without the option being declared in DirectSetup. To view the current complete list of options assigned to a computer, enable “View Advanced” pages and select the “Object” tab of a computer. Non declared values cannot have default or type based values.

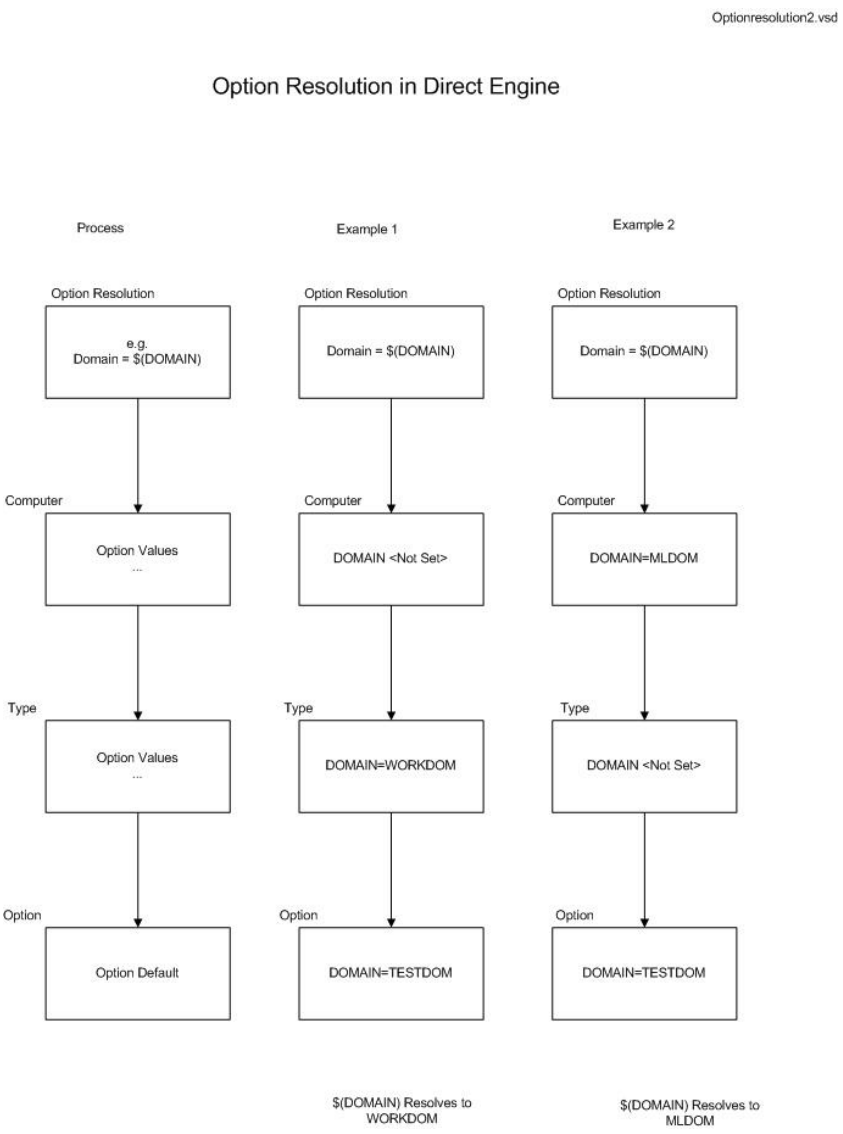
If a macro points to a value that does not exist, it will be resolved to ”<Error>”.

Recursive Option Value resolution

The value of a user defined option can resolve to another value. Circular resolution will be detected and result in the option value being `”<Recursion Error>”.`

If the value of an option resolves to an option name that does not exists, the option value will be `”<Error>”.`

The following diagram illustrates resolution examples:



6.2.9.5 Task Script Properties

Each type of script item in a Task has different properties available. The following table details the options available.

	Pre OS Script	OS Script	OS Command	Registry Edit	Registry Query	PXE Menu	Event	Power Management	Sleep	Show Progress
Progress Text	✓	✓	✓	✓	✓	✓		✓	✓	
Progress Maximum		✓	✓			✓			✓	

Timeout	✓	✓	✓	✓	✓	✓		✓	✓	
Timeout Seconds	✓	✓	✓	✓	✓	✓		✓	✓	
Type							✓	✓	✓	
Force								✓		
Wait for Script to complete		✓	✓							
Script timeout		✓	✓							
Param		✓							✓	
Description							✓			
Enabled										✓
Background										✓
Image										✓

Progress Text

The progress text is shown on the general tab of the computer properties window, and is also an available column on the Management Console. By default the Progress Text is the name of the script item.

Progress Maximum

Allows the task author to weight the script item, so the overall task progress more accurately reflects the time each script item takes. By default each script item has an equal weighting of 1.

Timeout

(Enabled/Disabled) Determines if the script step has a timeout value associated with it after which the task will fail. Timeout is defined in Timeout seconds.

Timeout Seconds

If timeout has been set to 'enabled' you can set the timeout in seconds. The timeout is the number of seconds during which the step has been active. If the step does not complete before the timeout, then the task fails.

Type

The Power Management Script Item is an internal one and has its own subset of types.

Power Management Types:

- Wakeup
- Restart
- Shutdown
- Suspend
- Hibernate
- Logoff
- Lock
- Display On
- Display Off

Sleep Script Item has its own list of specialised Types:

- Trigger
- Hours
- Minutes
- Seconds
- Console Logged On
- Console Logged Off

- Computer Online
- Computer Offline
- PreOS Online
- Computer Responding
- Computer Not Responding
- Attribute Not Empty
- Attribute Empty

Param
Used by the OS Script command and Sleep script item in order to set parameter values.
For the OS Script command it is used to pass command line string. Enables same script to be reused by using parameter input.
Sleep Item uses Param setting to name the 'Trigger' or Attribute name.

Description
Used by the Event script item to set text displayed for an event.

Force
Used solely by the power management script item, If enabled forces processes to close, otherwise simply instructs processes to terminate.

Wait for Script to complete
When this is set to true the next script item can not be executed until the current item has completed without error?

Script Timeout
Sets the maximum time in seconds for which the script can run. This timeout differs from the more general timeout, as it limits the time the script is allowed to run for, but does not include any time prior to the script starting.

Enabled
Show progress only parameter which controls whether the task progress is shown on the target device.

Background
Show progress script item parameter which is used to control what background is shown on the device running the script. Valid options are:- None, Image, Previous Setting, Desktop Colour and Desktop Wallpaper.

Image
Show progress script only item parameter. Image file of image to show on desktop. Only used if 'Image' is selected as background type.

6.3 DirectPXE

DirectPXE runs as a Component of UMS, and is a fully compliant PXE and TFTP server, which can co-exist with other PXE and DHCP Servers. The Server has the capability to deliver multiple PXE menus, depending on setup and device. The server provides responses to client PXE requests from computers on the network, and the response can be varied from no response, through to providing a default menu, or a custom menu.

