



Remote Management of BIOS Configuration

Whitepaper - Ian Godfrey

Ian Godfrey is a principal consultant for 1E, a specialist in large-scale Windows deployment and management. Feedback is welcome. You can reach him at iang@1e.com



1 Introduction

This paper aims to provide information about a number of different methods of remote management of BIOS settings on Windows workstations without having to manually boot into BIOS setup.

This paper was originally written for the benefit of 1E's customers who find it necessary to remote configure BIOS settings on Windows computers to:

- enable Wake-on-LAN for use with 1E WakeUp
- configure network boot for use with 1E PXE Lite
- configure APM/APCI support to make best use of 1E NightWatchman

However, before you get stuck in to the complexities of BIOS management, please consider whether you have a genuine need to reconfigure the BIOS on all your computers, as all that may be required is perform a few tests and manually fix the few machines that are different. Some troubleshooting tests are provided in the Wake-On-LAN section below.

The ability for Windows software to manage BIOS settings is dependant on individual computer hardware manufacturer models and network cards and whether the vendor provides software and drivers that support automated configuration while the computer is being used.

There is no single software product or solution that will manage BIOS settings for multiple vendors, although there are several systems management products that can report BIOS information. Most major hardware vendors have their own management system, and in some cases also provide utilities. 1E consultants have used knowledge of these to provide custom solutions for reporting and managing settings.

Organisations should test the capabilities of individual computer models and their revisions before purchasing hardware, and make their management requirements a condition of purchase agreements. If remote management of hardware is not a consideration before purchasing hardware an organization may be placed in a predicament where manual visits to hundreds or thousands of systems is required rather than a few clicks via a management tool. Vendor web-sites should be regularly checked for updated utilities for newer models.

1E solutions integrate with Microsoft Systems Management Server (SMS) and System Center Configuration Manager (ConfigMgr), therefore it is beneficial if these can be also used to report and manage BIOS settings. These Microsoft systems can report a number of BIOS settings, including serial number and asset tag, but they rely on vendor specific agents or utilities and custom scripts or code to expose other settings via WMI, and to manage them.

Disclaimer

1E does not provide support for any of these software, utilities, 3rd party products or scripts! Configuring BIOS settings is the customer's responsibility, and the computer vendor should be contacted for product support.

Your use of this document, software, utilities and scripts is at your sole risk. They are provided "as-is", without any warranty, whether express or implied, of accuracy, completeness, fitness for a particular purpose, title or non-infringement, and is supported or guaranteed by 1E. 1E shall not be liable for any damages you may sustain by using this document, software, utilities or scripts, whether direct, indirect, special, incidental or consequential, even if it has been advised of the possibility of such damages.

This edition of the paper does not cover other frequently asked questions about upgrading BIOS firmware, Trusted Platform Module (TPM), [AMT vPro](#) systems or IPv6.



1.1 Agent or Agentless?

Which is best is a continuing industry debate. Simply put, an agent is software that is permanently installed on a computer perhaps as a service or API, whereas agentless implies a utility that does not leave a footprint. Either way, a system management solution is helpful to deploy them if you have many computers to manage.

You are also likely to require scripts or programs to report and/or manage BIOS and Windows settings. However, an agent or utility that supports WMI will allow a system management solution like SMS/ConfigMgr to report settings as part of the hardware inventory, and run scripts to manage settings. To support scripts that use WMI, it is usually necessary to have Windows Scripting Host (WSH) and VBScript execution both enabled.

WMI is Microsoft's implementation of the Common Information Model (CIM) which is an open standard that defines how managed elements are represented as a common set of objects and relationships between them, intended to allow consistent management, independent of their manufacturer or provider. However this does not prevent vendors adding their own objects.

Below is a table that shows agents and utilities available from some of the world's top PC vendors¹.

	System Management	Standalone WMI Agent	Standalone Windows Utility
Acer	?	?	?
Asus	?	?	?
Dell	Dell OpenManage IT Assistant (ITA) Dell Client Manager ²	OpenManage Client Instrumentation (OMCI)	Dell Client Configuration Utility (DCCU)
Fujitsu - Siemens	DeskView ² There is also a DeskView SMS component	?	DeskView Instant-BIOS Management includes a utility called BIOSSET.exe
HCL	?	?	?
HP	HP Client Manager ² HP OpenView PC Configuration Management (aka Radia)	HP Client Management Interface (CMI)	HP System Software Manager (SSM) includes a utility called BiosConfigUtility.exe
Lenovo (IBM)	IBM Director with Remote Deployment Manager (RDM) LANClient Control Manager (LCCM) Available at cost from IBM	?	SRCMOS is a DOS boot-floppy utility There is a Windows version of SRCMOS that supports a limited number of ThinkPad models.
Sony	?	?	?
Toshiba	?	?	?

¹ Sources: IDC April 2008, Gartner July 2008. For Wintel compatible PCs, therefore excludes Apple.

² These products require Altiris® Notification Server®, not to be confused with Altiris® Deployment Server®



1.2 Extending SMS/ConfigMgr hardware inventory

SMS/ConfigMgr provides a comprehensive inventory of hardware details including BIOS version and date. For it to report vendor specific information it is necessary to configure the hardware inventory SMS_DEF.MOF file. An example is given in section 3.2.4 on page 17.



1E can assist you with developing relevant configuration details and reports for use on an enterprise scale and in an automated manner. Please contact your 1E representative for more information.

1.3 What is BIOS?

The BIOS is the first program to run when a computer is switched on. It initializes and tests the hardware (called Power On Self Test or POST) and if everything is OK it passes control to the operating system. The BIOS also provides Run-Time Services that help operating systems and application programs access hardware.

BIOS is an acronym meaning Basic Input / Output System. It is a software program stored in a chip called ROM (read only memory). Nowadays EEPROM(Electrically Erasable Programmable Read-Only Memory) is used, also known as 'Flash' BIOS.

Computer motherboards and add-on cards each have their own BIOS that determine how the hardware behaves, for example Network Interface Cards (NICs). Computer standards mean that different manufacturer hardware will behave in the same way. In some cases, the BIOS is configurable.

BIOS settings can be changed by running BIOS Setup, sometimes called CMOS Setup. CMOS is a generic term for a memory chip, and in this instance is where the configurable settings are stored.

The vast majority of PC motherboard manufacturers license a BIOS 'core' and toolkit from a BIOS manufacturer, known as an 'independent BIOS vendor' (IBV). The motherboard manufacturer then customizes the BIOS to suit its own hardware preferences, and any specialisation required from the computer vendor.

Some major computer vendors produce their own motherboards for some of their computers, but most source components from OEM manufacturers. Some outsource the complete manufacture.

IBVs include:

- Phoenix Technologies, the first PC BIOS manufacturer, now also owns Award Software International and General Software®
- Advanced Logic Research, Inc.
- American Megatrends (AMIBIOS),
- AMD® (Advanced Micro Devices, Inc.)
- DTK® (Datatech Enterprises Co.)
- Microid Research Inc.
- Insyde Software (previously SystemSoft Corporation)

Microsoft provides a list of Motherboard manufacturers in [KB243909](#).



2 Wake-On-LAN

Wake-On-LAN (WOL) is a well established standard for performing remote wakeup of systems.

This section provides useful hints and tips about preparing for and using Wake-On-LAN, and includes background on using WOL over a routed network.

WOL uses a special network packet called Magic Packet³ which contains MAC address information. The network adapter monitors all incoming packets that are destined for the adapter's MAC address, even when the machine is powered down. On receipt the network adapter will send a message to the motherboard to initiate boot up, providing the network adapter and system BIOS are WOL-enabled.

A Magic Packet is a directed broadcast, and in order for the packet to reach the client, the local network infrastructure must be able to forward it across all types of network hardware.

2.1 Troubleshooting Steps

System administrators often perceive there is a problem with their computer Wake-on-LAN settings which may be some other external problem such as network configuration. This section explains some of the fundamentals that may avoid unnecessary effort of configuring BIOS settings.

Typical troubleshooting steps are:

1. A quick way to tell if a system is WOL ready is to power down the system then look at the network adapter display LED's. If the lights are still on, then chances are that the system is OK.
2. Has the computer been gracefully shut down and is it plugged in? If there has been a power loss, the computer is unable to prepare itself for wakeup, and will need to be properly restarted.
3. Ensure the computer is receiving the Magic Packet. Use the 1E utility discussed below.
4. Verify the computer supports WOL and it is enabled in the BIOS. Some systems also require ACPI to be enabled. If using Windows XP and BIOS is set to APM then it must be reset to ACPI, and Windows re-installed to use a different HAL.
5. Verify WOL is turned on in the NIC configuration as described in section on *Windows Power Management Settings* below.
6. Verify the NIC adapter is connected to the network and has power. Most laptops do not respond to wakeup packets when running on battery or in low power mode.
7. Verify you are running the latest NIC drivers, and check for other hardware.
8. Check vendor support web-sites for specific issues.

2.2 Hints and Tips

- ★ Network configuration. Simple WOL solutions use subnet directed broadcasts which rely on network routers to forward a Magic Packet to the subnet where the target system resides. Subnet directed broadcasts and Unicast are explained below.

³ Magic Packet is a trademark of Advanced Micro Devices, Inc.



