

Windows Server 2008 R2 on HP Integrity Servers Installation Guide



© Copyright 2011 Hewlett-Packard Development Company, L.P.

Legal Notices

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Intel and Itanium are trademarks of Intel Corporation in the U.S. and other countries.

Java is a U.S. trademark of Sun Microsystems, Inc.

UNIX is a registered trademark of The Open Group.

Table of Contents

About This Document.....	9
Intended Audience.....	9
New and Changed Information in This Edition.....	9
Document Organization.....	9
Typographic Conventions.....	10
Related Information.....	10
Publishing History.....	11
HP Encourages Your Comments.....	11
 1 Preparing for Installation.....	 13
Task 1: Determine Current System Status.....	13
Task 2: Verify Hardware Compatibility.....	13
Ensure Brand Similarity Among Fibre Channel Host Bus Adapters (HBAs) in Multipath I/O (MPIO) Environments.....	13
Task 3: Back Up Existing Data.....	14
Task 4: Choose an Installation Environment.....	14
Using Windows Server 2008 R2 OS Media (Provided by Microsoft) + HP Smart Setup + Smart Update Media.....	15
Using HP Reinstallation Media.....	15
Task 5: Locate Your Microsoft Certificate of Authenticity (with Product Key).....	15
Task 6: Set Up an Installation Method.....	19
Set Up a Headless Console.....	19
Set Up a Headless Console Using a Null Modem Cable.....	20
Set up a Headless Console Using a LAN.....	20
Set Up a Headless Console Using a Remote Serial Console.....	20
Set Up a GUI Console.....	20
Set Up an Integrated Remote Console.....	22
Set Up a vMedia Drive.....	23
Set Up PXE/WDS.....	23
Set Up a WDS Server.....	24
Install WDS.....	25
Configure WDS.....	25
Authorize a WDS Server in Active Directory.....	26
Use the Client Installation Wizard.....	26
Task 7: Prepare the Server Hardware for OS Installation.....	26
Set Up the Boot Drive.....	27
Boot to EFI.....	27
Locate the DVD/CD Drive.....	27
Set ACPI Flag to Windows (Cell-Based Servers Only).....	28
Set Cell Local Memory to 100% (Cell-Based Servers Only).....	29
Specify the Network Interface Card for a Network Boot.....	29
 2 Installing the OS.....	 31
Install from a Headless Console.....	31
Install from a GUI Console.....	39
Install from PXE.....	47
Reinstall from a Headless Console.....	47
Load the System Image to the Boot Disk.....	47
Configure after the Initial Boot.....	49

Reinstall from a GUI Console.....	49
Load the System Image to the Boot Disk.....	50
Configure after the Initial Boot.....	51
Activate the OS.....	51
Apply OS Updates Using the Smart Update Media.....	54
Enable Windows Components.....	55
Set IP Addresses from a Headless Console.....	55
Enable and Run Remote Desktop Connection.....	55
Verify System Device Drivers and Register for Updates.....	56
Verify System Device Drivers.....	56
Register for HP Support Notifications.....	57
Register for Microsoft Security Notifications.....	57
Register for Microsoft Windows Update.....	57
Miscellaneous Installation Issues.....	57
Downgrading from Windows Server 2008 R2 (to Windows Server 2008 or Windows Server 2003).....	57
Installing Windows Server 2008 R2 on rx8640 and rx7640 Servers.....	58
Bootting Windows Preinstallation Environment (WinPE) from the Hard Drive Diagnostic Partition.....	58
Installing from the IRC.....	58
Enabling Hyperthreading on HP Integrity Servers.....	58
Device Manager Indicates “Unknown Device” with ID IFX0102.....	59
 3 Installing and Configuring the Management Tools.....	 61
Install the Integrity Support Pack (ISP).....	61
Configure and Verify the WBEM Providers.....	64
Enable Access Rights and Group Memberships.....	65
Enable Auto Page Refresh and Set the Interval.....	66
Verify Installation of the WBEM Providers.....	66
Configure System Management Homepage.....	66
Set Up Browser Access.....	66
Set Up and Change Your SMH Security Settings After Support Pack Installation.....	66
Initialize SMH	67
Verify Installation of the nPartition Management Tools.....	67
Verify nPartition Commands.....	68
Verify Partition Manager Installation.....	68
 A Preparing the Server for Microsoft SQL Server.....	 71
SQL Server 2005 Installation.....	71
Install SQL Server from the Command Prompt.....	72
Install SQL Server from the GUI.....	72
 B EFI Utilities.....	 75
Introduction to EFI.....	75
EFI Boot Manager.....	75
EFI Shell.....	75
Common EFI Shell Commands.....	76
EFI-Based Setup Utility.....	78
Creating a Backup Boot File Using the EFI Shell.....	80
Verify Successful Backup Boot File Creation.....	80

C nPartitioning.....	81
Quick Start.....	81
Getting to Know nPartitions.....	82
Partitioning Continuum.....	82
Cell Structure of nPartitions.....	82
Properties of nPartitions.....	83
Cell and nPartition Boot Phases.....	84
Cell Boot Phase	84
nPartition Boot Phase.....	85
Choosing a Management Tool.....	85
Management Interface Options.....	86
IPMI.....	86
IPMI Block Transfer (IPMI BT).....	86
IPMI over LAN.....	86
Managing nPartitions Using IPMI over LAN.....	87
Running Partition Manager Using IPMI over LAN.....	87
Running nPartition Commands Using IPMI over LAN.....	87
WBEM.....	87
Securing the WBEM Connection.....	88
Managing nPartitions Using WBEM.....	88
Running Partition Manager Using WBEM.....	89
Running nPartition Commands Using WBEM.....	89
Choosing a Management Mode.....	89
Local Management.....	89
Remote Management Using IPMI.....	90
Remote Management Using WBEM.....	90
Authentication and Authorization Issues.....	90
Local Management.....	90
Remote Management Using IPMI.....	91
Remote Management Using WBEM.....	91
Setting up the Management Station.....	92
Controlling the Management Station Remotely.....	92
Remote Control.....	92
Terminal Services.....	92
Remote Desktop.....	92
Telnet.....	92
Performing nPartition Management Tasks.....	93
Listing the Status of an nPartition or Complex.....	93
Using Partition Manager.....	93
Using nPartition Commands.....	93
Using the Management Processor Command Menu.....	93
Using the EFI Shell.....	94
Creating nPartitions.....	94
Creating the First nPartition in a Server Complex.....	94
Creating a Genesis Partition for a Server Complex.....	94
Creating Additional nPartitions in a Server Complex.....	94
Modifying nPartitions.....	95
Bootting and Resetting nPartitions.....	96
Using the MP Command Menu.....	97
Using the EFI Shell.....	97
Using Microsoft Windows Commands.....	97
D SMH and the WBEM Providers.....	99
WBEM Providers.....	99

Using SMH.....	99
Accessing WebAgents.....	100
Navigating SMH.....	100
The SMH Home Page.....	103
Overall Status Summary.....	103
System Status.....	103
System Category.....	103
Operating System Category.....	104
Network Category.....	104
System Software Category.....	104
Storage Category.....	104
System Configuration Category.....	104
System Report.....	105
 E Headless Windows Installations.....	107
Why Headless?.....	107
What is a Headless System?.....	107
Benefits of Headless Systems.....	107
How to Access a Headless System.....	108
Console Definitions.....	108
In-Band vs. Out-of-Band.....	108
Remote Desktop.....	108
Physical Aspects of Integrity Consoles.....	108
Management Processor.....	108
Emergency Management Services (EMS).....	108
Firmware Redirection.....	109
Special Administration Console.....	109
Configuring Consoles.....	109
Management Processor Settings.....	109
Cellular Systems.....	110
Noncellular Systems.....	110
EFI Console Settings.....	110

List of Figures

1-1	Headless Console Configurations.....	19
1-2	GUI Console Configuration.....	21
1-3	PXE/WDS Configuration.....	24
2-1	EBSU Main Menu.....	32
2-2	EBSU Firmware Update Screen.....	33
2-3	EBSU Partition Disk Screen.....	33
2-4	EBSU Install Options Screen.....	34
2-5	EBSU Prompt Screen.....	34
2-6	EBSU Product Key Screen.....	35
2-7	EBSU Screen #1.....	36
2-8	EBSU Screen #2.....	36
2-9	EBSU Screen #3.....	37
2-10	EBSU Screen #4.....	37
2-11	EBSU Screen #5.....	37
2-12	EBSU Screen #6.....	38
2-13	Initial Configuration Tasks Screen.....	38
2-14	EBSU Main Menu.....	40
2-15	EBSU Firmware Update Screen.....	41
2-16	EBSU Partition Disk Screen.....	41
2-17	EBSU Install Options Screen.....	42
2-18	EBSU Prompt Screen.....	42
2-19	EBSU Screen #1.....	43
2-20	EBSU Screen #2.....	43
2-21	Install Windows Screen #1.....	44
2-22	Install Windows Screen #2.....	45
2-23	Initial Configuration Tasks Screen.....	46
2-24	System Window #1.....	52
2-25	Windows Activation Screen.....	53
2-26	System Window #2.....	54
2-27	Unknown Device Properties page > Details tab.....	59
3-1	HPSUM Select Installation Host(s) Screen.....	61
3-2	HPSUM Select Bundle Filter Screen.....	62
3-3	HPSUM Select Items to be Installed Screen.....	63
3-4	HPSUM Installation Results Screen.....	64
B-1	EFI Boot Manager.....	75
C-1	System Overview.....	81
C-2	Partitioning Continuum.....	82
E-1	Emergency Management Services and Special Administration Console.....	109

List of Tables

1-1	Installation Matrix.....	15
1-2	Location of the COA on Your Server.....	16
1-3	Graphics Support and Server Models.....	21
1-4	EFI Device Mapping Fields.....	28
B-1	EFI Shell Commands and Descriptions.....	76

About This Document

This document describes how to install and configure the operating system and HP software on HP Integrity servers running Microsoft® Windows Server™ 2008 R2 Itanium™ Edition.

The document publication date and part number indicate the document's current edition. The publication date changes when a new edition is printed. Minor changes may be made at reprint without changing the publication date. The document part number changes when extensive changes are made.

Document updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for more information.

For the latest version of this document, see the HP Technical Documentation website:

<http://www.hp.com/go/windows-on-integrity-docs>

Intended Audience

This document is intended for system administrators and HP support personnel responsible for installing, configuring, and managing HP Integrity servers. This document is not a tutorial.

New and Changed Information in This Edition

This document includes the following changes since its last release:

- *About This Document*: updated URL
- Chapter 1: new COA photo (rx2800i2.png) in section, *Locate Your Microsoft Certificate of Authenticity*
- Chapter 1: changes to section, *Set Up an Integrated Remote Console*
- Chapter 2: added iLO note to section, *Reinstall from a GUI Console*
- Chapter 3: updated URL in section, *Verify Installation of the nPartition Management Tools*
- Appendix A: updated URL in section, *SQL Server 2005 Installation*
- Appendix C: updated URL
- Appendix D: updated two URLs
- Global change: added rx2800 i2 support throughout document
- Global change: replaced “iLO 2” with generic “iLO” to prevent multiple changes every time iLO revs

Document Organization

This document is organized as follows:

“Preparing for Installation” (page 13)	Describes the steps to prepare the server for installation of the operating system, SmartSetup, and management software.
“Installing the OS” (page 31)	Describes how to install the operating system software.
“Installing and Configuring the Management Tools” (page 61)	Describes how to install the server management software.
“Preparing the Server for Microsoft SQL Server” (page 71)	Describes how to configure and install Microsoft SQL Server 2005.
“EFI Utilities” (page 75)	An overview of the server's Extensible Firmware Interface (EFI) and EFI-Based Setup Utility (EBSU).
“nPartitioning” (page 81)	An overview of how to configure a single system into several independent, partitioned systems, each with hardware and software isolation.

"SMH and the WBEM Providers" (page 99)	An overview of the WBEM Providers and how to configure System Management Homepage (SMH) to administer your system locally or remotely.
"Headless Windows Installations" (page 107)	An overview of the benefits, concepts, and terminology of headless operating system installation on HP Integrity servers.

Typographic Conventions

This document uses the following typographical conventions:

WARNING	A warning calls attention to important information that, if not understood or followed, results in personal injury or nonrecoverable system problems.
CAUTION	A caution calls attention to important information that, if not understood or followed, might result in data loss, data corruption, or damage to hardware or software.
IMPORTANT	This alert provides essential information to explain a concept or to complete a task.
NOTE	A note contains additional information to emphasize or supplement important points of the main text.
KeyCap	The name of a keyboard key or graphical interface item (such as buttons, tabs, and menu items).
Computer output	Text displayed by the computer.
User input	Commands and other text that you type.
Command	A command name or qualified command phrase.
Ctrl+x	A key sequence. A sequence such as Ctrl+x indicates that you must press the key labeled Ctrl while you press another key or mouse button.
[]	The contents are optional in command-line syntax. If the contents are a list separated by , you must choose one of the items.
{ }	The contents are required in command-line syntax. If the contents are a list separated by , you must choose one of the items.
...	The preceding element can be repeated an arbitrary number of times.
Ⓢ	Indicates the continuation of a code example.
	Separates items in a list of choices.

Related Information

For more information about HP Integrity servers, server management, and software, see the following:

- Windows on HP Integrity servers — An Overview:
<http://h20341.www2.hp.com/integrity/w1/en/os/windows-on-integrity-overview.html>
- HP technical support resources (drivers, patches, upgrades, migration issues, to sign up for alerts, and so on):
<http://hp.com/support/itaniumservers>
- Documentation supporting Windows Server 2008 R2 on HP Integrity Servers:
— to locate documents by operating system: <http://www.hp.com/go/windows-on-integrity-docs>

— to locate documents by server model number: http://www.hp.com/go/integrity_servers-docs

- Microsoft's Windows Server 2008 R2 support website:
<http://www.microsoft.com/windowsserver2008/en/us/default.aspx>

Publishing History

The document part number and publication date indicate the document's current edition. The publication date will change when a new edition is printed. Minor changes may be made at reprint without changing the publication date. The document part number will change when extensive changes are made. Document updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details. You can find the latest version of this document on line at: <http://www.hp.com/go/windows-on-integrity-docs>

Manufacturing Part Number	Supported Operating Systems	Supported Smart Setup Version	Supported Products (Servers)	Publication Date
5992-5680	Microsoft Windows Server 2008 R2 Itanium Edition	Version 7.0	BL860c BL870c BL860c i2 BL870c i2 BL890c i2 rx2800 i2 rx2660 rx3600 rx6600 rx7640 rx8640 Superdome sx2000	November, 2010

HP Encourages Your Comments

HP encourages your comments concerning this document. We are committed to providing documentation that meets your needs. Send any errors found, suggestions for improvement, or compliments to:

docsfeedback@hp.com

Please include the document title, manufacturing part number, and any comment, error found, or suggestion for improvement you have concerning this document.

1 Preparing for Installation

Installing Microsoft Windows Server 2008 R2 for Itanium-based systems on an HP Integrity server involves preparing the hardware for operating system (OS) installation, loading the OS, and updating the system with the latest OS patches (Microsoft QFEs). This chapter helps you plan the installation based on the server model, the OS edition, the source of the OS media, and your network environment. Subsequent chapters guide you through the installation process.

If the Windows Server 2008 R2 operating system is installed on your system, or if it was installed by HP before your system was delivered, you need not perform the steps described in Chapter 1 “Preparing for Installation”) and Chapter 2 “Installing the OS”. Proceed to Chapter 3 “Installing and Configuring the Management Tools”, and install your management tools software.

If you want to install or reinstall the Windows Server 2008 R2 operating system, you must perform the following tasks:

- “Task 1: Determine Current System Status” (page 13)
- “Task 2: Verify Hardware Compatibility” (page 13)
- “Task 3: Back Up Existing Data” (page 14)
- “Task 4: Choose an Installation Environment” (page 14)
- “Task 5: Locate Your Microsoft Certificate of Authenticity (with Product Key)” (page 15)
- “Task 6: Set Up an Installation Method” (page 19)
- “Task 7: Prepare the Server Hardware for OS Installation” (page 26)

Task 1: Determine Current System Status

When you purchase an HP Integrity server, you can order additional hardware, support options, and an OS enablement kit (such as the HP Insight Foundation suite for Integrity with Windows). You can also order factory installation of the OS. So depending on your order (and subsequent use), your system is in one of the following conditions:

- Factory-installed Windows Server 2008 R2
- Factory-installed OS other than Windows Server 2008 R2
- No operating system installed
- Incorrect or inoperable installation of Windows Server 2008 R2

Task 2: Verify Hardware Compatibility

To verify that your existing hardware is compatible with Windows Server 2008 R2, follow these steps:

1. Verify existing device compatibility at the HP Integrity server connectivity website:
<http://www.hp.com/products1/serverconnectivity/index.html>
2. Verify storage compatibility by reviewing the HP Integrity Server-Storage support matrices at http://www.hp.com/products1/serverconnectivity/support_matrices.html. The list on the website is not exhaustive. Storage vendors can support more configurations than those indicated at the site. As a general rule, verify with your storage vendor and an HP sales representative for a definitive statement on server and storage compatibility.

Ensure Brand Similarity Among Fibre Channel Host Bus Adapters (HBAs) in Multipath I/O (MPIO) Environments

If the target server will run in an MPIO environment, with redundant physical I/O paths (adapters, cables, switches, and so on) between the server and its storage devices, you must ensure that all Fibre Channel HBAs in the system are manufactured by the same vendor before installing the

operating system. HBAs from different vendors rarely support the same maximum I/O packet size. This can create I/O conflicts that cause the system to lock up with a blue screen, a stopcode of 0X000000D1, and a reference to the file `elxstor.sys`.

The solution to this problem is to make sure that all HBAs in the system are manufactured by the same vendor (and therefore have the same maximum I/O packet size). Current HBA vendors include Emulex and Qlogic. The following lists summarize HBA sourcing, so you can ensure brand similarity in your system.

HBAs from Emulex (with HP part number) include:

- HP StorageWorks Single Port 8 Gb PCI-e Fibre Channel (AH402A)
- HP StorageWorks Dual Port 8 Gb PCI-e Fibre Channel (AH403A)
- HP StorageWorks 4 Gb Single Port 64-bit 266 MHz Fibre Channel (AD167A)
- HP StorageWorks 4 Gb Dual Port 64-bit 266 MHz Fibre Channel (AD168A)
- HP StorageWorks FC2142 PCIe Single Port 4 Gb Fibre Channel (A8002A)
- HP StorageWorks FC2242 PCIe Dual Port 4 Gb Fibre Channel (A8003A)

HBAs from Qlogic (with HP part number) include:

- HP StorageWorks Single Port 8 Gb PCI-e Fibre Channel (AH400A)
- HP StorageWorks Dual Port 8 Gb PCI-e Fibre Channel (AH401A)
- HP StorageWorks 4 Gb Single Port 64-bit 266 MHz Fibre Channel (AB429A)
- HP StorageWorks 4 Gb Dual Port 64-bit 266 MHz Fibre Channel (AB379A)
- HP StorageWorks 4 Gb Dual Port 64-bit 266 MHz Fibre Channel (AB379B)
- HP StorageWorks FC1142 PCIe Single Port 4 Gb Fibre Channel (AE311A)
- HP StorageWorks AD300A PCIe Dual Port 4 Gb Fibre Channel (AD300A)

For more information about MPIO, see the Microsoft Storage web site:

<http://www.microsoft.com/WindowsServer2003/technologies/storage/mpio/default.mspix>

Task 3: Back Up Existing Data

To restore critical data on the server hard disk after installing or migrating to Windows, you must first back up the data and verify that you can restore it by following these steps:

1. Back up your server using your existing backup utilities
2. Verify the integrity of the backup by restoring samples of data to another server
3. Store the backup in a safe place

Task 4: Choose an Installation Environment

Your installation environment consists of the server model number, the installation method (GUI or Headless Console, Integrated Remote Console, or PXE/WDS), and the installation media used to perform the installation. Table 1-1 lists the installation environments available.

Table 1-1 Installation Matrix

Server Model	Installation Method	Installation Media
<u>Non Cell-Based Servers</u> rx2660 rx3600 rx6600 BL860c BL870c BL860c i2 BL870c i2 BL890c i2 rx2800 i2	Headless Console	Windows Server 2008 R2 OS disc (provided by Microsoft) + HP Smart Setup disc + HP Smart Update disc
		HP Reinstallation disc + HP Smart Setup disc + HP Smart Update disc
	GUI Console	Windows Server 2008 R2 OS disc (provided by Microsoft) + HP Smart Setup disc + HP Smart Update disc
		HP Reinstallation disc + HP Smart Setup disc + HP Smart Update disc
	Integrated Remote Console	- Virtual Media (vMedia) + Windows Server 2008 R2 disc (provided by Microsoft) + HP Smart Setup disc + HP Smart Update disc - Virtual Media (vMedia) + HP Reinstallation disc + HP Smart Setup disc + HP Smart Update disc
	PXE/WDS	
<u>Cell-Based Servers</u> rx8640 rx7640 Superdome sx2000	Headless Console	Windows Server 2008 R2 OS disc (provided by Microsoft) + HP Smart Setup disc + HP Smart Update disc
		HP Reinstallation disc + HP Smart Setup disc + HP Smart Update disc
	GUI Console	Windows Server 2008 R2 OS disc (provided by Microsoft) + HP Smart Setup disc + HP Smart Update disc
		HP Reinstallation disc + HP Smart Setup disc + HP Smart Update disc
	PXE/WDS	

Using Windows Server 2008 R2 OS Media (Provided by Microsoft) + HP Smart Setup + Smart Update Media

You can purchase your Microsoft Windows Server 2008 R2 OS media from HP or from a Microsoft Windows reseller. You can also use a volume license for Windows Server 2008 R2 that your organization already has. However you obtain your OS media, you will need it, a product key, and the HP Smart Setup and Smart Update discs to install Windows Server 2008 R2.

The Smart Setup media automates the setup of boot controllers, drivers, and disk partitions. The Smart Update media provides operating system and security updates from Microsoft. In addition, after completing the installation, HP recommends connecting to Microsoft's Windows Update website to obtain the latest Microsoft updates.

Using HP Reinstallation Media

HP Integrity servers that come factory-installed with Windows Server 2008 R2 are shipped with the HP Reinstallation media, which you can use to restore the server to its factory condition, if necessary. This media prepares the boot controllers, sets up the required disk partitions, and installs the OS. You must have the corresponding product key to reinstall Windows Server 2008 R2. The product key is on the Certificate of Authenticity (COA) of your server.

Task 5: Locate Your Microsoft Certificate of Authenticity (with Product Key)

This certificate contains your Microsoft Windows Server 2008 R2 product key. You must enter the product key during the installation, to activate the operating system. The physical location of the Certificate of Authenticity (COA) depends on the server model. Table 1-2 shows the COA location on supported HP Integrity servers.



NOTE: Table 1-2 shows the location of your primary product key. Another key, the “virtual” key, is also required if you are installing a Windows Server 2008 R2 guest in a virtualized host.

Table 1-2 Location of the COA on Your Server

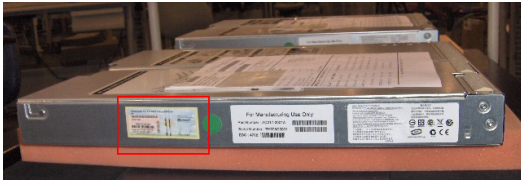
Integrity Server	Location
rx2660	The COA is located on the left side panel, in the middle, as shown. 
rx3600	The COA is located on the left side panel, as shown. 
rx6600	The COA is located on the left side panel. 
BL860c and BL870c	The COA is located on the left side panel. If there is more than one label on the side panel, the COA is the one farthest left, as shown. 

Table 1-2 Location of the COA on Your Server *(continued)*

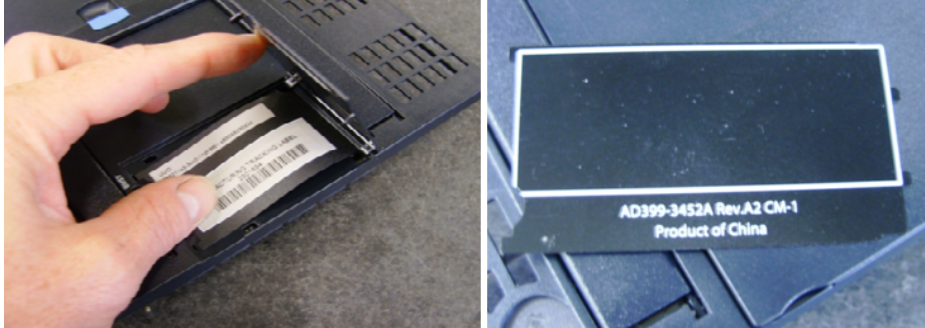
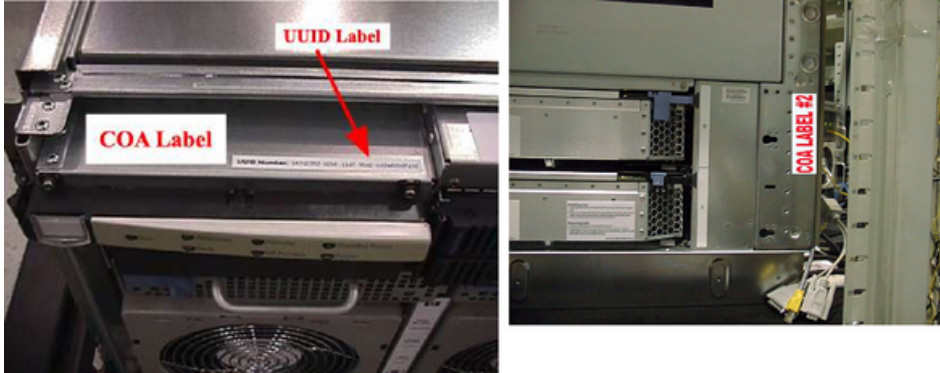
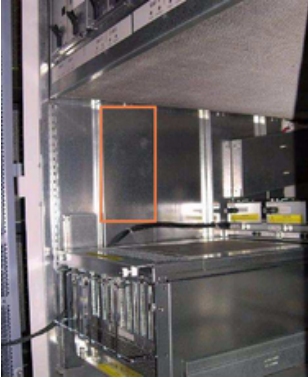
Integrity Server	Location
BL860c i2, BL870c i2, and BL890c i2	The COA is located on the back side of the Scalable Blade Links (SBL) label card. Lift the lid open, push the label card to one side so you can grip an edge, remove the card, and flip it over. The COA should be affixed inside the white square. 
rx2800 i2	The COA is located on the pullout slide on the left side of the front bezel, as shown. 
rx7640	The COA is located on the front of the system, above the light panel, next to the UUID label, as shown in the first image. Additional COAs are shown in the second image. 

Table 1-2 Location of the COA on Your Server *(continued)*

Integrity Server	Location
rx8640	The COA is located in the front of the system, at the bottom, near the power supply as shown in the first image. If additional COAs are required, they are located as shown in the second image. 
Superdome sx2000	The COA is located inside the unit, on the left, in the open space between the cells and the extended I/O cabinet (IOX). 

Task 6: Set Up an Installation Method

Choose one of the following methods to install the operating system:

- Local installation methods:
 - Headless console
 - GUI console
- Remote installation methods:
 - Integrated Remote Console (IRC)
 - Preboot execution environment (PXE) + Windows Deployment Services (WDS), or PXE/WDS

If you are installing locally, you must set up your server with a headless or GUI console.



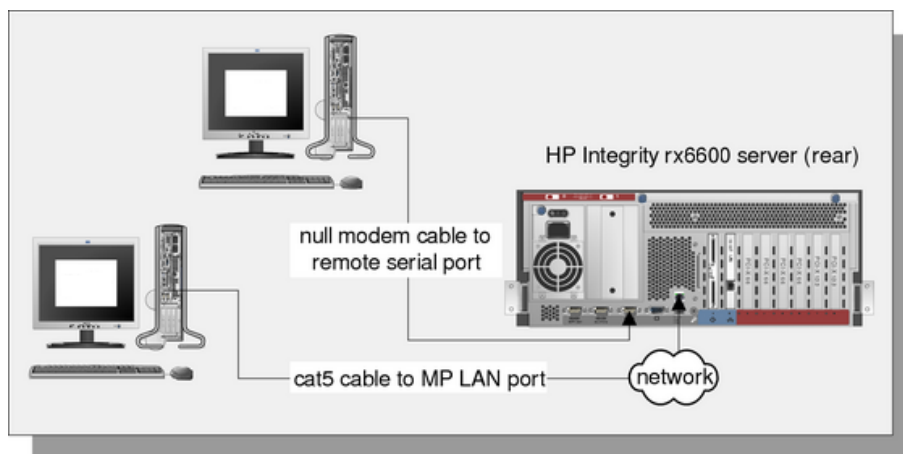
NOTE: For an overview of the benefits, concepts, and terminology of headless operating system installation on HP Integrity servers, see “Headless Windows Installations” (page 107).

Set Up a Headless Console

A **headless console** is a PC running terminal emulation software such as **PuTTY** (available from the web) or **HyperTerminal**, which connects to the server through its management processor (MP) serial port or LAN port, or through its Integrated Lights-Out (iLO) management processor. A headless console provides a method for connecting to servers that do not have legacy VGA graphics, or PS/2 keyboard and mouse hardware. HP recommends that you configure servers this way (without legacy VGA, or keyboard/mouse hardware) because they are easier to set up, maintain, and operate.

Figure 1-1 shows headless consoles connected to an HP Integrity server.

Figure 1-1 Headless Console Configurations



When you use a headless console to install Windows, you can view detailed installation information for each component by monitoring the setup log channels. For more information about how to view this information, see the *Windows Server 2008 R2 and Windows Server 2008 SP2 for HP Integrity Servers Hardware Administrator's Guide*.

From the headless console, you can access the EFI Shell, the management processor (MP), and the Microsoft Special Administration Console (SAC). You can use these utilities while installing and administering Windows Server 2008 R2 on HP Integrity servers. For more information about the MP and SAC, see the *Windows Server 2008 R2 and Windows Server 2008 SP2 for HP Integrity Servers Hardware Administrator's Guide*.