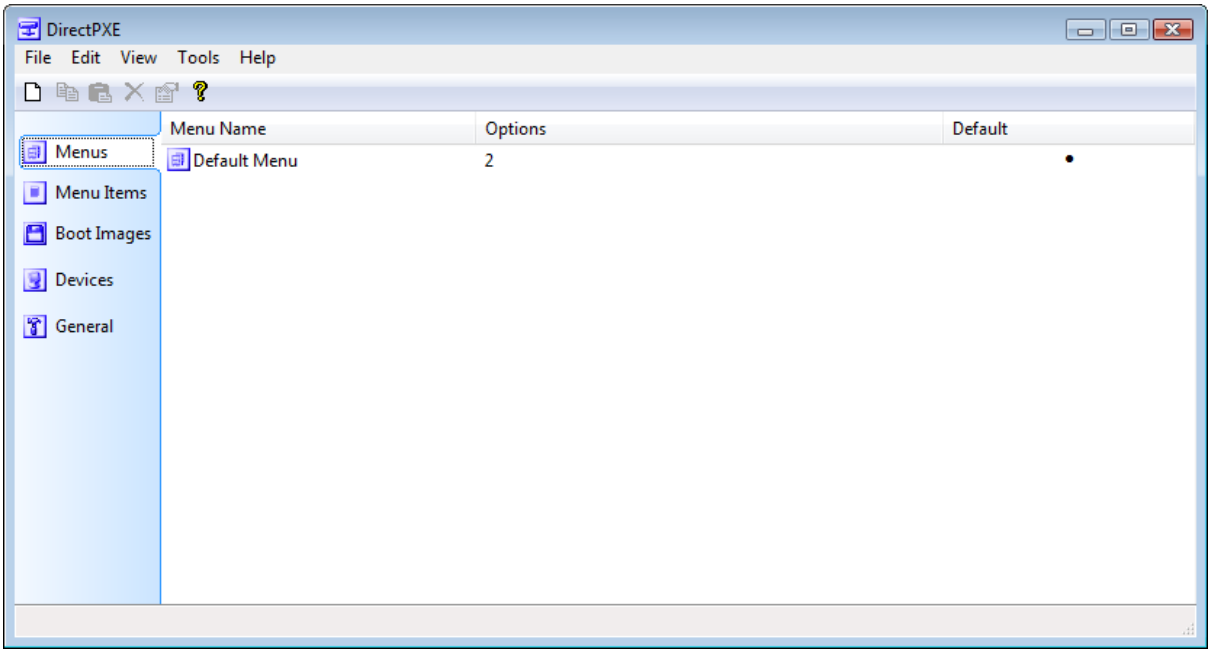
As part of the UMS framework the responses can be controlled from within DirectEngine tasks.

In this section
Menus
Menu Items
Boot Images
Devices
General
Ports
Running on a DHCP server

DirectEngine macros
Make CD Image
Importing and Exporting

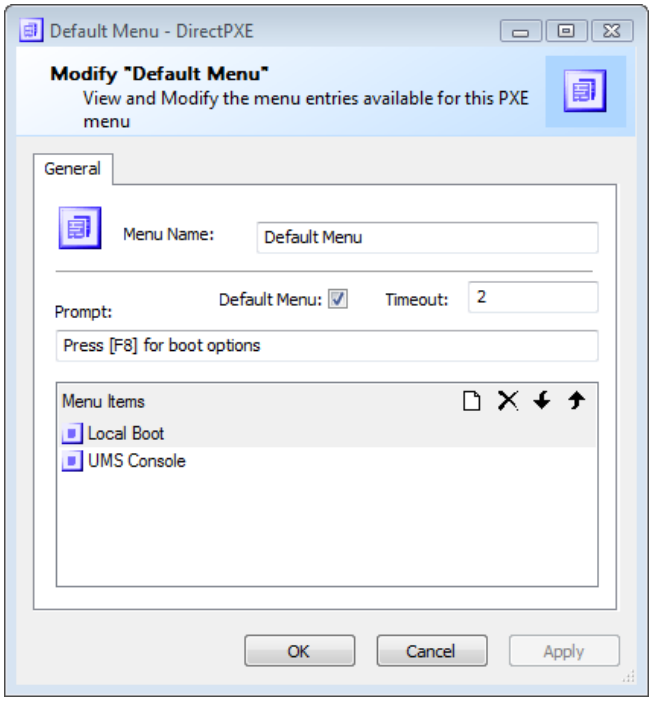
6.3.1 Menus

Selecting the Menus tab in the left pane displays at list of available PXE menus which can be returned to a device that performs a PXE broadcast. The console lists the PXE menu name, the number of menu options for the menu, and whether the menu is the default one.



It is possible to deliver custom menus to specific devices and therefore you can create as many different menus as you like. The default template that was used to configure UMSincludes one default menu called 'Default Menu'.

To view the properties of a Menu select it in the right hand pane and select properties from the context menu.



Menu Name

The Menu Name is the name shown in the list.

Default Menu

Tick the Default Menu option if the menu is to be the default delivered to devices. If another menu is already marked as the default menu, it will be un-ticked when the menu is saved.

Timeout

The Timeout is set in seconds. This is the time the menu option is displayed for at client PXE boot.

Prompt

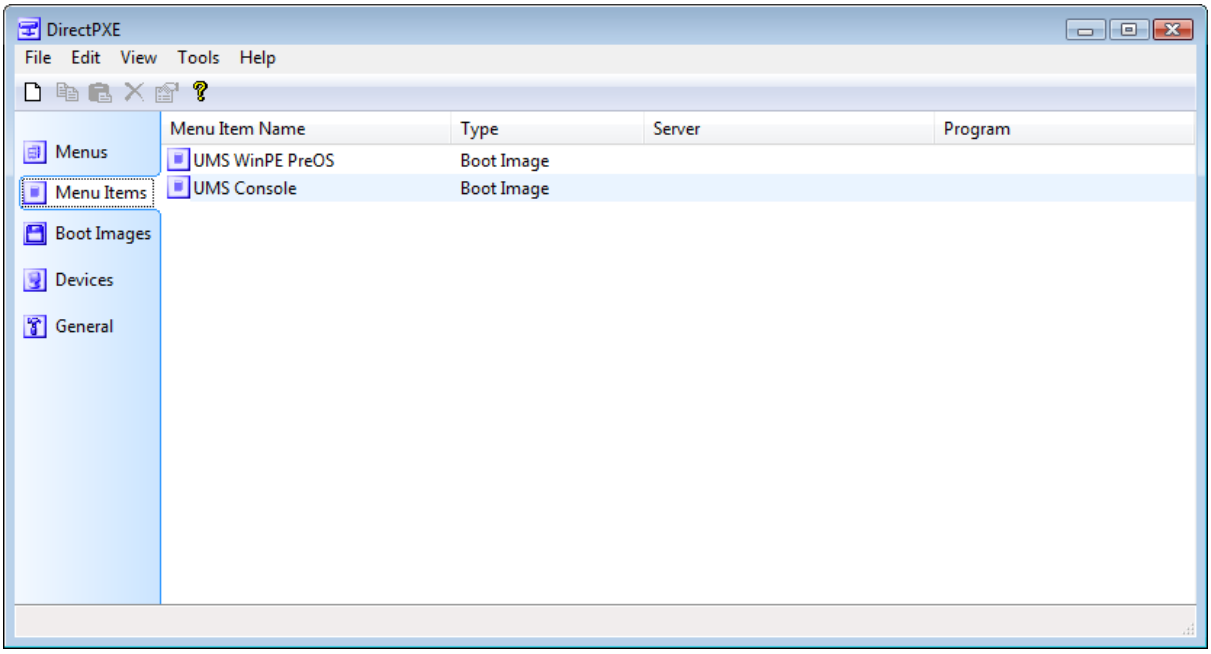
You can edit the Prompt that is displayed at client PXE boot. You should ensure the text states to 'Press F8' as this is the standard action used to display the menu.

