

HP Integrity Servers with Microsoft® Windows Server™ 2003 for Itanium-Based Systems Installation Guide



© Copyright 2008 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 US 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 the Installation.....	13
Task 1: Determine Current System Status.....	13
Task 2: Verify Hardware Compatibility.....	13
Task 3: Back up Existing Data.....	14
Task 4: Choose an Installation Environment.....	14
Using Windows Server 2003 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.....	18
Set up a Headless Console.....	18
Set up a Headless Console Using a Null Modem Cable.....	19
Set up a Headless Console Using a LAN.....	19
Set up a Headless Console Using a Remote Serial Console (rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 Servers Only).....	19
Set up a GUI Console.....	20
Set up an Integrated Remote Console (rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 Servers Only).....	21
Set up a Virtual Media (vMedia) Drive.....	22
Set up PXE/WDS.....	22
Set up a WDS Server.....	23
Install WDS.....	24
Configure WDS.....	24
Authorize a WDS Server in Active Directory.....	25
Use the Client Installation Wizard.....	25
Task 7: Prepare the Server Hardware for OS Installation.....	26
Set Up the Boot Drive.....	26
Boot to EFI.....	26
Locate the DVD/CD Drive.....	26
Set ACPI Flag to Windows (Cell-Based Servers Only).....	27
Set Cell Local Memory to 100% (Cell-Based Servers Only).....	28
Specify the Network Interface Card for a Network Boot.....	28
 2 Installing the OS.....	29
Install from a Headless Console.....	29
Run EBSU.....	30
Run Windows Setup.....	33
Enter the Product Key.....	33
Install from a GUI Console.....	34
Run EBSU.....	34

Run Windows Setup.....	36
Specify Server Settings.....	37
Install from PXE.....	37
Reinstall from a Headless Console.....	38
Load the System Image to the Boot Disk.....	38
Configure after the Initial Boot.....	39
Reinstall from a GUI Console.....	40
Load the System Image to the Boot Disk.....	40
Configure after the Initial Boot.....	41
Apply OS Updates Using the Smart Update Media.....	42
Enable Windows Components.....	42
Install TCP/IP.....	42
Install SNMP.....	43
Configure SNMP.....	43
Set IP Addresses from a Headless Console.....	43
Enable and Run Remote Desktop Connection.....	44
Update Firmware, Drivers, and Software.....	44
Update Firmware.....	44
Update Device Drivers.....	45
Register for HP Support Notifications.....	46
Register for Microsoft Security Notifications.....	46
Register for Microsoft Windows Update.....	46
Miscellaneous Installation Issues.....	46
Using Integrated Remote Console to Install Windows on rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 Servers.....	46
Installing a Windows Guest on an HPVM Host.....	47
Enabling Hyperthreading on HP Integrity Servers.....	48
Enable Hyperthreading Using EFL.....	48
Enable Hyperthreading Using Partition Manager.....	49
3 Installing and Configuring the Management Tools.....	51
Install the Integrity Support Pack (ISP).....	51
Configure System Management Homepage.....	54
Set Up Browser Access.....	55
Set Up and Change Your SMH Security Settings After Support Pack Installation.....	55
Initialize SMH	55
Configure the Management Agents.....	56
Activate and Deactivate Agents.....	56
Configure the Event Notifier.....	57
Set the SNMP Data Collection Interval.....	59
Monitor Server Processes.....	60
Send SNMP Traps to Management Applications by IP Address.....	61
Verify Installation of the nPartition Management Tools.....	62
Verify nPartition Commands.....	63
Verify Partition Manager Installation.....	63
A Preparing the Server for Microsoft SQL Server.....	65
SQL Server 2005 Installation.....	65
Install SQL Server from the Command Prompt.....	66
Install SQL Server from the GUI.....	66
B EFI Utilities.....	69
Introduction to EFI.....	69

EFI Boot Manager.....	69
EFI Shell.....	69
Common EFI Shell Commands.....	70
EFI-Based Setup Utility.....	73
Creating a Boot File Using the EFI Shell.....	74
Verify Successful Boot File Creation.....	74