You can configure a headless console by using one of the following:

- A null modem cable
- A cat5 LAN cable
- A Remote Serial Console

The first two methods require a terminal emulation application such as HyperTerminal or PuTTY. PuTTY is a free implementation of telnet and SSH for 32-bit Windows and UNIX. PuTTY provides an X terminal. You must use PuTTY version 0.59 or higher, available from the PuTTY website:

<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>

Set Up a Headless Console Using a Null Modem Cable

To set up the headless console using a null modem cable, follow these steps:

1. Connect the PC to the server MP serial port with a null modem cable.
2. Install PuTTY on the client PC and specify the following port settings:
 - Bits per second: 9600
 - Data bits: 8
 - Parity: none
 - Stop bits: 1
 - Flow control: Xon/Xoff
3. Use the Keyboard Configuration Panel to map the **backspace** key to **Control + H**.
4. Boot the server.
5. Run PuTTY and press **Enter**. The MP login prompt displays.
6. Enter your user name and password. The MP command prompt displays.
7. Enter the CO command to access the headless console.
8. The set up is complete. Proceed to the Headless Console installation process, “Install from a Headless Console” (page 31).

Set up a Headless Console Using a LAN

To set up the headless console over a LAN, follow these steps:

1. Connect the PC to the server LAN port with a cat5 cable.
2. Use telnet to access the MP. The MP login prompt displays.
3. Enter your user name and password. The MP command prompt displays.
4. Enter the CO command to access the headless console.
5. The set up is complete. Proceed to the Headless Console installation process: “Install from a Headless Console” (page 31).

Set Up a Headless Console Using a Remote Serial Console

To set up the headless console using a Remote Serial Console, follow these steps:

1. Using a secure web browser, enter the name or IP address of the server MP.
2. Enter your user name and password to log in to the System Management Homepage.
3. On the Remote Console tab, select **Remote Serial Console** in the left panel.
4. Click **Launch**. A new window displays, providing access to the headless console.
5. The set up is complete. Proceed to the Headless Console installation process, “Install from a Headless Console” (page 31).

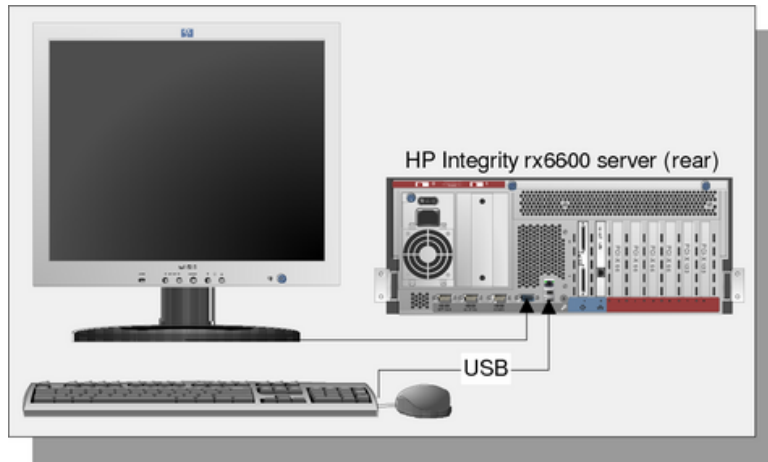
Set Up a GUI Console

A **GUI console** is a VGA monitor, a USB HP keyboard, and a USB mouse connected to the server. (You can use a USB-to-PS2 converter to connect to a console switch.) If a VGA card is not installed,

you must install the HP Graphics and USB Combo Card to use a GUI console. No other graphics card is supported by HP Integrity servers. Also, only HP keyboards are supported with this card.

Figure 1-2 shows a GUI console connected to an HP Integrity server.

Figure 1-2 GUI Console Configuration



A GUI console provides complete access to all installation and administration tasks that you can perform on the server. Use the GUI console to:

- Prepare the server for installation
- Install the OS
- Verify server status after installation

On servers configured with an internal graphics card, you can connect a monitor, keyboard, and mouse directly to the relevant ports. On servers without an internal graphics card, you must install an HP Graphics and USB Combo Card, and connect the console to the relevant ports. Then, from an existing headless console, modify system configuration to redirect the output to the GUI console. The following table lists available graphics support.

Table 1-3 Graphics Support and Server Models

Server Model	Graphics Card
• rx2660 • rx3600 • rx6600 • BL860c • BL870c • BL860c i2 • BL870c i2 • BL890c i2 • rx2800 i2	Built-in video graphics
• rx7640 • rx8640 • Superdome sx2000	Optional HP Graphics and USB Combo Card (HP part number A6869B)

To install the HP Graphics and USB Combo Card using the Legacy interface (black background), follow these steps:

1. Install the HP Graphics and USB Combo Card in an open PCI slot in the server.
2. Connect a VGA monitor, USB HP keyboard, and USB mouse to the relevant ports.
3. Boot the server to EFI.
4. At the headless console, from the EFI Boot Manager, select **Boot Option Maintenance Menu**.

5. Select **Select Active Console Output Devices**.
6. Highlight the line with the graphics card PCI device.
If the line does not begin with an asterisk, the device is disabled. Use the space bar to change the state of the card from disabled to enabled (as indicated by the asterisk).
7. Select **Save Settings to NVRAM**; and then, **Exit**. The video display is now directed to the GUI console.
8. The set up is complete. Proceed to the GUI Console installation process: “Install from a GUI Console” (page 39).

To install the HP Graphics and USB Combo Card using the Enhanced interface (gray background), follow these steps:

1. Install the HP Graphics and USB Combo Card in an open PCI slot of the server.
2. Connect a VGA monitor, USB HP keyboard, and USB mouse to the relevant ports.
3. Boot the server to EFI.
4. From the EFI Boot Manager, select **Boot Configuration**.
5. Select **Console Configuration**.
6. Select **Select Output Console**.
7. Select the graphics card PCI device, and press **Enter**. The video display is now directed to the GUI console.
8. The set up is complete. Proceed to the GUI Console installation process: “Install from a GUI Console” (page 39).

Set Up an Integrated Remote Console

The Integrated Remote Console (IRC) lets you use Windows clients running Internet Explorer to remotely view and manage HP Integrity servers featuring the iLO management processor. This functionality is only supported on rx7640, rx8640, and Superdome sx2000 servers when the HP Lights Out Advanced KVM card is installed (HP part number AD307A). On all other platforms, IRC support is embedded and does not require the additional card.

The IRC combines keyboard, video, and mouse into a remote, virtual interface. Use it to view the server display and to interact with it. When you use IRC in combination with Virtual Media (See “Set Up a vMedia Drive” (page 23)), you can perform remote GUI installations of server operating systems and software. You can also use the IRC to perform server maintenance tasks and run applications remotely that require keyboard and mouse input.



NOTE: You can use the IRC instead of the GUI Console method of installation.

The IRC and vMedia features are enabled only after you obtain and install an iLO MP Advanced Pack license (HP part number AB500A). If you are not licensed and try to use these features, the message `iLO feature not licensed`, displays. Free limited-term trial licenses are available.

For more information about iLO functionality on HP rx7640, rx8640, and Superdome sx2000 servers using the HP Lights Out Advanced KVM card, see the following website:

http://www.hp.com/products1/serverconnectivity/misc/iLOADVKVMCard.html?jumpid=reg_R1002_USEN

Follow the factory installation or manual installation instructions on the *Integrated Lights-Out Advanced Pack for HP Integrity Servers; Certificate of License to Use; License Installation Card* to activate your license. This document does not provide a complete description of IRC or vMedia. For more information about these powerful features, see the *HP Integrity iLO 3 MP Operations Guide* at the following web address:

<http://h20000.www2.hp.com/bc/docs/support/SupportManual/c02111169/c02111169.pdf>

To set up an IRC, follow these steps:

1. Using a secure web browser, enter the name or IP address of the server MP.

2. Enter your user name and password to log in to the System Management Homepage.
3. On the Administration tab, select **Licensing** in the left panel.
4. Enter the license number.
5. In the Remote Console tab, select **Integrated Remote Console** in the left panel.
6. Click **Launch**. (If **Launch** is grayed out, the license might be invalid or expired.) A new window displays, providing access to the IRC.

Set Up a vMedia Drive

Virtual Media (vMedia) provides you with virtual devices that mimic physical hardware devices as if they were physically connected, such as a virtual CD/DVD drive that can connect through a network to the managed server. A vMedia device can be a physical CD/DVD drive on the management workstation, or it can be an image file stored on a local disk drive or network drive. Floppy disk or USB memory devices are not supported.

Bootimg from the iLO MP CD/DVD enables you to:

- upgrade the host system ROM
- upgrade device drivers
- deploy an OS from network drives
- perform disaster recovery of failed operating systems

The iLO MP device uses a client/server model to perform vMedia functions. The iLO MP device streams vMedia data across a live network connection between the remote management console and the host server. The vMedia Java™ applet provides data to the iLO MP as required.



NOTE: You can use a vMedia drive instead of a local CD or DVD drive.

To set up a vMedia drive, follow these steps:

1. Using a secure web browser, enter the name or IP address of the server MP.
2. Enter your user name and password to log in to the System Management Homepage.
3. On the Administration tab, select **Licensing** in the left panel.
4. Enter the license number.
5. In the Virtual Devices tab, select **Virtual Media** in the left panel.
6. Click **Launch**. (If **Launch** is grayed out, the license might be invalid or expired.) A new window displays, providing access to Virtual Media.
7. Complete one of the following actions:
 - Select **Local Media Drive**, specify the CD or DVD drive on your client machine, and insert the CD or DVD into that drive.
 - Select **Local Image File** and specify the ISO image of the CD or DVD.
8. Click **Connect**. The server now detects a new USB drive attached to it. This is the vMedia drive.

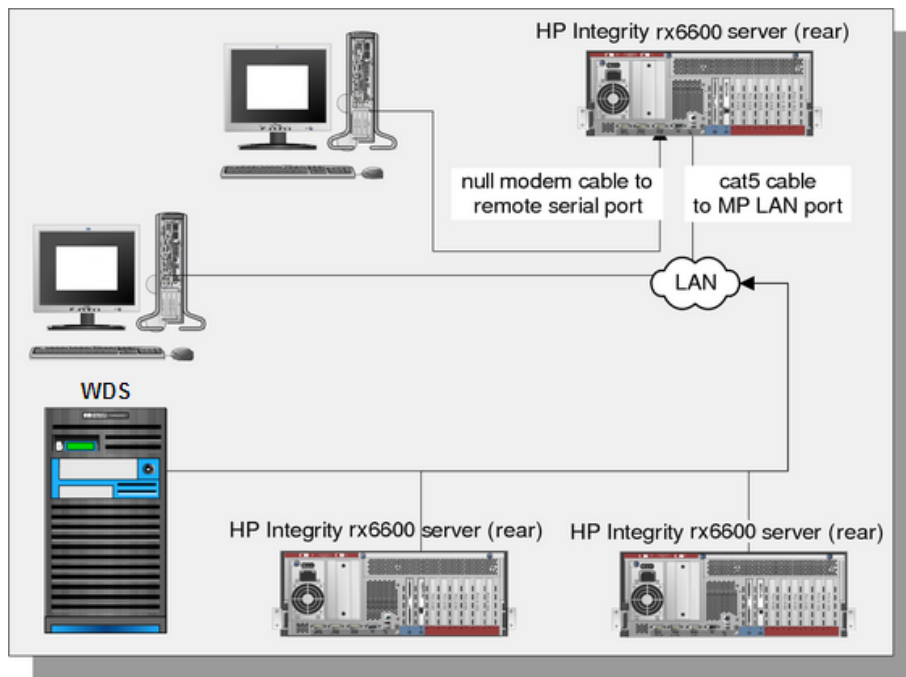
Set Up PXE/WDS

A Windows Deployment Services server (WDS) is a specialized Windows server used to perform multiple software installations across a network. The WDS server, working with a Preboot Execution Environment agent (the PXE client) residing on target systems, performs automated installations. This method of installation offers the following advantages:

- Installations are automated. No user intervention is needed.
- You can install multiple servers in one batch job.
- Each server receives a standardized image.
- You can perform an installation from anywhere on the intranet.

Figure 1-3 shows a sample PXE/WDS setup.

Figure 1-3 PXE/WDS Configuration



NOTE: When you perform a PXE/WDS headless installation, note the following:

- Headless installations using PXE/WDS are not supported with Windows Server 2008 R2. Use the HP Reinstallation media instead.
- Do not connect the WDS server to the Integrity server using your intranet during initial Windows OS installation. Set up a small private network, populated with the WDS server, a hub, and the system LAN NIC of the HP Integrity server. This protects the intranet from errors that might occur during the Windows installation. When the Windows OS installation is complete, connect the WDS to the target Integrity servers using your intranet.

WDS enables you to create, maintain, and quickly install identical OS and software configurations on multiple headless systems, with a predefined level of user interaction. WDS uses the PXE to enable client computers without an operating system to boot remotely to a WDS server. The WDS server then installs the OS over a TCP/IP network connection.

You can create different sets of WDS images for different groups of client computers. You can also use the Group Policy settings to limit the installation options that WDS presents to clients. In addition, you can configure WDS for interactive or automated installations.

Set Up a WDS Server

Setting up WDS servers on your network requires careful planning, design, and implementation. The following checklist provides an overview of the tasks involved in setting up a WDS server:

- Ensure that your WDS server and client (Integrity server) hardware meet the WDS hardware requirements. The server hardware must meet the minimum requirements for the version of Windows Server 2008 that you are installing.
- Ensure that your network is based on TCP/IP, and that a Domain Name System (DNS) server exists on the network. You need not use the Microsoft version of DNS.
- Ensure that a Dynamic Host Configuration Protocol (DHCP) server exists on the network. You need not use the Microsoft version of DHCP.
- Ensure that Active Directory exists on the network.
- Install the WDS component on the WDS server.
- Run the WDS Setup Wizard.

Install WDS

You can install WDS using the Control Panel or an unattended Setup answer file. To install WDS using Add or Remove Programs, follow these steps:

1. Click **Start** → **Settings** → **Control Panel**, double-click **Add or Remove Programs**, and select **Add/Remove Windows Components** to install the WDS component.
2. Open the WDS Setup Wizard, and click **Next**. The WDS Setup wizard prompts you for information about specific settings used in the WDS installation. The wizard prompts you to follow these steps:
 - a. Enter the disk drive and directory to install WDS. The disk must be dedicated to the WDS server with a recommended minimum 4 GB of space.
 - b. Select **Respond to client computer requesting service**. The WDS server begins responding to client computers when the wizard is complete. If you want the WDS server to respond only to prestaged client computers in Active Directory, select **Do not respond to unknown client computers**.
 - c. Enter the location of the client images. This can be the Windows Server 2008 R2 CD or a shared folder on the network that contains the installation files.
 - d. Enter help text that describes the OS installation choices to users or clients of WDS.

Configure WDS

After the WDS Setup Wizard completes, depending on the settings chosen, the WDS server services client computers or pauses, while you configure advanced settings using WDS administration settings. The following configuration options are available:

- Specify which WDS servers are allowed to run on your network. This option prevents the use of unauthorized (often referred to as rogue) WDS servers, ensuring that only WDS servers authorized by administrators can service clients. If an attempt is made to start an unauthorized WDS server on the network, it is shut down and cannot service client computers. A WDS server must be authorized before it can service client computers.
- Use the Active Directory Users and Computers snap-in to set properties on WDS servers that control how the server supplies WDS to requesting clients. To access the snap-in go to **Start** → **Programs** → **Administrative Tools**, and then select the **Active Directory Users and Computers**.
- Use Group Policy to specify which installation options are presented to groups by the Client Installation wizard (CIW). For example, you can choose to allow a group access only to the automatic setup option, and restrict access to all other options to administrators.
- Use security descriptors or discretionary access control lists (ACLs) to specify which users or groups can access the OS images available on the WDS server. You can use this method to guide users through the selection of the unattended OS installation relevant for their account privileges. By default, when an OS image is added to a WDS server, the image is available to all users serviced by that WDS server.

To configure settings for new clients for WDS, follow these steps:

1. Open Active Directory Users and Computers.
2. In the console tree, click **Active Directory Users and Computers** → **Applicable domain** → **Applicable organizational unit** (such as Computers/Applicable WDS server), and right-click the applicable WDS server.
3. Click **Properties**. Then, in the Properties dialog box, click **Remote Install** and select **Advanced Settings**.
4. In the Advanced Settings dialog box, click **New Clients**.
5. Select the client computer naming format you want to use, or click **Customize** to create a client computer naming format.

6. To specify where to create the client computer account, click one of the following options:
 - Default directory service location
 - Same location as the user setting up the client computer
 - The following directory service location
7. If you choose the last option in **Step 6**, click **Browse**, and specify where to create the computer accounts.

Authorize a WDS Server in Active Directory

A WDS server must be authorized in Active Directory to respond to clients requesting service. If WDS is installed on a server that is not an authorized DHCP server, or is added to a DHCP server that is not authorized in Active Directory, follow these steps:

1. Log in to the domain in which the WDS server resides. The account you use must be a member of the Enterprise Admins group.
2. From the Start menu, point to Programs and Administrative Tools, and click **DHCP** from the list. This starts the DHCP Management snap-in.
3. Right-click the DHCP root node in the scope pane, and click **Manage Authorized Servers**.
4. Click **Authorize**, enter the IP address or name of the WDS server, and click **OK**. When prompted to ensure that this is the correct WDS server to authorize, click **Yes**.

The server does not respond to client requests until the changes to Active Directory take effect. For these rights to apply immediately, on the domain controller where your rights have been set, follow these steps:

1. On the Start menu, click **Run**.
2. Enter the cmd command.
3. At the command prompt, enter the following command:
`secedit /refreshpolicy /MACHINE_POLICY`

Use the Client Installation Wizard

The following installation options are included in the Client Installation Wizard (CIW). Automatic setup is available by default. WDS uses Group Policy settings that allow access to the automatic setup option only, which restricts administrators from the other installation options in the following list:

- **Automatic Setup:** This option enables you to select which OS to install, but it does not prompt you for specific configuration settings. If only one operating system option is offered, you are not prompted, and an unattended installation of the OS image starts.
- **Custom Setup:** This option enables you to override the automatic computer naming process and the default location in Active Directory, where client computer accounts are created. Help desk or administrators can use this option to preinstall a client computer for someone within the enterprise.
- **Restart a Previous Setup Attempt:** This option restarts the OS installation process when an installation attempt fails before completion. This option does not copy files from where the previous installation attempt failed; however, you are not required to answer questions answered in the CIW from the previous setup attempt.
- **Maintenance and Troubleshooting:** This option provides access to third-party maintenance and troubleshooting tools that you can use before installing the OS. Examples of these tools include system flash BIOS updates, computer diagnostic tools, and virus scanning utilities.

Task 7: Prepare the Server Hardware for OS Installation

If you are installing Windows Server 2008 R2 on a server currently running Windows Server 2008 with SP2 or Windows Server 2003, you must first upgrade the system firmware to the latest version. You can download the latest system firmware at <http://www.hp.com>. In addition,

installation of Windows Server 2008 R2 will wipe out the current installation (there is no upgrade path to Windows 2008 R2; the new installation completely overwrites the existing one).

Follow these steps to set up the server hardware for OS installation.

Set Up the Boot Drive

The OS installs, through the boot controller detected as adapter zero, to the drive detected as drive zero.



CAUTION: HP strongly recommends that only the target OS drive is connected during installation. This ensures that the OS is installed on the correct drive. Also, make sure that the Z: drive is free. Windows Server 2008 creates the EFI partition there.

To set up the boot drive, follow these steps:

1. Power off the server.
2. Make a note listing all device connections, so that you can reconnect them after the installation.
3. Disconnect mass storage devices from all controllers except the boot controller.
4. Configure the boot controller and the boot drive. HP recommends that you install the boot controller in the root cell.



NOTE: If you are using an HP Smart Array controller, see the controller user guide for more information. You can interrupt the boot process to invoke the EFI-Based Option ROM Configuration for Arrays (ORCA). To invoke this utility:

1. Press **F8** on the GUI console.
2. Press **ESC 8** on the headless console.

Boot to EFI

To launch the EFI Shell, follow these steps:

1. Boot the server. The server automatically goes to the EFI Boot Manager Menu.
2. Scroll down, and select **EFI Shell**.
3. Press **Enter**.
4. Choose from the following:
 - If you are using the Enhanced EFI Boot Manager Menu (gray background), select **EFI Boot Manager Menu** → **EFI Shell**.
 - If you are using the Legacy EFI Boot Manager Menu (black background), select **EFI Boot Manager Menu** → **EFI Shell [Built-in]**.

Locate the DVD/CD Drive

When hardware (for example, the HDD, a USB device, vMedia, or a DVD-ROM drive) is added to a system after it has booted to the EFI, the EFI Shell environment does not detect the new device. You must reconnect the device driver for the EFI Shell to recognize the device.

The EFI Shell environment creates default mappings for device handles that support a recognized file system. After you change the system configuration or add a new device, you must regenerate these mappings.

To enable the EFI Shell to detect and access the DVD/CD drive, follow these steps:

1. From the EFI Shell, enter the `reconnect -r` command.

The `reconnect` command reconnects drivers from a device, disconnecting drivers from all devices and then reconnecting them. If you do not specify a device handle, the `reconnect` operation is performed on all handles in the system. If you specify a device handle, only the device handle and the devices following it are reconnected.

2. From the EFI Shell, enter the `map -r` command.

The `-r` option regenerates all mappings in a system. The EFI Shell displays the device mapping table, as follows.

```
fs0 : Acpi (PNP0A03,0) /Pci (2|0) /Ata (Primary,Master) /CDROM (Entry1)
blk0 : Acpi (PNP0A03,1) /Pci (1|0) /Scsi (Pun0,Lun0)
blk1 : Acpi (PNP0A03,0) /Pci (2|0) /Ata (Primary,Master)
blk2 : Acpi (PNP0A03,0) /Pci (2|0) /Ata (Primary,Master) /CDROM (Entry1)
```

3. Note the device name of the CD device (in the above example):

`fs0`

Use the device name to explore the contents of the CD or DVD.

The `map` command displays or defines a mapping between a user-defined name and a device handle. The most common use of this command is to assign drive letters to device handles that support a file system protocol. When these mappings are created, the drive letters can be used with all file manipulation commands.

Use the `map` command to create or to delete mappings with the `-d` option. If you use the `map` command without parameters, all current mappings are listed. If you use the `-v` option, the mappings are shown with additional information on each mapped handle. The following table describes the device mapping fields.

Table 1-4 EFI Device Mapping Fields

Item	Description
blk n	This is a block device that indicates a physical drive or a partition on a physical drive. A physical drive can be a hard disk drive or a removable media drive. A Part n message displays when a disk drive contains a partition.
Acpi (Device,X)	Acpi is Advanced Configuration and Power Interface. The device type is the first entry in parentheses. The second entry, X, is the PCI host number.
Pci (D/F)	This indicates PCI-related information. D is the PCI device/slot number and F is the PCI function number.
Scsi (Pun.Lun)	This denotes the physical characteristic of the SCSI disk. Pun is the SCSI number and Lun is the LUN number on the physical device.
HD (Part,Sig)	This indicates the partition, Part, and EFI signature, Sig, on the partition.

Set ACPI Flag to Windows (Cell-Based Servers Only)

On cell-based servers, you must set the Advanced Configuration and Power Interface (ACPI) flag to the value relevant for the OS that it boots. For the server to boot to Windows Server 2008 R2, set the ACPI flag to **windows**.

If you purchased your server with a Windows OS option, this flag is set to **windows** in the factory. If you purchased the server with a different OS or no OS, you must set this flag to **windows**.



CAUTION: If you boot the server to Windows Server 2008 R2 without setting the ACPI flag to **windows**, the OS displays a blue screen error.

To set the ACPI flag, follow these steps:

1. From the EFI Shell, enter the `acpiconfig` command.
EFI displays the current ACPI settings. If the flag is set to **windows**, EFI displays the text, `acpiconfig: windows`.
2. If the flag is not set to **windows**, enter the `acpiconfig windows` command.
3. Enter the `acpiconfig` command again, to display the settings again, and verify that the flag is set correctly.



NOTE: Updating the system firmware can reset this flag to **default**. Verify that the flag is set to **windows**, after you flash the system firmware.

Set Cell Local Memory to 100% (Cell-Based Servers Only)

HP recommends that you initially set all cell local memory (CLM) parameters to 100%, for optimal server performance. You should also do this again, whenever you add or remove cells from a partition. This setting allocates all available cell local memory for the use of that cell only, preventing unnecessary reads and writes to physical memory over the server backplane.

Modify CLM settings for each nPartition using the `nPartition` command (`parmodify`). You must first install nPartition tools on the Integrity server or on a remote management station. For information on installing these tools, see the *nPartition Guide* at the following web addresses:

- to locate documents by operating system: <http://www.hp.com/go/windows-on-integrity-docs>
- to locate documents by server model number: http://www.hp.com/go/integrity_servers-docs

To set the CLM parameter, follow these steps:

1. From the server console, run the `parmodify` command with `-p#` and `-m#` options to modify each cell's attributes in each nPar you modify.

For example:

```
parmodify -p0 m0::::100%
```

where `-p` is the partition number, and `-m` is the cell number in that partition. Sets cell local memory to 100% in cell 0, partition 0.

2. Restart the server for the changes to take effect.

Specify the Network Interface Card for a Network Boot

PXE is built on common Internet protocols and services, including TCP/IP, DHCP, and TFTP. PXE extensions to DHCP enable WDS servers to communicate with the network-bootable HP Integrity servers.

You can specify the network interface card (NIC) for PXE to use to communicate with the WDS server. When the HP Integrity server boots from this NIC, it effectively boots from the remote WDS server. Working with the WDS server, PXE installs a new image of Windows Server 2008 R2 on the HP Integrity server.

To enable PXE on the HP Integrity server from the EFI Shell, follow these steps:

1. From the EFI Boot Manager, select **EFI Shell**. The device mapping table displays.
2. Enter the `lanboot select` command.
3. At the `Select desired LAN:` prompt, enter the number of the NIC connected to the PXE server.
4. Exit the EFI Shell.

2 Installing the OS

This chapter provides instructions for installing the operating system (OS) using a headless console, a GUI console, or a Preboot Execution Environment (PXE) enabled network interface card (NIC). This chapter also provides reinstallation instructions for Windows Server 2008 R2. Each method comprises a series of tasks, concluding with two tasks that verify that the OS was installed correctly. You must install the HP Integrity Support Pack after installing the OS. You must also install the operating system updates and security updates using the Smart Update media.

If the Windows Server 2008 R2 operating system is installed on your system, or if it was installed by HP before your system was delivered, you need not perform the steps in this chapter. Proceed to [“Installing and Configuring the Management Tools”](#) (page 61), and begin the installation of your management tools software.

If you want to install or reinstall the Windows Server 2008 R2 OS, or if you want to migrate to Windows Server 2008 R2 from another OS, install the OS and OS updates by performing the steps described in this chapter, as follows:

- If you are installing your OS for the first time, or migrating from a different operating system:
 - If you are installing locally, select one of the following options:
 - [“Install from a Headless Console”](#) (page 31)
 - [“Install from a GUI Console”](#) (page 39)
 - If you are not installing locally, select one of the following options:
 - [“Install from PXE”](#) (page 47)
 - [“Installing from the IRC”](#) (page 58)
- If you are reinstalling your OS, select one of the following options:
 - [“Reinstall from a Headless Console”](#) (page 47)
 - [“Reinstall from a GUI Console”](#) (page 49)
- After installing or reinstalling your OS, perform the following tasks:
 - [“Activate the OS”](#) (page 51)
 - [“Apply OS Updates Using the Smart Update Media”](#) (page 54)
 - [“Enable Windows Components”](#) (page 55)
 - [“Verify System Device Drivers and Register for Updates”](#) (page 56)
 - To determine whether you need to perform any final tasks, see [“Miscellaneous Installation Issues”](#) (page 57)

Install from a Headless Console

Installing from a headless console involves booting from the HP Smart Setup media, running EBSU, launching Windows Setup, loading OS files to the boot disk, and booting the server from the boot disk. You must be connected to the management processor (MP) of the target server using a terminal emulation application such as HyperTerminal.



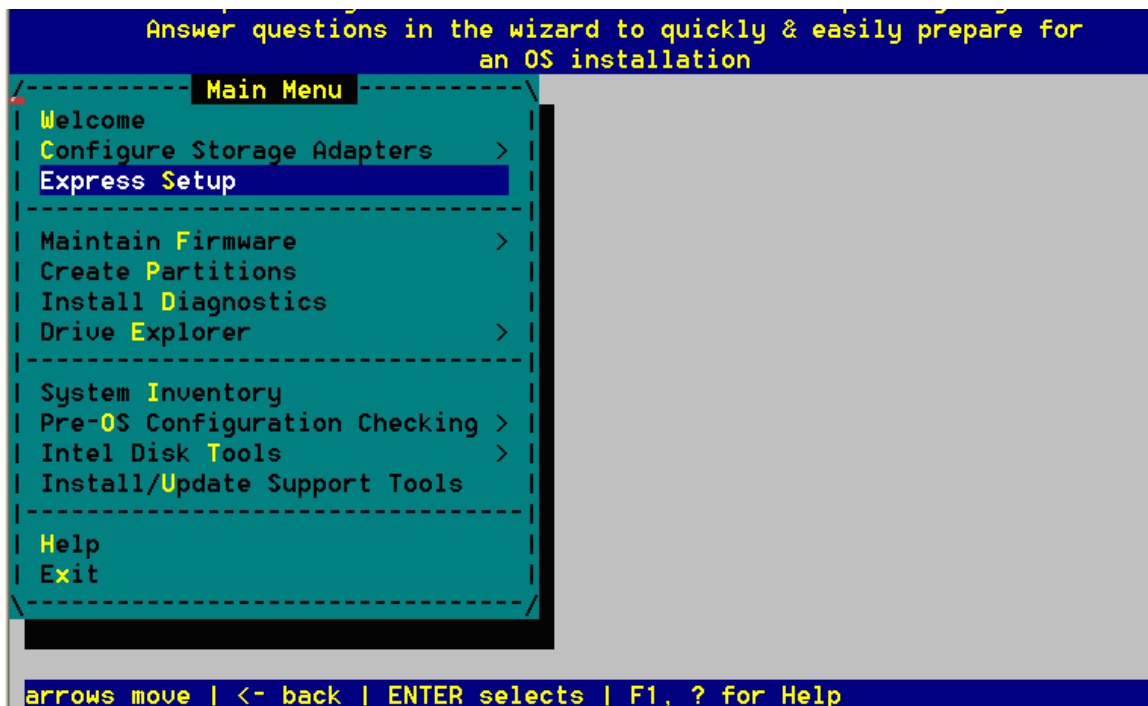
NOTE: For an overview of the benefits, concepts, and terminology of headless OS installation on HP Integrity servers, see [“Headless Windows Installations”](#) (page 107).