- ★ BIOS must be WOL capable. Use an inventory system such as Microsoft SMS/ConfigMgr to report computer models and BIOS versions. Then check a sample set to confirm the BIOS supports WOL and already enabled. Inventory systems will also tell you the MAC address necessary to create the Magic Packet, and the IP address and subnet to enable you to send it.
- ★ Many computer models have multiple BIOS settings for Wake-On-LAN, so you need to check them all and refer to the manufacturer's documentation. This may include the type of activity that allows the machine to wakeup such as Wake on Magic Packet, Wake on ARP, Wake on broadcast, Wake on Multicast, Wake on Unicast and Wake on physical activity. Wake on Magic Packet is normally the only option required.
- ★ Some systems do not respond to a WOL unless shut down in a controlled manner, so that they properly enter sleep (G1) or soft-off (G2) ACPI state⁴. That is, will not wakeup if switched off by disconnecting the power or by holding in the power button (G3 state).
- ★ Windows compatible network card drivers should be installed and tested, with the NIC properties configured to allow WOL. A script to enable this is provided below.
- ★ Power-on passwords, disk encryption or protection passwords will prevent Windows starting, giving the impression there has been a WOL failure.
- ★ [KB815304](#) describes a fix for Windows XP blanking when woken from hibernation or standby.
- ★ Some computer models do not support waking up from hibernation.
- ★ Some PS/2 devices may not function on resumption if it experiences a power loss after going into hibernation.
- ★ Some NIC adapters require a password to be included in the magic packet.
- ★ Some NIC adapters require a physical wire to the motherboard.
- ★ Wake on LAN maintenance mode must not be configured in the BIOS.
- ★ For 802.1x, ports must be set to unidirectional to transmit pre-authenticated frames.
- ★ Some WiFi adapters support WOL. If using subnet directed broadcast you will need to confirm your WiFi routers are capable of forwarding. Some WiFi routers provide a facility to generate WOL packets. If the vendor claims to support WOL, check they are referring to wireless and not just the physical ports.
- ★ Some Dell systems using 3com 3C905C or 3C920 require NIC registry change described in http://www.myitforum.com/forums/m_99547/tm.htm

2.3 Subnet Directed Broadcasts or Unicast

For WOL to be sent across routers, only Subnet Directed Broadcasts and Unicast are relevant⁵.

Whichever method is adopted, whether on corporate networks or the internet, each requires firewalls and routers to be configured to forward packets on a chosen UDP port number. UDP is required because the target machine is off and therefore cannot use TCP.

1E provide a free **Magic Test** utility to test whether a network is already configured to support these methods. This utility can be used to send a single packet to a remote subnet. A complimentary utility called **Receive From** is used to test if the packet is received. More info on this is provided below.

⁴ Wikipedia has a useful article on ACPI global and sleep states, although this may not be authoritative.

⁵ Multicast is an option but not flexible. It requires a multicast group ID to be assigned and a sufficiently high TTL for the packet to traverse routers to reach its final target. The packet is also sent to unnecessary subnets.

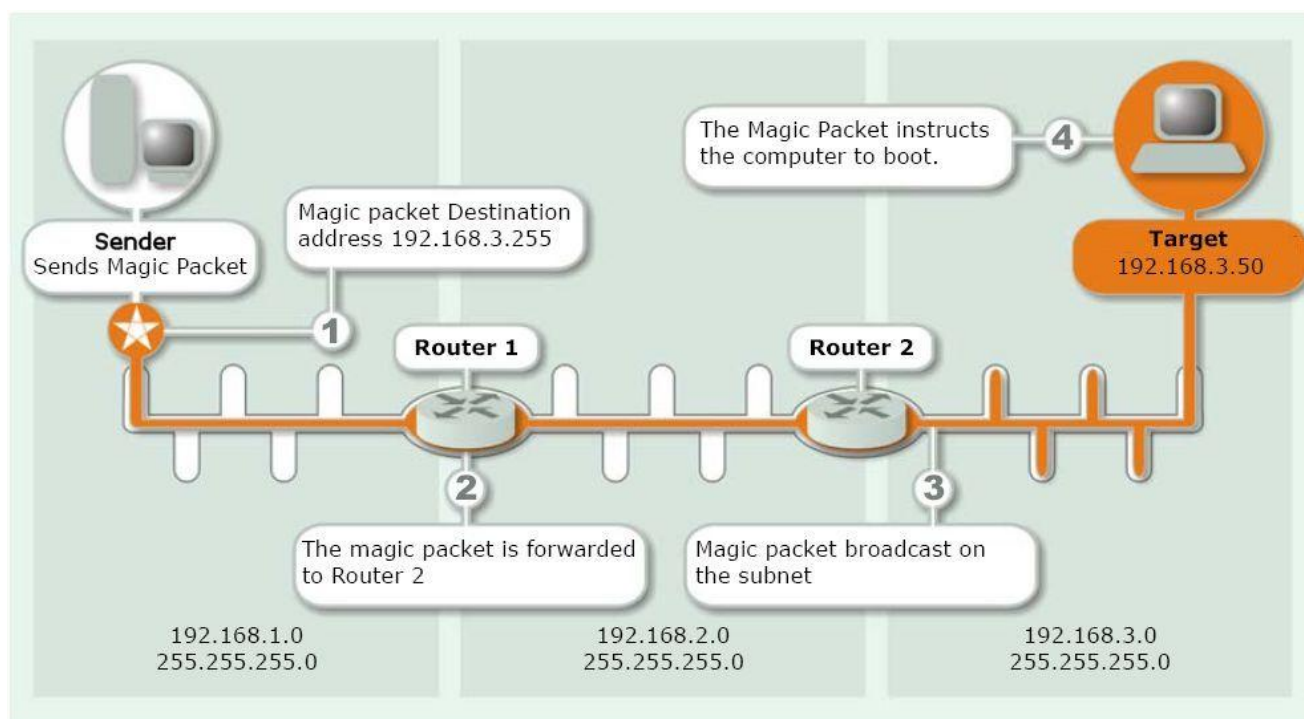
Subnet directed broadcast

This method does not require the IP address of the target machine, it requires only the subnet.

Simple WOL solutions use subnet directed broadcasts which rely on network routers to forward the 'Magic Packet' to the subnet where the target computer resides. All WOL compatible NICs support subnet directed broadcast because it has been around the longest. However, networks are often configured to prevent directed broadcasts because it makes them more open to Denial of Service (DoS) attacks, such as 'Smurf'.

A subnet directed broadcast uses the IP subnet of the target computer so that the UDP packet reaches the local router which then broadcasts to all the computers on the local network. The packet contains the MAC address, therefore provided the computer remains connected to the same subnet with the same network adapter then it should wake even if has changed its IP address. Routers must be configured to forward this type of packet, but to be more secure, routers should be configured to forward broadcasts from a specific sender and use a non-standard port.

As an example, consider a sender situated on subnet 192.168.1.0 and the client on 192.168.3.0, linked by two routers, Router 1 and Router 2. The target computer has an address of 192.168.3.50 therefore the subnet broadcast address is 192.168.3.255. To reach the target the Magic Packet would have to take the following steps, as shown below.



1. The Destination address for the Magic Packet is set to the subnet broadcast address for the target machine: 192.168.3.255
2. The Magic Packet reaches the local default gateway and is forwarded to Router 2 based on the network address portion of the Magic Packet's IP header
3. Router 2 realises that the magic packet is at the right destination network, recognises it as a subnet directed broadcast packet and broadcasts it to the subnet.
4. The target system recognises the frame as a Magic Packet, matches the 16-bit MAC address, and instructs the computer to boot.



Unicast

This method requires the IP address of the target machine.

Unicast sends the UDP wake-up packet directly to the computer using its IP address. Routers will forward the UDP packet the same as any other IP packet until it reaches the target's local router. Although the packet contains the MAC address, the router looks up the IP address in its ARP cache to obtain the MAC address to be able to send the packet directly to the computer.

However, there are several significant problems.

- The IP address must be known and is very likely to have changed
- The ARP cache record may have been cleared if the computer has been switched off longer than the ARP cache's Time to Live (TTL) setting. The default on Cisco equipment is 4 hours. **If the target machine in the above example has been off for more than 4 hours you will be unable to wake it up**
- Older NICs do not support this method, and can have difficulty in some sleep states

Solution

The solution is none of the above methods. To solve the above problems experienced by Subnet directed broadcast and Unicast methods, the most comprehensive WOL solutions such as 1E WakeUp use local agents.



1E WakeUp still needs to know the IP subnet to determine which agent to instruct, and obtains this from the SMS/ConfigMgr or 1E Agility Framework database.

2.4 Power-on Passwords

Laptops and other machines often have software installed or BIOS configured that requires a password to be entered on boot-up before the operating system loads. WOL will power-up these machines but they will remain powered on with the password prompt displayed until a user responds, at which point the operating system will load and the SMS/ConfigMgr advertised program will run, assuming it hasn't expired. Some software or BIOS versions will automatically power off if the password is not entered.

A workaround for this problem when using 1E WakeUp with SMS/ConfigMgr is to **Create a separate Collection and Advertisement** in SMS/ConfigMgr for these systems and include the text "NoWakeUps" in the SMS advertisement name, however this currently also stops the 1E WakeUp policy refresh too.

Alternatively, **disable WOL for these machines**. The downside is if they are switched off then 1E WakeUp success reporting will treat these machines as failed wakeups unless they are excluded from advertisements.