Menu Items

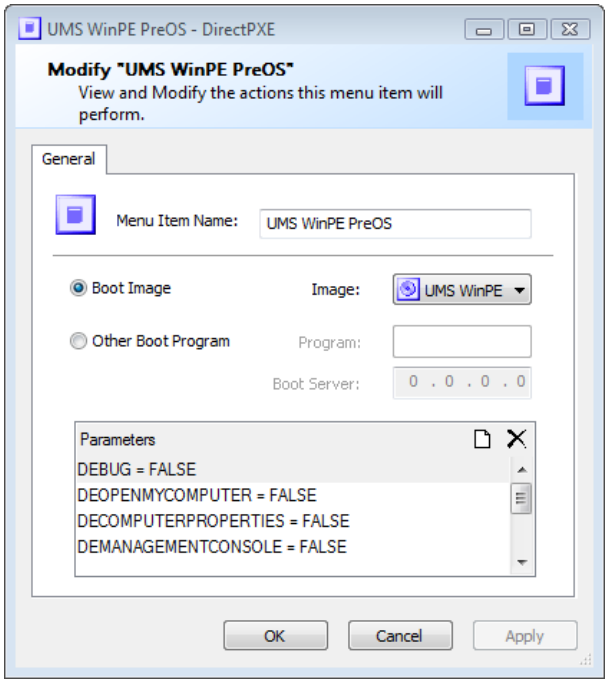
Menu Items can be added, deleted, or the order changed. Menu Items can only be added once they have been created in the Menu Items tab of the DirectPXE console.

6.3.2 Menu Items

Menu Items shows a list of all possible menu items, and any menu item can be associated to any PXE menu.



To view the properties of a Menu Item click on it in the right hand pane and select properties from the context menu.



Menu Item Name

The Menu Item Name is the name shown in the list of Menu Items, and the name the displayed at the 'F8' menu computer when a network boot is performed.

Boot Image

If a UMS Boot Image is to be used it can be selected from the drop down list. This shows available images configured in the Boot Images tab

Other Boot Program

DirectPXE also supports the use of other boot servers. The Other Boot Program option allows an IP address and boot program to be set. For example it is possible to start a RIS build by entering the

server IP address and appropriate boot program. An IP Address of 0.0.0.0 refers to the local server, in which case the Program must refer to an executable that is manually copied into the TFTPBOOT directory. This directory is a sub-directory of DirectPXE, and in a default installation would be at:

C:\Program Files\modus\UMS\Server\Default\DirectPXE\TFTPBOOT

Parameters

Parameters allow variables to be substituted with specific values when the image is deployed to the client. This allows the same image to be reused as the functionality of the image can be controlled by the parameters passed.

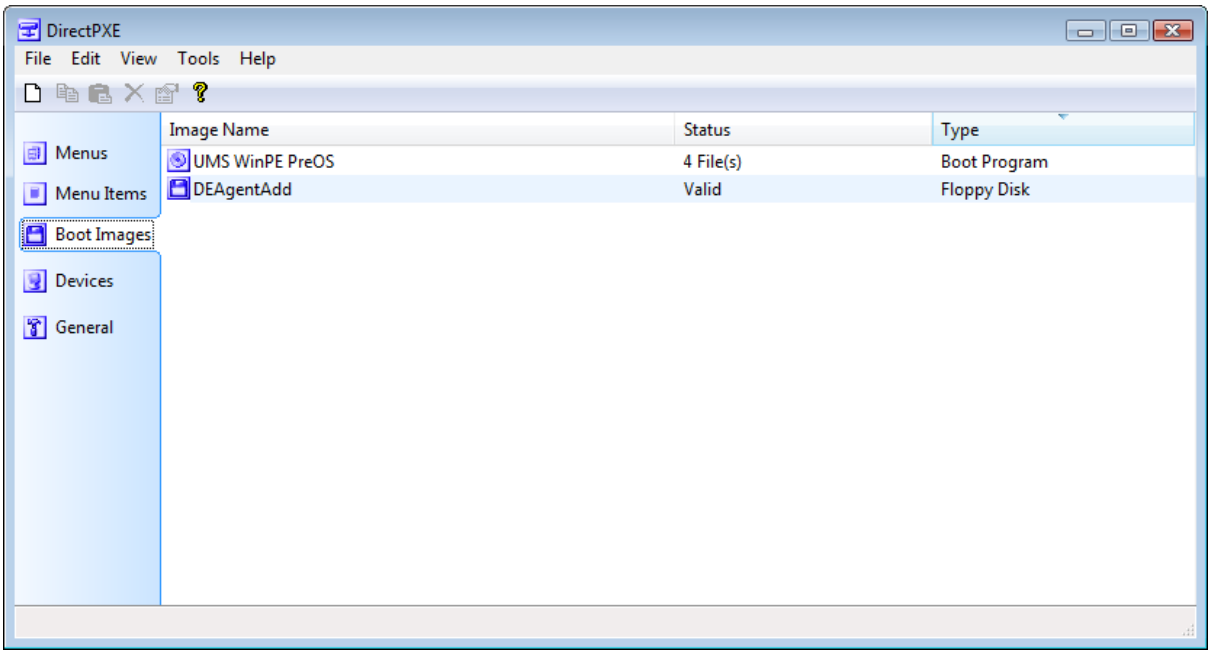
These parameters are used to set environment variables in both the DOS and the WinPE environments, and can be used to modify the behaviour of the environment. The template Boot Image uses the following parameters:

Parameter	Description
DEBUG	Launch WinPE in DEBUG mode. Connection information will be displayed
DEOPENMYCOMPUTER	When the boot image connects to the server, the Computer Properties windows will be launched for the current computer
DECOMPUTERPROPERTIES	The computer properties shortcut icon will be placed on the toolbar
DEMANAGEMENTCONSOLE	The mangement console shortcut icon will be placed on the toolbar
SHOWRUN	The shell will enable/disable the Run command

Note: Local Boot is an internal menu item and as such does not appear on the list of Menu Items when the Menu Item tab is selected.

6.3.3 Boot Images

Boot Images shows a list of the images held within the server. A boot image can be floppy disk image, or a boot program.



To create a new Boot Image entry right click on the right pane and select New from the menu. The Add Boot

Image Wizard will start. This will provide you with the following image options:

- Create from existing floppy disk

Use this option if you have a real floppy disk inserted into the floppy disk drive of your local computer. The wizard will create an image of the floppy disk that will be used to create the boot image. This option will create a Floppy Disk boot image.

- Create from Floppy Disk Image file

If you already have a floppy disk image, you can add it to the server. The image must be in the IMA format and cannot be compressed. This option will create a Floppy Disk boot image.

- Create from existing Boot Program

Select the PXE boot program and folder name for the program. The binary image will be uploaded to the server. Once the boot image has been created other files required files can be added to the boot program, and optionally a CD image. This option will create a Boot Program boot image.

6.3.3.1 Floppy Disk

The properties for an image are for informational purposes. Once a floppy disk image has been created and associated with a server file, the file cannot be changed. If the server file has been lost (manually deleted), then the image should be re-added by using the new image wizard. The wizard allows either for images to be selected from an existing image, or for the image to be created directly from a floppy disk.

The status indicates if the file is Valid. There are two states, either Valid, which indicates the file is available on the server, or File Missing which indicates that the file is missing from the server.

Image files are held within the server data path (as defined in UMS Admin) and then within the \DirectPXE\TFTPDATA directory.

6.3.3.2 Boot Program / Dynamic CD

The Boot Program that is installed at setup time is called "UMS WinPE PreOS. This is required for the default deployment templates to work and is referred to here for example.

General tab

The General tab of a Boot Program properties allows the name to be modified, and shows the path that was entered when the boot program was created. This path cannot be modified and is the relative path below the TFTPDATA directory. Note that there are no restrictions on the boot image path and it is possible to create two separate boot images referring to the same path, however this should be avoided as when a boot program is deleted the contents of the folder are deleted.

Attributes:

- Scan hardware for network card type

Performs an inline PCI device scan on the workstation and populates the DirectPXE device NIC type field, and forwards the result of the scan to the DirectDrivers module if it is available.