To run EBSU, follow these steps:

1. Power on the server. The server boots to EFI.
You can use the EFI Boot Manager from the Enhanced interface (gray background) or the Legacy interface (black background).
2. Load the HP Smart Setup media into the server DVD drive.

3. From the EFI Boot Manager Boot Menu, select **Internal Bootable DVD**, and press **Enter**. EBSU starts and displays the Welcome screen.
4. Click **OK**, and press **Enter**.
5. From the Main Menu, select **Express Setup** and press **Enter**.

Figure 2-1 EBSU Main Menu



NOTE: In rx7640/rx8640/Superdome cellular systems, and in BL860c i2/BL870c i2/BL890c i2/rx 2800 i2 server blades, the EBSU Main Menu includes the **Pre-OS Configuration Checking** option. In other systems, this option is not available.

Also, in BL860c i2/BL870c i2/BL890c i2 server blades, the EBSU Main Menu does NOT include the **Install/Update Support Tools** option.

6. EBSU displays a screen with special instructions for RAID users. Follow the instructions, if applicable, and press **Enter** to continue.
7. EBSU displays the firmware update screen, listing each device, its installed firmware version, and the firmware version on the Smart Setup media. Select the firmware devices you want to update. To continue, select **Next**, and press **Enter**.

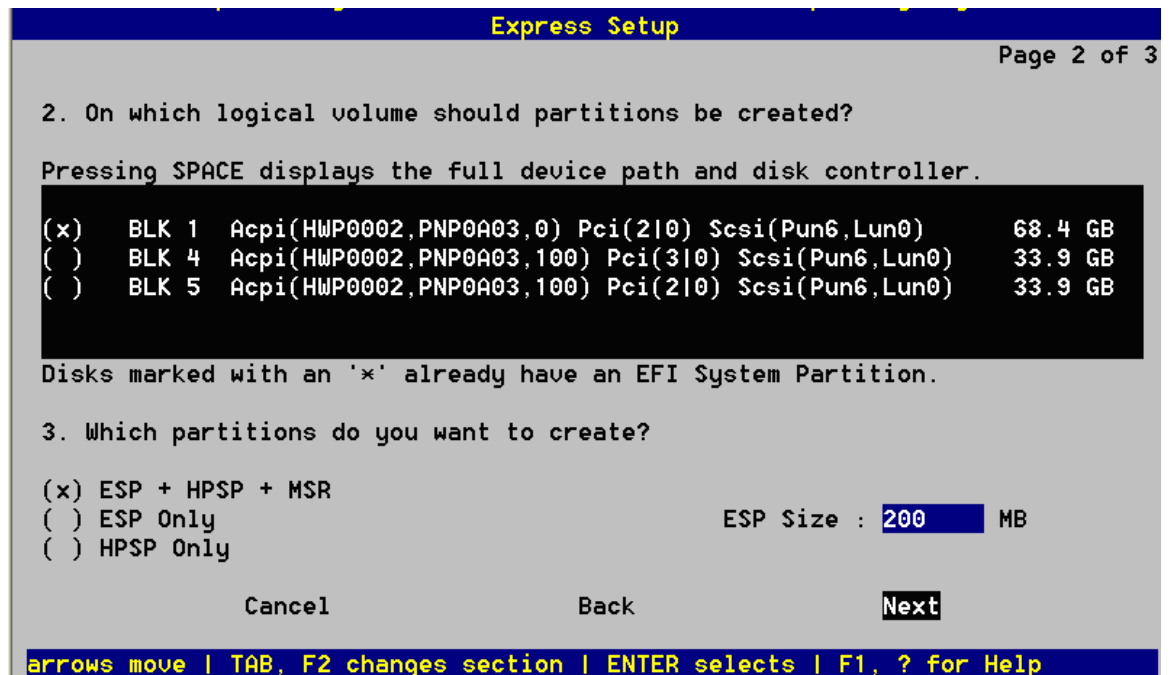
Figure 2-2 EBSU Firmware Update Screen



NOTE: You might not be able to use EBSU to flash the firmware of some devices. You cannot flash the firmware if the installed version is the same or higher than the version on the Smart Setup media.

8. EBSU displays the partition disk screen. Select **ESP + HPSP + MSR** or **ESP Only**. HP recommends the default (ESP + HPSP + MSR) as a way to simplify the maintenance of your server.

Figure 2-3 EBSU Partition Disk Screen



9. EBSU displays the install options screen. Accept the default options to install the Drive Explorer utility (for browsing a drive in EFI) and offline diagnostic tools (from the HP

Integrity Offline Diagnostics CD) in the HPSP partition. Also specify which version of the Windows OS Installer to launch (in this case: **Windows Server 2008 R2**). Then select **Next** and press **Enter**.

Figure 2-4 EBSU Install Options Screen

Express Setup Page 3 of 3

4. Do you want to install the Drive Explorer utility on the HPSP?

(x) Yes
() No

5. Do you want to install the HP Integrity Offline Diagnostics on the HPSP?

(x) Yes
() No

6. Which version of the Windows OS installer should be launched?

() None
() Windows Server 2008 SP2
(x) Windows Server 2008 R2

Cancel Back Next

arrows move | TAB, F2 changes section | ENTER selects | F1, ? for Help



NOTE: In BL860c i2/BL870c i2/BL890c i2/rx 2800 i2 server blades, this screen does not include the **Windows Server 2008 SP2** option.

10. EBSU prompts you to execute an unattended Windows Server 2008 installation. Press **Yes** to continue.

Figure 2-5 EBSU Prompt Screen

(?) QUESTION: Obsidian 2 USB/UGA video device was found. The unattended wizard is optional. Would you like to execute an unattended Windows Server 2008 installation?

NOTE: Make sure that the video card firmware is updated if you want to execute an attended Windows Server 2008 installation. Please see the website for the latest video card firmware:
<http://www.hp.com/support/itaniumservers>

No Yes

11. In BL860c i2/BL870c i2/BL890c i2/rx 2800 i2 server blades, EBSU displays information about setting the memory interleave value. After reading, press **Enter** to continue.
12. When prompted by EBSU, enter the Product Key, Administrator Password, and OS language. Remember that passwords are case-sensitive, so check your **Caps Lock** key first.

Figure 2-6 EBSU Product Key Screen

Express Setup Page 4 of 4

The following information is required to execute an unattended Microsoft Windows Server 2008 installation.

Product Key: [REDACTED]

NOTE: The Product Key consists of 25 characters in the following format:
XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX.
Make sure you have entered the correct Product Key because it will only be validated during the Windows installation process.

Administrator Password: [REDACTED]

Re-enter Password: [REDACTED]

Windows NTFS partition size: **69407** MB

language-region: **en-US** NOTE: e.g. en-US, ja-JP, ..., etc.

Cancel Back Setup

arrows move | TAB, F2 changes section | ENTER selects | F1, ? for Help

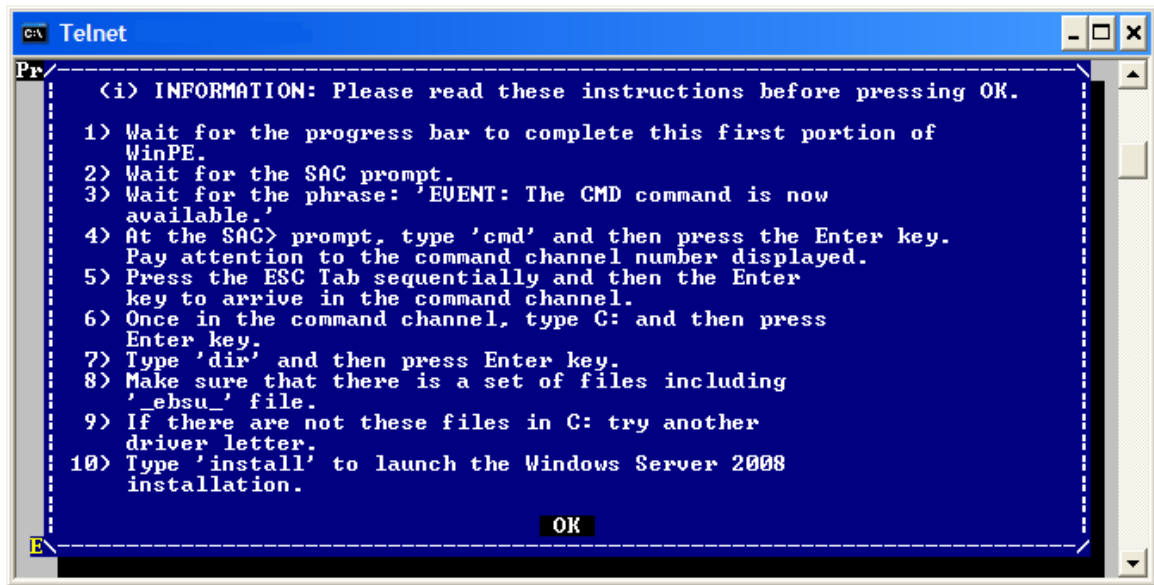
13. EBSU displays a warning that all partitions on the disk will be overwritten. Select **Continue** and press **Enter**.
14. EBSU displays a warning that a temporary MSDATA partition will be created. Press **Enter**.
15. EBSU displays an informational pop-up that the installation will begin. Press **Enter**.
16. The installation begins and progresses through partition creation and firmware updates. Insert the HP Integrity Offline Diagnostics CD when prompted, then press **Enter**.



NOTE: At this point, if you cannot locate the Offline Diagnostics CD, select **Skip** and press **Enter** to bypass installation of the diagnostic utilities. You can always install them later onto the HPSP partition, from the CD.

17. EBSU displays an informational screen. Write down the instructions, in case you need them later (for example, if the system cannot locate the Internal Bootable DVD drive), and press **Enter**.

Figure 2-7 EBSU Screen #1



18. When EBSU prompts you, insert the Microsoft Windows Server 2008 R2 operating system CD and press **Enter**.

Figure 2-8 EBSU Screen #2



19. Press any key when prompted to boot from the CD or DVD (be ready to do this quickly, or the system could time out).
20. Windows begins loading files from the disk. When the progress bar reaches 100%, the screen displays the message: The CMD command is available.
21. Type **cmd** to launch a CMD prompt session.
22. Press the **Esc + Tab** keys to open a command channel.
23. Move to the drive where the **_ebsu_** directory is located (this could be **C: **, or **H: **, or some other drive letter, depending on your system configuration).

Figure 2-9 EBSU Screen #3

```
H:\>dir
Volume in drive H is MSDATA
Volume Serial Number is D822-BD45

Directory of H:\

07/27/2009  11:58 PM                0 _ebsu_
11/08/2007  11:40 AM                70 delmsdata_tmp.txt
11/08/2007  11:40 AM             833 install.cmd
11/08/2007  11:40 AM             592 launch_setup.cmd
06/30/2008  01:27 PM             391 chkdriver.cmd
07/27/2009  11:58 PM           5,388 win2008_tmp.xml
12/18/2007  11:16 AM          80,896 getdiskid.exe
              7 File(s)           88,170 bytes
              0 Dir(s)        10,350,592 bytes free

H:\>
```



NOTE: In BL860c i2/BL870c i2/BL890c i2/rx 2800 i2 server blades and not shown in the above image, there are two more files (`delthisvolume.cmd` and `readme1st.txt`) and two more directories (`$WinPEDriver` and `data`).

24. Type `install.cmd` to begin.
25. Press the **Esc + Tab** keys to open a different command channel. Verify there are no error messages in the `SACSetupErr` channel.

Figure 2-10 EBSU Screen #4

```
EVENT:  A new channel has been created.  Use "ch -?" for channel help.
Channel: Cmd0003
SAC>
EVENT:  A new channel has been created.  Use "ch -?" for channel help.
Channel: SACSetupAct
SAC>
EVENT:  A new channel has been created.  Use "ch -?" for channel help.
Channel: SACSetupErr
SAC>
```

26. The system will restart during the installation. Wait until the `EVENT :` prompt displays, and then type `cmd`.
27. Press **Esc + Tab**, and when prompted, enter the Administrator username and password. Remember that passwords are case-sensitive.

Figure 2-11 EBSU Screen #5

```
Please enter login credentials.
Username: Administrator
Domain  :
Password: *****_
```

28. Type `hostname` to display the hostname information (you will enter the hostname information exactly as it appears, in the next step).

29. Type the following: `wmic RDToggle where ServerName="hostname" call SetAllowTSConnections 1`

This command enables display of the remote desktop.

Figure 2-12 EBSU Screen #6

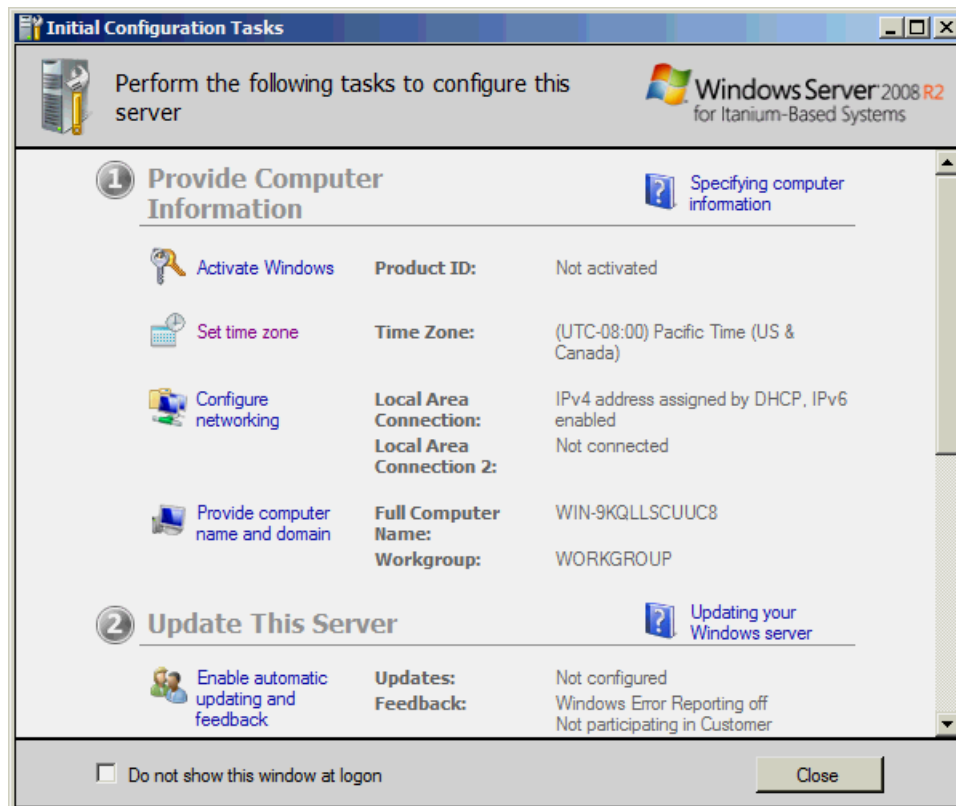
```
Microsoft Windows [Version 6.0.6002]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Windows\system32>hostname
WIN-KMZAJUH6A53

C:\Windows\system32>
C:\Windows\system32>wmic RDToggle where ServerName="WIN-KMZAJUH6A53" call SetAllowTSConnections 1
```

30. The system finishes booting to the Desktop for the first time and launches the Initial Configuration Tasks screen.

Figure 2-13 Initial Configuration Tasks Screen



31. At this screen, you can set up and configure system-wide settings and perform tasks such as the following:
- Set time zone
 - Configure networking
 - Provide computer name and domain info
 - Enable automatic updating and feedback
 - Download and install updates
 - Add roles
 - Add features

- Enable Remote Desktop
- Configure Windows Firewall

You must configure some of these settings, to prepare your system for its intended use in your production environment. However, it is beyond the scope of this document to make specific recommendations, as each user has a unique combination of factors such as system I/O, storage, intended use, and so on. See your System Administrator and the operating system online help.

32. Installation of the OS is complete.

After installing the OS, perform these tasks next:

1. “Install the Integrity Support Pack (ISP)” (page 61)
2. “Activate the OS” (page 51)
3. “Apply OS Updates Using the Smart Update Media” (page 54)
4. “Enable Windows Components” (page 55)
5. “Verify System Device Drivers and Register for Updates” (page 56)
6. To determine whether you need to perform any additional tasks, see “Miscellaneous Installation Issues” (page 57).

Then, see the sections describing configuration of the management tools, and perform these tasks:

1. “Configure System Management Homepage” (page 66)
2. “Configure and Verify the WBEM Providers” (page 64)
3. “Verify Installation of the nPartition Management Tools” (page 67)

Install from a GUI Console

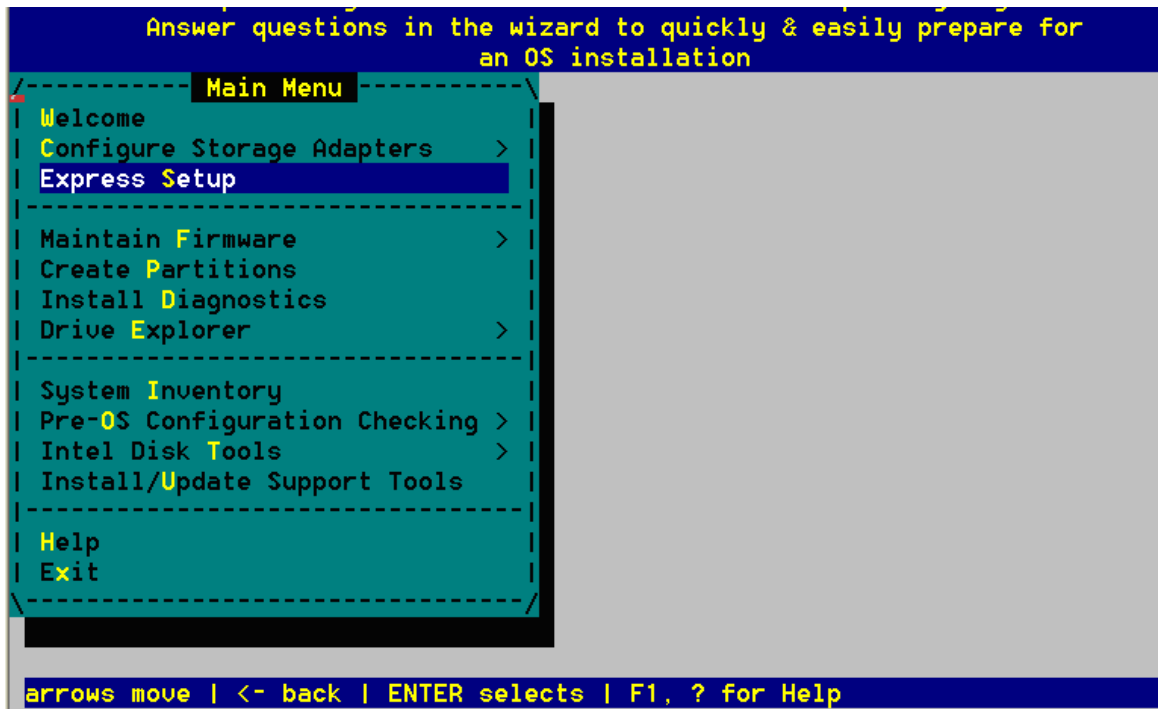
This section describes how to install the OS using a GUI console and the EFI-Based Setup Utility (EBSU). EBSU provides an easy-to-use interface to complete the following tasks:

- flash the firmware
- partition the hard disk
- install diagnostic tools
- configure storage controllers
- run other EFI utilities.

To run EBSU, follow these steps:

1. Power on the server. The server boots to EFI.
You can use the EFI Boot Manager from the Enhanced interface (gray background) or the Legacy interface (black background).
2. Load the HP Smart Setup media into the server DVD drive.
3. From the EFI Boot Manager Boot Menu, select **Internal Bootable DVD**, and press **Enter**. EBSU displays the Welcome screen.
4. Click **OK** and press **Enter**.
5. From the Main Menu, select **Express Setup** and press **Enter**.

Figure 2-14 EBSU Main Menu



NOTE: In rx7640/rx8640/Superdome cellular systems, and in BL860c i2/BL870c i2/BL890c i2/rx 2800 i2 server blades, the EBSU Main Menu includes the **Pre-OS Configuration Checking** option. In other systems, this option is not available.

Also, in BL860c i2/BL870c i2/BL890c i2 server blades, the EBSU Main Menu does NOT include the **Install/Update Support Tools** option.

6. EBSU displays a screen with special instructions for RAID users. Perform the instructions if applicable, then press **Enter** to continue.
7. EBSU displays the firmware update screen, listing each device, its installed firmware version, and the firmware version on the Smart Setup media. Select the firmware devices you want to update. To continue, select **Next** and press **Enter**.

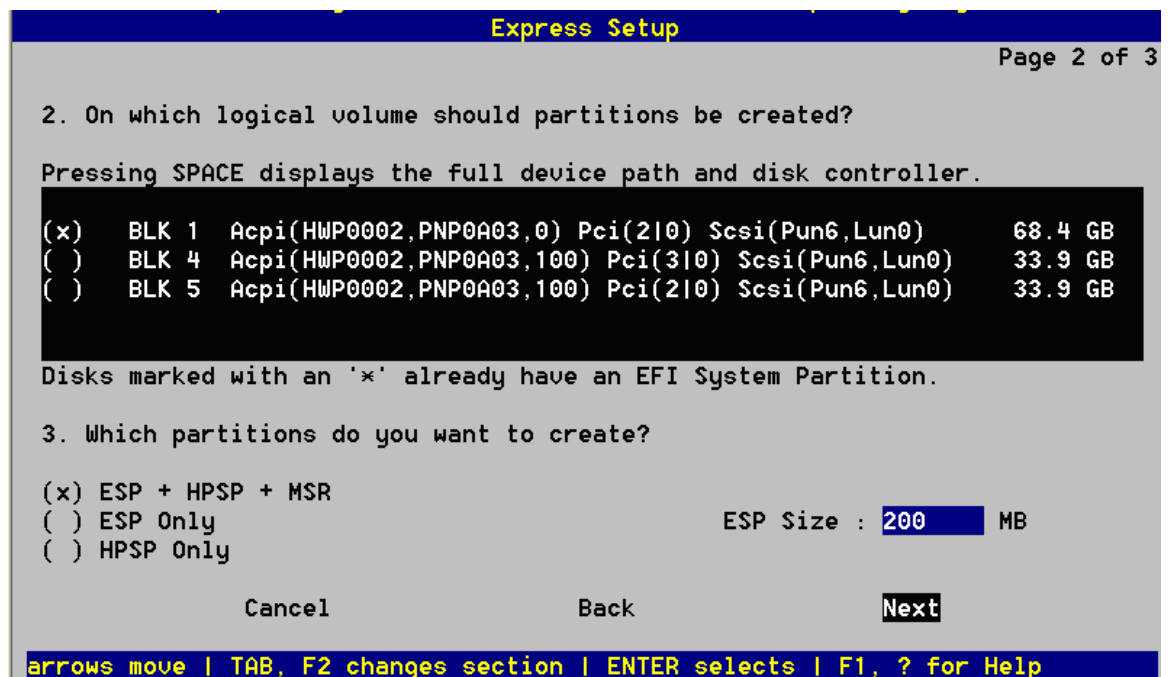
Figure 2-15 EBSU Firmware Update Screen



NOTE: You might not be able to use EBSU to flash the firmware of some devices. You cannot flash the firmware if the installed version is the same or higher than the version on the Smart Setup media.

- EBSU displays the partition disk screen. Select **ESP + HPSP + MSR**, or **ESP Only**. HP recommends the default (ESP + HPSP + MSR) as a way to simplify the maintenance of your server.

Figure 2-16 EBSU Partition Disk Screen



- EBSU displays an install options screen. Accept the default options to install the Drive Explorer utility (for browsing a drive in EFI) and offline diagnostic tools (from the HP

Integrity Offline Diagnostics CD) in the HPSP partition. Also, specify which version of the Windows OS Installer to launch (in this case, **Windows Server 2008 R2**). Then, select **Next** and press **Enter**.

Figure 2-17 EBSU Install Options Screen

The screenshot shows the 'Express Setup' window, page 3 of 3. It contains three questions with radio button options:

- 4. Do you want to install the Drive Explorer utility on the HPSP?
☒ Yes
☐ No
- 5. Do you want to install the HP Integrity Offline Diagnostics on the HPSP?
☒ Yes
☐ No
- 6. Which version of the Windows OS installer should be launched?
☐ None
☐ Windows Server 2008 SP2
☒ Windows Server 2008 R2

At the bottom are three buttons: 'Cancel', 'Back', and 'Next'. A footer bar contains the text: 'arrows move | TAB, F2 changes section | ENTER selects | F1, ? for Help'.



NOTE: In BL860c i2/BL870c i2/BL890c i2/rx 2800 i2 server blades, this screen does not include the **Windows Server 2008 SP2** option.

10. EBSU prompts you to execute an unattended Windows Server 2008 installation. Press **No** to continue.

Figure 2-18 EBSU Prompt Screen

The screenshot shows a blue prompt screen with white text. It asks: '(?) QUESTION: Obsidian 2 USB/UGA video device was found. The unattended wizard is optional. Would you like to execute an unattended Windows Server 2008 installation?'. Below this is a note: 'NOTE: Make sure that the video card firmware is updated if you want to execute an attended Windows Server 2008 installation. Please see the website for the latest video card firmware: <http://www.hp.com/support/itaniumservers>'. At the bottom are two buttons: 'No' and 'Yes'.

11. In BL860c i2/BL870c i2/BL890c i2/rx 2800 i2 server blades, EBSU displays information about setting the memory interleave value. After reading, press **Enter** to continue.
12. EBSU displays a warning that all partitions on the disk will be overwritten. Select **Continue** and press **Enter**.

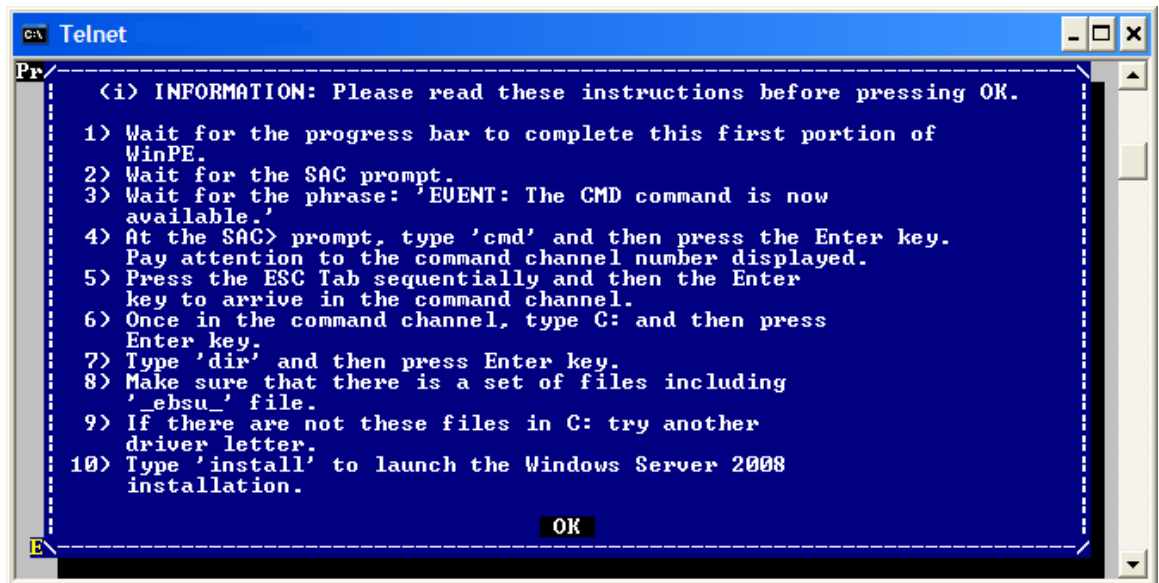
13. In BL860c i2/BL870c i2/BL890c i2/rx 2800 i2 server blades, EBSU displays information that a temporary MSDATA partition will be created. After reading, press **Enter**.
14. EBSU displays an informational pop-up that the installation will begin. Press **Enter**.
15. The installation begins and progresses through partition creation and firmware updates. Insert the HP Integrity Offline Diagnostics CD when prompted, then press **Enter**.



NOTE: At this point, if you cannot locate the Offline Diagnostics CD, select **Skip** and press **Enter** to bypass installation of the diagnostic utilities. You can always install them later onto the HPSP partition, from the CD.

16. EBSU displays an informational screen. Record the instructions, in case you need them later (for example, if the system cannot locate the Internal Bootable DVD drive), and press **Enter**.