System passwords

BIOS setup passwords can prevent BIOS being configured. Most vendor utilities allow passwords to be provided, however you need to consider the implications if they are supplied as clear text.

Disk encryption and passwords

A computer may be configured to prevent the operating system starting up after it has been switched on or woken up that defeats the purpose of WOL. For example, boot disks may be configured with a password or a security software product, or BitLocker enabled.

Some security products can be configured to be WOL aware, and allow Windows to start without a power-up password for a specific number of times. Details can be found in the vendor product guides.

Some NIC adapters support a password being included in the magic packet, but this is only for the adapter and not passed to the security software or operating system.



2.5 1E Magic Test



This comprises two Wake-On-LAN testing tools, *Magic Test* and *Receive From*. The *Magic Test* tool allows you to send a magic packet to a single machine to test the functioning of Wake-On-LAN hardware. The *Receive From* tool enables you to test whether a particular machine is receiving wake-up packets.

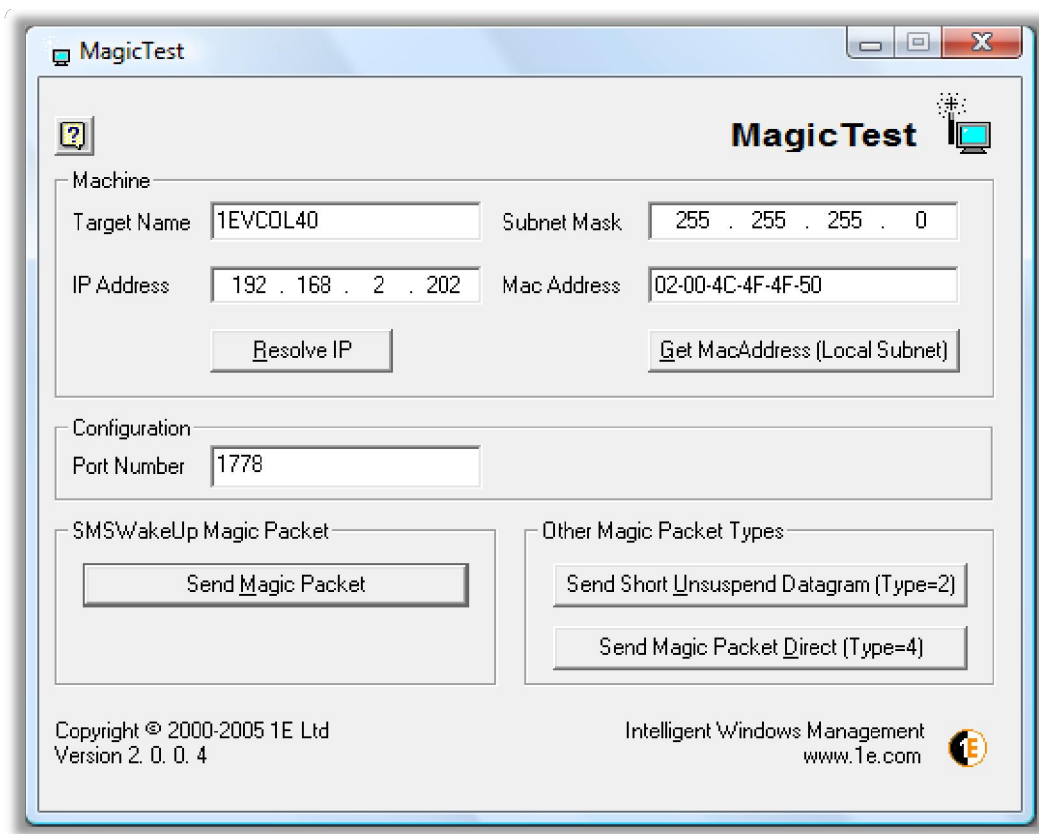
Apart from being able to test a machine is capable of being woken, the utility is useful to determine if the sender has correct firewall settings, and if routers have been configured to allow subnet directed broadcasts to be forwarded, or unicast port enabled. Remember that configuring routers is not required if using 1E WakeUp agents.

The Magic Test Tool

Magic Test works by sending types of Magic Packet explicitly to the destination system to see if the system wakes up, or to see if the system is receiving the Magic Packets at all.

When using **Magictst.exe**, there are three types of Magic Packet which can be sent. These are:

1. **Send Magic Packet** This is a subnet directed broadcast and will fail if directed broadcast is disabled on any intervening routers.
Note: The above method should be used to test for 1E WakeUp compatibility.
2. **Send Short Unsuspend Datagram (Type=2)** This sends an arp packet which will wake the computer from sleep/standby state. This is sent directly to an IP address and is the equivalent of a ping.
3. **Send Magic Packet Direct (Type=4)** This is unicast and will work over routers where directed broadcast is disabled.





1. Make sure both systems are powered on.
2. On the sender system, start the Magic Test utility – `magictst.exe` (shown below)
3. In the 'Target Name' field, fill out the name of the target system.
4. Click on the 'Resolve Name' button. This will automatically complete the 'IP Address' and 'Subnet Mask' fields. If you know the IP information already you can fill in the fields manually.
5. Once the IP Address information is complete – click on the 'Ping for MAC Address' button. This will complete the MAC Address field.

The MAC Address can be resolved providing your router is currently aware of it. The resolution uses ARP, which can only resolve the MAC address if the MAC info is currently in the sender computer or router ARP cache. This means that for the resolution to work the target machine would need to have been recently on as the router ARP cache is normally cleared out frequently.

For testing purposes the MAC address can be entered manually. The resolution issue with Magic Test will not affect 1E WakeUp as 1E WakeUp retrieves the MAC address information directly from SMS/ConfigMgr.

6. If sending through routers or firewalls, select a port number that you know will work for you. This will be the port your network administrator has enabled on the routers to allow subnet directed broadcasts to be forwarded. This is not required for local subnets. **Note:** most network administrators prefer not to open up forwarding ports because of the risk of DoS attacks as described above.
7. If testing sleep/standby, ensure the Windows NIC configuration on the target system has been enabled to allow wakeup.
8. Shutdown the target system, or put to sleep/standby.
9. On the sender system, use one of the Send buttons, which should cause the remote system to restart.

The Receive From Tool

The Receive From diagnostic tool listens for magic packets. This tool can be run on a target system and log all magic packets that are received for that system.

When you run this tool, you will see a command window open similar to the example below, which shows how the utility responds to each type of Magic Packet sent by the Magic Test tool.

A screenshot of a Windows command window titled "E:\MagicTest.v2.3\recvfrom.exe". The window shows the following output:

```
Listening for magic packets on port no 1778
12/09/2008 13:59:45
  broadcast magic packet(hdr) - 02:00:4C:4F:4F:50 from 10.18.2.1 <len=118>
12/09/2008 13:59:46
  short unsuspend(hdr)      - 02:00:4C:4F:4F:50 from 10.18.2.1 <len=28>
12/09/2008 13:59:46
  direct magic packet(hdr)  - 02:00:4C:4F:4F:50 from 10.18.2.1 <len=120>
```



2.6 Windows Power Management Settings

To determine which devices can be managed; which devices are enabled; and enable a device you can use the POWERCFG.EXE utility available on Windows XP and later.

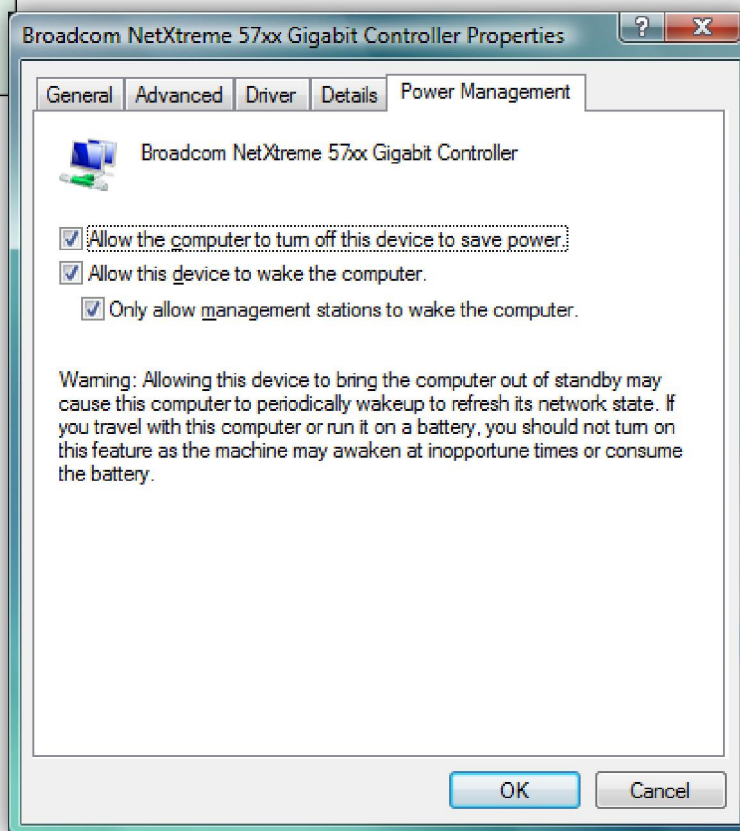
```
POWERCFG.EXE /DEVICEQUERY wake_programmable
POWERCFG.EXE /DEVICEQUERY wake_armed
POWERCFG.EXE /DEVICEENABLEWAKE "<Name>"
```

Windows NIC Power Management tab

To ensure that a computer wakes up from sleep/standby when a network card receives a Wake-on-LAN command, the Windows Power Management settings should all be enabled on the network card properties.