- Enable Dynamic CD driver injection

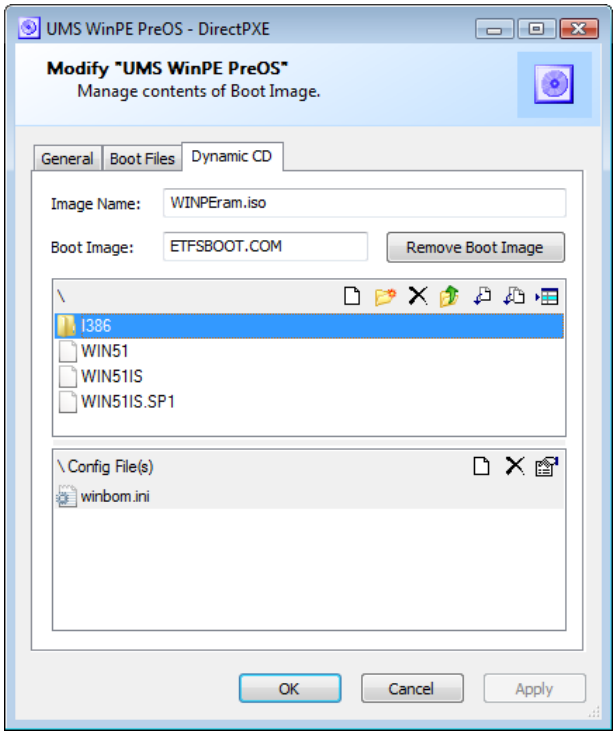
This feature is designed to deliver a Microsoft Windows Preinstallation CD, populated with appropriate drivers for the device. It requires DirectDrivers to be started at the time of the devices PXE boot. The directories used to inject the drivers are selected on the Dynamic CD tab. For more information see DirectDrivers, DirectPXE Integration on page 40.

Boot Files tab

The 'Boot Files' tab shows the contents of the boot image folder. The contents of the folder can be modified and which file is used as the initial boot program can be selected.

Dynamic tab

The 'Dynamic CD' tab enables the creation of a dynamic CD when any request for the 'Image Name' file, in the Boot Program folder, is received by the integrated TFTP server.



A boot image file (required to make the dynamic CD bootable) can be added or removed by pressing the Boot Image button.

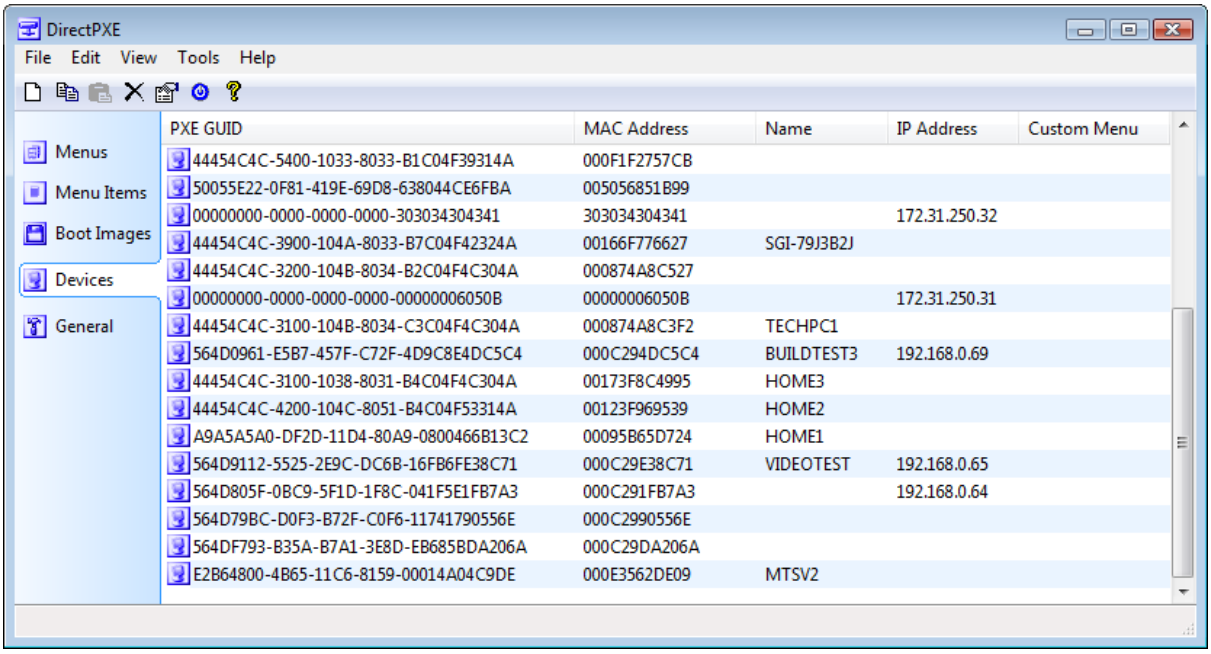
The next window allows the real content of the dynamic CD to be modified, and the Config Files window allows the dynamic content of the current selected directory to be modified.

The Config files are file that have replaceable macros within them. These values are always available, along with any additional parameters set on the Menu Item.

Parameter	Description
COMPUTERNAME	The booting device computer name, stored in the Devices page
OEMDRIVERPARAMS	Populates the [OemDriverParams] section of a WinPEOEM.SIF file with detected Mass Storage device drivers as part of the driver injection process
PARAMETERS	All DirectPXE parameters in the format: PARAMETER=VALUE Including customs parameters set in the Menu Item page
SERVERNAME	The computer name of the DirectPXE server
SERVERIPADDRESS	The IP address of the server that received the PXE request

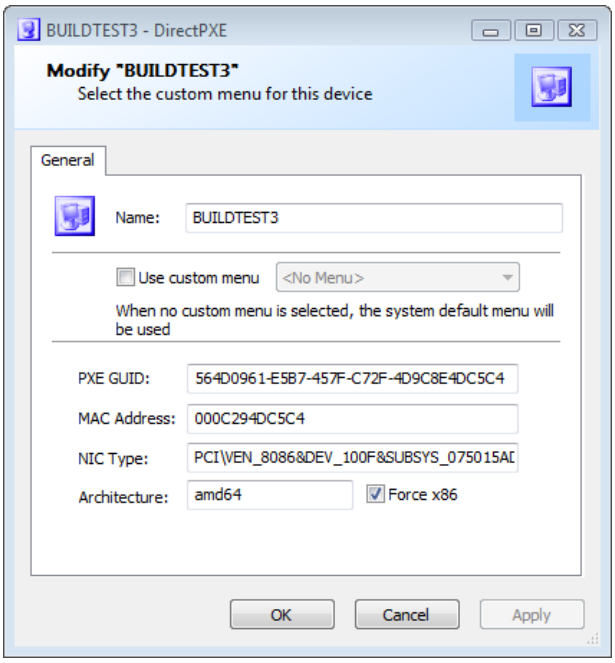
6.3.4 Devices

Each device which performs a PXE broadcast is recorded in the devices list. This list can be used to select specific actions when the server receives a device PXE request.



It is possible to add devices manually via the New Device wizard. Once a device is known to the system the PXE servers response can be customised from within the device properties dialog.

The Device properties page allows a user to define a device and alter the PXE server's response to a client PXE broadcast by the device in question. To view the properties of a device select it in the right hand pane and select properties from the context menu.



Use custom menu

Custom Menus allow you to specify a menu other then the default, to be sent to the device during PXE boot. It can be useful to exclude devices such as servers by creating a different menu for such devices and allocating the custom menu to the device.

To set a custom menu tick the option Use custom menu and then select the menu from the drop down list box.

If no custom menu is selected then the system default menu is returned to any client PXE broadcast requests.

6.3.5 General

The General tab page three tick box options.