Figure 2-19 EBSU Screen #1



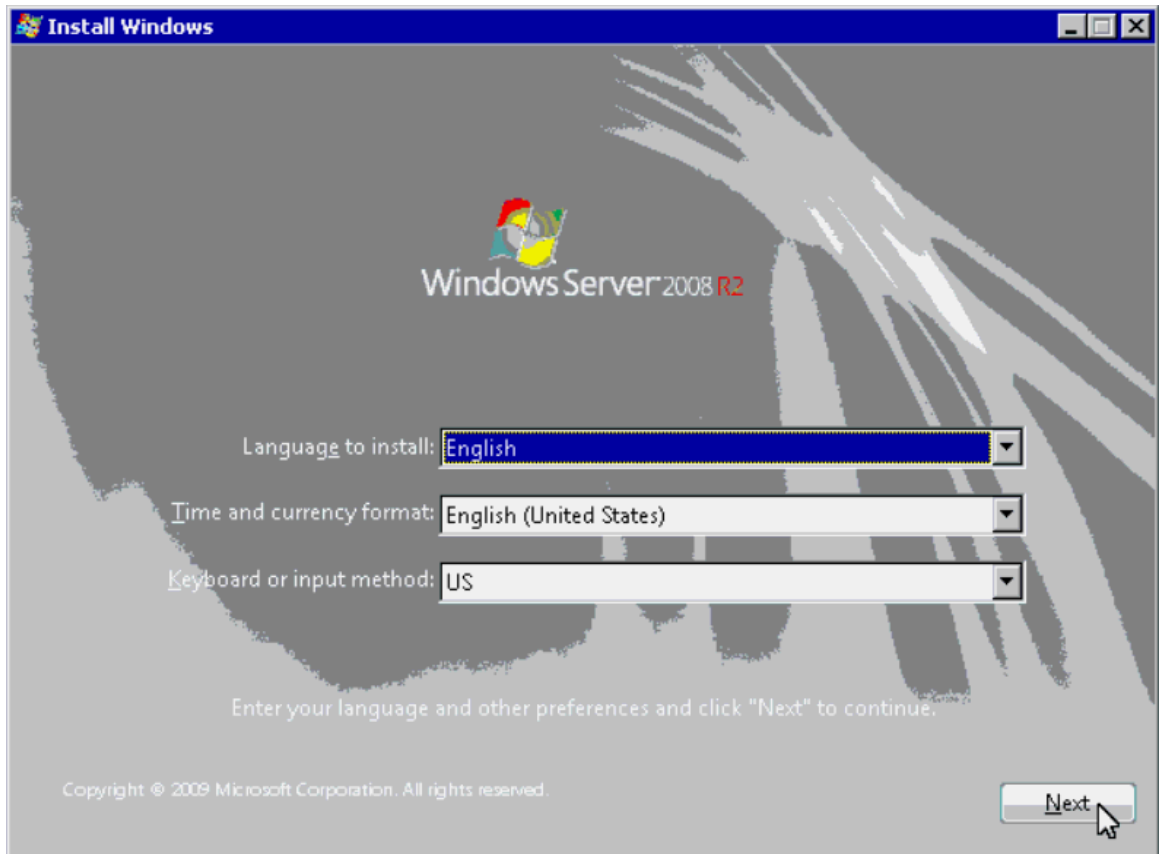
17. When EBSU prompts you, insert the Microsoft Windows Server 2008 R2 operating system CD and press **Enter**.

Figure 2-20 EBSU Screen #2



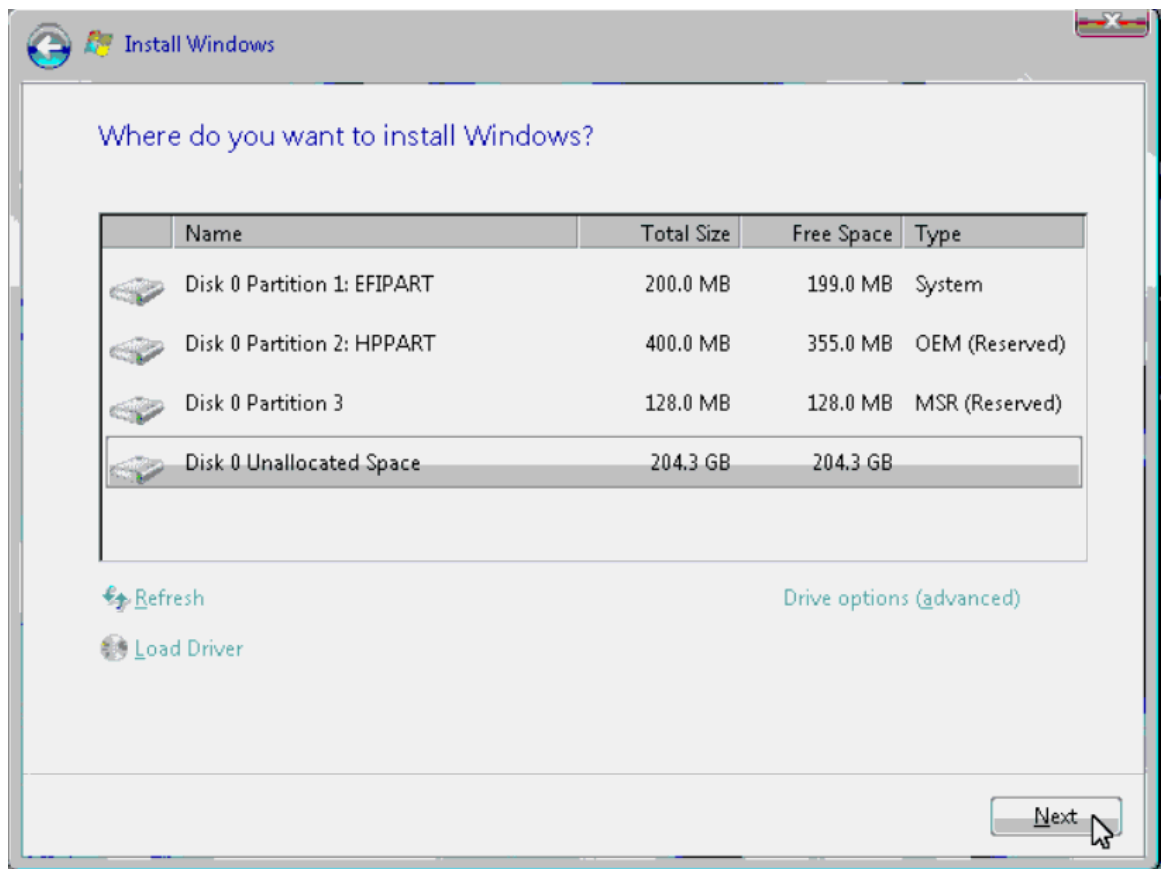
18. Press any key when prompted to continue (be ready to do this quickly or the system could time-out).
19. Windows begins loading files from the disk. When the progress bar reaches 100%, the Install Windows screen displays. Select your default language, time and currency formats, and keyboard or input method, then click **Next**.

Figure 2-21 Install Windows Screen #1



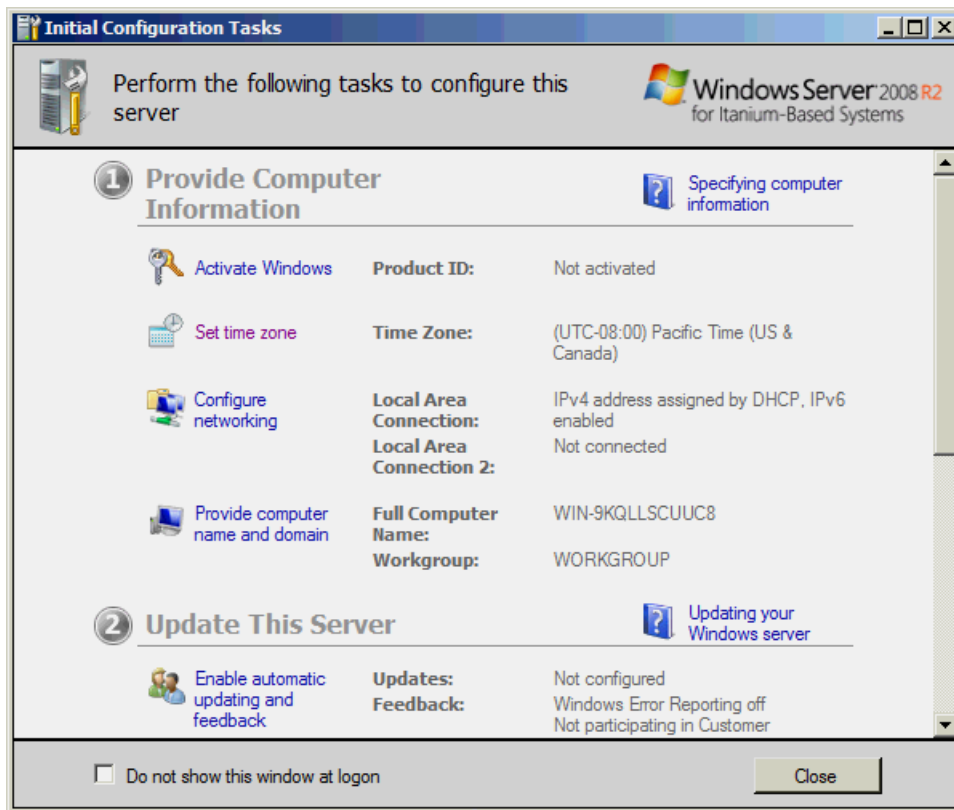
20. At the next screen, click **Install Now**.
21. At the next screen, enter your product key again and click **Next**.
22. At the License Terms screen, check the **I accept the license terms** box and click **Next**.
23. At the next screen, click **Custom (advanced)**.
24. At the next screen, you are asked on which system partition to install the operating system. If more than one partition is available, you should select one that is marked "Unallocated", and also one that is formatted as NTFS. Then click **Next**.

Figure 2-22 Install Windows Screen #2



25. At the next pop-up screen, click **Next** to continue. Installation of the operating system begins.
26. When the installation finishes, you are prompted to change your password to log on the first time. Click **OK**.
27. Enter the new system administrator password twice and click the arrow button.
28. The password change is confirmed. Click **OK** to continue.
29. The system finishes booting to the desktop for the first time and launches the Initial Configuration Tasks screen.

Figure 2-23 Initial Configuration Tasks Screen



30. At this screen, you can set up and configure system-wide settings, and perform tasks such as:

- Set time zone
- Configure networking
- Provide computer name and domain info
- Enable automatic updating and feedback
- Download and install updates
- Add roles
- Add features
- Enable Remote Desktop
- Configure Windows Firewall

You must configure some of these settings, to prepare your system for its intended use in your production environment. However, it is beyond the scope of this document to make specific recommendations, since each user has a unique combination of factors such as system I/O, storage, intended use, and so on. See your System Administrator and the operating system online help.

31. In BL860c i2/BL870c i2/BL890c i2/rx 2800 i2 server blades, navigate to the MSDATA partition, open the file named `readme1st.txt`, and follow any directions given there.



NOTE: This step is optional. The MSDATA partition does not affect Windows usage. You can delete it, if desired, to avoid confusion.

32. Installation of the OS is complete.

After installing the OS, perform these tasks next:

1. "Install the Integrity Support Pack (ISP)" (page 61)
2. "Activate the OS" (page 51)

3. “Apply OS Updates Using the Smart Update Media” (page 54)
4. “Enable Windows Components” (page 55)
5. “Verify System Device Drivers and Register for Updates” (page 56)
6. To determine whether you need to perform any additional tasks, see “Miscellaneous Installation Issues” (page 57).

Then, see the sections describing configuration of the management tools, and perform these tasks:

1. “Configure System Management Homepage” (page 66)
2. “Configure and Verify the WBEM Providers” (page 64)
3. “Verify Installation of the nPartition Management Tools” (page 67)

Install from PXE

When a PXE-enabled client connected to the network boots up, the computer initiates a network service request. A DHCP discover packet is sent to the network requesting the IP address of an available WDS server. The DHCP server responds to the request by providing an IP address to the client. Any available WDS server can respond with its IP address, and the name of the boot file the client should request if the client selects that WDS server for service.

To install Windows Server 2008 R2 from PXE, follow these steps:

1. From EFI, select the **Boot Manager**.
2. At the Boot Manager, select the **Boot Options** menu.
3. From the list of available boot sources, select the NIC to boot from and press **Enter**.
4. At the PXE boot status window, press **Enter** to continue.
5. At the login screen, enter a valid user name and password, and press **Enter**.
6. At the OS selection screen, select the OS to be installed and press **Enter** to start the installation.
7. Complete the installation by following the instructions on the screen.

Reinstall from a Headless Console

HP Integrity servers that are factory-installed with Windows Server 2008 R2 are shipped with HP Reinstallation media, which enables you to restore the system to its factory settings. Reinstalling the operating system involves loading the image from the Reinstallation media onto the boot disk and, after the initial boot, configuring the system.

Load the System Image to the Boot Disk

To reinstall Windows Server 2008 R2 from a headless console, follow these steps:

1. Configure your boot controller and drive. If you are using a RAID adapter, follow the RAID installation documentation to prepare the adapter and configure the RAID type. Then disconnect or unplug all drives except the one connected to the boot controller, to prevent unintentional data loss.



CAUTION: Reinstallation overwrites all files on the boot disk. The boot disk is determined by bus search order and might not be the disk you expect it to be. HP strongly recommends disconnecting or unplugging all drives from the server except the boot disk. This includes all SAN storage.

2. Insert the HP Reinstallation media into the DVD drive.



NOTE: You can also use Virtual Media (vMedia) as the source of the reinstallation image.

3. From the headless console, log in to the MP port using a terminal emulator such as HyperTerminal or PuTTY. Then enter the MP user name and password.



NOTE: The default MP “user name/password” is “Administrator/Admin” for BL8x0 i2 and rx2800 i2 server blades, and “Admin/Admin” for all other servers.

4. Type `co` and press **Enter**.
5. Deletion of existing Windows Boot Manager entries is recommended. To delete boot entries, choose one of the following methods:
 - Use the EFI Maintenance menu:
 - If you are using the Enhanced EFI Boot Manager Menu (gray background), select **EFI Boot Manager Menu** → **Boot Configuration** → **Remove Boot Entry**.
 - If you are using the Legacy EFI Boot Manager Menu (black background), select **EFI Boot Manager Menu** → **Boot Option Maintenance Menu** → **Delete Boot Option(s)**.

Then scroll down to the desired boot entry and press **Enter**.

- Clear the NVRAM using the instructions in your Platform Reference Guide.
6. If there were boot entries that required deletion in the previous step, reboot the system now by typing `reset` and pressing **Enter**.
 7. Log in to the MP port again using HyperTerminal or PuTTY, and enter the MP user name and password.
 8. At the `MP>` prompt, type `co` and press **Enter**.



NOTE: You can also use Remote Serial Console to perform this step.

9. Boot from the Reinstallation media using one of the following methods:
 - **Method 1:** Select **EFI Boot Manager menu** → **Internal Bootable DVD** from EFI Boot Manager (if this choice is available). If you use this method, you can skip steps 10 and 11 and go directly to step 12.
 - **Method 2:** Select **EFI Shell** and go to the `/CDROM(Entry0)` file system by typing `fs0 :` and pressing **Enter**.
10. Start the WinPE OS Loader by typing `cd \efi\boot` and pressing **Enter**.
11. Type `bootia64.efi` and press **Enter**.
12. When the SAC prompt appears (`EVENT:`), type `cmd` and press **Enter**.
13. Hold down the **Esc** key, press the **Tab** key once, then release both keys and press **Enter** to switch to a new command channel.
14. At the command prompt, type `txtrestore` and press **Enter**.
15. If the system indicates that the current date is invalid, use the `date` command to enter the current date. Then reenter the `txtrestore` command again.
16. Read the Image Restore Tips displayed in the next screen and follow the suggestions provided. When ready to continue, press **y** and then **Enter**. If you want to abort, press **n** and then **Enter** instead.
17. The system prompts you to select which adapter to install. Select the desired adapter number from the list displayed.
18. The system prompts you to select which drive to install. Select the desired drive number from the list displayed.
19. Select the partition size (64 GB is the default, and in most cases, the minimum recommended size) and press **Enter**. The maximum partition size is limited to the size of the drive.
20. Select **Y** to continue. The installation process copies files to the hard disk. Do not power off the server during the installation.
21. When all files from the DVD drive are copied to the server boot disk, read the displayed message. If there were any errors during this process you must address the cause of the

errors and repeat this procedure over again from the beginning. If the installation was successful, the system displays: `Reinstall Finished [OK]`.

22. At the prompt, press a letter from the menu displayed (E = Exit; R = Reboot; S = Restart the restore process) and press **Enter** to proceed.
23. Go to the next section for instructions on how to specify the server settings and complete the reinstallation.

Configure after the Initial Boot

To configure Windows Server 2008 R2 after the initial boot from a headless console, follow these steps:

1. Open a terminal server client and log in to Windows Server 2008 R2 by typing `Administrator` for the user name and `Abcdef12` (case-sensitive) for the password.



NOTE: After any period of inactivity, a timeout screen saver displays and you must log back in again using the default system password (case-sensitive): `Abcdef12`.

2. The system prompts you to insert the HP Smart Setup media to install the latest HP drivers and utilities.
 - Click **Yes** if you want to do this now. You will be guided through an installation process similar to the one described here: “[Install the Integrity Support Pack \(ISP\)](#)” (page 61). After you finish this reinstallation procedure, you should also perform the other configuration tasks outlined in the chapter: “[Installing and Configuring the Management Tools](#)” (page 61).
 - Click **No** if you want to do this later and continue. If you click **No**, it is strongly recommended that you inspect the system and update the drivers and utilities before bringing it online in your production environment. See “[Installing and Configuring the Management Tools](#)” (page 61) for instructions on how to do this, especially the first section describing how to install the Integrity Support Pack using your Smart Setup media: (“[Install the Integrity Support Pack \(ISP\)](#)” (page 61)).
3. The system indicates the default password (`Abcdef12`) and asks if you want to change it. HP recommends that you change it now.
4. Enter **y** to change the default password. When the screen prompts you to enter the new password, enter it (strong password format required).
5. When prompted, enter the new password again.
6. At the Welcome screen, click **OK** and the system displays a countdown to zero.
7. The system reminds you to install the latest system updates from Microsoft using your HP Smart Update media, and prompts you to reboot. Click **Yes** to reboot.
8. Activate your operating system. For instructions, see: “[Activate the OS](#)” (page 51).
9. Install any available operating system updates using your HP Smart Update media. For instructions, see: “[Apply OS Updates Using the Smart Update Media](#)” (page 54)
10. Your system is now ready to go online.

Reinstall from a GUI Console

HP Integrity servers that are factory-installed with Windows Server 2008 R2 are shipped with HP Reinstallation media, which enables you to restore the system to its factory settings. Reinstalling the operating system involves loading the image from the Reinstallation media onto the boot disk and, after the initial boot, configuring the system.



NOTE: On systems with an Integrated Lights-Out management processor, you can connect remotely to the target server first (using the instructions provided in this section: “Set Up an Integrated Remote Console” (page 22)), and then follow the reinstallation instructions provided in this section.

Load the System Image to the Boot Disk

To reinstall Windows Server 2008 R2 from the local GUI console, follow these steps:

1. Configure your boot controller and drive. If you are using a RAID adapter, follow the RAID installation documentation to prepare the adapter and configure the RAID type. Then disconnect or unplug all drives except the one connected to the boot controller, to prevent unintentional data loss.



CAUTION: Reinstallation overwrites all files on the boot disk. The boot disk is determined by bus search order and might not be the disk you expect it to be. HP strongly recommends disconnecting or unplugging all drives from the server except the boot disk. This includes all SAN storage.

2. Deletion of existing Windows Boot Manager entries is recommended. To delete boot entries, choose one of the following methods:
 - Use the EFI Maintenance menu:
 - If you are using the Enhanced EFI Boot Manager Menu (gray background), select **EFI Boot Manager Menu** → **Boot Configuration** → **Remove Boot Entry**.
 - If you are using the Legacy EFI Boot Manager Menu (black background), select **EFI Boot Manager Menu** → **Boot Option Maintenance Menu** → **Delete Boot Option(s)**.

Then scroll down to the desired boot entry and press **Enter**.

 - Clear the NVRAM using the instructions in your Platform Reference Guide.

3. Insert the HP Reinstallation media into the DVD drive.
4. Boot from the Reinstallation media using one of the following methods:
 - **Method 1:** Select **EFI Boot Manager menu** → **Internal Bootable DVD** from EFI Boot Manager (if this choice is available). If you use this method, you can skip steps 5 and 6 and go directly to step 7.
 - **Method 2:** Select **EFI Shell** and go to the /CDROM(Entry0) file system by typing `fs0 :` and pressing **Enter**.
5. Start the WinPE OS Loader by typing `cd \efi\boot` and pressing **Enter**.
6. Type `bootia64.efi` and press **Enter**.
7. Click **Reinstall** when the HP Reinstall screen displays.
8. If the system indicates that the current date is invalid, use the `date` command to enter the current date.
9. Read the Warning dialog text and click **Yes** to continue.
10. Read the Image Restore Tips text and type **Y** to continue.
11. The system prompts you to select which adapter to install. Select the desired adapter number from the list displayed.
12. The system prompts you to select which drive to install. Select the desired drive number from the list displayed.
13. Select the partition size (64 GB is the default, and in most cases, the minimum recommended size) and press **Enter**. The maximum partition size is limited to the size of the drive.
14. Select **Y** to continue. The installation process copies files to the hard disk. Do not power off the server during the installation.

15. When all files from the DVD drive are copied to the server boot disk, read the displayed message. If there were any errors during this process you must address the cause of those errors and repeat this procedure over again from the beginning. If the installation was successful, the system displays: `Reinstall Finished`. Click **OK** to continue.
16. At the prompt, press a letter from the menu displayed (E = Exit; R = Reboot; S = Restart the restore process) and press **Enter** to proceed.
17. The system will reboot one or more times and then boot to Windows.
18. You are logged in automatically as Administrator the first time that Windows Server 2008 R2 boots. However, after any period of inactivity, a timeout screen saver displays and you must log back in again using the default system password (case-sensitive): `Abcdef12`.
19. Go to the next section for instructions on how to specify the server settings and complete the reinstallation.

Configure after the Initial Boot

To configure Windows Server 2008 R2 after the initial boot from the local console, follow these steps:

1. The system prompts you to insert the HP Smart Setup media to install the latest HP drivers and utilities.
 - Click **Yes** if you want to do this now. You will be guided through an installation process similar to the one described here: [“Install the Integrity Support Pack \(ISP\)”](#) (page 61). After you finish this reinstallation procedure, you should also perform the other configuration tasks outlined in [“Installing and Configuring the Management Tools”](#) (page 61).
 - Click **No** if you want to do this later and continue. If you click **No**, HP strongly recommends that you inspect the system and update the drivers and utilities before bringing it online in your production environment. See [“Installing and Configuring the Management Tools”](#) (page 61) for instructions on how to do this, especially the first section describing how to install the Integrity Support Pack using your Smart Setup media: [“Install the Integrity Support Pack \(ISP\)”](#) (page 61).
2. The system indicates the default password (`Abcdef12`) and asks if you want to change it. HP recommends that you change it now.
3. Enter **y** to change the default password. When the screen prompts you to enter the new password, enter it (strong password format required).
4. When prompted, enter the new password again.
5. At the Welcome screen, click **OK** and the system displays a countdown to zero.
6. The system reminds you to install the latest system updates from Microsoft using your HP Smart Update media, and prompts you to reboot. Click **Yes** to reboot.
7. Activate your operating system. For instructions, see: [“Activate the OS”](#) (page 51).
8. Install any available operating system updates using your HP Smart Update media. For instructions, see: [“Apply OS Updates Using the Smart Update Media”](#) (page 54)
9. Your system is now ready to go online.

Activate the OS

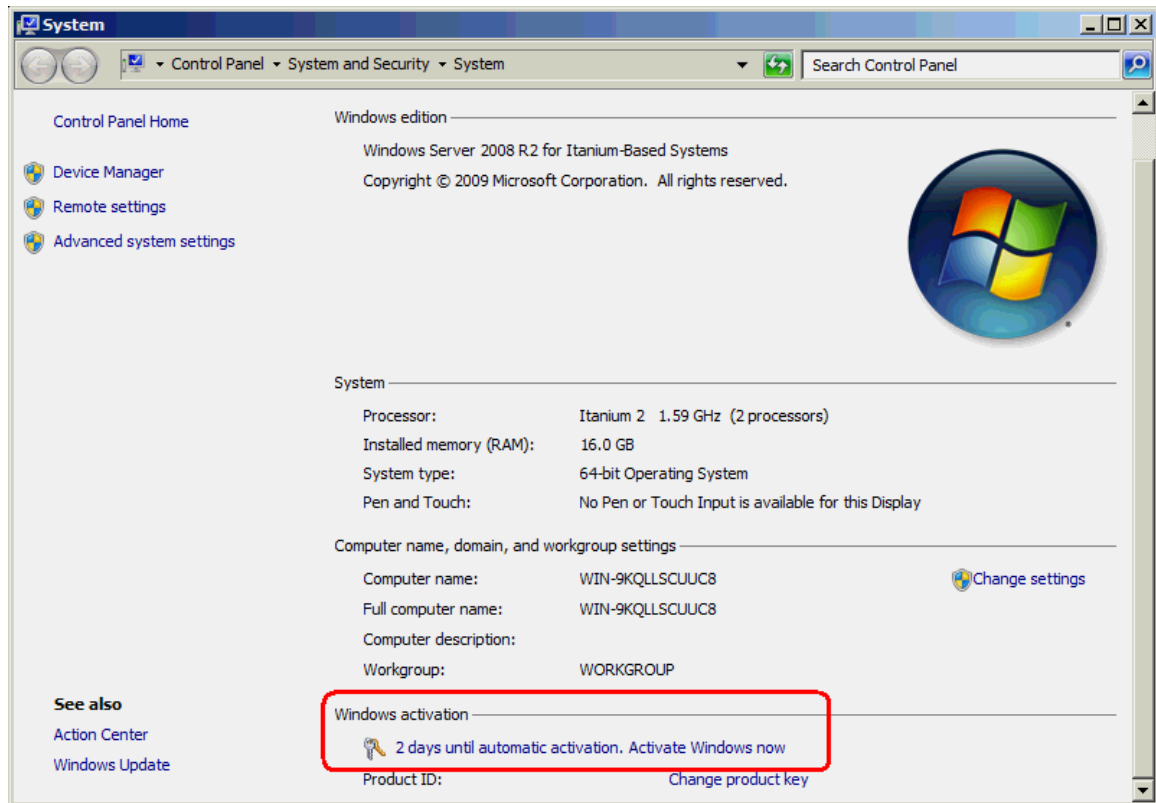
You must manually activate Windows Server 2008 R2 (with Microsoft) no more than 3 days after the system boots for the first time following installation. HP recommends that you manually activate the OS immediately after the first boot. Otherwise the Activation wizard will run at the next reboot and force the activation process.

You can activate your OS by phone, or manually, in which case an internet connection is required. If you attempt to activate without an internet connection, the process aborts. Once you establish an internet connection after a failed attempt, the activation process differs from the one described below. In this situation you should follow the instructions given on-screen.

To activate the OS, follow these steps:

1. Click **Start**.
2. Right-click **Computer** and select **Properties**. The System window displays.
3. Scroll down to the Windows Activation section at the bottom of the window and click **x days until automatic activation. Activate Windows now**.

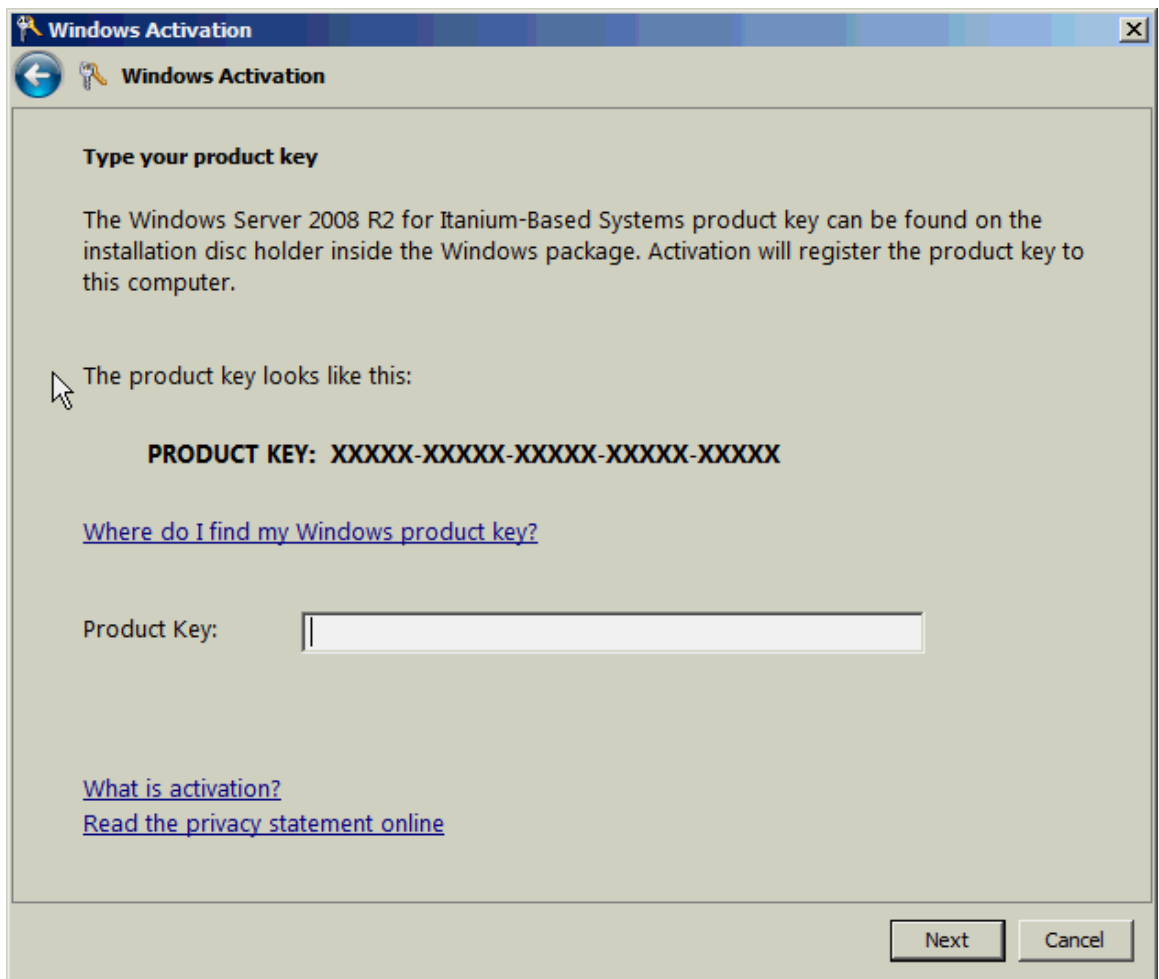
Figure 2-24 System Window #1



NOTE: If you click **Change product key** instead of **Activate Windows now** you are prompted to enter the key and then the Activation wizard runs. This method can be used for entering a test product key when the computer is disconnected from the internet.

4. The Windows Activation screen displays. Click **Type a different product key**.
5. In the next screen, enter the product key found on your COA label and user license agreement.