C nPartitioning.....	77
Quick Start.....	77
Getting to Know nPartitions.....	78
Partitioning Continuum.....	78
Cell Structure of nPartitions.....	78
Properties of nPartitions.....	79
Cell and nPartition Boot Phases.....	80
Cell Boot Phase	80
nPartition Boot Phase.....	81
Choosing a Management Tool.....	81
Management Interface Options.....	82
IPMI.....	82
IPMI Block Transfer (IPMI BT).....	82
IPMI over LAN.....	82
Managing nPartitions Using IPMI over LAN.....	83
Running Partition Manager Using IPMI over LAN.....	83
Running nPartition Commands Using IPMI over LAN.....	83
WBEM.....	83
Securing the WBEM Connection.....	84
Managing nPartitions Using WBEM.....	84
Running Partition Manager Using WBEM.....	85
Running nPartition Commands Using WBEM.....	85
Choosing a Management Mode.....	85
Local Management.....	85
Remote Management Using IPMI.....	86
Remote Management Using WBEM.....	86
Authentication and Authorization Issues.....	86
Local Management.....	86
Remote Management Using IPMI.....	87
Remote Management Using WBEM.....	87
Setting up the Management Station.....	88
Controlling the Management Station Remotely.....	88
Remote Control.....	88
Terminal Services.....	88
Remote Desktop.....	88
Telnet.....	89
Performing nPartition Management Tasks.....	89
Listing the Status of an nPartition or Complex.....	89
Using Partition Manager.....	89
Using nPartition Commands.....	89
Using the Management Processor Command Menu.....	90
Using the EFI Shell.....	90
Creating nPartitions.....	90
Creating the First nPartition in a Server Complex.....	90
Creating a Genesis Partition for a Server Complex.....	90
Creating Additional nPartitions in a Server Complex.....	90
Modifying nPartitions.....	91

Booting and Resetting nPartitions.....	92
Using the MP Command Menu.....	93
Using the EFI Shell.....	93
Using Microsoft Windows Commands.....	93
D SMH and Management Agents.....	95
HP Insight Management Agents.....	95
HP Insight Foundation Agents.....	95
HP Insight Server Agents.....	95
HP Insight NIC Agents.....	96
HP Insight Storage Agents.....	96
HP Insight Management Services.....	96
Using SMH.....	97
Accessing WebAgents.....	97
Navigating SMH.....	98
The SMH Home Page.....	98
System Status.....	99
Overall System Status.....	99
System Report.....	99
Network.....	100
Storage.....	100
Operating System.....	100
System.....	101
System Configuration.....	101
E Headless Windows Installations.....	103
Why Headless?.....	103
What is a Headless System?.....	103
Benefits of Headless Systems.....	103
How to Access a Headless System.....	104
Console Definitions.....	104
In-Band vs. Out-of-Band.....	104
Remote Desktop.....	104
Physical Aspects of Integrity Consoles.....	104
Management Processor.....	104
Emergency Management Services (EMS).....	104
Firmware Redirection.....	105
Special Administration Console.....	105
Configuring Consoles.....	105
Management Processor Settings.....	105
Cellular Systems.....	106
Noncellular Systems.....	106
EFI Console Settings.....	106

List of Figures

1-1	Headless console configurations.....	18
1-2	GUI console configuration.....	20
1-3	PXE/WDS configuration.....	23
2-1	Enter EBSU.....	30
2-2	Select Express Setup.....	31
2-3	Firmware update.....	31
2-4	Partition disk.....	32
2-5	Install diagnostic tools.....	32
2-6	Insert the Microsoft Windows Server 2003 CD.....	33
2-7	Enter EBSU.....	34
2-8	Select Express Setup.....	34
2-9	Firmware update.....	35
2-10	Partition disk.....	35
2-11	Install diagnostic tools.....	36
2-12	Insert the Microsoft Windows Server 2003 CD.....	36
2-13	Enabling hyperthreading in the Partition Manager.....	49
3-1	HPSUM Select Installation Host(s) screen.....	51
3-2	HPSUM Select Bundle Filter screen.....	52
3-3	HPSUM Select Items to be Installed screen.....	53
3-4	HPSUM Installation Results screen.....	54
3-5	Services tab.....	56
3-6	Welcome message.....	57
3-7	Mail (SMTP) server information.....	57
3-8	Event recipients information.....	58
3-9	Adding a new user.....	58
3-10	Event selection window.....	59
3-11	SNMP Settings tab.....	59
3-12	Process Monitor tab.....	60
3-13	Component Services window.....	61
3-14	SNMP traps tab.....	62
3-15	SNMP service configuration.....	62
B-1	EFI Boot Manager.....	69
C-1	System overview.....	77
C-2	Partitioning continuum.....	78
E-1	Emergency Management Services and Special Administration Console.....	105

List of Tables

1-1	Installation matrix.....	14
1-2	Locating the Microsoft Certificate of Authenticity (COA) on your server.....	16
1-3	Graphics support on server models.....	20
1-4	EFI device mapping fields.....	27
2-1	Integrity servers supporting PXE/WDS installations.....	37
B-1	EFI Shell Commands and Descriptions.....	70

About This Document

This document describes how to install and configure the operating system and HP software on HP Integrity servers running Windows Server 2003.