Listen on DHCP port

By default this is selected. This tells the PXE server to listen for DHCP requests, as the PXE broadcast is a DHCP sub-type. As two services can not listen on the DHCP port this option must be unchecked when the PXE server resides on a DHCP server. See Running on a DHCP server for more information.

Set new devices menu to <no menu>

Set this option to restrict this PXE server to only respond to known devices. This can be useful if other PXE servers are in use.

Default x64 Architecture to x86

Set this option to treat x64 platform architecture as x86

6.3.6 Ports

DirectPXE acts as a both a DHCP server and a TFTP server. These services use the following ports:

The PXE server listens to requests on ports:
UDP port 67 (Bootstrap Protocol Server)
UDP port 4011 (Alternate Service Boot)

The TFTP server responds to requests on port:
UDP port 69 (Trivial File Transfer)

6.3.7 Running on a DHCP server

If DirectPXE is to be run on the same server as DHCP Server services, additional configuration is required.

1. Select the General tab in DirectPXE Setup.

2. Make sure the Listen on DHCP port option is unchecked, and click Apply.

3. You can now close DirectPXE Setup.

4. Additionally, the DHCP server needs to be configured to provide the 'PXEClient' option.

   To configure the Microsoft DHCP server to provide the PXEClient option, open a command prompt and enter the following.

   Note: the commands are case sensitive.

```
netsh dhcp server add optiondef 60 ClassID STRING 0
netsh dhcp server set optionvalue 60 STRING PXEClient
```

6.3.8 DirectEngine macros

These macros are populated when the PXE menu item is selected as the result of a DirectEngine task script executing against the computer.

Parameter	Description
COMP_ID	The DirectEngine System ID of the computer

COMPUTERNAME	The DirectEngine Computer Name, overriding any DirectPXE value
WKSNAME	The DirectEngine Computer Name, overriding any DirectPXE value. This is provided for backwards compatibility
PWD	The PreOS netbios share password. Note this password changes regularly and cannot be cached.
TASK_ID	The DirectEngine task number of the currently executing task
TASK_NAME	The DirectEngine task name of the currently executing task
TYPE_ID	The DirectEngine type of the computer

6.3.9 Make CD Image

The Make CD Image tool allows a CD ISO image to be created of one of the DirectPXE Boot Images. The ISO image can then be burnt to CD or used by a bootable USB drive to connect to the UMS Server when PXE is not available.

The wizard requires a destination file, DirectPXE Boot image, and the IP address of the server. Then select which devices need to be supported by the ISO image. Every selected device will have the required drivers included in the image.

Pressing next will then generate the ISO image.

6.3.10 Importing and Exporting

The Import and Export tools allow the entire DirectPXE configuration to be transferred from one server to another via XML files.

6.4 DirectReports

DirectReports provides reporting capabilities in order to assist in measuring the benefit of UMS. There are different types of report depending on the information being reported on, covering both exportable data (XML) for processing in other applications such as Microsoft Excel, Access or SQL, as well as print formatted management reports.

Configured and available reports appear in the UMS console tools menu.

6.4.1 Computer Details

The Computer Details Report is the UMS report that allows you to export data for analysis in another application. The export format is XML, providing a wide range of choice of applications with which to analyse the data.

There are two Computer Details reports: Monthly Detail Report and Daily Detail Report. Both reports show the same data, as per the table below. The monthly report has a row for each computer with the data summed for the month. The daily report has a row for each day's information for each computer that has recorded data that day.

Field	Description
Month/Date	Month shows the first of the month for the period of the monthly report. Date show the individual date for the daily report.
Computer	Computer host name
Model	Computer make and model
Watts	The consumption rating configured for the computer make

	and model (or Default if not configured).
Profile	The last UMS Profile assigned to the computer for the period.
On Hours/Minutes	Shows the total hours on for the monthly report and total minutes on for the daily report.
Logged On Hours/Minutes	Shows the total hours logged on time for the monthly report and total minutes logged on time for the daily report.
Idle Hours	Shows the total hours of idle time whilst logged on for the monthly report and total minutes of idle time whilst logged on for the daily report.
On kWh	The total units of energy consumed in kWh.
On CO2	The total Kgs of CO2 emissions for the month/day calculated from the consumption figure for the make and model, the hours on time, and the CO2 conversion formula.
On cost	The total cost of the kWh consumed for the month/date calculated from the On kWh and the Electricity unit cost configured.
Last User	This shows the last user logged in to the computer before the report was run.
AD OU	The Microsoft AD OU that the computer is in.
AD Site	The Microsoft AD Site that the computer is in.

➔When exported, kWh is /1000, CO2 is /100, and Cost is /100, in order that more accurate analysis can be carried out.

6.4.2 Daily Usage by Group

The Daily Usage by Group report is one of the reports which is produced ready formatted for printing rather than export. It provides a means to view certain key data for a specific day or days. This is particularly useful for analyzing smaller snapshots of time, especially when creating a baseline. It provides the added benefit of being able to be filtered by group; a group being either a static (manually created) group from the Management Console or a Profile.

6.4.3 Monthly Power Reports

The Monthly Power Reports are a set of reports which are produced ready formatted for printing rather than export. They are structured as management summary reports and allow an immediate view of the key information required from reporting on power management by month. The data is all based on a period of month and as such are only valid for any given complete month. There are five reports:

- Monthly Summary Report
- Monthly Carbon Report
- Monthly Energy Report
- Monthly Financial Report
- Monthly Efficiency Report

The Monthly Summary Report shows the ‘headline’ figures for efficiency, cost, consumption, and emissions. Each of the other reports takes its specific headline figure and further shows charts for emissions breakdown and performance overview, as well as a list of the best and worst performing computers for the month.

The efficiency breakdown chart illustrates the headline figures as a chart for easy visual comparison. The performance overview chart illustrates the key information broken down across the percentage on time (in three bands) for the period. For example, the performance overview for the Monthly Financial Report shows the total cost split across computers that were on 0-10% of the time, 10-40% of the time, and 40-100% of the time.

6.5 Intelligent Install

The Intelligent Install component is configured with a configuration file in the components folder on the server. By default this will be in the following location:

```
C:\Program Files\Modus\UMS\Server\Default\IIUMS\IIUMS.INI
```

This file should only be modified to locate the Intelligent Install installation for your environment. If you have used the default installation options of a share name of II$ on the server, no modifications are necessary.

To locate a non-default installation, modify the file to define the location of the IINSTALL.INI file, example:

```
[Settings]
IINSTALL=\\Server\Share\Bin\IINSTALL.INI
```

Once the configuration file is modified, the Intelligent Install component will need to be restarted for the changes to take effect.

6.6 Powerwise

Powerwise is a component that allows central configuration and control of the power management settings of your PC estate. This can lead to savings in the overall electricity costs of your organisation, and more importantly reduce the carbon emissions the electricity would have generated.

This section covers configuring Powerwise. To configure Powerwise you will need to launch the Management Console. By default the Management Console is installed on the server, however we recommend you run it from a workstation.

In this section

Costs
Profiles
Profile Properties
Web Wakeup

6.6.1 Costs

Launch the UMS Management Console and select **Tools, Powerwise Costs** from the menu bar to launch the Costs dialog box.

This dialog allows figures used to estimate the amount of electricity and carbon emissions used by each computer, and is used by the reports to give estimated figures for computer power usage.

The following table describes each value.

Attribute	Description
• Default computer and monitor power usage	This value is the global average power usage for all computers and screens for your organisation. When a new computer model is detected, this is the type power usage value assigned to it (in Watts).
• Electricity unit cost	This is the cost of electricity per kWh. The actual currency does not matter, as the cost shown is just a factor of this figure.
• CO_2 conversion factor	This is the figure used to convert a single kWh into a single unit of of CO_2 emissions. By default this is Kg. This conversion figure is set by Government.