These options are only configurable if you enable "Allow the computer to turn off this device to save power."

The option "Only allow management stations to wake the computer" should be enabled to ensure the NIC will only wake the computer when intended. Leaving this box unchecked configures the system to wake on both Magic Packets and operating system defined programmable patterns, which by default is just about any network activity as discussed below.



The following script will enable these NIC Power Management options.

```
'See disclaimer on page 2
'Script to enable Power Management options for all NICs
On Error Resume next

Set objWMI = GetObject("winMgmts://./root/WMI")
Set objCIMV2 = GetObject("winMgmts://./root/CIMV2")

Set colDevices2 = objCIMV2.ExecQuery("SELECT * FROM Win32_NetworkAdapter where AdapterTypeId=0")

WScript.Echo "Enabling WOL for the following adapters:"

For Each objDevice2 In colDevices2
    WScript.Echo right("000" & objDevice2.Index & " ",5) & objDevice2.MACAddress & " " & objDevice2.Name
    strdevice2 = UCase(objDevice2.PNPDeviceID)

    Set colDevices1 = objWMI.ExecQuery("SELECT * FROM MSPower_DeviceEnable")
    For Each objDevice1 In colDevices1
        strdevice1 = UCase(Left(objDevice1.InstanceName, Len(strdevice2)))
        If StrComp(strdevice1, strdevice2)=0 Then
            objDevice1.Enable = True      'True is bit3 off for PnPCapabilities
            objDevice1.Put_
```



```

        if Err.Number=0 Then WScript.Echo " Allow the computer to turn off this device=" _
                                           & objDevice1.Enable

    End If
Next

Set colDevices1 = objWMI.ExecQuery("SELECT * FROM MSPower_DeviceWakeEnable")
For Each objDevice1 In colDevices1
    strdevice1 = UCase(Left(objDevice1.InstanceName, Len(strdevice2)))
    If StrComp(strdevice1, strdevice2)=0 Then
        objDevice1.Enable = True      'True is bit4 off for PnPCapabilities
        objDevice1.Put_
        if Err.Number=0 Then WScript.Echo " Allow this device to wake the computer=" _
                                           & objDevice1.Enable

    End If
Next

Set colDevices1 = objWMI.ExecQuery("SELECT * FROM MSNdis_DeviceWakeOnMagicPacketOnly")
For Each objDevice1 In colDevices1
    strdevice1 = UCase(Left(objDevice1.InstanceName, Len(strdevice2)))
    If StrComp(strdevice1, strdevice2)=0 Then
        objDevice1.EnableWakeOnMagicPacketOnly = True      'True is bit8 on for PnPCapabilities
        objDevice1.Put_
        if Err.Number=0 Then WScript.Echo " Only allow management stations to wake the computer=" _
                                           & objDevice1.EnableWakeOnMagicPacketOnly

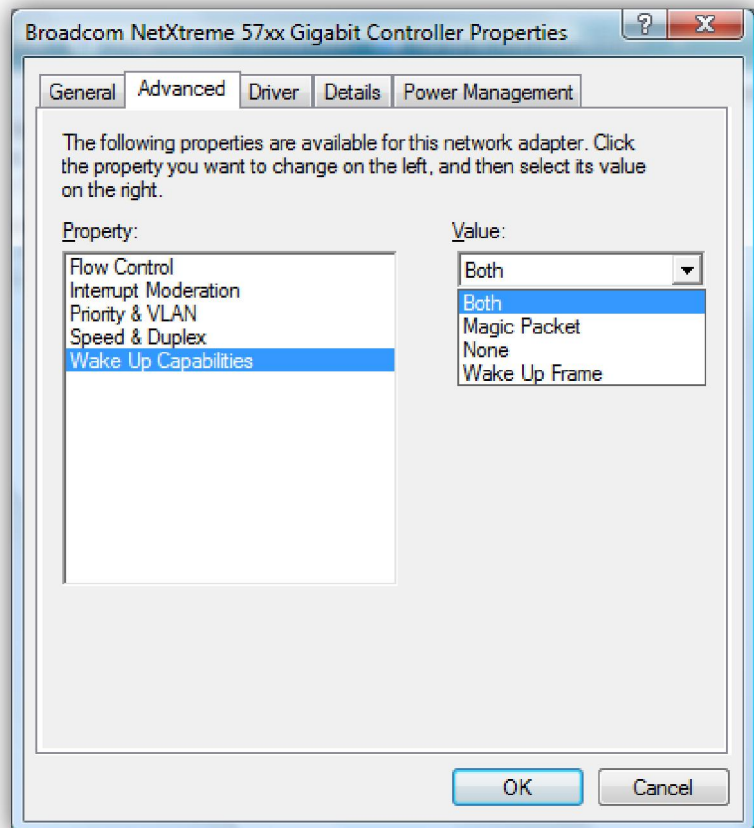
    End If
Next
Next 'bit5 on by default for PnPCapabilities
    
```

Windows NIC Configuration

In addition to the above Windows Power Management settings, there may be vendor specific settings that need to be configured.

Wake Up Frame means support for the [Microsoft NDIS 5 specification](#) where a 3rd party application can specify a programmable pattern to match. By default this will include any network activity such as ping, ARP request and multicast traffic even if not intended for the target workstation. This setting is overridden if the “Only allow management stations to wake the computer” option is enabled.

The method for scripting these options is vendor specific and generally only manageable using WMI if the vendor has WMI software.





It is also possible to modify registry settings under the key

```
HKLM\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002bE10318}
```

As well as vendor specific settings, you can also control the Windows NIC Power Management options by setting the PnPCapabilities value. [KB837058](#) provides some detail. Bits 3, 4 and 8 correspond to the options in the NIC Power Management tab and script above.



1E can assist with these settings for various vendors on an enterprise scale and in an automated manner. Please contact your 1E representative for more information.



3 Dell

3.1 Introduction to Dell Tools

Dell Tools and solutions for managing Dell Precision workstations, OptiPlex desktops, and Latitude laptops are available for download at

http://www.dell.com/content/topics/global.aspx/sitelets/solutions/management/client_software

However, for simple remote BIOS configuration, Dell recommend using SMS/ConfigMgr and Dell OpenManage Client Instrumentation ([OMCI](#)). However, this requires WMI scripting which may be prevented if security lockdown settings prevent such scripts from running.

- **Pros:** Exposes the Dell BIOS to WMI and therefore enables almost any modification to be made by running VB script. It also means SMS hardware inventory can then report upon BIOS settings by extending the SMS_DEF.MOF
- **Cons:** Requires agent software to be run on the client

The Dell Client Configuration Utility ([DCCU](#)) can be used as an alternative to the OMCI client to create stand-alone executables that can output configuration settings ('Get Values') to an XML file and/or configure BIOS settings ('Set Values'), including enabling WOL.

- **Pros:** Leaves no footprint on the client as it optionally deletes itself after running
- **Cons:** An executable file needs to be created for every action you want to perform against the BIOS; meaning heavier network utilization, testing and risk

The Inventory Tool for Dell Updates ([ITDU](#)) allows administrators to determine compliance and deploy the necessary updates for Dell Servers, supporting BIOS versions (not BIOS settings), firmware, drivers, and Dell applications. Updates are deployed using the same SMS 2003 process utilised by ITMU.

Dell Client Manager is a further Dell solution consisting of suite of integrated tools developed by Dell and Symantec (previously Altiris) that uses Altiris Notification Server. Dell Client Manager discovers supported Dell computers and installs the Dell OpenManage Client Instrumentation (OMCI), EnTech SoftOSD, and Dell Client Manager Agent software to these computers. The Dell Client Manager Agent software works as a link between the OMCI and EnTech software and the Altiris Agent. Dell Client Manager can also connect to a target Dell computer directly through WMI and query OMCI for inventory and configuration information and display this information in the Symantec (Altiris) Management Console's Resource Manager, in the Real-Time view.

An overview of the various Dell Client Management editions can be found at

http://www.dell.com/content/topics/global.aspx/sitelets/solutions/management/client_overview



3.2 DELL OpenManage Client Instrumentation

The DELL OpenManage Client Instrumentation (OMCI) agent software can be installed on DELL client systems to expose configuration data from the BIOS, including the WOL status, through WMI. The latest version of OMCI enables Dell client systems to be managed using CIM and Alert Standard Format (ASF) standards.

A Dell whitepaper is available at http://www.dell.com/downloads/global/solutions/omci_info.pdf. There are various scripts included with some further scripts on the Dell web-site; versions of some are provided below.

3.2.1 Installing OMCI

OMCI v7.x can only be installed on DELL systems with SMBIOS version 2.3 or above. (BIOS upgrades can be performed using the DELL Client Configuration Utility described later in this document).

The download is an executable which should be run to extract SETUP.EXE to a specified location. The following command line can then be used to install silently.

```
setup.exe /s /v"/qn REBOOT=ReallySuppress /l %windir%\temp\OMCI.log"
```

1E recommend testing this with delivery using SMS/ConfigMgr as it may restart the WMI service on the client, which may cause the SMS/ConfigMgr client to report a failed installation.