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

The latest version of this document can be found online at: <http://docs.hp.com>.

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:

- removed references to Service Pack 1 (SP1) because it is no longer supported
- removed section "Enable More Than 256 Interrupts (Cell-Based Servers Only)" because it only applied to systems with SP1
- changed Step 2 in section: "Apply OS Updates Using the Smart Update Media"
- added Notes to section: "Preparing the Server for Microsoft SQL Server"
- changed HP part number "A6968A" to "A6869B"; changed "A6968B" to "A6869B"
- changed paragraph describing iLO Ops Guide; replaced outdated URL to: <http://docs.hp.com/en/5991-6005/5991-6005.pdf>
- changed paragraph describing WDS Group Policy settings in section: "Use the Client Installation Wizard"
- added missing paren in Step 2, section: "Locate the DVD/CD Drive"
- standardized all references to "HPSUM" (from HP SUM and HP-SUM)
- changed inactive URL in section "EFI Shell" to: <http://www.intel.com/technology/efi/>
- changed server name to "rx8620" in Figure C-1, section: "System Overview"
- added Note to section: "Partitioning Continuum"
- changed URL in "Related Information" section to: <http://hp.com/support/itaniumservers>
- changed Table 1-1 and two paragraphs following it

Document Organization

This document is organized as follows:

"Preparing for the Installation" (page 13)	Describes the steps to prepare the server for installation of the operating system, SmartSetup, and management software.
"Installing the OS" (page 29)	Describes how to install the operating system software.
"Installing and Configuring the Management Tools" (page 51)	Describes how to install the server management software.
"Preparing the Server for Microsoft SQL Server" (page 65)	Describes how to configure and install Microsoft SQL Server 2005.

"EFI Utilities" (page 69)	An overview of the server's Extensible Firmware Interface (EFI) and EFI-Based Setup Utility (EBSU).
"nPartitioning" (page 77)	An overview of how to configure a single system into several independent, partitioned systems, each with hardware and software isolation.
"SMH and Management Agents" (page 95)	An overview of the HP Insight Management Agents and how to configure System Management Homepage (SMH) to administer your system locally or remotely.
"Headless Windows Installations" (page 103)	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 will result in personal injury or nonrecoverable system problems.
CAUTION	A caution calls attention to important information that if not understood or followed may 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). Note that Return and Enter both refer to the same key.
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 hold down 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

You can find more information about HP Integrity servers, server management, and software in the following locations:

- For an overview of the HP Integrity server family:
<http://hp.com/go/integrity>
- For other documents supporting Windows Server 2003 on HP Integrity Servers:
<http://docs.hp.com/en/hw.html#Windows%2064-bit%20on%20HP%20Integrity%20Servers>

- For technical support resources (drivers, patches, upgrades, migration issues, to sign up for alerts, etc.):
<http://hp.com/support/itaniumservers/>
- For information about HP Integrity Virtual Machines (Integrity VM):
<http://h71028.www7.hp.com/enterprise/cache/262803-0-0-0-121.html>

Publishing History

The publishing history below identifies the edition dates of this manual. Updates are made to this publication on an unscheduled, as needed, basis. The updates will consist of a complete replacement manual and pertinent online or CD documentation.

Manufacturing Part Number	Supported Operating Systems	Supported SmartSetup Version	Supported Products (Servers)	Publication Date
5992-4479	Microsoft Windows Server 2003 for Itanium-based Systems, 64-bit	Version 6.1	BL860c, BL870c, rx2660, rx3600, rx6600, rx7620, rx7640, rx8620, rx8640, Superdome, Superdome/sx2000	September, 2008

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 the Installation

Installing Microsoft® Windows® Server 2003 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 2003 operating system is installed on your system, or if it was installed by HP before your system was delivered, you do not need to perform the steps described in Chapter 1 “Preparing for the Installation”) or in Chapter 2 “Installing the OS”. Proceed to Chapter 3 “Installing and Configuring the Management Tools” and install your management tools software.