Attribute	Description
• Model specific power usage	Each computer installed with the UMS Agent will have an entry in this table, and allows the estimated power usage to be tuned by computer model.

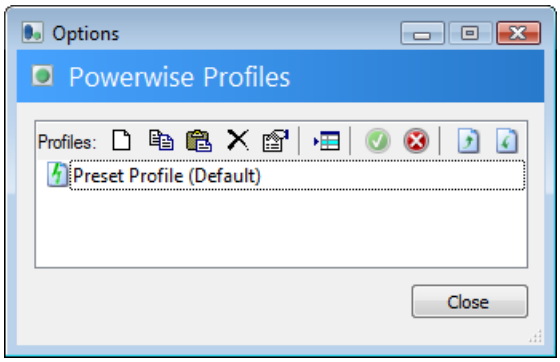
6.6.2 Profiles

Launch the UMS Management Console and select **Tools, Powerwise Profiles** from the menu bar to launch the Profiles dialog box.

Powerwise Options

Each computer is assigned a UMS Profile which is used to define the power options for the device. A schedule allows differing power settings to be applied at different times of the day. Shutdown and Wakeup events can be scheduled to enable remote management of the devices (e.g. for patching).

How many Profiles should you have? It depends on your users working habits, but typically an organisation will have between 2 and 6 Profiles. It's often the case that some Profiles are quite similar and can be combined, without losing energy saving opportunities. The default installation comes with a single Preset Profile as shown below:



After selecting a Profile, the icons on the menu bar allow the following actions to be performed:

Attribute	Description
Create a New Profile	Create a brand new Profile which can be configured manually.
Copy the Profile	Copy an existing Profile to reuse features of the Profiles, without having to re-enter all the details.
Paste the Profile	Pastes and copied Profile, appending a number on the end of the name to make it unique.
Delete the Profile	Remove any Profile no longer needed. You cannot delete the default Profile. To delete the currently default Profile, set another Profile as the default and then delete the original Profile.
Show Profile Properties	View and change the Profile energy saving settings. All energy settings and schedules are configured here.
Set the Profile as the Default	Only one Profile can be the default at any point in time. The default Profile is assigned to any new computer which connects to the UMS server.
Enable the Profile	A Profile is only active if it is enabled. All computers

Attribute	Description
	which have the Profile will be managed according to the Profile definition.
Disable the Profile	Disabling the Profile stops UMS from implementing any power saving features. This is often used to monitor computers to collect metrics without triggering any changes.
Import Configuration	Import Profile configuration settings.
Export Configuration	Save Profile configuration settings so you can import them later to other UMS servers.

When a Profile is deleted, any computers which were still using that Profile get allocated the default Profile

6.6.3 Profile Properties

This section covers the configuration of the Powerwise Profiles. A Profile is a group of power settings which can be applied to one or more computers. A Profile is divided into four parts; the General settings, which include items such as Enabling Hibernation, the Schedule settings, which is where sets of power controlling events can be configured, User Notifications, which allows you to configure what feedback the user receives. Idle Options provide the final set of Profile power settings which allow specific programs to be added to the exception list to prevent shutdown if the given process is running.

➔ By creating and managing Profiles in co-operation with end user representatives you can help improve user acceptance of the new central management of power saving settings.

In this section

Profile tab	Description
General	Enable or disable the Profile. Set hibernation, WOL and password settings
Schedule	Define how and when computers should enter different power saving states
User Notifications	User notification display settings
Idle Options	Define specific processes which if running can stop a computer from a shutdown or hibernate event

.

6.6.3.1 General

General Properties

Each Profile has a set of properties which determine whether the Profile is enabled (actively enforcing Powerwise Profile), as well as a number of settings which determine how Windows power settings are configured. If the Profile is not enabled then metrics are captured by Powerwise server but no power savings are enforced.

The **Name** field allows a unique name for the Profile. **ID** is a read only field that cannot be amended. The ID

can be used within DirectEngine scripts to set the Profile via script.

Tick the **Enabled** check box to enable the Profile. The Profile can be enabled or disabled from the Options dialog once the Profile has been created. This will enable or disable all Powerwise features for all the computers currently using the selected Profile.

The **Comments** text box allows a description of the Profile to be recorded.

Each Profile has the following **Attributes**:

Attribute	Description
• Enable Hibernate if supported	Enables Hibernate on the workstation. If you want to use hibernation then this will need to be checked.
• Allow network cards to wakeup computer when in hibernate	Enables Wake on LAN (WoL) for resuming from hibernate (if supported). By default this is disabled for Windows XP computers, and must be enabled if you wish to use Wake-on-LAN to wakeup hibernated computers. If Intel vPro functionality is available and device has been provisioned then Powerwise can use vPro to wake devices.
• Prompt for password when computer resumes from hibernate	Password protect a computer when is resumes from hibernation.
• Lock computer when display turns off	Whenever display turns off, computer is automatically locked and user is required to authenticate before using computer.
• Prevent user changing power options	Ensures users do not change the options you are managing with Powerwise.
• Use hibernate when sleep requested for pre-Vista computers	When some Windows XP computers are placed into sleep (standby) they refuse to wake. Setting this option will prevent Windows XP computers assigned to this Profile from using sleep. Otherwise hibernate will be used if supported.
• Use hibernate when sleep requested for non S3 (Standby) computers	Setting this option will only use standby if state S3 is supported. Otherwise hibernate will be used if supported.

Hibernate works on both desktops and laptops. Hibernate is used extensively in laptops but its also available for use on desktops. It works in exactly the same way, allowing users to resume work without losing data.

If users are able to change Power Options then they can temporarily change options as normal in the control panel in special cases where users don't want to be disturbed. The Profile will however reset the changes to the Profile settings whenever the Profile scheme next changes, or the Agent reconnects.

6.6.3.2 Schedule

The Schedule tab controls what power saving events are configured for the Profile. These events can be set to occur at any time and on any given day or days of the week and there is no limit to the number of events that can be configured for a Profile. The schedule settings will dictate how large your potential saving opportunity is. Schemes with low settings don't affect the user much but have limited savings opportunity. Aggressive settings maximize savings opportunity but can interrupt your users unnecessarily. Use timed scheme changes to gain savings benefit when users will be least impacted.

To show the properties of an event either double click on it, or select it and then click on the properties icon on the menu bar of the Schedule tab. The properties of the selected event always appear in the bottom half of the already open window.

Schedule event	Purpose
Scheme Change	Sets the power options for the computer during the hours defined. Sets display, disk, CPU and shutdown power options. All options are based on computer idle time. If a user is actively using computer then no power saving action is taken until computer becomes idle for specified time.
Wakeup	Will issue a one off Wake on LAN (and Intel vPro wakeup if supported and provisioned) at the time specified. Used for both automated power on at the start of the work, as well as to allow computers to be woken for remote patching and maintenance tasks outside of normal working hours. The computer will keep the all other power options from the current **scheme change** in effect. Target computers must support Wake On LAN and have their BIOS configured correctly for this event to be successful. Adaptive Wake on LAN allows wakeup to tailor itself to wake up 10 minutes prior to the individual computers switch on time as monitored over the last 4 weeks of logon times. Selective Wakeup will only execute the wake up if the Agent computer has been connected and logged in during the last week.
Shutdown	Instructs any computer running the Profile to shut down at a given time. Optionally will allow the user if currently working to cancel shutdown operation. Unsaved data will be lost.
Display	Can turn the display off and on at the set time. Used to turn off presentation displays as used in reception areas etc.

Scheme Changes

A scheme change is the main power saving configuration as it the way to configure what power management is applied based on inactivity of the computer. Multiple Scheme Changes can be configured in a single Profile allowing an unlimited configuration of power management based on day of the week, time of the day, and activity/inactivity.