OMCI creates a new WMI namespace root/Dellomci

3.2.2 Some annoying OMCI habits

Chassis Intrusion Alerts

A 'chassis intrusion' alert occurs when the computer system unit has been opened to upgrade or fix hardware at any point in its life. You can momentarily see the alert during Power On Self Test (POST) but it is often missed. A warning is also logged in the Windows event log.

When OMCI is installed, it will popup an alert message if there has been a 'chassis intrusion' each time the OMCI service is restarted until the alert has been acknowledged, and the preferable way to do this is by manually rebooting the computer into BIOS setup, which is not practical for most users.

The alert can only be reset by going into BIOS setup, Security, Intrusion Alert and selecting Acknowledge. The 'Intrusion Alert' option is visible only when there is an alert that needs to be acknowledged. Engineers should be trained to follow this procedure each time they open the system unit.

The alert is not critical and does not cause any problems other than being annoying. The OMCI message is often mistaken as being caused by OMCI. When OMCI is deployed, Helpdesk staff should be trained to re-assure users that new software has recognised the user's computer has previously had a hardware fix and the engineer had not reset the BIOS.

It is possible to turn off 'chassis intrusion' alerts using the script below but that disables a key feature of OMCI. You may not want to do this if this feature is a reason for using OMCI and all you really want to do is reset the original alert.

```
'See disclaimer on page 2
'Script to disable Dell Chassis Intrusion Detection. Requires Dell OMCI.

Option Explicit
On Error Resume Next

'*** Declare variables
Dim strNamespace, strComputerName, strClassName, strKeyValue, strPropName, strPropValue
Dim objInstance

'*** Initialize variables
```




```

strNameSpace      = "root/Dellomci"
strComputerName   = "."
strClassName      = "Dell_SMBIOSSettings"
strKeyValue       = "0"
strPropName       = "ChassisIntrusionStatus"

'*** Retrieve the instance of Dell_SMBIOSSettings class, there should be only one
Set objInstance = GetObject("winMgmts:{impersonationLevel=impersonate}://" & _
    strComputerName & "/" & strNameSpace & ":" & strClassName & "=" & _
    Chr(34) & strKeyValue & Chr(34))

strPropValue = objInstance.Properties_.Item(strPropName).Value

'*** Clear the value of ChassisIntrusionStatus only if it = 3
'    A value of 3 = "Detected"
'    Setting this value to 5 (Clear) will cause the ChassisIntrusionStatus
'    property to really be reset to 4 (Not Detected).

If strPropValue = 3 then

    '*** Set the new value for the property and save the instance
    objInstance.Properties_.Item(strPropName).Value = 5
    objInstance.Put_

    '*** If any errors occurred, let the user know
    If Err.Number <> 0 Then
        WScript.Echo "Clearing the chassis intrusion alert failed."
    End If
End If

Set objInstance = Nothing
If Err.Number = 424 Then WScript.Echo strNameSpace & " not registered."
WScript.Quit(Err.Number)
    
```

Dell also provides a script that turns off all messages and popups. This option should be considered with care, depending on your reasons for installing OMCI.

Disk Space Alerts

If users complain they receive popup messages saying "Warning event notification, disk free space has dropped below the minimal threshold ..." then you can tweak the registry value for

```
[HKEY_LOCAL_MACHINE\SOFTWARE\DELL\OpenManage\Client\SysInfo\HDDThresholdValue]
```

This is a DWord value which can be changed to 0 to turn off the threshold checks.

3.2.3 OMCI Script to enable WOL

DELL OMCI can also use WMI scripting to enable WOL. A VBScript sample is available in the DELL OMCI User Guide to enable WOL on all NICs (i.e. setting the WakeupOnLAN attribute to 6). This script is reproduced below.

```

'See disclaimer on page 2
'Script to enable WOL on Dell computers. Requires Dell OMCI.

Option Explicit
On Error Resume Next

'*** Declare variables
Dim strNameSpace, strComputerName, strClassName, strKeyValue, strPropName, strPropValue
Dim objInstance
    
```



```

'*** Initialize variables
strNameSpace      = "root/Dellomci"
strComputerName   = "."
strClassName      = "Dell_SMBIOSSettings"
strKeyValue       = "0"
strPropName       = "wakeupOnLan"

'*** Retrieve the instance of Dell_SMBIOSSettings class
Set objInstance = GetObject("winMgmts:{impersonationLevel=impersonate}://" & _
    strComputerName & "/" & strNameSpace & ":" & strClassName & "=" & _
    Chr(34) & strKeyValue & Chr(34))

strPropValue = objInstance.Properties_.Item(strPropName).Value

'*** Set the value of wakeupOnLan only if it is not already '6'
'    A value of 6 = "Enable for all NICs"
If strPropValue <> 6 then

    '*** Set the new value for the property and save the instance
    objInstance.Properties_.Item(strPropName).Value = 6
    objInstance.Put_

    '*** If any errors occurred, let the user know
    If Err.Number <> 0 Then
        WScript.Echo "Enabling WakeUp On Lan failed."
    End If
End If

Set objInstance = Nothing
If Err.Number = 424 Then WScript.Echo strNameSpace & " not registered."
WScript.Quit(Err.Number)

```

3.2.4 Reporting WOL configuration in SMS Hardware Inventory

Once the OMCI client software has been installed on clients, the WOL properties can be reported through SMS Hardware Inventory by adding the following Reporting Class definition to SMS_DEF.MOF.

```

//=====
// Define the DELL SMBIOSSettings reporting class
//=====

[SMS_Report(TRUE),
 SMS_Group_Name("Dell_SMBIOS_Settings"),
 ResID(7500), ResDLL("dellwmi.dll"),
 SMS_Class_ID("Dell|SMBIOSSettings|1.0"),
 Namespace("root\\\\"DellOMCI")]

class Dell_SMBIOSSettings : SMS_Class_Template
{
    [SMS_Report(TRUE),Key] uint32 DellInstanceID;
    [SMS_Report(TRUE)] sint32 WakeupOnLAN;
    [SMS_Report(TRUE)] sint32 WakeupOnLANMethod;
};

```

As the OMCI installation creates the data classes on the client (in the DELLOMCI namespace), there is no need to do anything further on the client to enable SMS to report this data.



The WakeupOnLAN attribute will have one of the following values.

Value	Description
1	Other
2	Unsupported
3	Disabled
4	Enabled for add-in NIC
5	Enabled for onboard NIC
6	Enabled for all NICs
7	Enabled with boot to NIC
8	LAN or WLAN
9	WLAN only

The WakeupOnLANMethod attribute will have one of the following values. This value is for reporting only and is not manageable.

Value	Description
1	Other
2	Unsupported
3	Magic Packet

The above tables may be used in custom web reports to translate the values returned in the inventory.

3.3 DELL Client Configuration Utility (DCCU)

DCCU v3.0 was released in October 2008. The previous version was V1.2.1.

<http://support.dell.com/support/downloads/download.aspx?releaseid=R200703&deviceid=19801&fileid=278576>

This utility can be downloaded from the DELL website and the Console installed on an administrator's workstation. The help file contains installation and usage instructions. Once installed, the Console is used to create a stand-alone executable (called a 'package'). This executable must then be run on the client, for example using SMS/ConfigMgr. When run, it temporarily loads a OMCI which means DCCU theoretically supports the same WMI properties as OMCI.

The v3 console is similar to the previous v1.2.1 release except it places a shortcut icon on your desktop and in the system tray; the user interface has been improved. The principle enhancement is packages now support command line options allowing for scripting logic; also the package no longer self-deletes.

The minimum requirements for installing and using the DCCU v3.0 are:

- Windows XP SP2 or later with .NET framework 2.0 installed
- Microsoft Internet Explorer® Version 7.0 or later
- Available disk space 20 MB
- Memory 64 MB

3.3.1 Creating a DCCU Settings Package

To enable the BIOS functionality for Wake On LAN it is first necessary to create an executable package using the Console which has to be installed and run on an admin workstation. The screenshot below indicates how to configure the WOL option.



Dell Client Configuration Utility - Powered by Altiris - Windows Internet Explorer

http://localhost:1000/

Dell Client Configuration Utility - Powered by Altiris

Version 3.0.1213 **DELL**

BIOS Update

BIOS Inventory

BIOS Settings

Select the properties you want to configure on client systems. Click 'Create BIOS Settings Package' and save the file. Click 'Import Collected BIOS Inventory' link to import and view collected inventory data. You can modify inventory data in grid below to create new bios settings package.

Select task output XML file (TaskResult.xml): [Import Collected BIOS Inventory](#)

Data Class	Property	Value
☐ Power and Performance Management	LowPowerS5	Unsupported
☐ Power and Performance Management	MultiCore	Unsupported
☐ Power and Performance Management	Power management settings	Unsupported
☐ Power and Performance Management	Single Core Turbo Mode	Unsupported
☐ Power and Performance Management	Speed Step	Unsupported
☐ Power and Performance Management	Suspend Mode	Unsupported
☐ Power and Performance Management	UART Power Down	Unsupported
☒ Power and Performance Management	Wakeup on LAN	Unsupported Disabled Enabled for add-in NIC Enabled for on-board NIC Enabled for all NICs Enabled with boot to NIC LAN or WLAN Unsupported
☐ Security	Chassis intrusion	Unsupported
☐ Security	Chassis intrusion status	Unsupported
☐ Security	No execute	Unsupported
☐ Security	Password Bypass	Unsupported
☐ Security	Trusted Platform Module	Unsupported
☐ Security	Trusted Platform Module Activation	Unsupported

The BIOS password below required by newer computers with a BIOS setup password established.