If your Windows Server 2003 operating system is not installed, if you want to reinstall it, or if you want to migrate to Windows Server 2003 from another 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 18)
- “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 Integrity Essentials Foundation Pack for Windows). You can also order factory installation of the OS. Depending on your order (and subsequent use), your system is in one of the following conditions:

- Factory-installed Windows Server 2003
- Factory-installed OS other than Windows Server 2003
- No operating system installed
- Incorrect or inoperable installation of Windows Server 2003

Task 2: Verify Hardware Compatibility

To verify that your existing hardware is compatible with Windows Server 2003, complete the following steps:

1. See the Options & Accessories page for each server to check supported hardware configurations. For example, the Options & Accessories page for the rx8620 server found here:

<http://h20341.www2.hp.com/integrity/cache/342107-0-0-0-121.html>

lists the processors, memory, adapters, cards, and controllers that are available for that server.

2. Verify existing device compatibility at the HP Integrity server connectivity website:

<http://www.hp.com/products1/serverconnectivity/index.html>

3. Verify storage compatibility by reviewing the HP Integrity Server-Storage support matrices here:

http://www.hp.com/products1/serverconnectivity/support_matrices.html

This list is not exhaustive. Storage vendors can support more configurations than those indicated at the site. As a general rule, check with your storage vendor and an HP sales representative for a definitive statement on server and storage compatibility.

Task 3: Back up Existing Data

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

1. Perform a complete server backup 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 to you.

Table 1-1 Installation matrix

Server Model	Installation Method	Installation Media
rx2660 rx3600 rx6600 BL860c BL870c	Headless console	Windows Server 2003 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 2003 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 (rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 only)	• Virtual Media (vMedia) + Windows Server 2003 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		
Cell-based servers		

Table 1-1 Installation matrix *(continued)*

Server Model	Installation Method	Installation Media
rx7620 rx8620 rx8640 rx7640	Headless console	Windows Server 2003 OS disc (provided by Microsoft) + HP Smart Setup disc + HP Smart Update disc HP Reinstallation disc + HP Smart Setup disc + HP Smart Update disc
Superdome (sx1000 and sx2000)	GUI console	Windows Server 2003 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	
	GUI console	HP Reinstallation disc + HP Smart Setup disc + HP Smart Update disc
	Headless console	HP Reinstallation disc + HP Smart Setup disc + HP Smart Update disc

Using Windows Server 2003 OS Media (Provided by Microsoft) + HP Smart Setup + Smart Update Media

You can purchase the Microsoft Windows Server 2003 OS media from HP, or you can purchase it separately from a Windows reseller. Your organization might already have a volume license for Windows Server 2003. Regardless of how you obtain it, you will need the OS media, a valid license key, and the HP Smart Setup and Smart Update discs to install Windows Server 2003 if the OS is not factory-installed by HP.

In installation environments that include Microsoft-supplied OS media, HP provides Smart Setup and Smart Update media. Smart Setup media automates the setup of boot controllers, drivers, and disk partitions. The Smart Update media provides operating system updates from Microsoft. After completing the installation, HP recommends connecting to Microsoft's website to obtain the latest security updates.

Using HP Reinstallation Media

HP Integrity servers that come factory-installed with Windows Server 2003 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 license key to reinstall Windows Server 2003. The license key is found on the Certificate of Authenticity (COA) of your server. Reinstallation media is the only option available for Windows Server 2003 Datacenter Edition.

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

This certificate contains your Microsoft Windows Server 2003 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](#) identifies the COA location on supported HP Integrity servers.