Scheme changes are time zone aware. Each computer will apply the scheme change at the computers time. Note Wake on LAN is an exception to this and will occur at UMS server time .

Each scheme change remains in effect until the next timed change. Therefore the last change on Friday will remain in effect until Monday morning, unless a scheme change is scheduled over the weekend.

Display, Disk and CPU settings can save valuable energy. Shutting down the computer (or using hibernate) gives a much higher saving opportunity overall.

Shutdown, Hibernate and display events can be stopped by using idle option settings to set programs which should not be interrupted.

Turn off Display

Apart from shutting down the computer, turning off the display is the most obvious sign of ongoing power saving activity to users. All displays attached to the computer can be instructed to enter standby after a specific time of user inactivity.

Users are notified 2 minutes prior to the display entering standby if notifications are turned on.

Turn off Disks

Fixed disks can be allowed to spin down if idle. Various background tasks can prevent the disks turning off even though there is no user activity. If required by Windows then the disks will continue to be used and will not spin down to enter a low power mode.

Processor Throttle

Windows XP and Vista allow the CPU throttle to be set according to the following parameters:

Processor Throttle	Description
None	Highest performance state
Constant	Lowest performance state
Adaptive	Performance state chosen according to demand

Computer shutdown options

User Status	Action	Purpose and recommended use
Logged On	Hibernate	Computer will hibernate the device, allowing user to resume without losing data. Useful where devices are not shared amongst users and data should be preserved where possible.
Logged On	Shutdown	Computer will shutdown and any unsaved files will be lost. Useful for shared devices used in a pool where computer availability is important and overrides possible loss of data.
Logged On	Sleep	Computer will suspend to RAM if supported (Standby). Sleep can actually hibernate if the conditions are met by settings on the general tab. Sleep provides the quickest computer start time.
Logged On	Logoff	User will be logged off. Unsaved data may be lost. Where machines are shared (training classroom for example) then it can be important to ensure devices are available for other users.
Logged Off	Hibernate	Computer is Hibernated. As no user is logged on, there is no user data to lose.
Logged Off	Shutdown	Computer is shutdown. Recommended option as no opportunity for data loss.
Logged Off	Sleep	Computer will suspend to RAM if supported (Standby). Sleep provides the quickest computer start time.

Ignore System Standby Disabled

There are applications and processes which incorrectly set the Microsoft Operating System flag ES_System_Required (System Standby Disabled). When this occurs computers will ignore all attempts for power saving to occur, often referred to as PC/Windows insomnia. UMS provides an option to ignore this flag after a period of time in order that this 'insomnia' does not effect the objective of improved power management and the resulting savings. We recommend you test to see whether the flag is set correctly or incorrectly before using this which you can do by monitoring the Power Status tab of the computer properties in the Console. The Profile Idle Options are still honoured even with this setting in use.

Standby is not supported as a power option within UMS as the power saving benefits are very limited compared to Shutdown or Hibernate.

Event tracking

Events actions are recorded as they occur and can be seen on the Computer Events properties page within the UMS Management Console.

6.6.3.3 User Notifications

The User Notifications tab allows you to configure what information the user receives, if any.

Warning Popups

We recommend that you always enable Warning Popups so users are notified of upcoming power events.

Notification area

The notification area is available to the user from the UMS system tray icon.

Attribute	Description
Enable idle event popups	Select whether the user will see notifications prior to power saving actions occurring. The popup appears approximately 2 minutes before the power saving action occurs.
Play a sound for Standby and Logoff prompt	When a warning popup is displayed, also play an alert sound so users not looking at the screen can be aware the event is about to take place.
Show power usage tray icon	Enables a notification area icon showing the logged on user the power usage statistics for the computer: Task tray icon:  • Percentage of time the computer has been On • Percentage of time the computer has been on but idle • Percentage of time the computer has been on with no one logged on The power usage tray icon is not shown if the Profile is not enabled.
Enable Keep Awake	Allow users to use the 'Keep Awake' feature. Away Mode allows the user to hibernate immediately for a set amount of time, and then wakeup after the time interval. This can be used if it is known that the computer will not be used, for example when the user has a lunch break. The console user can always use this feature, regardless of Profile.
Enable Away Mode	Allow users to use the 'Away Mode' feature. Keep Awake mode prevents any of the UMS idle functions from triggering for a set amount of time, and then returns to normal operation. The console user can always use this feature, regardless of Profile.

User notification popup

6.6.3.4 Idle Options

This allows the definition of one or more running processes which should prevent the monitor and/or system from powering down. Applications and processes defined here are honoured even if the Ignore System Standby Disabled is set within a Scheme Change event in the Schedule tab.

Attribute	Description
Process	Lists the specific process which should be monitored. process can either be specified with or without path. Specifying the path of the process ensures only process from a specific location is monitored. Process requires complete image name: e.g. notepad. exe rather than simply notepad.
Prevent Display	By ticking this checkbox the device will not switch off the display, even if the Profile scheme determines that it should.
Prevent Standby	When the process is detected (running), this setting will prevent the system from shutdown or hibernate triggers.

Powerwise checks Windows and ensure the system can be safely shut down or the display turned off. Many programs (such as when applying windows patches and AV updates) set the Standby Disabled flag indicating that windows cannot be shut down at this time. These programs don't need to be added to this exception list unless you are using the Ignore System Standby Disabled setting with a Scheme Change event in the Schedule tab.

6.6.4 Web Wakeup

Web Wakeup allows a remote user to use the UMS Server to turn on a computer remotely. The service can also be used to see if a managed computer is already online.

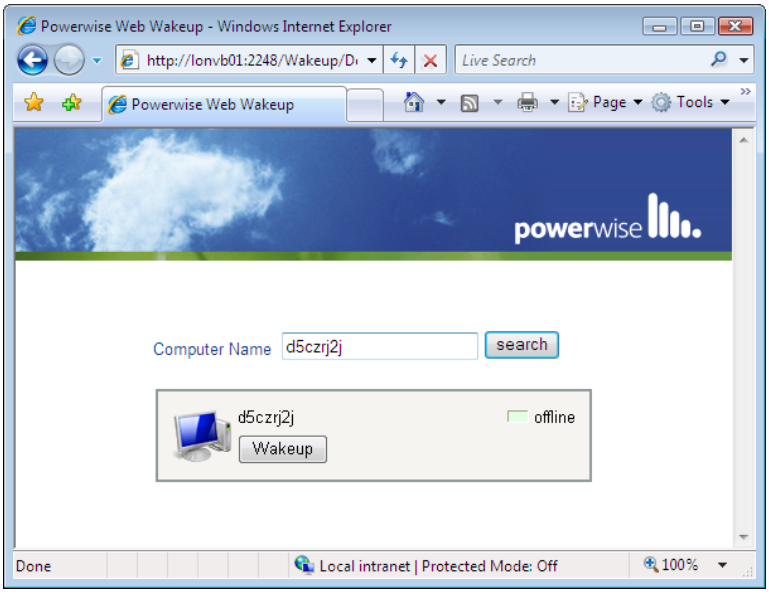
To access the service, open a web browser and type the following address:

HTTP:// UMSServer:2248/Wakeup

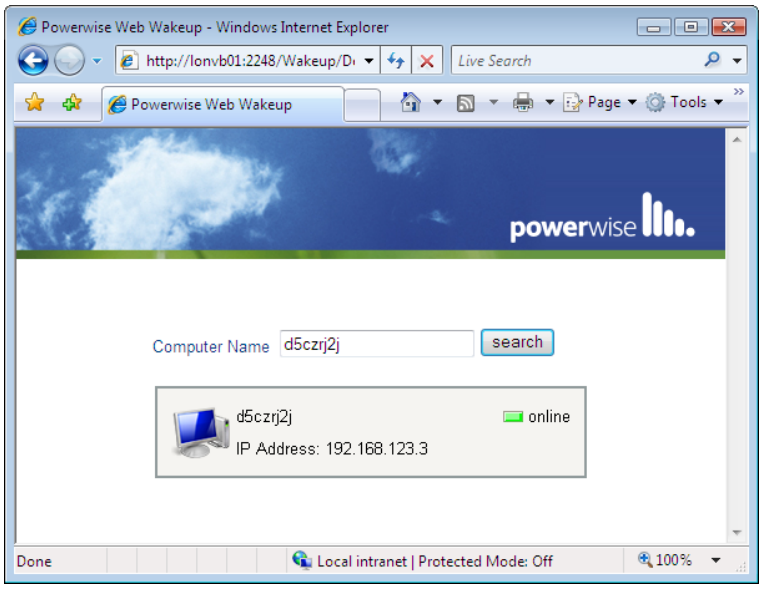
The server can be configured to respond on port 80, if so the address would be:

HTTP:// UMSServer/Wakeup

The browser page should appear as follows:



Enter the computer name to query in the field and click search. If your computer is offline, then you can issue a Wakeup by clicking the Wakeup button. Click search again to detect when the computer has booted.



Web Wakeup can be disabled by removing or renaming the <Server Install Directory>\Server\Default\Powerwise\Wakeup\Default.html file.

Part VII

Advanced Configuration

7 Advanced Configuration

7.1 Upgrading UMS

UMS 2011 can upgrade from UMS 2.0 and UMS 3.x. Different upgrade techniques exist, and a suggested method is presented here. Depending on the amount of customisation applied, alternate upgrade techniques may be more appropriate.

Always ensure a complete backup of the UMS Server before starting an upgrade process. A backup can be achieved by:

- Stopping the UMS Server
- Copying the servers data directory, by default: "C:\Program Files\UMS\Server\Default" to a backup location
- Start the UMS Server

It is also possible to backup the server's data directory while the server is running, as the data files are only written to approximately every 20 minutes, and are not held open.

It is also recommended that any upgrade process be performed on a temporary server, built as a replica of the real environment. This enables the process to be tested before creating a new 2011 script that can be used to build your 2011 servers.

The suggested upgrade method has been split into 2 steps:

Step 1: Create Corporate UMS 2011 XML Config. This step is typically performed in a lab environment and is used to make a master template script that is used to build and upgrade servers within your environment. This step has 2 versions for upgrading from either 2.0 or 3.x

Step2: Upgrade Server. Once a master template has been created, live UMS servers can be upgraded. The upgrade process actually removes the existing server and installs the new version, with the new template script that includes required parts from the previous installation. Once the server is upgraded, Clients can be upgraded using the 'Install Agent' template task

Step 1: Create Corporate UMS 2011 XMLconfig from a 2.0 server

⇨ Remove UMS 2.0 (leave all data files in place)
⇨ Install UMS 2011 to same folder as 2.0
⇨ Export: DirectEngine & DirectPXE to 'XMLconfig_2.0'
⇨ Remove UMS 2011 & data files
⇨ Install UMS 2011, with default template
⇨ Import previous 'XMLconfig_2.0'
⇨ Adjust previous scripts for conflicts, and test
⇨ Export to 'XMLconfig_2011'

Step 1: Create Corporate UMS 2011 XMLconfig from a 3.x server

⇨ Export: DirectEngine & DirectPXE to 'XMLconfig_3.x'
⇨ Remove UMS 3.x & data files
⇨ Install UMS 2011 with default template
⇨ Import previous 'XMLconfig_3.x'
⇨ Adjust previous scripts for conflicts, and test

⇨ Export to 'XMLconfig_2011'

Step 2: Upgrade Server

⇨ Remove UMS 2.0/3.x & data files (leave computer.dat*)
⇨ Install UMS 2011
⇨ Import 'XMLconfig_2011'
⇨ Upgrade Clients with 'Install Agent'

* If you wish to keep the list of Computers/Computer Groups, do not remove Computers.DAT or ComputerGroups.DAT

7.2 Advanced Client Installation Options

The Installation section gives an overview of the different methods available for installing the Clients.

Properties of `UMSAgent.MSI` can be set on the command line to modify a default installation. This can be used for unattended installs, or to change options not available through installation interface.

Property	Description
AGENTSTART	Start the agent at the end of the installation 0 – Disable, 1 – Enable (Default)
CLIENTCONNECTATSTARTUP	When the Client starts, automatically connect to the server 0 – Disable, 1 – Enable (Default)
CLIENTCONNECTATSTARTUPNAME	The name of the server used when connecting. The default value is UMS.mydomain.com and should be replaced with the actual server name
CLIENTCONNECTDISCOVER	Set whether server discovery is used 0 – Disable, 1 – Enable (Default)
INSTALLDIR	The folder to install the product

The `UMSClient.MSI` contains the Client and Server Manager features:

Feature	Description
Client	Allows a user to run components from the UMS Server
Server_Admin	Allows an administrator to modify settings of a UMS Server

The following properties can be used to modify the default installation.

Property	Description
CLIENTCONNECTATSTARTUP	When the Client starts, automatically connect to the server 0 – Disable, 1 – Enable (Default)

CLIENTCONNECTATSTARTUPNAME	The name of the server used when connecting. The default value is UMS.mydomain.com and should be replaced with the actual server name
CLIENTCONNECTDISCOVER	Set whether server discovery is used 0 – Disable, 1 – Enable (Default)
CLIENTLAUNCH	Start the Client at the end of the installation 0 – Disable, 1 – Enable (Default)
CLIENTRUNATSTARTUP	Sets the Client to run when Windows first starts up 0 – Disable, 1 – Enable (Default)
INSTALLDIR	The folder to install the product

7.3 Advanced Server Installation Options

Properties of `UMSServer.MSI` can be set on the command line to modify a default installation. This can be used for unattended server installs, or to change options not available through installation interface.

Property	Description
INSTALLDIR	The folder to install the product
PIDKEY	The supplied product key, using the format: XXXX-XXXX-XXXX-XXXX-XXXX-XXXX-XXXX
SERVICEACCOUNTPASSWORD	Override the automatic account password generation with this password
SERVICEACCOUNTUSERID	Override the automatic account creation with this UserID with the format DOMAIN\UserID. For local accounts, use .\UserID
UMSACTIVATELICENSE	Attempt to activate the license at the end of the installation 0 – Disable, 1 – Enable
UMSCLIENTALLOWPASSWORDCHANGES	Allow connected Clients to change their password 0 – Disable, 1 – Enable
UMSCLIENTALLOWUSERSTOCLOSE	Allow connected Clients to close their Client 0 – Disable, 1 – Enable
UMSCLIENTIDLETIME	Number of seconds with no keyboard/mouse activity before a connected Client is flagged as idle
UMSCOMPONENTINSTALL	Install UMS Components at the same time as installing the server 0 – Disable, 1 – Enable
UMSINSTALLCLIENTS	Install UMS Clients at the same time as installing the server 0 – Disable, 1 – Enable
UMSINSTALLICON	Install UMS Clients at the same time as installing the server 0 – Disable, 1 – Enable
UMSSERVERENABLEAUTHENTICATION	Clients must be authenticated before being allowed to connect 0 – Disable, 1 – Enable

UMSSERVERNAME	Change the server instance name, allowing multiple instances of UMS Server on a single computer.

Example:

Command line to install UMSServer, using a specific service account, overriding the automatic service account creation:

```
msiexec /I D:\Components\UMSServer.MSI
SERVICEACCOUNTUSERID=modusDOM\UMS_account SERVICEACCOUNTPASSWORD=secret
```