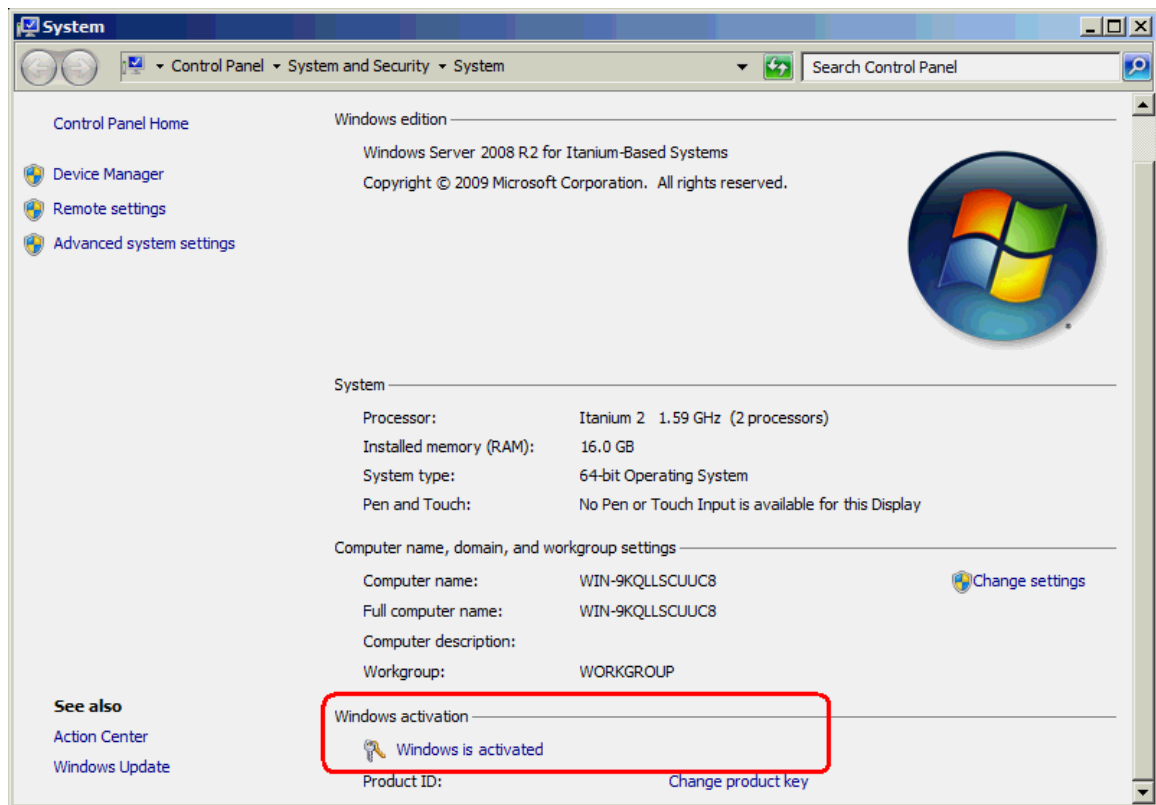
Figure 2-25 Windows Activation Screen



6. The Activation screen displays a progress bar and the message: This might take a few minutes. During this time, the system attempts to connect to the internet. If it cannot connect, you are prompted to setup an Internet connection. In this situation you must follow the on-screen instructions and disregard the rest of this procedure because it assumes you have a valid internet connection.
7. When the process finishes, the screen displays: Activation was successful. Click **Close** to exit the wizard.

8. Confirm the activation by going back to the System window and looking at the activation section at the bottom. It should indicate: Windows is activated.

Figure 2-26 System Window #2



Apply OS Updates Using the Smart Update Media

Install the latest OS and security updates from the HP Smart Update media. You can find the Smart Update media in the Insight Foundation suite for Integrity with Windows kit with the Smart Setup media.

To apply the OS updates using the HP Smart Update media, follow these steps:

1. Insert the HP Smart Update media. The Smart Update screen appears.
2. Click the **QFEs for WS2008 R2** tab.
3. Use the links on the left navigation bar to go to Operating System Updates, Security Updates, Clustering Updates, or Documents.
4. To install all operating system updates, click **Install** in the Operating System Updates section. The HP Package Setup screen appears.
5. Click **Install**. The HP Setup screen appears.
6. Click **Install** to continue with the installation or click **Close** to exit setup. When you click **Install**, a command window appears, listing each update as it installs. Sometimes these are large updates that can take several minutes each to install.
7. When prompted, click **Reboot** to complete the installation. HP recommends rebooting after each QFE bundle installs to ensure correct installation.
8. To install all Security updates, click **Install** in the Security Updates section. The HP Package Setup screen appears.
9. Click **Install**. The HP Setup screen appears.

10. Click **Install** to continue with the installation or click **Close** to exit setup. When you click **Install**, a command window appears, listing each update as it installs. Sometimes these are large updates that can take several minutes each to install.
11. When prompted, click **Reboot** to complete the installation. HP recommends rebooting after each QFE bundle installs to ensure correct installation.
12. To read a detailed description about an update, click on its Knowledge Base (KB) ID number. You are linked to the relevant article on the Microsoft website. You can do this at any time.
13. If your server will function in a SAN environment or as a node in a Microsoft Cluster, install the Clustering Updates in the same manner.
14. After installing updates, use Microsoft Windows Update (**Start** → **Help and Support** → **Support Tasks** → **Windows Update**) to check for updates that have been issued since your Smart Update media was released.



NOTE: You can also extract Smart Components to your hard drive and install the QFEs individually, but HP recommends installing them as a group, as described above.

Enable Windows Components

This section describes installation of the Windows components that enable networking.

Set IP Addresses from a Headless Console

To set the MP IP from a headless console, follow these steps:

1. Use an RS232 cable to connect the target server console port to the COM port of a working system.
2. Launch a terminal emulation program, such as HyperTerminal.
3. In the Connect Using pull-down list, select the COM port connected to the RS232 cable and click **OK**.
4. When prompted, enter the default baud rate of **9600**, and HyperTerminal connects to the MP.
5. Log in to the MP using the default MP administration user name and password **Admin / Admin**.
6. Enter the CM command to access the Command menu.
7. Enter the LC command to configure the network settings. Enter **A** to configure all parameters, or enter the letter designating the parameters you want to modify. Typically, I = IP address, S = Subnet mask, and G = Gateway address.

To set the server IP address from a headless console, follow these steps:

1. Use HyperTerminal or PuTTY to log in to the MP.
2. Enter the CO command to go to the SAC prompt.
3. At the SAC> prompt, enter the I command to specify the network number, IP address, and subnet mask. For example:

```
I<network#><IPaddress><subnet mask>
```

Enable and Run Remote Desktop Connection

The remote administration mode is enabled by default on Windows Server 2008 R2 if you use the HP Reinstall media. If you install or reinstall using Microsoft OS media (for example, if you have a volume license from Microsoft), Remote Desktop functionality is disabled. Users must have unique user names. Windows does not permit two users with the same name to log on simultaneously.

To enable remote desktop connections from a GUI console, follow these steps:

1. From the Windows Desktop, select **Start** → **Server Manager**.

2. In the Server Summary section, click **Configure Remote Desktop**.
3. On the Remote tab, select the desired RDC connection option and assign user access rights as needed.
4. Click **Apply** and then **OK** to apply the changes.

To enable remote desktop connections from a headless server, follow these steps:

1. Go to the SAC console.
2. Log in as Administrator.
3. At the SAC> prompt, enter cmd.
4. Press **Esc+Tab** to enter the Command Prompt console.
5. Enter the following command from the Windows command prompt:

```
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
```
6. If your installation uses media supplied by Microsoft, enable Remote Desktop traffic through the default Windows Firewall settings at the C:\Windows\system32> prompt by entering the following command:

```
netsh firewall set service remotedesktop enable all
```

To run Remote Desktop Connection, follow these steps:

1. Click **Start** → **All Programs** → **Accessories** → **Remote Desktop Connection**.
2. Click the **Computer** drop-down list.
3. Select **Browse for more**.
4. Select the HP Integrity server you want to establish a connection with.
5. Click **OK**.
6. Click **Connect**.
7. Log in to the remote server. The server desktop appears remotely.

Verify System Device Drivers and Register for Updates

Verify System Device Drivers

The Windows Device Manager is a comprehensive tool for detecting and evaluating problems with installed hardware devices and resource conflicts.



NOTE: If you installed the OS from Microsoft OS media, you must install new drivers for all devices displaying a yellow “bang (!)” icon in the Windows device manager. These drivers are available on the HP Smart Setup media.

To verify driver status and update if necessary, follow these steps:

1. From Windows Desktop, select **Start** → **Server Manager**.
2. In the Server Summary section, click **Change System Properties**.
3. In the System Properties window, click on the Hardware tab. Then click **Device Manager**.
4. All of the system devices are shown, grouped by Type. Expand each group, verifying that no devices display a yellow bang (!) or a question mark (?).
 - A **yellow bang** (exclamation mark) indicates a hardware problem, a device driver problem, a missing .ini file, or a resource conflict with the flagged device.
 - A **question mark** indicates that Windows has received information that the flagged device is installed but cannot find it or recognize it.



NOTE: A yellow bang might appear under **Non-Plug and Play Drivers** in the Windows Device Manager when hidden devices are enabled. The yellow bang appears only if the **Show hidden devices** option is enabled under the Non-Plug and Play Drivers in the Windows Device Manager.

If no serial legacy device is found in the system, the OS generates a yellow bang for the Serial option.

5. If a device is flagged with a fault indicator (bang or question mark), insert the HP Smart Setup media in the server's drive and accept the End User Licensing Agreement.
6. Right-click the flagged device and select **Update Driver Software** from the pop-up menu.
7. In the Update Driver Software screen, click **Browse my computer for driver software**.
8. Browse to the system drive where the Smart Setup media is inserted and click **Next**.
9. If you see a warning dialog indicating the driver is not digitally signed, ignore it and click **Next** to continue.
10. When successful installation is indicated, click **Finish**.

Register for HP Support Notifications

HP recommends that you register for alerts and notifications to stay informed of updates to the drivers, patches, and other components specific to your server. Register at:

<http://www.hp.com/united-states/subscribe/gateway/>

Register for Microsoft Security Notifications

HP recommends that you register for Microsoft security notifications to stay informed of patches that may apply to your OS. Register at:

<http://www.microsoft.com/technet/security/bulletin/notify.msp>

Register for Microsoft Windows Update

HP recommends that you use the Microsoft Update feature to download the latest patches and hot fixes for the OS. Register at:

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

Miscellaneous Installation Issues

This section describes OS installation issues that apply only to specific server models, features, or situations.

Downgrading from Windows Server 2008 R2 (to Windows Server 2008 or Windows Server 2003)

Microsoft gives customers who purchase a license for Windows Server 2008 R2 the right to “downgrade” and install Windows Server 2008, or Windows Server 2003 Datacenter Edition. For a complete listing of these downgrade rights, refer to the chart on Microsoft’s website:

<http://www.microsoft.com/windowsserver2008/en/us/downgrade-rights.aspx>

Downgrading requires all of the following:

- the purchase of a Windows Server 2008 R2 license
- the Windows Server 2008 or Windows Server 2003 installation media

To perform such a downgrade, use your previously purchased installation media for Windows Server 2008 or Windows Server 2003. The installation media can come from either Hewlett-Packard, Microsoft, or some other Microsoft Authorized Reseller. If you use media that is not supplied by Hewlett-Packard, HP recommends using the HP Smart Setup media and HP

Smart Update media after the OS installation, in order to obtain the latest HP value-added software (drivers, tools, utilities, manageability agents) for HP Integrity Servers.

Installing Windows Server 2008 R2 on rx8640 and rx7640 Servers

On rx8640 and rx7640 servers, you must run the `reconnect -r` command at the EFI shell *before* launching the Windows Server 2008 R2 installation. Failure to run this command can result in the following error message during the installation:

```
Windows Setup cannot locate valid Hard Drive to store temporary
installation files. To install Windows create more free space on the
hard drive or add a new hard drive.
```

Bootting Windows Preinstallation Environment (WinPE) from the Hard Drive Diagnostic Partition

Beginning with the Reinstall media in Windows Integrity Release 7.00 (for both Windows Server 2008 SP2 and Windows Server 2008 R2), the Microsoft WinPE boot environment is now pre-loaded on the diagnostic partition of the OS boot drive. The purpose of this change is to provide an additional tool for support team members to run diagnostics more efficiently. Also, customers can use this environment for offline file copying and restoration if needed.

To boot WinPE from the diagnostic partition of the OS boot drive, follow these steps:

1. After completing the image restore and booting the OS, restart the system.
2. At the Extended Firmware Interface (EFI) command prompt, type `map` and press **Enter**.
3. Identify the File System number associated with hard drive partition #2 (usually either "FS1" or "FS2"). Assuming it is "FS2", type `fs2` and press **Enter** to gain access to hard drive partition #2.
4. Type `\efi\boot\bootx64.efi` and press **Enter** to boot WinPE.
5. Wait about 35 seconds for a command prompt to display.
6. Perform any desired actions (diagnostics, file copy, file restoration) at the command prompt.
7. Type `exit` and press **Enter** to reboot the system.

Installing from the IRC

If you are using the Integrated Remote Console (IRC) to remotely install Windows Server 2008 R2 on servers with a graphics console attached to the local VGA port, complete one of the following:

- Install the OS remotely from a headless console instead. See [“Install from a Headless Console” \(page 31\)](#).
- Disconnect the local graphics console before you install Windows using IRC, and then reconnect it afterwards. This method is easy and therefore recommended.

Enabling Hyperthreading on HP Integrity Servers

HP Integrity servers now support Intel® Dual-Core Itanium processors. These processors, in addition to providing two CPUs in the space previously occupied by one, support a new feature called hyperthreading.

Hyperthreading enables each physical processor to present itself to the OS and applications as two virtual processors. This means each processor can work on two or more sets of tasks simultaneously. This feature makes use of resources that would otherwise sit idle, enabling your HP Integrity server to perform more work in less time.



NOTE: When enabled, hyperthreading is activated for all CPUs in the system. You cannot apply hyperthreading to a single CPU, cell, or nPartition.

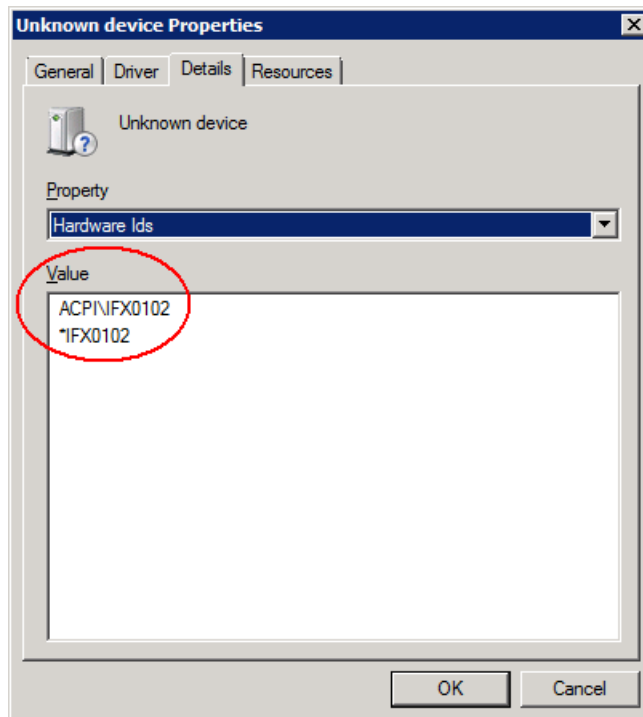
To enable hyperthreading on partitionable and nonpartitionable HP Integrity servers using the Extensible Firmware Interface (EFI), follow these steps:

1. Reboot the system to the EFI Shell.
2. Issue the `cpuconfig threads` command. The system indicates whether hyperthreading is turned ON or OFF.
3. If hyperthreading is currently OFF, issue the `cpuconfig threads on` command to turn it on.
4. Verify success by rebooting to the EFI Shell again and issuing another `cpuconfig threads` command, which should indicate ON.

Device Manager Indicates “Unknown Device” with ID IFX0102

On BL860c i2, BL870c i2, and BL890c i2 platforms, the Windows Device Manager may indicate a “yellow bang” or “Unknown Device” error. The Hardware ID for this unknown device, reported on the Properties page > Details tab, is IFX0102.

Figure 2-27 Unknown Device Properties page > Details tab



This unknown device is actually the Trusted Platform Module, or TPM. The TPM is an integrated device on some I/O controller hub mezzanine cards. Since the TPM is not supported in Windows operating systems, it is normally disabled in manufacturing. But if for some reason your system lists this unknown device, it means the option was NOT disabled in manufacturing and you must disable it manually.

To disable the unknown device with ID IFX0102, follow these steps:

1. At the EFI shell prompt, run the System Security Configuration command by typing `secconfig tpm off` and pressing **Enter**. The following (or similar) text should display on-screen:

```
SYSTEM SECURITY CONFIGURATION
```

```
TPM: Enabled
```

```
TPM Next Boot Status: Disabled
```

```
TPM Vendor ID: 0x15D1
```

```
TPM Product ID: 0x000B
```

```
TPM TCG Spec Version: 1.2.1.0
```

```
secconfig: A reset is required for security configuration changes  
to take effect.
```

2. At the shell prompt, run the Reset command by typing `reset` and pressing **Enter**.
3. Reboot the system, run the Device Manager again, and confirm that the “Unknown Device” error is resolved.

3 Installing and Configuring the Management Tools

This chapter describes how to install the tools, applications, and drivers needed to manage your Integrity server.

Install the Integrity Support Pack (ISP)

This procedure describes how to install the Integrity Support Pack locally (onto the same system that the SmartSetup CD is inserted into). If you want to install the Support Pack onto one or more systems remotely, see the procedures found in the *HP Smart Update Manager (HPSUM) User Guide* found here:

- to locate documents by operating system: <http://www.hp.com/go/windows-on-integrity-docs>
- to locate documents by server model number: http://www.hp.com/go/integrity_servers-docs

Also, you *must* install the Integrity Support Pack if you use Microsoft media to install the OS.

To install the Integrity Support Pack, follow these steps:

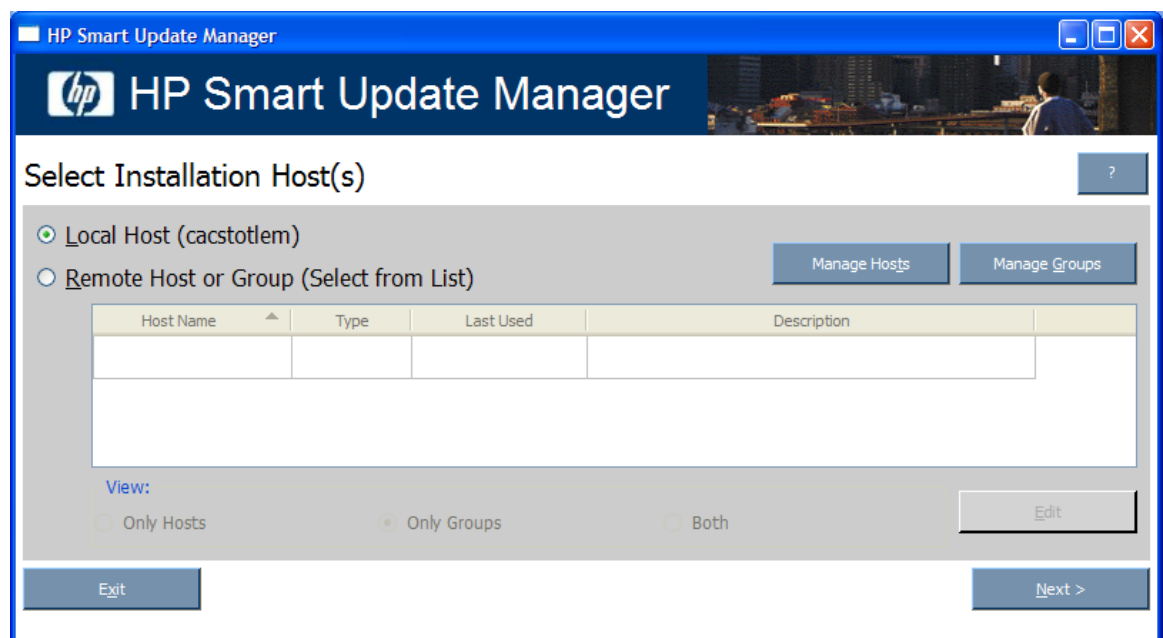
1. Insert the HP Smart Setup media into the DVD drive of the target machine. The Smart Setup media starts running and the License Agreement screen appears.



NOTE: If an AutoPlay screen displays before the License Agreement screen, press **Enter** to run the file `autorun.exe`. The License Agreement screen should appear.

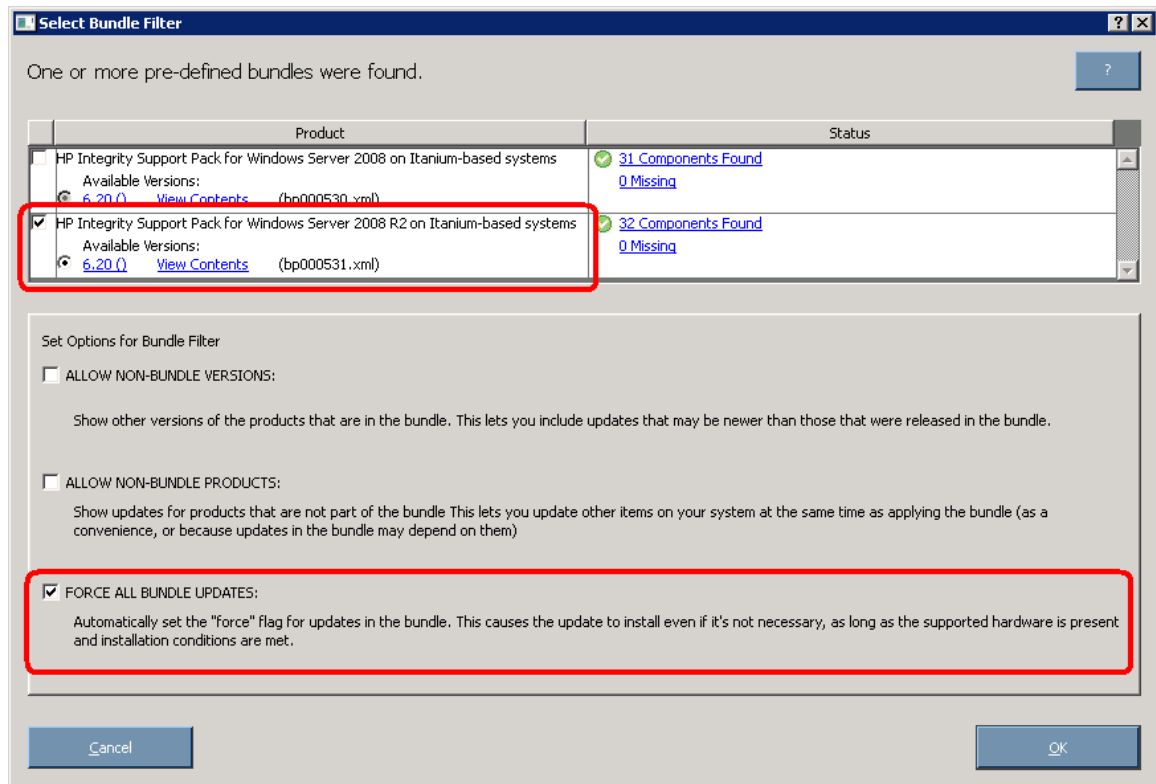
2. Click **Agree** to accept the license agreement. The HP Smart Setup Welcome screen appears.
3. Click the **Software** tab.
4. In the Software tab, click on the **Install the Integrity Support Pack** link.
5. At the first Security Warning pop-up, click **Run**.
6. At the second Security Warning pop-up, click **Run** again.
7. HP Smart Update Manager (HPSUM) starts running and builds an inventory of available updates. When the Select Installation Host(s) screen displays, select the **Local Host** button and click **Next**.

Figure 3-1 HPSUM Select Installation Host(s) Screen



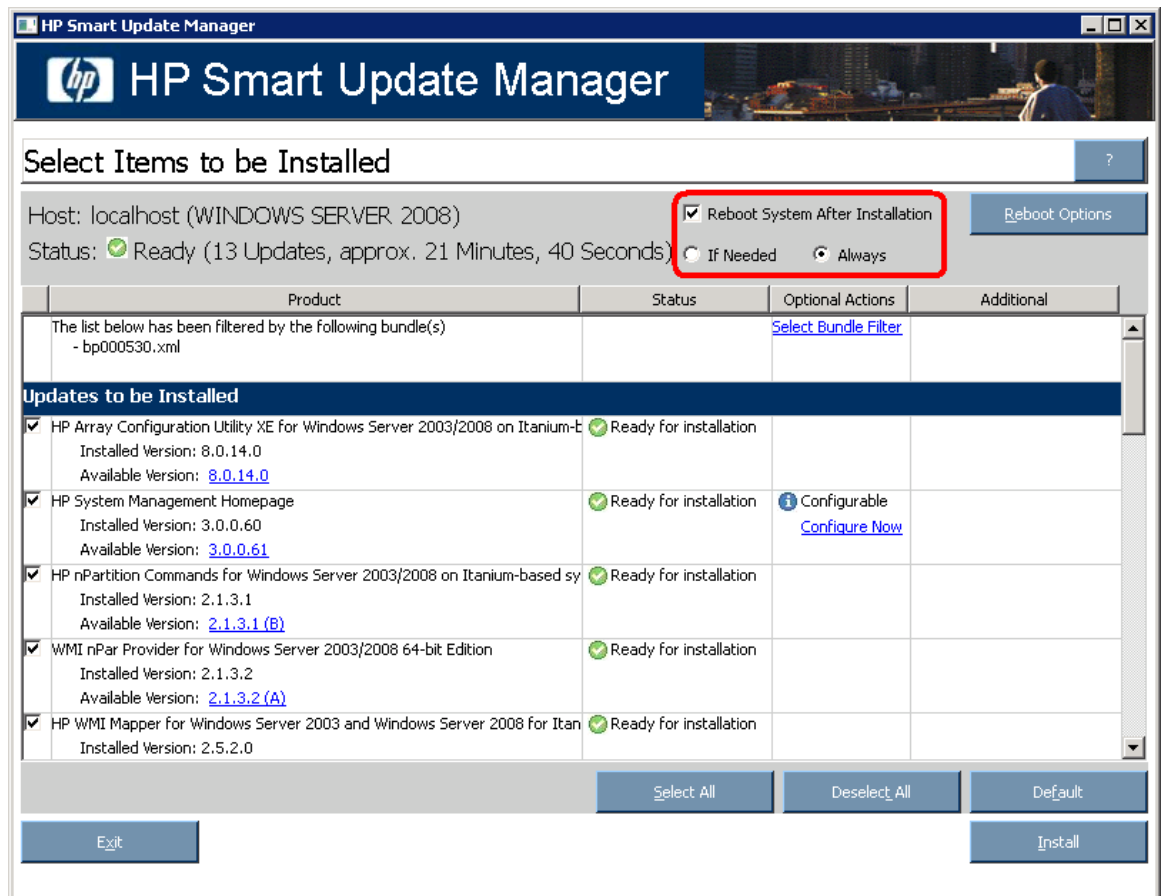
8. The Discovery Progress screen displays as HPSUM checks the system to see which components are currently installed.
9. When the discovery process finishes, the Select Bundle Filter screen displays and lists the Integrity Support Packs that were found on the Smart Setup media. Select **HP Integrity Support Pack for Windows Server 2008 R2 on Itanium-based Systems** (if multiple Integrity Support Packs are available, you **must** select the one marked “2008 R2”). Also select “FORCE ALL BUNDLE UPDATES”. Then click **OK**.

Figure 3-2 HPSUM Select Bundle Filter Screen



10. The Select Items to be Installed screen appears. It lists all of the individual updates in the Integrity Support Pack, with a check mark next to each, by default. Select the “Reboot System After Installation” box and the “Always” radio button, then click **Install** to install all items. Installation will take a minimum of 15 minutes.

Figure 3-3 HPSUM Select Items to be Installed Screen



- When the installation finishes, the Installation Results screen appears. You might be prompted to reboot the server to complete the installation of some components. Even if you are not prompted, reboot the server by clicking **Reboot Now**.

Figure 3-4 HPSUM Installation Results Screen



The latest Integrity Support Pack can also be downloaded from the HP Integrity server support website: <http://www.hp.com/support/itaniumservers/>. On the Technical Support page, click on your Integrity server model number. On the Business Support Center page, click **Download drivers and software**. To see the latest drivers and software, you must select **English (American)** or **Japanese** from the Language drop-down list at the top of the Download Drivers and Software page.



IMPORTANT: You MUST select **English (American)** or **Japanese** here to access the correct drivers and software.

After that, click on the Right Arrow button next to the drop-down list. Finally, click on the link that describes your operating system to go to the page where you can download the latest Integrity Support Pack.

Configure and Verify the WBEM Providers

This section describes how to configure and verify installation of the WBEM (Web-Based Enterprise Management) Providers after you install the Integrity Support Pack. For a complete listing and description of these providers, see this section: [Appendix D "SMH and the WBEM Providers"](#).



NOTE: Concurrent installation of the WBEM Providers (from Smart Setup version 6.5 or later) and the HP Insight Management Agents (from earlier versions of Smart Setup) is *not* supported. If the HP Insight Management Agents were previously installed on the system, you must manually uninstall them before installing the version 6.5 WBEM Providers. If the system has Management Agents version 6.2, you can upgrade from WBEM Providers 6.2 to 6.5 without manually uninstalling Agents 6.2 first. In this case, the upgrade process will automatically uninstall Agents 6.2. However, you must restart the WMI service from the Services window after the upgrade, otherwise the WBEM indications may not generate correctly.

The WBEM Providers are a group of services that report system health and status information back to the System Management Homepage (SMH) application, where it can be monitored by the System Administrator. They are installed by default when you install the Integrity Support Pack. WBEM is a Web-based approach for exchanging data across different technologies and platforms. WBEM data is usually encoded using Extensible Markup Language (XML) and then transmitted using Hypertext Transfer Protocol (HTTP).