Table 1-2 Locating the Microsoft Certificate of Authenticity (COA) on your server

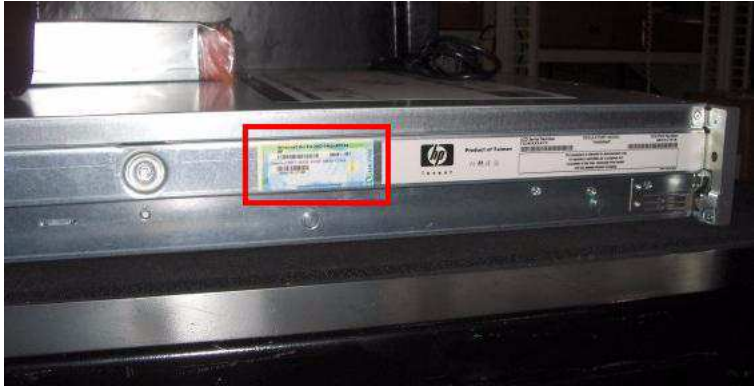
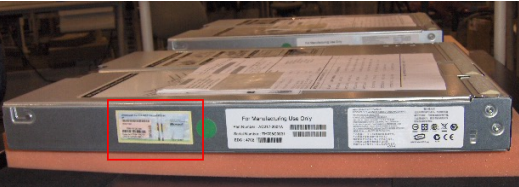
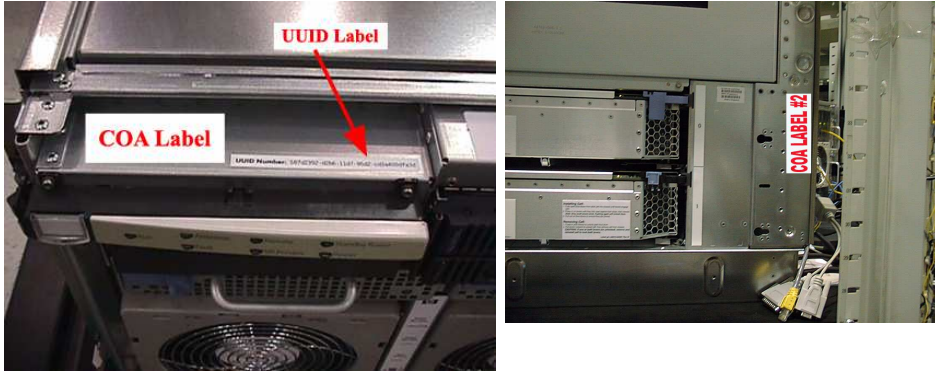
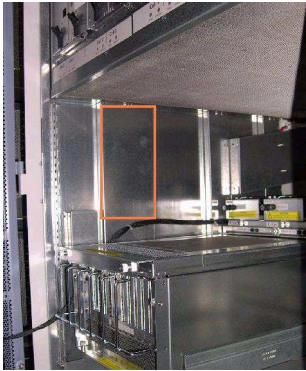
Integrity Server	Location
rx2660	The COA is located on the left side panel, in the middle, as shown here. 
rx3600	The COA is located on the left side panel, as shown here. 
rx6600	The COA is located on the left side panel, as shown here. 
BL860c and BL870c	The COA is located on the left side panel. If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

Table 1-2 Locating the Microsoft Certificate of Authenticity (COA) on your server *(continued)*

Integrity Server	Location
rx7620 and 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 illustration that follows. Additional COAs are shown in the second illustration. 
rx8620 and rx8640	The COA is located in the front of the system, at the bottom, near the power supply as shown in the first illustration that follows. If additional COAs are required, they are located as shown in the second illustration. 
Superdome (sx1000 and 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), as shown here. 

Task 6: Set up an Installation Method

You must 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), available on rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 servers only
 - 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.



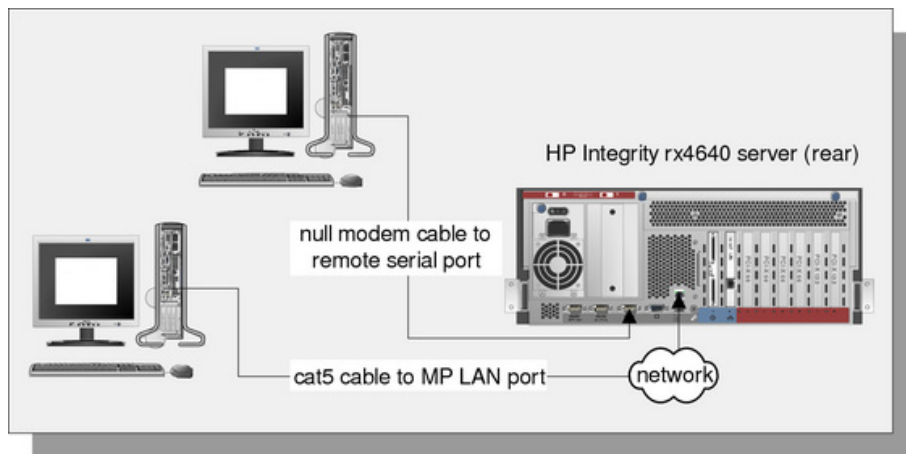
NOTE: For an overview of the benefits, concepts, and terminology of headless operating system installation on HP Integrity servers, see “Headless Windows Installations” (page 103).