BIOS password:

After running:

Time-out period before restart: minutes.

[Create BIOS Settings Package](#)

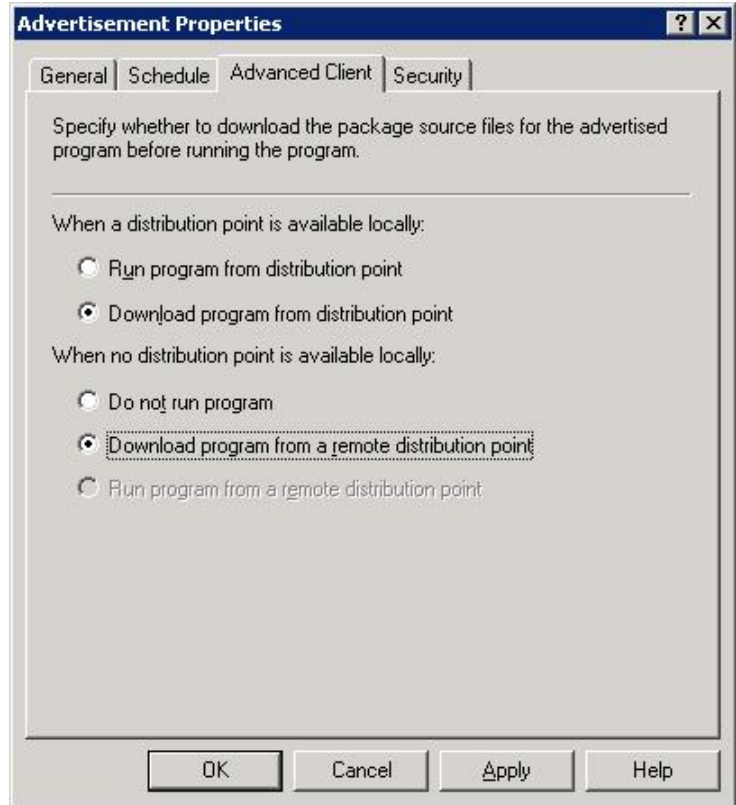
The 'Create BIOS Settings Package' link is then used to create the executable that can be deployed using SMS/ConfigMgr or other method.



It is necessary for SMS/ConfigMgr to download the package into its cache and run from there. If using 1E's Nomad Branch with SMS, then it will download and run from its cache.

During execution, a number of temporary files and folders are created in the same folder as well as the TaskResult files.

This means the package must be run with administrative access.



A v3 settings package also provides the option to shutdown or restart the computer after applying the settings. However, with SMS/ConfigMgr these options should not be used and the SMS/ConfigMgr program options should be used instead.

By default, the v3 settings package is saved as SETTINGS.EXE, although this can be renamed later.

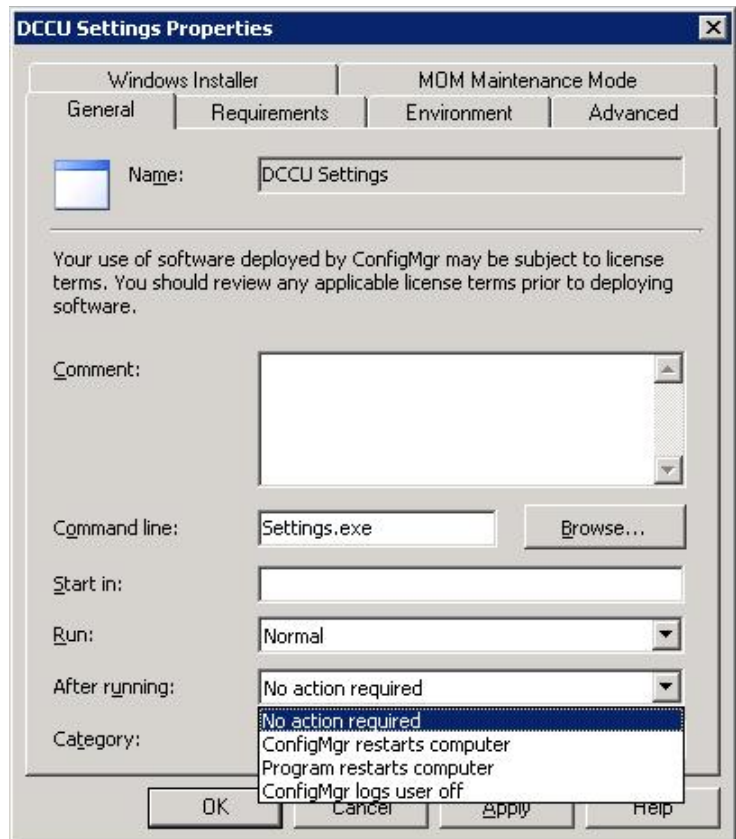
As previously stated, it is possible to manage one or more settings using a command line. The syntax is:

```
settings.exe -<property.name>:<value>
```

For example:

```
settings.exe -PWR.WakeupOnLAN:6
```

Details of property.name options can be found in the template BIOSInventory.xml file.

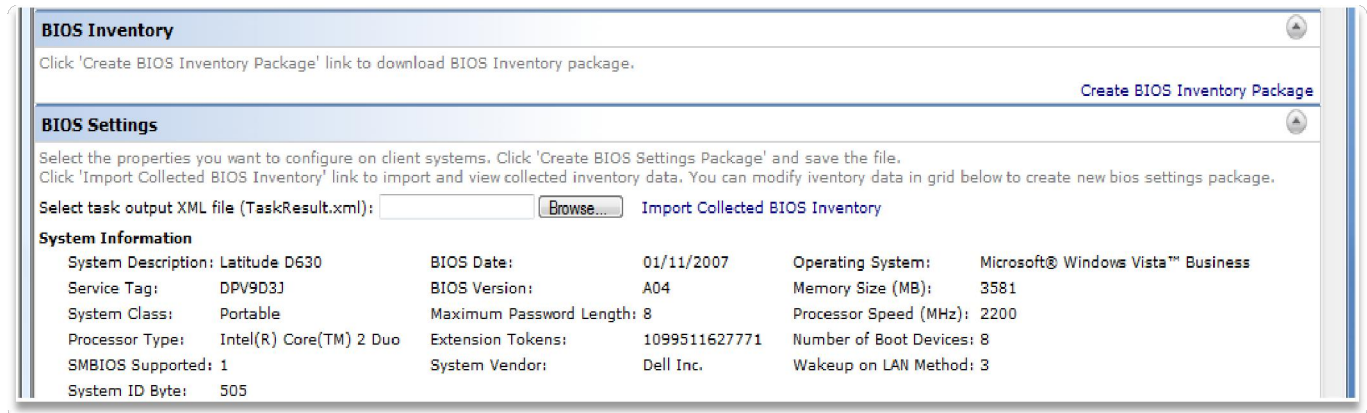




3.3.2 Creating a DCCU Inventory Package

DCCU provides the ability to create an inventory package to report BIOS settings. By default the DCCU v3 inventory package is saved as INVENTORY.EXE, although this can be renamed later. The report is produced in a xml file which can be imported into the console. There is no method of centralised reporting other than Dell Client Manager (Altiris).

The inventory package reports all properties specified in the template BIOSInventory.xml file. Although not recommended, the template can be edited to produce different versions of the inventory package, however please ensure the SS.BIOSDate property is not deleted otherwise the TaskResult.xml file will not import into the Console.



The following represent properties displayed under the 'System Information' section in the Console when importing the results of an inventory package.

```
<property name="PWR.WakeupOnLANMethod" />
<property name="SS.BIOSDate" />
<property name="SS.BIOSVersion" />
<property name="SS.ServiceTag" />
<property name="SS.SystemDescription" />
<property name="SS.SystemVendor" />
<property name="SS.ProcessorType" />
<property name="SS.ProcessorSpeed" />
<property name="SS.SystemClass" />
<property name="SS.ExtensionTokens"/>
<property name="SS.NumberOfBootDevices"/>
<property name="Configuration.MaximumPasswordLength" />
<property name="Configuration.SMBIOSSupported" />
<property name="Configuration.SystemIDByte" />
<property name="Memory.Size" />
<property name="OperatingSystem.Caption" />
```

There are a number of inventory properties that are reported by the default template BIOSInventory.xml file, but not viewable in the current version of the Console, for example all the 'DCCU specific OMCA Operating System' properties. This is probably because they are non-editable and therefore cannot be used in a settings package.

3.3.3 Running a DCCU Package

When a DCCU package is run on a client, it creates the following result files in the same folder as the executable:

- TaskResult.xml
- TaskResult.nse



This is different to v1.2.1 which created a file called DCCUResults.xml plus a file appended with _FAIL or _SUCCESS depending on the success or failure of running the package. The .nse file created by v3 is only used by the Dell Client Manager (Altiris).