The standard user accounts that will access the HP WBEM Providers management information must have access rights and security group memberships to allow remote access by HP SIM or other clients querying WMI data. An administrator account has sufficient rights and security group memberships to access the HP WBEM Providers management information.

Enable Access Rights and Group Memberships

To enable remote access of the Insight Providers via WMI for non-administrator user accounts, follow these steps:

1. Add the standard user account to the “Distributed DCOM Users” group.
2. Add the standard user account to namespace security for the following namespaces:
 - root\HPQ
 - root\HPQ\default
 - root\HPQ\TestEvent
 - root\Interop
 - root\CIMv2

To add the standard user account to namespace security, follow these steps for each namespace:

- a. Right-click **My Computer** → **Manage** → **Services and Applications**.
- b. Right-click **WMI Control**.
- c. Select **Properties**.
- d. Select the Security tab.
- e. Select the namespace.
- f. Click the **Security** button. Verify that permissions are set as follows for the standard user:
 - Execute Methods
 - Full Write
 - Partial Write
 - Provider Write
 - Enable Account
 - Remote Enable
 - Read Security
 - Edit Security

Enable Auto Page Refresh and Set the Interval

You can configure SMH with an Auto Refresh interval to get updates from the WBEM Providers. To enable WBEM Auto Refresh and to set the Refresh interval, follow these steps:

1. Click **Settings** → **Auto Refresh** → **Configure Page Refresh Settings**.
2. Select a refresh interval between 5 seconds and 30 minutes.
3. Use the radio button to enable Auto Refresh.

After WBEM Auto Refresh is enabled, the browser refreshes the pages at the specified interval.

Verify Installation of the WBEM Providers

To confirm error-free installation and functionality of the WBEM Providers, follow these steps:

1. Check the installation log file named `HP_WBEM_Providers.log` in the directory `c:\Windows\SysWOW64\cpqmgmt`. This file summarizes the progress and status of the installation. There should be no error messages in the log file.
2. Check the Windows System Log, looking for log entries under the source named **hpWbemDump**. There should be one or more `hpWbemDump` entries showing "ID 2001" with an "Informational" severity rating. These entries indicate the data provided by the WBEM Providers was successfully retrieved. If there are any `hpWbemDump` entries showing "ID 2002" with a "Warning" severity rating, these indicate a failure in retrieving data from the WBEM Providers. In such cases, the failed classes are listed in the log entries.
3. Log in to System Management Homepage (SMH) and verify that the Data Source is configured as "WBEM", and that the homepage reports valid information (such as the correct System Model). Perform a simple test using the following steps:
 - a. Go to the Settings tab and click **Send Test Indication**.
 - b. Send a test event with the following information: "Event ID=2, Type=Warning". Send another test event with the information: "Event ID=3, Type=Error".
 - c. Check the Windows System Log and verify there are two new entries under the source named "HP Test", one with a "Warning" rating, and the other with an "Error" rating.

Configure System Management Homepage

This section describes the configuration of SMH on Integrity servers. After configuring SMH you can use [Appendix D "SMH and the WBEM Providers"](#) for an overview of how to use it to administer your system locally or remotely.

Set Up Browser Access

To display data from the WebAgents using SMH, you must use a browser that includes support for tables, frames, Java, and JavaScript. You must turn on the following options:

- Enable Java
- Enable JavaScript
- Accept all cookies

HP's web-enabled management software requires Java Virtual Machine (JVM) for full functionality. Depending on the web-enabled management software installed, some features might require the presence of Java support in the browser.

You can also download Java support from the Sun Java Technology website: <http://java.sun.com>.

Set Up and Change Your SMH Security Settings After Support Pack Installation

When you install SMH using the Support Pack it is configured using default security settings. Use the SMH online help for more information about these security settings. To access the help:

1. Click **Help** on the System Management Homepage.
2. Click **System Management Homepage Help**.
3. On the left navigation bar, select **Settings Tab** → **Security**.
4. Change these settings as necessary for your system and production environment.

The SMH Settings tab allows you to set some parameters. This capability requires security that includes the three predefined users. For agents running on Microsoft operating systems, there are no default passwords.

On a fresh install, the administrator password, the operator password, and user passwords are configured during installation. For agents running on other operating systems the default passwords are defined in the following table:

Account	User Name	Password
anonymous		
user	user	public
operator	operator	operator
administrator	administrator	administrator



NOTE: These are the only user accounts available in this release, and they cannot be changed except for the password.

Anonymous access is disabled by default but can be turned on through the Options link on the SMH home page.

The data access types are as follows:

- Default (read only)
- Sets (read/write)

Initialize SMH

After you install and configure HP SMH, a private key and corresponding self-signed Base64-encoded certificate are created. This certificate is a Base64-encoded PEM file.

The public and private keys are stored in the \hp\sslshare directory of the system drive. To protect the key, this subdirectory is only accessible to administrators if the file system allows such security. For private key security reasons, HP recommends that you install Windows installations of HP SMH on the NT file system (NTFS).



IMPORTANT: For Windows operating systems, the file system must be NTFS for the private key to have administrator-only access through the file. If the private key is compromised, the administrator can delete the \hp\sslshare\cert.pem file and restart the server. This causes HP SMH to generate a new certificate and private key.



NOTE: Certificate and private key generation only occur the first time HP SMH is started or when no certificate and key pair exist. You can use a certificate from a certificate authority (CA), such as Verisign or Entrust, to replace a self-generated certificate. These certificates and key files are shared with other HP management software, such as HP Systems Insight Manager.

Verify Installation of the nPartition Management Tools

To verify correct installation of the nPartition management tools, you should perform two tests. For a detailed discussion about using the nPartitioning management tools, see “nPartitioning”

(page 81). For a description of nPartitioning and associated tools and concepts, see the *nPartition Administrator's Guide* found here:

<http://h20000.www2.hp.com/bc/docs/support/SupportManual/c02058520/c02058520.pdf>

Verify nPartition Commands

1. Perform a local management test by opening a command prompt window and issuing the following command:

```
C:\Documents and Settings> parstatus -X
```

If you run this command on an nPartition, it displays information about the local server's nPartition configuration. No error messages should be returned. However, if you run this command on a non-nPartition, the following message should appear (which is the expected response in this situation, and not an error):

```
Error: unsupported platform
```

2. If you are using the IPMI over LAN connection method to verify access and communication with the server, as well as installation of the nPartition commands, enter the following command:

```
C:\Windows> parstatus -X -h <mp> -g <password>
```

where <mp> is the IP address or the host name of the server MP, and <password> is the MP IPMI password. This command should result in the display of approximately 10 server attributes, including the server name, model number, and so on. You might experience a delay of a few seconds, or even a minute or more, depending on network distance between the management station and the server.



NOTE: If you are using the WBEM/WMI connection method, substitute the -u option for the -g option shown above. This also requires copying the WBEM certificate for the remote nPartition into the WBEM trusted certificate store on the system where the command is being run.

Verify Partition Manager Installation

Partition Manager requires the presence of nPartition commands. Before proceeding, verify that the commands are installed correctly by following the procedure in the previous section. To verify Partition Manager installation, follow these steps:

1. Launch a web browser and log in to SMH on the system where Partition Manager is installed. For example, if you are testing on the local server, use `https://localhost:2381`.
2. To continue the verification at the SMH, on the Tools tab, click **Partition Manager**. If Partition Manager is running, you will go directly to the top-level view of the local complex (no additional login is required). If Partition Manager is not running on an nPartition, you are presented with a dialog asking for one of the following:
 - The host name and IP address and the login/password for a remote nPartition (for remote WBEM connections)
 - The host name and IP address and the IPMI password of an MP (for remote IPMI connections)

If you are running Partition Manager on an nPartition, omit steps 3 and 4 and go directly to step 5 where you verify correct operation of the Partition Manager.

3. To test remote WBEM connections, do the following:
 - a. Copy the remote nPartition WBEM certificate into the local WBEM trusted certificate store.
 - b. Enter the host name and IP address of the remote nPartition that you want to connect to, along with an account and password with administrative privileges on the remote nPartition in the top half of the Partition Manager login screen.
 - c. Click **OK**.
4. In order to test remote IPMI connections, do the following:
 - a. Enter the host name and IP address of the remote management processor that you want to connect to, along with the IPMI password for that MP in the bottom half of the Partition Manager login screen.
 - b. Click **OK**.
5. Verify correct operation of Partition Manager.

After you log in to Partition Manager, the following message should appear for several seconds up to a minute or so:

Loading complex information

After that, Partition Manager should display top-level information about the complex, including configured nPartitions and their associated cells and I/O chassis.
6. When Partition Manager is running, verify that the complex information looks correct and that no error messages appear. For example, in the Action menu on the right side of the screen, click **Complex** to expand the complex-level submenu. Click **Show Complex Details** to display a complete listing of the complex configuration. Verify that this information is correct, and that no error messages appear. Click **OK** to close the Complex Details window.
7. In the same Complex menu, click **Clear All LEDs**. A dialog box should appear, stating that the command ran successfully. If possible, verify that server LEDs are off by looking at the server.

If these tests do not give the desired results, you can perform additional tests to help pinpoint the problem. Consult the *nPartition Administrator's Guide* mentioned previously.

A Preparing the Server for Microsoft SQL Server

This appendix describes the server configuration tasks needed to install Microsoft SQL Server.



NOTE: The Itanium version of Microsoft® SQL Server® 2008 is designed for use with the following operating systems:

- Windows Server 2003 for Itanium-based Systems with Service Pack 2, or later
- Windows Server 2008 for Itanium-based Systems, or later
- Windows Server 2008 R2 for Itanium-based Systems, or later

NOTE: The minimum requirements for running Microsoft® SQL Server® 2005 on Windows Server 2008 R2 systems are found here:

<http://support.microsoft.com/kb/955725>

NOTE: If you are running Microsoft® SQL Server® 2005 "Server + CAL" licenses on a partitioned server, you can only run the software on the number of partitions for which you have valid software licenses. If you are running Microsoft® SQL Server® 2005 or 2008 "Per Processor" licenses on a partitioned server, you can only run the software on the number of CPUs for which you have valid software licenses.

NOTE: For Microsoft® SQL Server® 2005 Enterprise Edition Software users:

You may only run the Microsoft SQL Server 2005 Enterprise Edition software in place of Microsoft SQL Server® 2008 Enterprise software in order to exercise your Downgrade rights under the SQL Server 2008 Enterprise License Terms. The SQL Server 2008 License Terms apply to your use of the SQL Server 2005 Software.

SQL Server 2005 Installation

This section is an overview of the steps needed to install SQL Server 2005. For further installation and configuration information, see the SQL Server 2005 documentation.

1. Configure the server:
 - a. Set the system ACPI Config Flag to Windows.
 - b. Verify that system nPartitions are set to 100% cell local memory (CLM) by using the ParCLI parstatus command. Adjust the value to 100% if necessary, using the parmodify command. See the *nPartition Guide*.
 - c. Data Warehousing: For decision support and data warehousing, set the number of CPUs to a higher number, such as four, up to the actual number of CPUs.
2. Configure SQL Server 2005:
 - a. Check affinity masks. By default these are set to zero. Set them to actual CPU configurations for all CPUs using Spconfigure.
 - b. Confirm the degree of parallelism settings:
 - i. If you have a large system (more than four CPUs), do not set this number to zero using SPconfigure. Also, increase parallelism if you expect highly complex queries.
 - ii. Online transaction processing (OLTP): For these workloads, set the level of parallelism low (one query should not use more than one CPU, so set to 1).
3. Verify networking issues:
 - a. Confirm that you have enough network interface cards (NICs). If you have more than 10,000 packets/second on a NIC, add another NIC.
 - b. Enable TCP and IP, and Rx and Tx checksum off-loading.

4. Verify storage/Fibre Channel HBAs:
 - a. Maximum queue depth: Ensure that the HP AH402A or AH403A (Emulex) driver options set in LPutil are equal to or greater than the number of physical drives (default = 20).
 - b. Maximum queue depth: For HP AH400A or AH401A (Qlogic) NVRAM, ensure that the Sanblade execution throttle setting is equal to or greater than the number of physical drives (default = 16).
 - c. Enable write cache: It is important to have a cached log for the database.

For more information regarding the installation of SQL Server 2005 and tuning of system parameters once installed, refer to the document, *Tuning SQL Server 2005 on HP Integrity Servers*:
<http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01977135/c01977135.pdf>

For additional resources to help deploy and maintain SQL Server on HP Integrity servers, refer to the document, *HP Integrity Servers and Microsoft SQL Server Smart Resources Card*:

<http://h20000.www2.hp.com/bc/docs/support/SupportManual/c01978945/c01978945.pdf>

Install SQL Server from the Command Prompt

To install a standalone instance of SQL Server from the command prompt, do the following:

1. Insert the SQL Server 2005 installation media into the disk drive.
2. For instance-aware components (the Database Engine, SQL Server Agent, Analysis Services, and Reporting Services) use the following syntax:

```
Start /wait <CD or DVD Drive>\setup.exe /qb INSTANCENAME=<InstanceName> ADDLOCAL=SQL_Engine,  
SQL_Replication PIDKEY=<pidkey value with no "-"> SAPWD=<StrongPassword>  
SQLACCOUNT=<DomainName\UserName> SQLPASSWORD=<DomainUserPassword>  
AGTACCOUNT=<DomainName\UserName> AGTPASSWORD=<DomainUserPassword>  
SQLBROWSERACCOUNT=<DomainName\UserName>  
SQLBROWSERPASSWORD=<DomainUserPassword>
```

To install a clustered instance of SQL Server 2005 from the command prompt, do the following:

1. Insert the SQL Server 2005 installation media into the disk drive.
2. For a new failover cluster, use the following syntax:

```
Start /wait <DVD Drive>\setup.exe /qn VS=<VSName>  
INSTALLVS=SQL_Engine INSTANCENAME=<InstanceName>  
ADDLOCAL=SQL_Engine,Client_Components ADDNODE=<NodeName1,NodeName2>  
GROUP=<Diskgroup> IP=<IP,Networkname> ADMINPASSWORD=<StrongPassword>  
SAPWD=<StrongPassord> INSTALLSQLDIR=<InstallationPath>  
INSTALLSQLDATADIR=<ShareDrivePath> SQLACCOUNT=<domain\user>  
SQLPASSWORD=<DomainUserPassword> AGTACCOUNT=<domain\user>  
AGTPASSWORD=<DomainUserPassword>
```

Install SQL Server from the GUI

To install SQL Server from the GUI, follow these steps:

1. Insert the SQL Server 2005 DVD into the DVD drive. If the autorun feature does not launch the installation program, navigate to the root of the DVD and launch the `splash.hta` file. If you are installing from a network share, navigate to the network folder and launch `splash.hta`.
2. From the autorun dialog, click **Run the SQL Server Installation Wizard**.
3. On the End User License Agreement page, read the license agreement, and then accept the licensing terms and conditions. Click **Next**.
4. On the SQL Server Component Update page, Setup installs software required for SQL Server 2005. To begin the component update process, click **Install**. To continue after the update completes, click **Finish**.

5. On the Welcome page of the SQL Server Installation Wizard, click **Next**.
6. On the System Configuration Check (SCC) page, the installation computer is scanned for conditions that may block setup. To interrupt the scan, click **Stop**. To display a list of check items grouped by result, click **Filter** and then select a category from the drop-down list. To view a report of SCC results, click **Report** and then select an option from the drop-down list. To proceed with setup after the SCC scan completes, click **Continue**.
7. On the Registration Information page, enter the required information, then click **Next**.
8. On the Components to Install page, select the components to install. When you select **SQL Server or Analysis Services**, if setup detects that you are installing to a virtual server, the **Install as a Virtual Server** check box is enabled. You must select this option to install a failover cluster.
9. If you clicked **Advanced** on the Components to Install page, the Feature Selection page appears. On the Feature Selection page, select the program features to install using the drop-down boxes. To install components to a custom directory, select the feature and then click **Browse**. For more information about the functionality of this page, click **Help**. When your feature selections are complete, click **Next**.
10. On the Instance Name page, select a default or named instance for the installation. If a default or named instance is installed and you select the existing instance for your installation, setup upgrades it and provides you the option to install additional components. To install a new default instance, a default instance must not exist on the computer. To install a new named instance, click **Named Instance** and then enter a unique instance name in the space provided.
11. Optionally, specify an individual account for each service by selecting **Customize** for each service account, selecting a service name from the drop-down box, and then providing login credentials for the service. Click **Next**.
12. On the Authentication Mode page, select the authentication mode to use for the SQL Server installation. You must also enter and confirm a strong password for the system administrator login. When you finish, click **Next**.
13. To set separate collation settings for SQL Server and Analysis Services, select the **Customize for each service account** check box. After you select the check box, a drop-down selection box appears. Select a service from the drop-down selection box and then assign its collation. Repeat for each service. Click **Next**.
14. If you selected **Reporting Services** as a feature to install, the Report Server Virtual Directories page appears. Accept the default directory names, or specify a location for the directories. For more information about this page, click **Help** at the bottom of the page. When you are finished, click **Next**.
15. If you selected **SQL Server Authentication**, provide a user name and password with administrative privileges for that instance. Confirm the Report Server Database Name. Click **Next**.
16. If you selected **Reporting Services** as a feature, the Report Server Delivery Settings page appears. Specify an SMTP server address and an email address to be used as the sender of email messages from Report Server. When you finish, click **Next**.
17. On the Error Reporting page, optionally clear the check box to disable error reporting. For more information about error reporting functionality, click **Help** at the bottom of the page. When you finish, click **Next**.
18. On the Ready to Install page, review the summary of features and components for your SQL Server installation. Click **Install**.
19. On the Installation Progress page, you can monitor installation progress as setup proceeds. To view the log file for a component during installation, click the product or status name on the Installation Progress page.
20. On the Completing the Microsoft SQL Server Installation Wizard page, you can view the setup summary log by clicking the link provided. To exit the SQL Server Installation Wizard, click **Finish**.
21. If prompted, restart the computer. It is important to read the message from the setup program when you finish the installation. Failure to restart the computer can cause failures when you run the setup program in the future.

B EFI Utilities

This appendix provides an overview of the Extensible Firmware Interface (EFI) and the EFI-Based Setup Utility (EBSU). The EFI provides access to the server before the operating system (OS) stage, which enables you to flash the firmware, partition the hard disk, install diagnostic tools, configure storage controllers, and run other EFI utilities.

Introduction to EFI

EFI is an interface between operating system, firmware, and hardware. EFI serves the same purpose on Itanium-based computers as BIOS does on x86-based computers. EFI provides a standard environment for running preboot applications and for booting the OS.

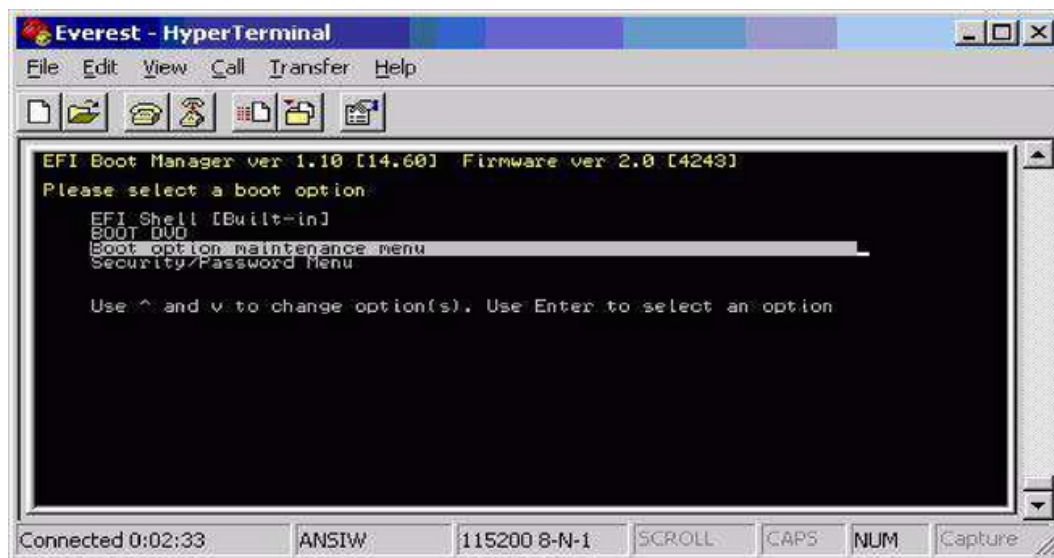
HP Integrity servers use EFI to initialize the platform firmware and load the OS. After the system is initialized, EFI provides two interfaces that you can interact with:

- EFI Boot Manager
- EFI Shell

EFI Boot Manager

First displayed when you power on the server, the EFI Boot Manager provides a menu-based interface with options for booting the OS, loading EFI applications, configuring the server, and other preboot operations. You use arrow keys to scroll through the menus.

Figure B-1 EFI Boot Manager



EFI Shell

Available as a selection from the EFI Boot Manager, the EFI Shell provides a command-line interface to obtain information about the system, install an OS, boot the OS, execute batch scripts, launch EFI applications, load EFI drivers, and manage files and system variables.

See Also

- *EFI documentation:*
<http://www.intel.com/technology/efi/>
- *EFI Shell commands:*

From the EFI shell, enter **help** or **?** at the EFI prompt for a list of EFI Shell commands.

Common EFI Shell Commands

The following table lists common EFI commands.

Table B-1 EFI Shell Commands and Descriptions

Command	Description
Boot Commands	
autoboot	Set and view the autoboot timeout variable.
bcfg	Display and modify the driver and boot configuration.
boottest	Set and view BootTest bits.
dbprofile	Display and modify direct boot profiles for use by lanboot.
lanboot	Boot over the LAN.
reconfigreset	Reset the system (nPartition) for reconfiguration. The nPartition remains inactive, in the shutdown for reconfig state.
reset	Reset the system (nPartition).
search	Connect drivers for bootable devices.
Configuration Commands	
Commands for changing and retrieving system (nPartition) information.	
acpiconfig	Set and view ACPI configuration mode.
cellconfig	Deconfigure and reconfigure cells. (Set cell use-on-next-boot values.)
cpuconfig	Deconfigure and reconfigure CPUs.
date	Display the current date or set the date of the system (nPartition).
dimmconfig	Deconfigure and reconfigure memory (DIMMs).
err	Display and change the error level.
errdump	View and clear logs.
fru	View FRU data.
info	Display hardware information.
monarch	Set and view a monarch processor.
palproc	Make a PAL call.
romdrivers	Enable and disable PCI expansion ROM drivers.
rootcell	Set/view preferred root cells. (Set nPartition core cell choices.)
salproc	Make a SAL call.
tftp	Perform TFTP operation to a bootp/DHCP enabled UNIX boot server.
time	Display the current time or set the time of the system (nPartition). EFI time is set and presented in Greenwich Mean Time (GMT).
variable	Save and restore specific EFI variables.
ver	Display version information.
Device, Driver, and Handle Commands	
Commands for managing devices, drivers, and handles.	
baud	View serial port com settings.

Table B-1 EFI Shell Commands and Descriptions *(continued)*

Command	Description
connect	Bind a driver to a device.
dblk	Hex dump – BlkIo devices.
devices	Display devices managed by EFI drivers.
devtree	Display tree of devices.
dh	Dump handle information.
disconnect	Disconnect drivers from devices.
drivers	Display list of drivers.
drvcfg	Invoke the Driver Configuration Protocol.
drvdiag	Invoke the Driver Diagnostics Protocol.
guid	Dump known GUID IDs.
lanaddress	Display the MAC address.
load	Load EFI drivers.
map	Map shortname to device path.
openinfo	Display the open protocols for a handle.
pci	Display PCI devices or PCI function configuration space.
reconnect	Reconnect drivers from a device.
unload	Unload a protocol image.
File System Commands Commands for managing files, directories, and attributes.	
attrib	Display and change the attributes of files and directories.
cd	Update and view the current directory.
comp	Compare the contents of two files.
cp	Copy files and directories to another location.
edit	Edit an ASCII or UNICODE file in full screen.
eficompress	Compress infile and write to outfile.
efidecompress	Decompress infile and write to outfile.
hexedit	Edit a file, block device, or memory region using hex.
ls	Display a list of files and subdirectories in a directory.
mkdir	Create directories.
mount	Mount a file system on a block device.
rm	Delete files and directories.
setsize	Set the size of a file.
touch	Update time of a file or directory with the current time.
type	Display the contents of a file.
vol	Display volume information of the file system.

Table B-1 EFI Shell Commands and Descriptions *(continued)*

Command	Description
Memory Commands Commands for listing and managing memory, EFI variables, and NVRAM details.	
default	Set default NVRAM values.
dmem	Dump memory or memory-mapped I/O.
dmpstore	Display EFI variables.
memmap	Display the memory map.
mm	Display and modify MEM/IO/PCI.
pdt	View and clear nPartition or cell memory page de-allocation table (PDT).
Shell Navigation and Other Commands Commands for basic EFI Shell navigation and customization.	
alias	Set and get alias settings.
cls	Clear the standard output with an optional background color.
exit	Exit EFI Shell environment.
getmtc	Display current monotonic counter value.
help or ?	Display help.
mode	Display the mode of the console output device.
set	Set and get environment variable.
xchar	Turn on and off extended character features.
Shell Script Commands / Programming Constructs EFI shell script commands.	
echo	Echo message to stdout or toggle script echo.
else	Script-only: Use with IF THEN.
endfor	Script-only: Delimiter for FOR loop construct.
for	Script-only: Loop construct.
goto	Script-only: Jump to label location in script.
if	Script-only: IF THEN construct.
input	Take user input and place in EFI variable.
pause	Script-only: Prompt to quit or continue.
stall	Stall the processor for some microseconds.

EFI-Based Setup Utility

The EFI-Based Setup Utility (EBSU) provides an easy-to-use interface to flash the firmware, partition the hard disk, install diagnostic tools, configure storage controllers, and run other EFI utilities. EBSU provides the following functions:

- **Express Setup** — Guides you through Windows installation and setup. Express Setup guides you through the following setup tasks:
 - Updating firmware
 - Creating disk partitions

- Installing offline diagnostic tools
- Installing Windows
- **Maintain Firmware** — Maintains the firmware for selected devices with flashable firmware. You can flash devices individually or all at once.



NOTE: You cannot flash the firmware if the installed version is the same as, or higher, than the version on the Smart Setup media. Also, you cannot use EBSU to flash the system firmware and System Management Firmware (iLO firmware) of Integrity BL860c i2/BL870c i2/ BL890c i2 server blades.

- **Create Partitions** — creates the following partitions:
 - **EFI System Partition.** This partition is required to boot the OS. Store only EFI drivers and OS system files here. This partition is labeled EFIPART.
 - **HP Service Partition (HPSP).** This is optional. The files from the HP Integrity Offline Diagnostics and Utilities CD are stored here. This partition is labeled HPPART.
 - **Microsoft Reserved Partition (MSR).** Windows requires this partition on the boot drive and all data drives. The MSR partition is created by this utility if the HPSP partition has also been created; otherwise, it is created by the Windows installer.
- **Install Diagnostics** — Installs a copy of the diagnostics programs from the HP Integrity Offline Diagnostics CD in the HPSP partition.
Some options available from the EBSU main menu are not part of Express Setup, but you can use them to diagnose problems or customize firmware settings.
- **Drive Explorer** — Offers the following options:
 - **Launch.** Launches the Drive Explorer, which displays the directories present on the disks in the EFI partition or executes EFI programs.
 - **Install.** Installs the Drive Explorer
- **System Inventory** — Retrieves system information and displays a report of the system hardware.
- **Pre-OS Configuration Checking** — Performs the following checks on cell-based systems and Integrity BL860c i2/BL870c i2/BL890c i2 server blades:
 - On cell-based systems:
 - **All.** Displays a message stating that these are checks on cell-based systems only and performs all checks if appropriate.
 - **ACPI.** Checks that the ACPI configuration setting is set to windows. If it is not set to windows, execute the `acpicfg` command in the EFI Shell, and then enter the reset command to reboot with the configuration set to windows.



NOTE: On cell-based HP Integrity servers, to boot the Windows operating system, you must set the ACPI configuration value of an nPartition to windows.

- **CLM.** Checks if a cell has the optimal amount of memory allocated. You can configure CLM for each cell as a percentage of the total memory in the cell or as an absolute number of gigabytes. For Windows, HP recommends assigning 100% CLM for each cell in the partition. See the *nPartition Guide* for instructions.
- On Integrity BL860c i2/BL870c i2/BL890c i2 server blades:
 - **Memory Interleave Setting.** Displays message describing how to set the Memory Interleave value in EFI.
- **Intel Disk Tools**
 - **Access these tools.** Displays a message stating that you must enter the EFI shell and go to the `\efi\efi_utils` directory to use Diskpart, Efifmt, or Efichk.
 - **Diskpart.** Creates and manages disk partitions.

- **Efifmt.** Formats the disk for use with EFI.
- **Efichk.** Checks the disk and displays a status report. This tool fixes some disk errors and recovers readable information from the disk.
- **Install/Update Support Tools** — Copies support tools to the HPSP partition and installs a Python interpreter. These tools are for use only by HP Support. Integrity BL860c i2/BL870c i2/BL890c i2 server blades do not need these tools.

Creating a Backup Boot File Using the EFI Shell

follow these steps to create a backup copy of the Windows Server 2008 R2 boot file:

1. Remove all media from the server's DVD drive.
2. Boot the server into the EFI Boot Manager interface.
3. In the EFI Boot Menu screen, select **Boot Configuration**.
4. In the Boot Configuration screen, select **Add Boot Entry**.
5. In the File System Explore screen, select the entry that defines your boot volume (the volume where the boot file and OS are installed). In most cases, where the boot volume has not been named, that entry appears as: **NO VOLUME LABEL**.
6. Moving through the next three File System Explore screens, select **EFI > Microsoft > Boot** to go to the Boot directory.
7. In the Boot directory, select the default boot file: `bootmgfw.efi`. This file will be copied to create the new backup boot file.
8. In the next screen, enter a description for the new boot file (for example, `WS2008 R2 backup boot file`) and press **Enter**.
9. In the next screen, enter the desired load options (or just press **Enter** if none).
10. When prompted to `Save changes to NVRAM? [Y/N] ?`, press **Y** (for Yes).
11. The backup file is created, and the new entry now appears at the bottom of the EFI Boot Menu screen.