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. 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 2003 and Windows Server 2008 Administration and User 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 2003 on HP Integrity servers. For more information about the MP and SAC, see the *Windows Server 2003 and Windows Server 2008 Administration and User Guide*.

You can configure a headless console in one of the following ways:

- Using a null modem cable
- Using a cat5 LAN cable
- Using a Remote Serial Console (for rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 servers only)

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, complete the following 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 these 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 appears.
6. Enter your user name and password. The MP command prompt appears.
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 29).

Set up a Headless Console Using a LAN

To set up the headless console over a LAN, complete the following 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 appears.
3. Enter your user name and password. The MP command prompt appears.
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 29).

Set up a Headless Console Using a Remote Serial Console (rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 Servers Only)

To set up the headless console (on rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 servers only) using Remote Serial Console, complete the following steps:

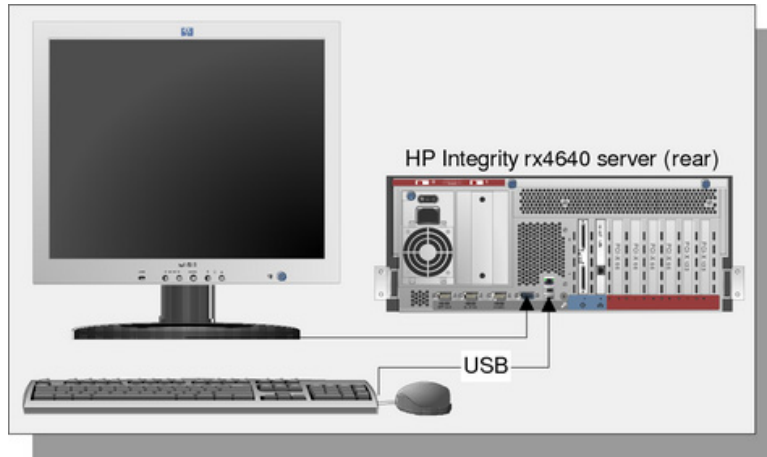
1. Using a secure web browser, enter the name or IP address of the server MP.
2. Enter your user name and password to log in to the System Management Homepage.
3. On the **Remote Console** tab, select **Remote Serial Console** in the left panel.
4. Click the **Launch** button. A new window appears, providing access to the headless console.
5. The set up is complete. Proceed to the Headless Console installation process: “Install from a Headless Console” (page 29).

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. You can use the GUI console to prepare the server for installation, install the OS, and 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 provides available graphics support.

Table 1-3 Graphics support on server models

Server Model	Graphics Card
rx2660, rx3600, rx6600, BL860c, BL870c	Built-in video graphics
rx7620, rx8620, Superdome/sx1000	Optional HP Graphics and USB Combo Card (HP part number A6869B)
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), complete the following 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 34).

To install the HP Graphics and USB Combo Card using the Enhanced interface (gray background), complete the following 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 34).

Set up an Integrated Remote Console (rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 Servers Only)

The Integrated Remote Console (IRC) lets you use Windows clients running Internet Explorer to remotely view and manage HP Integrity servers featuring the iLO 2 management processor. This functionality is supported on rx2660, rx3600, rx6600, BL860c, and BL870c servers only. It is also supported on rx7640, rx8640, and Superdome/sx2000 servers when the HP Lights Out Advanced KVM card is installed (part number: AD307A).

The IRC combines keyboard, video, and mouse into a remote, virtual interface. Use it to view the server display and interact with it. When you use IRC in combination with Virtual Media (See “Set up a Virtual Media (vMedia) Drive” (page 22)), 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 in place of the GUI Console method of installation anywhere the GUI method is described in this document.

The IRC and vMedia features are enabled only after you obtain and install an iLO 2 MP Advanced Pack license (part number AB500A). If you are not licensed and try to use these features, the message: *iLO 2 feature not licensed* appears. Free limited-term trial licenses are available. For more information about the iLO 2 MP Advanced Pack licensing or to obtain a free limited-term license, go to:

<http://h71028.www7.hp.com/enterprise/cache/279991-0-0-0-121.html>.