Below shows the contents of the TaskResults.xml for a settings package that sets the WakeupOnLAN option to 6. Result values are the same as described in the OMCI section 3.2.4 above. Result values for other properties can be found in the schema.xml file.

```
<root>
  <command name="Set">
    <property name="PWR.WakeupOnLAN" value="6" errorcode="0x0"/>
  </command>
  <command name="Set">
  </command>
  <command name="biossettings">
    <property name="task" value="Succeeded." errorcode="0x0"/>
  </command>
</root>
```

The output of an inventory package has a similar format. Below shows the contents of the TaskResults.xml that queries the WakeupOnLAN. The TaskResults.xml file may be imported into DCCU Console to view the results or as a template for creating a settings package, but only if the SS.BIOSDate property has also been queried.

```
<root>
  <command name="Inventory">
    <property name="PWR.WakeupOnLAN" value="6" errorcode="0x0"/>
    <property name="SS.BIOSDate" value="2007-11-01T00:00:00" errorcode="0x0"/>
  </command>
  <command name="inventory">
    <property name="task" value="Succeeded." errorcode="0x0"/>
  </command>
</root>
```

A script would need to be developed to convert the data from xml into MIF file format on the client so that SMS/ConfigMgr can include the data in Hardware Inventory. Optionally custom WMI classes could be created but instead it would be preferable to install and use OMCI as described in section 3.2 above.



4 Fujitsu

The following is an extract from the DeskView 10 User Manual, released August 2007.

DeskView is software that runs under Altiris® Notification Server™ software. Using Notification Server, you can use software delivery tasks to remotely install software agents on client computers. These agents send inventory data about client computers back to the Notification Server. This inventory data can be viewed in reports and Web-based consoles. You can also initiate computer management functions from Notification Server. You can manage computers singly or in groups by using collections.

[DeskView](#) has an add-on component called [DeskView SMS](#), which extends the SMS hardware inventory. This component depends on DeskView Client.

4.1 DeskView Instant - BIOS Management

This is a pair of free standalone utilities that can be found by searching for 'DeskView Instant - BIOS Management'. The download page on the Fujitsu web-site contains the following information, and a list of supported Fujitsu computers.

BIOS Settings (BIOSSET.exe)

- Change selected BIOS settings
- Set the BIOS password
- Change the Boot order

With BiosSettings you can change the BIOS Settings of different systems with one command.

BiosSettings does not support all Fujitsu workstations and notebooks. For details of supported functions on dedicated system please look to http://www.fujitsu-siemens.com/solutions/it_infrastructure_solutions/manageability/featurefinder.html.

```

BIOSSet Version 6.22
Copyright (C) 2005-2008 Fujitsu Siemens Computers

DeskView BIOS Settings - Change BIOS Settings

BIOSSET /NEWPWD=[<password>] [/PWD=<password>] [/Q]
BIOSSET <setting>=<state> [/PWD=<password>] [/Q]
BIOSSET /DEFAULT [/PWD=<password>] [/Q]
BIOSSET /BOOTORDER=<nr><device>{,<nr><device>...} [/PWD=<password>] [/Q]
BIOSSet /E

<password> : BIOS Settings Password (Allowed characters are A-Z and 0-9).
<setting>  : See allowed 'List of Settings' below.
<state>    : ON (switch setting on) | OFF (switch setting off).
<nr>       : Order inside the boot sequence (values from 1 to 5).
<device>   : Device in Bootorder.
              (F=Floppy, HDD=Harddisk, CD=CD-ROM,
              LAN=Netzwerk, LEG=Legacy Device)

/NEWPWD    : Change Password. <password> is the new Setup Password..
/PWD       : Current Setup Password; Is needed, when a setup password is set.
/DEFAULT   : Sets BIOS to default values (depending on Motherboard),
              disables BOOTORDER command till next reboot.
/BOOTORDER : Sets the boot order, the abbreviation is /BO.
  
```



```
/Q      : Quiet mode.
/E      : Display possible values of ERRORLEVEL.
```

List of Settings (<setting>):

```
/DC      : Activate/Deactivate DisketteController.
/USB     : Activate/Deactivate USB Host Controller.
/RB      : Activate/Deactivate Boot from remote (e.g. PXE, BOOTP).
/FW      : Activate/Deactivate Flashing the BIOS.
/WOL     : Activate/Deactivate Wake On LAN.
/AC      : Activate/Deactivate Audio Controller.
/HT      : Activate/Deactivate Hyperthreading.
/IR      : Activate/Deactivate Infrared Port.
/BT      : Activate/Deactivate Bluetooth.
/WLAN    : Activate/Deactivate Wirelesslan.
```

The new settings will become active with the next reboot.

Examples:

```
BIOSSET /PWD=mypwd /NEWPWD=    Clear password. Old password was "mypwd".
BIOSSET /WOL=ON /PWD=xy        Activates Wake On LAN.
BIOSSET /DEFAULT /PWD=1234     Set BIOS Settings to default values.
BIOSSET /BOOTORDER=1F,2HDD,5LAN Floppy is first boot device, Harddisk second
                                device and LAN the 5th device.
```

DeskFlash (DSKFLASH.exe)

This utility is able to:

- Update the BIOS
- Update BIOS settings
- Archive the BIOS and BIOS settings
- Update installed processor microcode patches

Appropriate Bios Update Files (BUP) can be created from the Flash-BIOS section of each system

```
DskFlash.exe, Version 6.22
Copyright (C) 2005-2007 Fujitsu Siemens Computers

DeskFlash - Update System BIOS and Settings

DskFlash /UPD [/WD=<dir>] [/LF[=<log>]] [/S] [/W] [/O=<file>|<dospat> ]
               [/NRB|/ARB|/FRB] [/OV]
DskFlash /AR  [/WD=<dir>] [/LF[=<log>]] [/S] [/W] [/O=<file>|<pattern>]
               [/OV]
DskFlash /NVU [/WD=<dir>] [/LF[=<log>]] [/S] [/W] [/O=<file>|<dospat> ]
               [/NRB|/ARB|/FRB] [/AFU]
DskFlash /MCU [/WD=<dir>] [/LF[=<log>]] [/S] [/W] [/NRB|/ARB|/FRB]
DskFlash /?
DskFlash /E

/UPD      : Update system BIOS, NVRAM settings and processor micro codes
/AR       : Archive BIOS and NVRAM settings.
/NVU      : Update NVRAM settings
/MCU      : Update processor micro codes
/AFU      : Allow DeskFlash to perform a full update to complete the
            selected action.
/ARB      : Allow DeskFlash to reboot the system if required.
```



```
/NRB      : Do not allow DeskFlash to reboot the system.
/WD       : Set the current working directory for loading and saving files
           and for storing the logfile too.
/O        : Name the object file or file pattern for loading and saving.
/S        : Hide control dialog and display warning dialog.
/W        : Hide warning dialog too.
/LF       : Enable logfile output and name the logfile.
/FRB      : Force DeskFlash to reboot the system after finishing the job.
/OV       : Allow DeskFlash to overwrite a current BIOS or an existing file.
/E        : Show errorcodes
/?        : Show help
```

```
<dospat>  : File specifier with wildcards, e.g. D1332*.bup
<file>    : File name in the current working directory, e.g. D1332_00.bup
<log>     : Name or path of the logfile.
<pattern> : Archive pattern with special placeholders
```

In <pattern> and <log> the following placeholders can be used

```
#system#  = BIOS ID of the system, e.g. D1332 (only in <pattern>)
#name#    = Network name of the system
#domain#  = Network domain (NT only)
#date#    = Current date
#time#    = Current time in the format HHMMSS
#no#      = Automatic created sequence number
```

```
Examples: DskFlash /UPD /WD="c:\my work folder" /LF /O=D1332*.BUP /FRB
          DskFlash /AR /O="MyArch_#system#_#date#.bup" /S /W
          DskFlash /MCU /S /W /FRB /LF=myMCU.log
```

The following parameter aliases are supported

```
/?        /help, /h
/UPD      /update
/NVU      /nvramupdate
/WD       /workingdirectory
/S        /silent
/W        /warningoff
/LF       /logfile
/FRB      /forcereboot
/ARB      /allowreboot
/NRB      /noreboot
/AFU      /allowfullupdate
/OV       /overwrite
```



5 HP

HP provides a number of tools based on the HP Client Management Interface ([CMI](#)) WMI agent. The exception is HP System Software Manager ([SSM](#)) which includes a bundled utility called **BiosConfigUtility.exe** that modifies BIOS settings through a text-based file format, which can be used independently of SSM. HP says a future version of HP SSM will leverage HP CMI on 32-bit and 64-bit platforms.

If you already have SMS/ConfigMgr then HP recommends using HP SSM for managing HP drivers and software updates, although if you only want to manage BIOS settings then it is simpler to use HP CMI or HP SSM's BiosConfigUtility.

HP BIOS Configuration for ProtectTools version 2.0 utilizes HP CMI.

HP Client Manager ([HPCM](#)) uses HP CMI. HP Client Manager is based on Altiris Notification Server 6.0 as an alternative to Microsoft's SMS/ConfigMgr, and provides the ability to obtain hardware inventory information, monitor system health status, run diagnostic tests, remotely install drivers and manage BIOS settings.

HP also provides [HP OpenView PC Configuration Management](#), based on Radia.

5.1 HP Client Management Interface (CMI)

This is a WMI agent that allows reporting and scripting using an appropriate systems management solution such as SMS/ConfigMgr, or it can be used standalone.

HP provide a comprehensive white paper at <http://www.hp.com/go/hpcm>

CMI is downloadable as a HP SoftPaq and available at the above link. It creates a new WMI namespace called root/HP/InstrumentedBIOS with several classes.