Verify Successful Backup Boot File Creation

follow these steps to verify valid boot file creation:

1. Remove all media from the server's DVD drive.
2. Boot the server into the EFI Boot Manager interface.
3. Select the `WS2008 R2 backup boot file` entry at the bottom of the EFI Boot Menu screen.
4. A successful boot into the operating system indicates the boot file is valid.

Getting to Know nPartitions

Partitions are physical or logical mechanisms for demarcating operational environments within a single system or across multiple systems. Partitioning lets you consolidate systems, allocate computing resources in response to fluctuations in demand, maximize resource use, and protect operating environments from disruptive events.

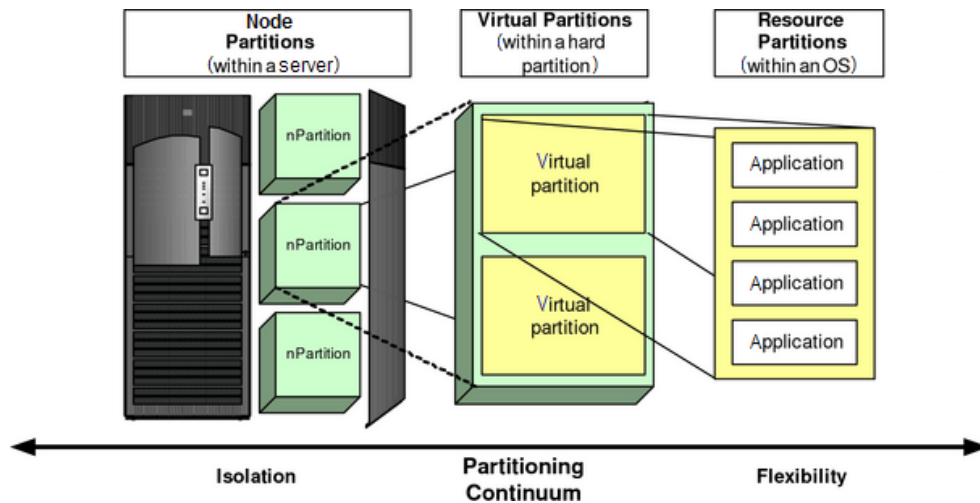
Partitioning Continuum

HP offers a continuum of partitioning technologies, as shown in Figure C-2.



NOTE: Virtual Partitions are only available in systems running HP-UX.

Figure C-2 Partitioning Continuum



Node Partition

A node partition (nPartition) is a hard partition in a cell-based server. Cell-based servers can be configured as single large symmetric multiprocessors or as several independent systems. An nPartition has exclusive use of the memory, processor, and I/O resources belonging to the cells assigned to that partition and can execute its own operating system image.

Virtual Partition

A virtual partition is a soft partition in a node or an nPartition. A virtual partition uses a subset of the system processor, memory, and I/O resources, and includes OS and application-related software.

Resource Partition

A resource partition is a soft partition in hard partitions or virtual partitions and is controlled by workload management services in the OS. Resource partitions enable an OS instance to allocate resources between competing applications.

Cell Structure of nPartitions

HP Integrity mid-range and high-end servers (rx7640, rx8640, and Superdome) are composed of **cells** or **cell boards**. A cell consists of up to four processor modules, contains memory modules (up to 32 DIMMs for Superdome cells, up to 16 DIMMs for rx7640 and rx8640 cells), and can connect to an I/O chassis that has I/O cards. A server cabinet can have several I/O chassis. Some cell-based servers support I/O expansion cabinets to provide additional I/O chassis.

The hardware of a cell-based server—including cells, I/O expansion cabinets, cables, cabinet hardware, fans, and power and utility components—is known as a server complex:

- A Superdome server complex can consist of one or two server cabinets and can include one or two I/O expansion cabinets (which provide additional I/O chassis).
- An rx8640 server complex consists of a single server cabinet and can include one I/O expansion cabinet (which provides two additional I/O chassis).
- An rx7640 server complex consists of a single server cabinet only.

An nPartition is a partition of the server complex that you can reconfigure without physically modifying the server hardware. An nPartition contains cells communicating coherently over a high-bandwidth, low-latency, crossbar fabric. Special firmware in each cell defines the boundaries of an nPartition to ensure isolation from other nPartitions.

Each nPartition has exclusive use of the memory, processor, and I/O resources belonging to the cells assigned to that nPartition. An nPartition must have at least one core I/O card to support console services, booting, and management operations. Each nPartition has its own system boot interface, boots independently, and executes its own operating system image.

Properties of nPartitions

An nPartition has the following properties:

Partition Numbers

Each nPartition is identified by a unique partition number. When you create an nPartition, it is assigned the lowest available number. That is, the first nPartition is partition 0 and the second nPartition is partition 1.

When you remove an nPartition, its partition number is released and you can reuse it when you create a new nPartition. Consider a server with partitions 0, 1, 2, and 3. When you remove partition 2, for example, and then create a new nPartition, the new nPartition is identified as partition 2.

Assigned and Unassigned Cells

If a cell in a server complex is not assigned to an nPartition, the cell is considered unassigned. If an I/O chassis is attached to an assigned cell, the chassis is assigned to that nPartition. Cells that are unassigned are available resources. They can be assigned to any existing nPartition or used to create a new nPartition.

Base Cells

All cells in an nPartition are base cells. If you do not specify the cell type, nPartition administration tools set the cell type to base cell.

Active and Inactive Cells

Active cells are assigned cells that boot to form an nPartition whose resources (processors, memory, and attached I/O) can be used by software running in that nPartition.

Inactive cells are not assigned to an nPartition or have not participated in **partition rendezvous** with other cells in the nPartition to form an nPartition. (Partition rendezvous is the event during the nPartition boot process when available cells in an nPartition join to determine which cells are active for the current boot of the nPartition.) The resources belonging to inactive cells are not used by an nPartition.

Core Cell

The core cell is an active cell that is attached to an I/O chassis with a functional core I/O. Each nPartition must have one core cell. Although an nPartition can have multiple core-capable cells (any assigned cell that has an

I/O chassis with core I/O), only one core I/O is actively used in an nPartition.

System firmware selects the core cell in the early stages of the nPartition boot process. When none of the core cell choices can serve as the active core cell, the nPartition attempts to select an eligible cell.

The core I/O in the I/O chassis connected to the core cell provides console access for the nPartition through the management processor. The monarch processor in the core cell runs the EFI while all other processors are idle until an OS is booted.

Cell Local Memory (CLM)

CLM is a portion of the memory in a cell that can be accessed quickly by processors residing on the same cell. You can configure CLM for each cell as a percentage of the total memory in the cell or as an absolute number of gigabytes.

For nPartitions running Microsoft Windows, HP recommends assigning 100% CLM for each cell in the nPartition. However, for other operating systems the CLM assignment will likely differ, depending on the nPartition configuration and workloads running.

Cell Property Details

Cells in an nPartition have properties that determine how the cells can be used and managed.

Active and Inactive nPartition Boot States

Each nPartition has a boot state of active or inactive. The boot state indicates whether the nPartition has booted so that it can be interactively accessed through its console (active nPartitions).

An active nPartition has at least one core-capable cell that is active (not in a boot-is-blocked state). When an nPartition is active, cells assigned to the nPartition have completed partition rendezvous, and the system boot interface (EFI) is loaded and appears through the nPartition console. An OS can be loaded and run from the system boot interface on an active nPartition.

An inactive nPartition is considered to be in a shutdown for reconfig state because all cells assigned to the nPartition remain at a boot-is-blocked state or are powered off.

Cell and nPartition Boot Phases

The nPartition boot process on HP Integrity servers involves two phases: the cell boot phase and the nPartition boot phase.

Cell Boot Phase

The cell boot phase occurs when cells are powered on or reset. The main activities that occur during the cell boot phase are power-on-self-test activities. During this phase, each cell operates independently of other cells in the complex. Cells do not necessarily proceed through this phase at the same pace, because each cell might have different hardware to test and discover, or cells might be reset or powered on at different times.

The main steps that occur during the cell boot phase are as follows:

1. A cell is powered on or reset, and the cell boot-is-blocked (BIB) flag is set. BIB is a hardware flag on the cell board. When BIB is set, the cell is considered to be inactive.
2. Firmware on the cell performs self-tests and discovery operations on the hardware components of the cell. Operations at this point include processor self-tests, memory tests,

I/O discovery, and discovery of interconnecting fabric (connections between the cell and other cells, I/O, and system crossbars).

3. The firmware completes self-tests and discovery, reports the hardware configuration of the cell to the management processor (MP), informs the MP that the cell is “waiting at BIB,” and then waits for the cell BIB flag to be cleared.

nPartition Boot Phase

After its cells have completed their self-tests, the nPartition is booted. The nPartition rendezvous occurs during this phase. Not all cells assigned to the nPartition need to participate in the rendezvous. Only one core-capable cell that has completed its cell boot phase is needed for the nPartition boot phase to begin.

By default, all cells assigned to the nPartition that have a “y” use-on-next-boot value are expected to participate in rendezvous. The MP waits for up to 10 minutes for such cells to reach the waiting at BIB state. Cells that have a “n” use-on-next-boot value do not participate in rendezvous and remain waiting at BIB.

The main steps that occur during the nPartition boot phase are as follows:

1. The MP provides a copy of the relevant Complex Profile data to the cells assigned to the nPartition. This data includes a copy of the Stable Complex Configuration Data and a copy of the Partition Configuration Data for the nPartition.

The Complex Profile represents the configurable aspects of a server complex. The Stable Complex Configuration Data contains complex-wide configuration details and the Partition Configuration Data contains details specific to the nPartition. For more information, see the *HP System Partitions Guide*.

2. The management processor releases BIB for cells assigned to the nPartition that have a “y” use-on-next-boot value and complete the cell boot phase in time. The management processor does not release BIB for any cell with an “n” use-on-next-boot value or for any cell that did not complete the cell boot phase within 10 minutes of the first cell to do so. When BIB is released for a cell, the cell is considered to be active.
3. The nPartition rendezvous begins, with the system firmware on each active cell using its copy of complex profile data to contact other active cells in the nPartition.
4. The active cells in the nPartition negotiate to select a core cell.
5. The chosen core cell manages the rest of the nPartition boot process. A processor on the core cell runs the nPartition system boot environment (EFI). The core cell hands off control to an operating system loader when the OS boot process is initiated.

Choosing a Management Tool

You can manage nPartitions using the following tools:

Partition Manager

Partition Manager provides a graphical interface for managing nPartitions. You can run Partition Manager on the complex, or on management stations used to remotely manage the complex.

nPartition commands

You can manage nPartitions using commands such as `parcreate`, `parmodify`, `parremove`, `parstatus`, `parunlock`, `fruled`, `frupower`, and `cplxmodify`. As with Partition Manager, you can run nPar commands on the complex nPartitions or from a management station used to remotely manage the complex. Also, you must set the admin IP address for nPartitions using the nPar commands. This cannot be done with any other tool.

EFI Boot Manager and EFI Shell commands

EFI provides support for nPartition management. The EFI interfaces are accessible from an nPartition console when the nPartition is in an active state but has not booted an OS.

Management processor (MP) menus Management processor menus provide a service interface that provides access to all hardware and nPartitions in the complex. The MP is always available, whether or not nPartitions are configured or booted in the server complex.

Management Interface Options

You can manage nPartitions remotely using one of two management interfaces: the Intelligent Platform Management Interface (IPMI) and the Web-Based Enterprise Management (WBEM) infrastructure. This section provides a brief overview of these interfaces.

IPMI

On cell-based HP Integrity servers, the MP supports IPMI. IPMI is an industry-standard interface that defines common, message-based interfaces to platform management hardware and common records for describing devices and their characteristics.

The IPMI specification supports extensions such as the nPartition and server complex management features introduced by HP. On cell-based servers, the MP supports two communication paths defined by the IPMI specification: Block Transfer and IPMI over LAN.

IPMI Block Transfer (IPMI BT)

IPMI Block Transfer (IPMI BT) provides a communication path between the MP and the OS running on an nPartition. IPMI BT uses the MP device driver and a hardware buffer on each cell to establish a private path (using the block transfer hardware on the core cell) from each nPartition to the MP. On Windows, the device driver that provides the IPMI BT interface is called the HP Health Driver.

The nPartition Configuration Privilege setting enables you to control the access of a user managing an nPartition on a complex. To set the nPartition Configuration Privilege, run the `PARPERM` command using the MP. The nPartition Configuration Privilege has two settings:

- | | |
|--------------|--|
| Unrestricted | (The default) Enables you to manage other nPartitions in the complex |
| Restricted | Restricts use of the IPMI BT interface to the following capabilities: <ul style="list-style-type: none">• Retrieving information about the server, including everything displayed by Partition Manager and the <code>parstatus</code> command.• Changing the local nPartition's Partition Configuration Data.• Manipulating attention indicators (LEDs).• Powering cells and I/O chassis belonging to the local nPartition. |

The nPartition Configuration Privilege does not restrict de-allocation of processors across nPartition boundaries. When the nPartition Configuration Privilege is restricted, some management tasks require IPMI over LAN instead.

IPMI over LAN

IPMI over LAN enables the management tool to communicate directly (without going through an nPartition) with the MP through its Local Area Network (LAN) port. To enable IPMI LAN access to the MP, use the `SA` command at the MP Command menu. The MP accepts IPMI requests at its LAN port only if the request is accompanied by the correct password. To set the IPMI password, use the `SO` command at the MP Command menu.

To secure communication between client and server, the IPMI specification uses the MD5 algorithm (RFC1321) to encrypt the IPMI password and to authenticate server and client. Other security mechanisms protect against replay attacks.

When the management tool sends a request, the nPartition Provider downloads a large data structure containing static configuration information about the server from the MP. This enables the Provider to request dynamic information about the server. When an nPartition command accesses a complex for the first time using IPMI over LAN, it can take a long time (two minutes or more) to complete, depending on network latency between the PC and the server MP.

The nPartition Provider caches the static data and reuses it for subsequent requests so that future command usage does not incur that initial overhead. If the PC is rebooted or the nPartition Provider is restarted, the cached data is lost. The first request to the MP after the restart requires the same initial overhead.

IPMI specifies that data be sent as UDP datagrams over the LAN. UDP does *not* guarantee delivery of datagrams. If datagrams fail to arrive in a reasonable amount of time, the nPartition Provider retries a number of times. But if the network connection between the PC and MP is too unreliable or too slow, the provider times out and returns an error. The error is often seen as the message: [X] data is not available, where [X] is a cell, I/O chassis, cabinet, or other element in the complex.

The speed and reliability of the network between the management station and the MP has a large effect on the reliability of command execution. When managing remotely using IPMI over a LAN, place the management station on the same subnet as and physically close to the target complex. If you cannot access the management station directly, you can use a Remote Desktop application or equivalent tool to connect to it from a remote terminal.

Managing nPartitions Using IPMI over LAN

Using IPMI over LAN, you can manage remote nPartitions through the MP. The management tool on the management station communicates directly with the local nPartition Provider. The nPartition Provider then communicates with the MP on the remote complex using IPMI over LAN.



NOTE: You *must* use IPMI over LAN to manage nPartitions remotely if none of the nPartitions on the target server have been booted or configured yet.

To use IPMI over LAN, you must enable IPMI LAN access at the MP, set the MP IPMI password, and install the nPar tools on your management station. You can then use any nPartition management tool to manage remote nPartitions.

Running Partition Manager Using IPMI over LAN

You can run Partition Manager using IPMI over LAN in one of two ways:

- When running Partition Manager on an nPartition: From the **Tools** menu, select the **Switch Complexes** task. In the **Switch Complexes** dialog, enter the host name or IP address of the MP in the target complex, and enter the IPMI password for that MP.
- When running Partition Manager on another system (not an nPartition): Partition Manager automatically displays the **Switch Complexes** dialog. Enter the host name or IP address of the MP in the target complex, and enter the IPMI password for that MP.

Running nPartition Commands Using IPMI over LAN

To run nPartitions commands remotely using IPMI over LAN, you must include the following command-line options with each command:

- `-g [password]`
The *password* is the IPMI password for the MP.
- `-h hostname | IPaddress`
The `-h` option specifies the host name or IP address in the target complex.

When you use the `-g . . . -h . . .` set of options, the command sends WBEM requests to the local nPartition Provider, which uses IPMI over LAN to communicate with the MP in the target complex.

WBEM

WBEM is an industry initiative that establishes management infrastructure standards and provides a way to combine data from hardware and software management systems. WBEM specifies standards that enable access to data from various technologies and platforms and to present that

data in a consistent fashion. Client applications can then use this information to manage an enterprise computing environment.

Because WBEM supports a distributed management architecture, client applications (nPartition management tools, for example) can run on a remote system and use the WBEM infrastructure to send requests to managed servers.

Partition Manager is a WBEM client application. Partition Manager uses WBEM when retrieving information about a server complex. Partition Manager uses nPartition commands for all other operations. The nPartition commands are also WBEM client applications.

Several software components support nPartition commands for Windows. The Windows OS provides the Windows Management Instrumentation (WMI) software, which is an implementation of WBEM standards. HP provides a WMI-based nPartition Provider and WMI mapper to convert CIM/XML WBEM requests from clients (like nPartition commands and Partition Manager) into WMI requests.

The nPartition commands and Partition Manager send management messages to the nPartition Provider. The nPartition Provider handles communication with the MP using the IPMI protocol, locally through an IPMI/BT device driver, or remotely using the MP IPMI/LAN interface.

Securing the WBEM Connection

WBEM secures the management connection using an SSL authentication process, which involves the following files:

- **WBEM SSL Certificate (cert.pem file)** The WBEM SSL certificate file resides on the system that is being managed and contains the local WBEM server's certificate.
On a Windows system, the WBEM SSL certificate file is in the location specified by the `sslCertificateFilePath` entry in the `%PEGASUS_HOME%\cimserver_current.conf` file, and is usually `%SystemDrive%\hp\sslshare\cert.pem`.
- **WBEM Trusted Certificate Store (known_hosts.pem file)** The WBEM Trusted Certificate Store file resides on the system from which you issue WBEM remote management commands.
On a Windows system, the WBEM Trusted Certificate Store file resides in the `%SystemDrive%\hp\sslshare` directory.
- **Partition Manager Trusted Certificate Store (parmgr.keystore file)** The Partition Manager Certificate Store file resides on the system from which you run Partition Manager. Partition Manager uses it to validate server certificates. On a Windows system, the Partition Manager Trusted Certificate Store file resides in the `%SystemDrive%\hp\sslshare` directory.

For remote WBEM SSL connections to succeed, the WBEM SSL server certificate from the remote system you are connecting to (the WBEM server) must be imported into the trusted certificate stores on the system where the remote WBEM commands are issued from (the client system).

Managing nPartitions Using WBEM

Using WBEM, you can manage remote nPartitions indirectly, through an nPartition on the server.



NOTE: You *cannot* use WBEM to manage nPartitions remotely if none of the nPartitions on the target server have been booted or configured yet, or if the nPartition provider or MP device driver components have not been installed yet.

To use WBEM, install the WMI Mapper and the nPartition commands software on your management station. After you install the tools, enable secure WBEM communications. Then you can use Partition Manager or nPartition commands to manage the remote nPartitions.

Running Partition Manager Using WBEM

You can run Partition Manager with WBEM in one of two ways:

- If you are running Partition Manager on an nPartition: Select the **Switch Complexes** task from the **Tools** menu. In the resulting dialog, enter the host name or IP address of the remote nPartition, and supply a user name and that user's password.
To display information about the target complex, specify a user defined on the remote nPartition. To make changes to the target complex, specify a user with superuser privileges on the remote nPartition.
- If you are running Partition Manager on another system (not an nPartition): Partition Manager automatically displays the **Switch Complexes** dialog.

Running nPartition Commands Using WBEM

To manage nPartitions remotely using WBEM, you must include two command-line options with each nPartition command:

- `-u username : [password]`

The `-u` option specifies a valid user name on the remote nPartition.

For the `parstatus` and `fruled` commands, you can specify a user name on the remote nPartition, but for other commands you must select a user with superuser privileges on the remote nPartition. If you do not specify the password, you are prompted to enter a password after executing the command. This method is more secure because the password is not displayed on the command line.

- `-h hostname | IPaddress`

The `-h` option specifies the host name or the IP address of the remote nPartition.

Choosing a Management Mode

The most common method for managing nPartitions involves a remote management station. This dedicated management station hosts management tools and issues commands over a network connection to the server's management processor, enabling you to manage the complex even if no nPartitions exist on the complex yet. This is called remote management mode.

The other option is to install nPar tools onto an nPartition on the server, and then use them to manage the other nPartitions in the system. This is called local management mode.

When nPartition tools run on an nPartition in local management mode, they default to managing the local complex using the IPMI/BT interface to the MP. This is the simplest mode to use. Because the tools run on the system being managed, you do not need to provide additional authentication or remote connection information to make them work.

For example, when you run nPartition commands in local mode, you do not need `-g`, `-u`, or `-h` options to manage the local complex. When you run Partition Manager in local mode, the connection to the local complex is made automatically (no additional connection or authentication information is required).

You can even manage another complex remotely, *from* an nPartition configured to run in local management mode, by using the `-g` or `-u` options with the nPartition commands, or by selecting **Tools** → **Switch Complexes** in Partition Manager.

A list of advantages and disadvantages of the management modes and connection methods follows. Also included are a listing of authentication and authorization issues associated with each mode.

Local Management

Advantages of local management are as follows:

- Simple installation: Install all components on an nPartition (fewer components must be installed manually when reinstall media is used).
- Simple connection: Log in to SMH and run Partition Manager, or run nPartition commands with no -g/-u options. No additional authentication or login steps are required to manage the local complex.
- Controlled configuration of specific nPartitions with the nPartition Config Privilege option: You can restrict to configuration of certain nPartitions.

Disadvantages of local management follow:

- Requires at least one nPartition to be configured and booted to Windows (or to another OS supporting nPartition tools).
- Requires nPartition tools to be installed on at least one nPartition in each partitionable complex.
- Requires login to an nPartition in each complex to be managed, through the SMH web (in the case of Partition Manager), telnet, or Remote Desktop (in the case of nPartition commands).

Remote Management Using IPMI

Some of the advantages of remote management using IPMI are as follows:

- Installs easily: Install all components onto a remote management station and enables you to manage all complexes in the data center.
- Enables you to manage a complex even if no nPartitions are currently configured in the complex.
- Enables you to manage all complexes in the data center from a single management station.

Disadvantages of remote management using IPMI are as follows:

- Does *not* allow configuration of specific nPartitions to be controlled by use of the nPartition Config Privilege option. Users logging in by remote IPMI have configuration privileges for all nPartitions in the complex.
- Requires the additional login step of providing the MP host name and address and IPMI password to connect to the MP remotely.
- Uses IPMI/LAN connections, which are slightly less secure than remote WBEM connections (using SSL). For this reason, HP recommends that the network connection between the management station and the MP be on a private network.

Remote Management Using WBEM

Some of the advantages of remote management using WBEM are as follows:

- Uses a secure HTTPS/SSL connection between remote management station and nPartition.
- Enables configuration of specific nPartitions to be controlled with the nPartition Config Privilege option. Users can be restricted to configuration of certain nPartitions.
- Enables you to manage all complexes in the data center from a single management station.

Some of the disadvantages of remote management using WBEM are the following:

- Requires at least one nPar to be configured and booted to Windows (or another supported OS) and running the WBEM/WMI nPartition Provider.
- Requires copying SSL certificates from the nPartition to the management station's trusted certificate store (not an automated process).
- Requires the additional login step of providing a user name and password for the remote nPartition being connected to.

Authentication and Authorization Issues

A list of authentication and authorization issues associated with each management mode and connection method follows.

Local Management

Authentication issues associated with the local management mode include the following:

- Authentication is implemented by the OS login to the nPartition (the account used to log in to Windows on the nPartition where the tools are run).
- For Partition Manager (a web application), you are prompted for login credentials when you first access an SMH or Partition Manager web page (locally or from a remote browser).
- The credentials you provide are the same as the OS credentials used to log in to the nPartition directly (for example, in Windows, you use your local or domain Windows account to log in to SMH).

Authorization issues associated with the local management mode include the following:

- Authorization is based on the OS authorization group of the account you use to log in.
- In Windows, if the login account is a member of the local or domain Administrators group, you are given full permission to view *and* modify nPartition configurations. Accounts that do not belong to the local or domain administrators group are given read-only access to nPartition tools.
- If the nPartition Config Privilege option is enabled for the complex, users logging in to an nPartition with full privileges can modify the configuration of that nPartition only. All other nPartition configurations are read-only for them.
- With HP SMH, you can grant read-only and read/write permissions to any OS group. Only Windows administrators are given full permissions. Other groups must be configured in SMH on the local nPartition to give those groups read-only or read/write permissions. This applies to Partition Manager only – when using nPartition commands, the rule is this: Administrators have full access and all other authenticated accounts have read-only access.

Remote Management Using IPMI

Authentication issues associated with the remote-by-IPMI management mode include the following:

- You must log in to the local OS to access the tools. However, local OS permissions do not apply when you use the remote modes of nPartition tools.
- You must specify a remote MP host name or IP address and an IPMI password to enable the remote IPMI connection to the MP.

Authorization issues associated with the remote-by-IPMI management mode include:

- Because only one remote IPMI account exists (which is fixed as “Admin,” and is therefore not specified in the tools), this account always has full (read/write) access to all nPartition configurations in the complex.
- The nPartition Config Privilege setting has no effect when you use remote IPMI to manage the complex. Users logged in through remote IPMI have full access to *all* nPartitions, regardless of the current nPartition Config Privilege setting.

Remote Management Using WBEM

Authentication issues associated with the remote-by-WBEM management mode:

- You must log in to the local OS to access the tools. However, local OS permissions do not apply when you use the remote modes of nPartition tools.
- You must specify a remote nPartition host name or IP address and an OS account and password that are used to log in to that remote nPartition.

Authorization issues associated with the remote-by-WBEM management mode:

- Authorization is based on the OS authorization group of the account you used to log in remotely.
- In Windows, if the login account is a member of the local or domain Administrators group of the remote nPartition, you are given full permission to view *and* modify nPartition configurations. Accounts that do not belong to the local or domain Administrators group are given read-only access to nPartition tools.
- If the nPartition Config Privilege option is enabled for the complex, users logging in to an nPartition with full privileges can modify the configuration of that nPartition only. All other nPartition configurations are read-only for them.

Setting up the Management Station

A management station is often used to configure and administer nPartitions on an HP Integrity server. If HP provided your management station (for example, the PC-SMS management system supplied with Superdome servers), then nPartition tools and support components are installed. However, if you provide your own PC as a management station (for example, an HP Integrity mid-range server), then you must install the tools and components on that system by using the Smart Setup media provided with your server.



NOTE: The nPar tools can also be installed on, and run from, an nPartition on the server being managed.

nPartition tools and components are supported on management stations running one of the following operating systems:

- Windows 2000, SP3 or later
- Windows XP
- Windows Server 2003 (both 32- and 64-bit editions)
- Windows Server 2008
- Windows Server 2008 R2

Controlling the Management Station Remotely

Locate the management station running the nPartition tools close to the server being managed to minimize the likelihood of UDP datagrams being lost in transmission. If, as a result, you cannot access the management station directly, use a remote desktop control or telnet application to access the management station remotely. To connect to the management station remotely, you can use any of the following applications.

Remote Control

To view the desktop of the management station from a remote terminal running an OS other than Windows Server 2008 R2, use third-party remote control software such as the free VNC (www.realvnc.com) or the Symantec pcAnywhere software.

Terminal Services

Windows Server 2000, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 include a Terminal Services feature that enables you to create a login session different from the console, leaving the console available for other administration tasks.

To enable Terminal Services on the management station, click its check box in **Add Windows Components**. Windows 2000 Professional and some Windows Server editions do not include a client for Terminal Services. Download the free client from www.microsoft.com.

Remote Desktop

The Remote Desktop Connection feature is not enabled by default in Windows Server 2008 R2. To enable Remote Desktop Connections on the management station, do the following:

1. Right-click the **My Computer** icon on your desktop and select the **Properties** option. The System Properties dialog appears.
2. Click the **Remote** tab.
3. Select the **Allow users to connect remotely to this computer** check box and click **OK**.
4. Select **Start** → **Administrative** → **Tools** → **Remote Desktops**.

Telnet

Because nPartition commands are executed from a command prompt, you can use a telnet application (the telnet command in Windows or a third-party application, such as Reflection 1) to open a command prompt on the management station. The management station must have the Telnet service installed and started.

To execute nPartition commands using a telnet connection to the management station, do the following:

1. Invoke telnet on the remote terminal, providing the host name or IP address of the management station.
2. Log in to the telnet server with a valid user name and password.
3. From the command prompt, execute nPartition commands as usual.



NOTE: The OS might limit the number of telnet connections permitted into the management station. Also, you cannot use nPartition management tools with a GUI such as Partition Manager using this method.

Performing nPartition Management Tasks

This section provides an overview of common nPartition management tasks.

Listing the Status of an nPartition or Complex

Use Partition Manager or nPartition commands to list server complex hardware details and nPartition configuration details:

Using Partition Manager

You can view nearly every aspect of the complex — the status of its nPartitions, cells, and other hardware — on a single page within Partition Manager. To access this information, do the following:

1. Open a web browser and enter the URL for the web server supporting the target system.
2. At the login page, enter a user name and password and click **Login** to access the SMH. It might take several minutes to load information about the complex.
3. Go to the SMH **Tools** tab and click the **Partition Manager** link in the nPartition Management box.
4. On the Partition Manager **Home** tab, select **Complex** → **Show Complex Details** to produce a summary of the status and configuration of the complex, its nPartitions, cells, and hardware.

Using nPartition Commands

The nPartition commands for listing hardware and nPartition status are as follows:

<code>parstatus -C</code>	List cell configurations.
<code>parstatus -V -c#</code>	List cell details.
<code>parstatus -I</code>	List I/O chassis and card slot details.
<code>parstatus -B</code>	List server cabinet summaries for the complex.
<code>parstatus -V -b#</code>	List server cabinet details.
<code>parstatus -X</code>	List product and serial numbers.
<code>parstatus -P</code>	List a configuration summary for nPartitions.
<code>parstatus -V -p#</code>	List nPartition configuration information.
<code>parstatus -w</code>	List the local nPartition number.
<code>frupower -d -C</code> or <code>frupower -d -I</code>	List power status for all cells (-C) or all I/O chassis (-I).

Using the Management Processor Command Menu

You can list hardware and nPartition status with the following commands, available from the management processor Command menu.

- CP List nPartition configurations, including assigned cells.
- PS List cabinet, power, cell, processor, memory, I/O, and other details.

- IO List connections from cells to I/O chassis on HP Superdome servers.
- ID List product and serial numbers.

Using the EFI Shell

EFI Shell methods for listing hardware and nPartition status include the following commands. Hardware and nPartition information displayed by the EFI Shell is limited to the local nPartition.

- `info sys` List the local nPartition number and active cell details.
- `info io` List the I/O configuration.
- `info mem` List memory details.
- `info cpu` List processor details.

Creating nPartitions

Creating an nPartition involves using an nPartition administration tool to assign cells in a complex to the new nPartition. When you create an nPartition, you can also optionally specify configuration options for the nPartition, such as its name, cell use-on-next-boot values, and other details.

When you create an nPartition, follow the HP nPartition requirements and guidelines. HP recommends only specific sets of nPartition configurations. For nPartition configuration requirements and recommendations, see the *HP System Partitions Guide*.

The method you choose for creating an nPartition depends on whether you are creating the first nPartition in a complex, creating a Genesis Partition for a complex, or creating an additional nPartition in a complex that has nPartitions defined.

Creating the First nPartition in a Server Complex

To create the first nPartition in a complex, complete one of the following tasks:

- From a remote management station, run Partition Manager (connected to the remote management processor) and use the **nPartition** → **Create nPartition** task.
- From a remote management station, use the `parcreate` command (with the `-g` and `-h` options to connect to the remote management processor).
- Create a Genesis Partition (described in the following section) from the management processor console.

Creating a Genesis Partition for a Server Complex

To create a Genesis Partition, use the MP CC command to specify that an initial, one-cell nPartition be created in the server complex. The complex must not have nPartitions defined, or nPartitions must be shut down for reconfig (inactive).

Creating Additional nPartitions in a Server Complex

Use one of the following methods to create nPartitions in a complex where nPartitions are defined:

- | | |
|-------------------------------|---|
| Create an nPartition locally | Log in to an nPartition in the same complex where the new nPartition will be created and use the Partition Manager Create Partition task, or issue the <code>parcreate</code> command. |
| Create an nPartition remotely | Log in to an nPartition in the same complex where the nPartition will be created and use the Partition Manager Create Partition task. You can also execute the <code>parcreate</code> command using the WBEM or the IPMI-over-LAN method. For remote administration using WBEM, the tool accesses the nPar Provider running on an nPartition in the target complex (for example, with the <code>-u . . . -h . . .</code> options). For remote administration using IPMI over LAN, the tool accesses the MP (for example, with the <code>-g . . . -h . . .</code> options). |

Modifying nPartitions

Modifying an nPartition involves using an nPartition administration tool to revise parts of the server Complex Profile data, which determines how hardware is assigned to and used by nPartitions:

- Use `parmodify` or Partition Manager from an nPartition running in the same complex as the nPartition. You can also modify some nPartition details locally from an nPartition console by using EFI Shell commands.
- Use `parmodify` or Partition Manager running on a remote management station or Windows system.
 - When you use WBEM, the tool accesses the nPartition Provider running on an nPartition in the target complex. Use the `-u...` `-h...` set of `parmodify` options (or equivalent Partition Manager login options).
 - When you use IPMI over LAN, the tool accesses the MP of the target complex. Use the `-g...` `-h...` set of `parmodify` options (or equivalent Partition Manager login options).

Modifying nPartitions includes the following tasks:

- Assign (add) or unassign (remove) cells from an nPartition:
 - In the Partition Manager **Hardware** tab, select an nPartition and cell and then select **nPartition** → **Assign cell(s)** / **Cell** → **Assign cell(s)** or **nPartition** → **Unassign cell(s)** / **Cell** → **Unassign cell(s)**.
 - Alternatively, use the `parmodify -p# -a#...` command to add a cell or the `parmodify -p# -d#...` command to remove a cell from the nPartition (-p#, where # is the partition number).
- Remove (delete) an nPartition:
 - Shut down all open applications on the target nPartition. Shut down Windows on the target nPartition. In the Partition Manager **Hardware** tab, select an nPartition and then select **nPartition** → **Delete nPartition**.
 - Alternatively, use the `parremove -p#` command to remove a specified nPartition (-p#, where # is the partition number).
- Rename an nPartition:
 - In the Partition Manager **Hardware** tab, select an nPartition and then select **nPartition** → **Modify nPartition**. In the **General** tab, enter a name in the nPartition Name text box and click **OK**.
 - Alternatively, use the `parmodify -p# -P name` command to set the name for a specified nPartition (-p#, where # is the partition number).
- Set cell attributes:
 - In the Partition Manager **Hardware** tab, select the nPartition that the target cell belongs to. Select **nPartition** → **Modify nPartition**. Click the **Set Cell Options** tab, change the **Use On Next Boot** attribute as desired, and click **OK**.
 - Alternatively, use the `parmodify -p# -m#...` command to modify cell attributes for a specified nPartition (-p#, where # is the partition number), or use the EFI Shell `cellconfig` command to set use-on-next-boot values.
- Set core cell choices:
 - In the Partition Manager **Hardware** tab, select the nPartition to which the target cell belongs. Select **nPartition** → **Modify nPartition**. Click the **Set Cell Options** tab, change the **Core Cell Choice** attribute, and click **OK**.
 - Alternatively, use the `parmodify -p# -r# -r#...` command to specify up to four core cell choices in priority order for a specified nPartition (-p#, where # is the partition number), or use the EFI Shell `rootcell` command to set core cell choices.
- Set cell local memory (vs. interleaved memory) values:
 - In the Partition Manager **Hardware** tab, select the nPartition to which the target cell belongs. Then select **nPartition** → **Modify nPartition**. Click the **Configure Memory** tab, change the **Requested CLM** attribute (as a fraction of total available memory, or as a fixed amount), and click **OK**.
 - Alternatively, use the `parmodify -p# -m#:::%command` (-p#, where # is the partition number, -m#, where # is the cell number, and where % is the cell local memory value, expressed as a percentage).
- Setting nPartition boot paths:
 - You must use the EFI Shell `bcfg` command to configure boot paths.

Booting and Resetting nPartitions

This section lists the main nPartition boot commands and tasks.

Using the MP Command Menu

The MP provides the following commands, available from the Command menu, to support boot and reset operations:

- RS Reset an nPartition. Reset an nPartition after self-tests and partition rendezvous are complete.
- RR Perform a shutdown for reconfig of an nPartition. Reset an nPartition after self-tests and partition rendezvous are complete.
- BO Boot the cells assigned to an nPartition past the waiting at BIB state and begin the nPartition boot phase.
- TC Perform a transfer of control reset of an nPartition.
- PE Power on or power off a cabinet, cell, or I/O chassis. On HP Integrity mid-range servers, nPartition power on and power off is also supported to manage power of cells and I/O chassis assigned to the nPartition using a single command.

Using the EFI Shell

EFI Shell provides the following commands to support boot and reset operations:

- | | |
|-------------------------------------|---|
| bcfg | Lists and configures boot options list for the local nPartition. |
| autoboot | Lists, enables, or disables the nPartition autoboot configuration value. |
| acpiconfig | Lists and configures the nPartition ACPI configuration setting, which determines whether HP-UX, Windows, or Linux can boot on the nPartition.

To boot Windows Server 2008 R2, you must set the ACPI configuration setting for the nPartition to windows. |
| acpiconfig enable
softpowerdown | When set, causes nPartition hardware to be powered off when the OS issues a shutdown for reconfig command. On mid-range servers with a windows ACPI configuration setting, this is the default behavior. This command is available only on mid-range servers. |
| acpiconfig disable
softpowerdown | When set, causes nPartition cells to remain at BIB when the OS issues a shutdown for reconfig command. In this case an OS shutdown for reconfig makes the nPartition inactive. This command is available only on mid-range servers. |
| reset | Resets the local nPartition, resetting cells and proceeding with the nPartition boot phase. |
| reconfigreset | Performs a shutdown for reconfig of the local nPartition, resetting cells and holding them at the wait at BIB state, making the nPartition inactive. |

Using Microsoft Windows Commands

Microsoft Windows includes the following commands for shutting down and rebooting an nPartition:

- | | |
|-------------|---|
| shutdown /r | Shuts down Windows and performs a reboot for reconfig of the nPartition. Cells are reset and nPartition reconfiguration occurs as needed. The nPartition then proceeds with the nPartition boot phase. |
| shutdown /s | Shuts down Windows and performs a shutdown for reconfig of the nPartition. The default behavior differs on HP Integrity Superdome servers and HP Integrity mid-range servers.

On HP Integrity Superdome servers, shutdown /s causes cells to be reset and nPartition reconfiguration to occur as needed. Cells then remain at a wait at BIB state, and the nPartition is inactive. |

On mid-range servers, the default behavior is for shutdown /s to cause nPartition hardware to be powered off. Use the EFI Shell command `acpiconfig disable softpowerdown` instead to make cells remain at a wait at BIB state.

D SMH and the WBEM Providers

The WBEM Providers are a group of services that report system health and status information back to the System Management Homepage (SMH) application, where it can be monitored by the System Administrator. They are installed by default when you install the Integrity Support Pack. WBEM is a Web-based approach for exchanging data across different technologies and platforms. WBEM data is usually encoded using Extensible Markup Language (XML) and then transmitted using Hypertext Transfer Protocol (HTTP).

The following sections describe the WBEM Provider services in more detail.

WBEM Providers

The WBEM Providers collect data from sources such as drivers and system firmware to populate the data model displayed by SMH. These providers include the following:

- Server providers:
 - Processor information and indications
 - Memory information and indications
 - PCI devices and system slots information
 - Sensor information and indications, including redundancy, fans, temperature sensors, and power supplies
 - Computer system information, including physical location, unit ID visual indicator, system firmware, and aggregate computer system status (rollup of connected components and devices)
 - Computer system indications, including ASR reboot, POST error, and thermal reboot
- Network providers:
 - Network controller information and indications
 - 10/100 Mb Ethernet
 - Gb Ethernet
 - NIC teaming
- Storage providers:
 - Storage controller information and indications
 - Ultra3 and Ultra320 SCSI
 - SmartArray 5x and 6x
 - SAS/SATA information
- Other providers:
 - C-Class blade enclosure provider – Enclosure information for c-Class blades
 - Management processor provider – Management processor information
 - Software inventory provider – Installed HP software and firmware information
 - Indications to event log provider – WBEM Provider indications are logged to the Windows system event log

For more information about the WBEM Providers, refer to the *HP Insight Management WBEM Providers on Integrity Servers User's Guide* found here:

<http://h20000.www2.hp.com/bc/docs/support/SupportManual/c02435640/c02435640.pdf>

Using SMH

The HP System Management Homepage (SMH) is a Web-based interface that consolidates and simplifies single system management for HP servers on Microsoft Windows operating systems. By aggregating the data from HP web-based agents and management utilities, SMH provides a common, easy-to-use interface for displaying the following information:

- Hardware fault and status monitoring
- Performance data

- System thresholds
- Diagnostics
- Software version control for an individual server

Before you can start using SMH you must first complete the tasks described earlier in this document, found here: “Configure and Verify the WBEM Providers” (page 64).



NOTE: This section is not intended to be an SMH tutorial. For a complete instructions on how to use this tool, see the *HP System Management Homepage User Guide*, found here: <http://www.hp.com/go/windows-on-integrity-docs>

Accessing WebAgents

The following section describes how to access WebAgents through a browser using SMH:

1. On a system with a network connection to the server, open a compatible browser.
2. Enter one of the following URLs:

`http://machine:2301/`

`https://machine:2381/`

Replace *machine* with the IP address or the computer name under DNS. The first time you navigate to this link, a Security Alert dialog box displays and asks if you want to trust the server. You should click **Yes** to continue.



NOTE: The Security Alert dialog box is unique to the Internet Explorer browser.

To implement your own PKI or install generated certificates into each managed device, you can install a Certificate Authority Root Certificate into each browser used for management. If you use this method, the Security Alert dialog box does not display. If an alert displays unexpectedly, you may have browsed to the wrong device. For more information about installing the Certificate Authority Root Certificate, see the online help in your browser.

3. The Sign In page displays. Enter your user name and password here to access SMH.



NOTE: If you have enabled Anonymous access, the System Management Homepage displays immediately and bypasses the Sign In page.

Components in the Sign In page include:

- User name input field (the user must be a member of a valid SMH user group)
- Password input field
- Sign in button (validates the user name and password)
- Clear button (erases the current user name and password input fields)
- Question mark icon (shows/hides a floating tooltip box with information about the authentication mechanism and sign in process)
- Checkbox (automatically imports the management server certificate when selected. This applies only when using SSO from HP SIM and the trust mode is set to **TrustByCert**).



NOTE: If an error occurs on a sign-in attempt, you are returned to the Sign In page.

A configuration mechanism enables the administrator to customize the image and the message in the Sign In page, such as a custom logo and warning message. As the pages load, SMH checks if personalized content is enabled and available. If such content is not available, SMH uses the default image and warning message.

Navigating SMH

SMH displays all of the HP Web-enabled system management software. In addition, SMH displays various categories, in boxes, with icons indicating their current status.

The SMH main page is divided into two major areas: the Header Frame and the Data Frame.

Header Frame	The Header Frame is constantly visible regardless of the page you are viewing.
Data frame	The Data Frame displays the status for HP Management software and utilities on the system.

The following informational areas and links appear in the Header Frame:

- Master header: The links show the path you are viewing, the user, and a **Sign Out** link.
- Menu. Each item is a direct link to a page or section including:
 - Home
 - Settings
 - Tasks
 - Tools
 - Logs
 - Webapps
 - Support
 - Help
- Main title area. The area under the master header and menu contains the following items:
 - Title: the title of the section of page you are viewing.
 - Host Name: the name of the system.
 - System Model: the model appears as Unknown if the WBEM Providers are not installed on the system.
 - Management Processor: the name of the management processor.
 - Data Source: indicates which source is populating the management data. For instance, WBEM for HP Insight Management WBEM Providers. If no source is installed, no data string displays.
 - Icons: an option that enables you to switch between Icon or List view modes.
 - Bread crumbs: an area under the main title that is divided into four parts.
 - First level menu item.
 - Legend: a link that, when clicked, displays a floating box listing all possible webapps status.
 - Refresh: a link that reloads the header and information areas.
 - Time: displays the time the page was loaded. When you mouse over the Time area, you can see the date the page was loaded.

The following sections or pages appear in the Data Frame:

- Boxes
- Icons
- Pages as configuration
- Support
- Help
- Webapps

The following informational areas can appear in the Header Frame or the Data Frame:

- SMH pages:
 - Getting Started - Signing In
 - Home
 - Settings
 - Tasks
 - Logs
 - Installed Webapps
 - Support
 - Help
- Current User: The identity of the user that is signed in.

- If the user is operating system-based, a **Sign Out** link displays.
- If anonymous access is enabled, the Current User displays **hpsmh_anonymous** and the **Sign In** link displays.
- If Local Access is enabled, the Current User displays **hpsmh_local_anonymous** or **hpsmh_local_administrator**, depending on what level of access has been enabled, and local access appears below user type.
- If user type is **local_access_administrator**, no **Sign In** or **Sign Out** link displays.
- Boxes: Boxes display webapps results in a list of items with their result status.
 - An overall status icon represents the worst status of items inside the box and displays in the title bar along with the title.
 - Under the title bar is a list of items in the box. Each item can have a status icon to the left of its name.
 - In the footer of the box is an expansion line with a link that, when clicked, expands the height of the box to include the total number of items, if the items exceed the five-line limit.
- Loading screen: When an item is selected, a status indicator displays as the Loading screen during the load process of the page. This prevents users from selecting other items after the initial selection.
- Number of columns: The number of boxes or columns presented in each line in the list view mode is defined by the display resolution setting. For example, if your resolution is set at 800 x 600, only three boxes display in a line. With greater resolution, the number of boxes increases to four.
- Notes: Notes are sections placed on the right side and used in most pages. They inform you how to use the controls and what kind of values are expected.
- Icon view: Icons appear for items and sections. When an icon is clicked, another page displays with its items as icons. You can view the status of the items inside the box by hovering your mouse over the icon to view a tooltip containing the total of Critical, Major, Minor, and Warning statuses of installed applications.
- Timeout Warnings: Timeout warnings appear as a floating box in the page footer on the right side when you do not load a page in SMH within the time limit set for timeouts.
- Dynamic Lists in Pages: A dynamically created list of elements displays for each item you want to add or remove to a page and are available for the following pages:
 - IP Binding
 - IP Restricted Login
 - Trust Mode
 - Kerberos Authentication
 - User Groups
- Legend: A link displaying a floating box listing all possible statuses of installed webapps.

Icon	Status
	Critical
	Major
	Minor
	Warning
	Normal
	Disabled

	Unknown
	Informational

- Management Processor: Displays a link to the Remote Insight Lights-Out Edition (RILOE) board or the Integrated Lights-Out (iLO) board. This information is provided by the WBEM Providers. If no WBEM Providers are installed, **none** displays.

The SMH Home Page

The Home page provides system, subsystem, and status views of the server. Information on the Home page is provided by the integrated Web-Based Enterprise Management (WBEM) property pages and management utilities. It also includes information provided by integrated version control, server, and storage agents.

Overall Status Summary

The Overall Status Summary displays links to all subsystems that have a critical, major, minor, or warning status, which the integrated HP Web-enabled System Management software provides. If there are no agents installed or no critical, major, minor or warning items, the Overall Status Summary displays **no items**.

System Status

The System Status displays a status icon with a label under it. A specific webapp sets the value of the System Status icon by using a predefined heuristic to signal the system status. When the webapp is not set for use, System Status displays the worst status reported in the Overall Status Summary box.

System Category

The System category presents the system hardware WBEM information. The first link is a System Summary that includes the system's identity information and health status. This health status is also propagated to the HP Systems Insight Manager (HP SIM). In addition to the summary, links show status and other information about subsystems, such as memory and processors. The System category displays the following information:

- Cooling and temperature: Provides information about the device environment, including thermal and fan status, temperature sensor condition, sensor location, current temperature, temperature threshold, type of threshold, and fan information.
- Memory: Provides information about memory modules, including index, location, description, HP serial number, and HP part number.
- Power: Provides information about power supply groups, including location, presence, status, redundancy state, used capacity, hot pluggable, model, maximum capacity, serial number, voltage, firmware revision, and group redundancy.
- Processors: Provides processor details, including cabinet number, cell number, socket, number of cores, threading status, processor type and speed, revision level, numeric coprocessor, cache amount, maximum speed, serial number, part number, total available cache, and number of active logical processors.
- FRU information: Provides information about Field Replaceable Units in the system, including index, name, part number, vendor, type, serial number, class, slot number, chassis number, I/O chassis number, and asset number.
- I/O chassis: Provides I/O chassis information, including power state and the identity of each device installed in the PCI expansion slots.

Operating System Category

The Operating System category contains links that show basic operating system configuration, usage, state, and other information. The Operating System category displays the following information:

- Logical Disks: Information includes volume, free space, queue length, and disk busy time.

Network Category

The Network category contains links that display basic network system configuration, usage, state, and other information. Information can describe a virtual NIC, a single NIC, or teams of NICs. The information displayed depends on the type of NIC, and can include details about all of the following:

- NIC controllers
- NIC interfaces
- Ethernet statistics
- Logical adapters

System Software Category

The System Software category contains links that display information about the software distributor bundles and products, including patch products.

Storage Category

The Storage category contains links that show basic storage system configuration, usage, state, and other information. Information displayed can include the following:

- File system space used
- SCSI disk information
- SCSI controller information
- Drive array controller information
- Fibre Channel storage information
- Fibre Channel tape controller information
- IDE controller information
- SAS host bus adapter information



NOTE: EMC, EVA, VA, and XP storage systems are not supported by WebAgents. Also MSA 30, MSA 1000, and MSA 1500 are not supported with Windows Server 2008 R2.

System Configuration Category

The System Configuration category displays the following information:

- Automatic Server Recovery: Provides Automatic Server Recovery (ASR) configuration information and displays when the server was last reset.
- Cell Boards: Provides information about the cell board, including product name, ROM version, power, number of CPUs in the cell, total cell memory, and CLM information.
- Partition Info: Provides information about the partition, including total number of active CPUs, number of installed cells, number of powered on cells, number of ready-for-reconfigure cells, partition name, root cell number, and total partition memory
- System Summary: Provides general information that includes system model name, operating system, HP Insight Agents version, system UUID, bay number, blade size, system firmware version, BMC firmware version, management processor firmware version, management processor host name, lights-out management processor IP address, lights-out management processor home page URL, crash dump information, and current and minimum paging file size.

Also provides system name, description, network management up time, contact information, location, and IP address. Specifies power management state. Provides asset control

information that includes device serial number and asset tag. Provides firmware versions including index, description, revision, location, and status.

- **Complex-wide Info:** Provides server complex information, including total number of cabinets, number of compute cabinets, number of IOX cabinets, complex name, and partition number.
- **Crash Dump Monitoring:** Allows you to enable or disable the monitoring of a crash dump condition.
- **Software Version Info:** Information includes the name of the software and the installed version number.
- **System Resources:** Information includes resource type, value, and slot.

System Report

The System Report is a one page report of items shown on other pages that you can print or save to a file. Information on the individual items appears in the other categories.

E Headless Windows Installations

Users of Microsoft Windows Server 2008 R2 are familiar with the setup, installation, and operation of systems using a keyboard, video, and mouse. However, these users might not be familiar with the set of headless functionality provided by HP Integrity servers.

Integrity servers provide a set of tools to set up, install, manage, and use the system in a headless manner. The benefits of headless servers include:

- Elimination of the last remnant of legacy hardware
- Simpler to reconfigure partitions
- Easier system deployment and maintenance
- Readiness for future fine-grained partitioning

Windows on Integrity can be installed using several flexible headless installation methods that match a full range of user scenarios. After the system is installed, all interaction occurs through the Remote Desktop feature. Remote Desktop provides the best user interface experience to a Windows system without the complexities related to a full Terminal Services deployment. The GUI resolution, color depth, and mouse interaction outperform other remote GUI methods.

Why Headless?

Integrity servers are built on an inherently legacy-free architecture. By building on this legacy-free foundation, systems are more stable and are easier to configure and maintain.

What is a Headless System?

Headless systems do not have a legacy VGA monitor or PS/2 keyboard/mouse hardware. A system with these hardware devices is not headless because these devices are detected by Windows and drivers are loaded for them. For example, a system with the A6869B Graphics USB card is not headless even if there is no monitor, keyboard, or mouse connected. This means that the advantages of a completely legacy-free system are not fully available.

As another example, a PCI card with hardware related to the head, such as the A6869B, cannot be hot-plugged. However, users can still take advantage of some of the benefits of interacting with a system using headless methods.

Benefits of Headless Systems

VGA hardware is the last legacy piece of hardware in Integrity systems. By eliminating this device, a system is easier to set up, maintain, and operate.

The presence of VGA hardware restricts the ease of repartitioning cellular systems. Because of the legacy hardware requirements of VGA, there are very specific rules for the IO slot location of the graphics card. As partitions are changed or created, the presence of this card in an IO chassis can create configurations that are invalid. This causes customer confusion and can require that the graphics card and other cards be moved. If an IO card connected to the boot drive must be moved, this can cause the installed OS to fail to boot.

As the system is powering on, much of the hardware must be initialized and configured before the IO path to the graphics card can be used. This delays the display of the firmware forward progress messages. All of these messages are immediately visible through the headless port, giving more visibility into the state of the system.

Customers can simplify their data center by avoiding the deployment or expansion of their console switch environment. Cabling and rack-mount monitors complicate the installation of servers in racks. Console switches with remote viewing capabilities do not present the same high resolution GUI that is available through Remote Desktop. Remote Desktop also provides a more responsive mouse input experience. These remote view console switches also require user authentication management, which further complicates systems that are being installed or repartitioned.

For future systems there may be many customized partitions that require careful allocation of IO slots. Avoiding the consumption of slots for non-critical use such as graphics will ease the deployment of future systems. Customers should start to deploy and operate systems using headless methods.

How to Access a Headless System

Users have full access to the GUI of a system through the use of Remote Desktop. From any client PC on the network, running the Terminal Services Client (mstsc.exe) presents a complete, high-performance GUI of the system's graphical console. All GUI-based interaction is the same as if the user was seated at a physical keyboard, monitor, and mouse attached to the system.

The user has full access to the system's EFI command prompt, boot loader, and OS command prompt by connecting to its service processor via telnet. On mid-range systems, a terminal emulator can be launched from any web browser connected to the service processor. On entry level systems, the user can also connect directly to the service processor via the Integrity Integrated Lights-Out (iLo) web interface or, if the iLO Advanced Pack is installed, through SSH.

Console Definitions

The term "console" can refer to many different things, which can lead to confusion. It can mean anything from a serial port connection into a management processor's command line interface, to the default GUI interface to a Windows system, or many possibilities in between.

In-Band vs. Out-of-Band

Connections to a system are referred to as in-band or out-of-band. An in-band connection is under the control of the OS and the port is visible in Windows Device Manager. Examples of this are a telnet connection to a network interface, a remote desktop GUI session, or a terminal connected to a serial port that is assigned a COMx name in device manager.

An out-of-band connection is not visible to the OS. An example is a connection to the network port or serial port of the management processor (MP). These ports do not appear in Windows Device Manager and are not controlled by a Windows device driver.

Remote Desktop

Windows provides complete remote GUI access through the Remote Desktop. Remote Desktop uses the same tools and software as Terminal Services but without the requirement of setting up a license server. A license for two connections to the Administrator account is included. This is the primary and preferred method for interaction with a healthy system.

Physical Aspects of Integrity Consoles

On the back panel of Integrity servers are network and serial connections to the service processor. The network port is identified as Management LAN and the serial port is identified as Console. On Superdome servers, this port is on the back panel. On other Integrity servers, the Console serial port is on a breakout cable, as are the Remote and UPS serial ports.

Management Processor

The management processor (MP) of a system is the place to go for headless console needs. Integrity systems have used different names for this function, such as GSP, MP, and iLO. Microsoft refers to this hardware as a Service Processor. Regardless of the name, this MP has the same role. It provides the virtualization of the serial port that is used for Emergency Management Services (EMS). This processor is powered by stand-by voltage and runs as long as AC power is applied, even if the rest of the system is not powered on.

Emergency Management Services (EMS)

EMS is the out-of-band communication path used for headless interaction. If a system has a serial port assigned as the EMS port, it is no longer available to the OS for any other use, such as the interface to a UPS.

This path can host multiple channels of communication, from firmware messages at power-on to a command-line interface when the OS has booted. In Integrity systems, this EMS port is connected to the MP and is accessible from the management LAN or management serial port.

Firmware Redirection

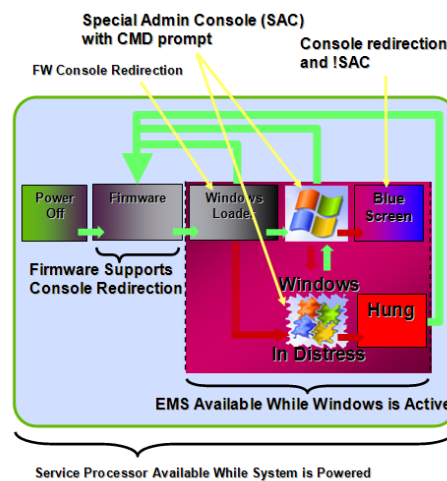
When the server powers on, the system firmware is responsible for configuring all hardware and loading EFI. This phase is also called FW or BIOS console redirection. EFI can be used to prepare the system for OS install or to choose an OS to boot.

The system uses a common serial port standard for this purpose and initializes all system Advanced Control and Power Interface (ACPI) variables to identify this port for use as the EMS port. This port is used by the boot loader and OS for EMS communication. The user can change these default settings using boot loader menus.

Special Administration Console

The Special Administration Console (SAC) runs on top of the EMS. The SAC prompt provides a basic set of commands to manage the setup, installation, and repair of the OS. These commands allow the user to examine logs, shutdown or reboot, kill processes or change process priority, and set network parameters. The SAC prompt can be accessed through the Integrity iLo console menu.

Figure E-1 Emergency Management Services and Special Administration Console



The connection for the SAC is directly into the kernel and is not dependent on user code or device drivers. This means that a user has more tools available to repair an unhealthy system that may be unresponsive from the GUI. This direct-to-kernel path is similar to the kernel debugger and is always available.

From the SAC prompt, the user can create and use a standard Windows command line. During setup, the SAC also starts three setup channels so the user can monitor installation progress. A subset of commands is available for use when the system is in distress. This is known as the !SAC prompt. This change from SAC to !SAC mode is automatic.

The SAC and !SAC prompts are primarily used for setup, or to bring a distressed system back to health so that in-band tools such as Remote Desktop can be used.

Configuring Consoles

Management Processor Settings

Headless connections to the system are made through the MP, preferably through the LAN interface. This management LAN must be configured and changed from factory default settings.

Cellular Systems

There are two options for changing network parameters in cellular systems:

- Systems can be connected to the LAN one at a time and the user can use telnet to connect to the factory default IP address and change the network address. After this address is changed, the next system can be connected to the LAN without creating an address conflict.
- The user can use the management serial port and connect a terminal or a PC running a terminal emulator such as Hyperterm. From this terminal connection, the network settings can be changed from the defaults and further connections can then use the network.

Noncellular Systems

These systems can be connected to the network at the same time. Each is addressed using the unique Medium Access Control (MAC) address of the service processor. The user can assign a fixed IP address associated with each MAC address using standard network address resolution protocol (ARP) and ping protocols.

EFI Console Settings

After system FW has initialized the system, EFI and the EFI Boot Manager will run. EFI Boot Manager is normally configured to launch the OS after a default time-out. The OS boot parameters can be configured before launching. EFI Boot Manager also presents the option to perform Boot Option Maintenance, which allows the configuration of input and output consoles. By changing these settings, the user can choose which physical port and terminal emulation settings to use for the EMS.