To install CMI silently, expand the SoftPaq and edit the setup.ini file using CmdLine=/s

Setup installs in %ProgramFiles%\Hewlett-Packard\HP Client Management Interface

This folder contains a copy of the whitepaper and three Windows Script files (ChangeSetting, ChangeSetupPassword and EnumSettings). There are additional scripts listed in the whitepaper.

However, all that is really necessary is to extract and copy the two executables to a suitable location on the local computer and install using:

```
hpqBIOS.exe /install
hpPwdCtl.exe /install
```

The HP CMI Password Control utility, hpPwdCtl is described in the white paper.

hpqBIOS and hpPwdCtl are uninstalled using /uninstall, and optionally /silent. This means the agent can be removed after use if necessary.

```
Usage: ChangeSetting.wsf /setting:value /value:value [computers1 computers2...]
```

Options:

```
setting    : A specific setting to modify. If a particular setting
              contains spaces, be sure to enclose the entire argument in
              quotation marks.
value      : The new setting value. If a particular value contains
              spaces, be sure to enclose the entire argument in quotation
              marks.
computers  : An optional list of computers to query specified by name
              or IP address, otherwise the local system is used. The dot
              nomenclature can also be used to include the local computer in
              the computer list.
```



For example, to enable Wake on LAN use the command:

```
ChangeSetting.wsf /setting:"S5 wake on LAN" /value:Enable
```

The whitepaper provides sufficient detail about the classes to enable you to extend the SMS/ConfigMgr inventory to report BIOS information, but no examples.

5.2 HP SSM BiosConfigUtility

HP Systems Software Manager (SSM) can be downloaded as a SoftPaq from <http://www.hp.com/go/SSM>, which includes the BIOS configuration utility. If you already have SMS/ConfigMgr installed and also wish to manage HP drivers and software updates, then it is recommended to install and use SSM.

BiosConfigUtility.exe is used to capture settings from a reference machine, and deploy to similar target machines. It is possible to edit the capture file to limit the specific values such as "S5 Wake on LAN".

```
Hewlett-Packard BIOS Configuration Utility
Copyright (c) 2005 - 2006, Hewlett-Packard Development Company L.P.

Usage:

BiosConfigUtility.EXE {options}

where the valid options are:

/GetConfig:"filename" - Gets the configuration data.
/SetConfig:"filename" - Modify the system BIOS configuration.
                        - Accepts only RESPET formatted files.
/Format:REPSET        - Specifies the GETCONFIG output format.
                        - /FORMAT:REPSET is the default.
/? or /Help           - Display this help message.
/cspwd:"pwd" or
/CurSetupPassword:"pwd" - Current BIOS Setup Password.
                        - Provide only if needed for /SETCONFIG
                        or if changing the password with
                        /NewSetupPassword
                        - Can specify multiple current passwords.
/nspwd:"pwd" or
/NewSetupPassword:"pwd" - New BIOS Setup Password.
                        - Used to modify the password.
                        - To remove the password use /NewSetupPassword:""

NOTE: BIOS passwords are converted from ASCII to English keyboard
      scan codes. If a character does not map directly to a scan
      code, the password is ignored.

valid 'characters' are mapped to keyboard keys as follows:

` 1 2 3 4 5 6 7 8 9 0 - =
  q w e r t y u i o p [ ] \ <KEYPAD 7> <KEYPAD 8> <KEYPAD 9> <KEYPAD *>
  a s d f g h j k l ; ' <KEYPAD 4> <KEYPAD 5> <KEYPAD 6> <KEYPAD ->
  z x c v b n m , . <KEYPAD 1> <KEYPAD 2> <KEYPAD 3> <KEYPAD +>
    <SPACE BAR> <KEYPAD 0> <KEYPAD .>

valid 'SHIFT+characters' are mapped to keyboard keys as follows:

~ ! @ # $ % ^ & * ( ) _ +
```



```
Q W E R T Y U I O P { } |
A S D F G H J K L ; '
Z X C V B N M <LT> <GT>
<SHIFT SPACE BAR>
```

Example BIOS set script

```
BiosConfigUtility.exe /SetConfig:"HP-DC7600.TXT" /cspwd:"P@ssw0rd"
```

Example BIOS set file to enable Wake-on-LAN on a HP DC7600

```
English
Boot Order
    Network Controller
    Hard Drive
    ATAPI CD-ROM Drive
    USB device Disabled
    Diskette Drive
    Multibay Device (except hard drive)
    PnP Device #2
    PnP Device #3
    PnP Device #4
    PnP Device #5
    PnP Device #6
    PnP Device #7
    PnP Device #8
    PnP Device #9
    PnP Device #10
    PnP Device #11
Num Lock State at Power-On
    *Off
    On
S5 wake on LAN
    *Enable
    Disable
```

5.3 HP System Software Manager (SSM)

The latest version of HP Systems Software Manager can be downloaded as a SoftPaq from <http://www.hp.com/go/SSM>, which includes the BIOS configuration utility. The details below refer to version 2.00 Rev D (SoftPaq SP32605).

HP SSM leverages the Inventory Tool for Custom Updates (ITCU) and the Custom Update Publishing Tool (CUPT) for SMS 2003 R2. HP provides a Client Catalogue for SMS 2003 R2 which contains software driver and patch information for desktops, notebooks, and workstations. These drivers and patches are stored in a HP SSM File-store and managed using CUPT and ITCU.

The readme for SSM contains a list of supported HP computer models.

Further detail is found in the HP White Paper "HP Client Catalog for SMS Technical White Paper"

http://h20331.www2.hp.com/Hpsub/downloads/HP_Client_Catalog_for_SMS_Technical_Whitepaper_Rev3-NC.pdf

Configuration of HP-SSM is not complicated, and requires selection of the synchronization and pre-production test clients and the creation of SSM packages and programs, all of which are subject to operational procedures. The following two sections are [cut+paste] extracts from "HP Client Catalog for SMS Technical White Paper".



How to deploy HP updates using HP SSM with Microsoft SMS

SMS administrators need to mindfully distribute software updates to clients by creating packages and notifications. One way to maximize the software update automation process is to use HP System Software Manager (SSM) combining with Microsoft SMS.

HP SSM is a free utility that helps streamline the mass deployment of system software updates to client PCs. SSM reduces the complexity of system software management by delivering the following capabilities:

- Deploying system software updates (for drivers and BIOS, for example) from a centralized file store to multiple client PCs—simultaneously and automatically.
- Deploying customer-created update packages.
- Enforcing BIOS configurations and passwords.
- Logging the changes made to each computer.

How to Combine Microsoft SMS and HP SSM for the Greatest Benefit

- Download HP SSM from <http://www.hp.com/go/SSM>
- Configure a network file share as the file store for SSM. *(For SIM, this will be the SMS Distribution Points.)*
- Deploy SSM to clients and configure SSM to run on clients with the configured file store on a scheduled basis using SMS.
- Download HP updates from the HP ftp site to the SSM file store. *(For SIM, the package source will be updated manually.)*
- Let SSM run on the clients and automatically figure out what updates the client need and install the updates needed.
- Import the HP Client Catalog for SMS to CUPT and publish HP updates in the catalog to SMS.

View the compliancy in SMS after the custom update scan process and hardware inventory cycle run on clients. Since you let SSM install HP updates, you do not need to distribute the same updates using SMS and should not do so. You only take advantage of the SMS custom update process to scan for compliancy here.



6 IBM & Lenovo

IBM workstation products are now entirely branded Lenovo.

Unfortunately, there is very limited support and no single solution for remote BIOS management of Lenovo desktops and/or notebooks. 1E recommend Lenovo users to contact their vendor and request the development of a free Windows based utility capable of supporting the full range of Lenovo models.

IBM's recommendation is to use [IBM Director](#) and the [Remote Deployment Manager](#) (RDM) extension, and deploys agents similar to SMS/ConfigMgr. However this must be purchased from IBM and provides many more management features for servers and workstations, and does not support BIOS configurations for a wide range of models.

IBM also provides the [System Installation Tool Kit](#) which must be purchased from IBM, which includes LANClient Control Manager (LCCM) for unattended installations of Win32 operating systems.

RDM and LCCM include the **SRCMOS** utility which may be downloaded separately for free. This manages some BIOS settings on a limited range of models, and is also known as the 'BIOS Settings Capture/Playback Utility'. This utility should be used with care as it fairly inflexible and changes all settings.

If you search for SRCMOS you will find the DOS boot floppy version (also supports USB memory and CD-RW) which is therefore not automatic, and of no use for remote management. It is only suitable for a trained engineer to use to copy configurations from one machine to the same models.

There is a less widely available Windows versions of SRCMOS for which there is little information, and appears to be available under different names, and sometimes called **Bios Settings Windows**. If you search for 'Windows version of SRCMOS' you should find [Version 1.04](#) that was released in April 2008 and supports the following ThinkPad models:

- ThinkPad R60, R60e, R61, R61e, R61i
- ThinkPad T60, T60p, T61, T61p
- ThinkPad X60 , X60s , X61, X61s
- ThinkPad X60 Tablet, X61 Tablet (Supports Vista and XP Tablet Edition 2005 only)
- ThinkPad X300
- ThinkPad Z61e, Z61m, Z61p, Z61t
- ThinkPad Reserve Edition

Some ThinkPad models require additional hardware in order to support WOL, as described in [Matrix that lists hardware required to enable WOL for certain ThinkPads \(ThinkPad 380Z, 390/E, 560Z, 600, 770, 1720\)](#).