For more information about iLO 2 functionality on HP rx7640, rx8640, and Superdome/sx2000 servers using the HP Lights Out Advanced KVM card, go to:

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

Follow the factory installation or manual installation instructions located 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 2 MP Operations Guide*:

<http://docs.hp.com/en/5991-6005/5991-6005.pdf>

To set up an IRC (on rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 servers only), complete the following 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. On the **Remote Console** tab, select **Integrated Remote Console** in the left panel.
6. Click the **Launch** button. If **Launch** is grayed out, the license might be invalid or expired. A new window appears, providing access to the IRC.

Set up a Virtual Media (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.

Booting from the iLO 2 MP CD/DVD enables you to upgrade the host system ROM, upgrade device drivers, deploy an OS from network drives, and perform disaster recovery of failed operating systems, among other tasks.

The iLO 2 MP device uses a client/server model to perform vMedia functions. The iLO 2 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 2 MP as required.



NOTE: You can use a vMedia drive in place of a local CD or DVD drive anywhere that a local CD/DVD drive is described in this document.

To set up a vMedia drive (on rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 servers only), complete the following 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. On the **Virtual Devices** tab, select **Virtual Media** in the left panel.
6. Click the **Launch** button. If Launch is grayed out, the license might be invalid or expired. A new window appears, 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.

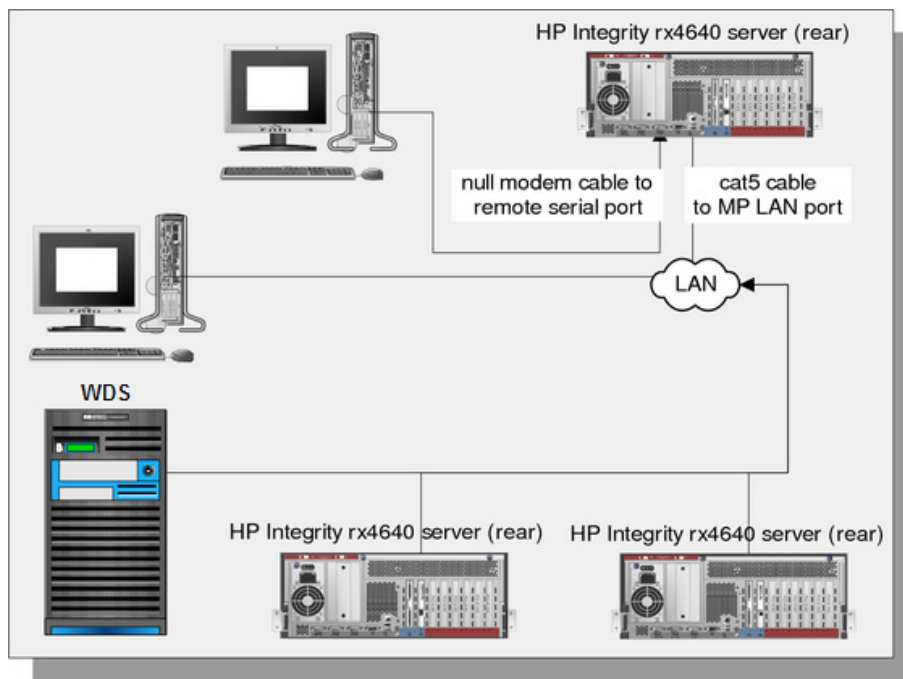
Set up PXE/WDS

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 2003, Datacenter Edition. 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 has completed, 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 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 2003 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 do not need to use the Microsoft version of DNS.
- Ensure that a Dynamic Host Configuration Protocol (DHCP) server exists on the network. You do not need to 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.

For detailed descriptions of the concepts, tasks, best practices, and troubleshooting tips for setting up a WDS server, see the Microsoft Windows Server 2003 Technical Reference website:

<http://www.microsoft.com/windowsserver2003/proddoc/default.mspx>

Specifically, go to this link:

<http://technet2.microsoft.com/WindowsVista/en/library/9e197135-6711-4c20-bfad-fc80fc2151301033.mspx?mfr=true>

Install WDS

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

1. Go to **Start > Settings > Control Panel**, double-click **Add or Remove Programs**, and then 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 do the following:
 - 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 2003 Enterprise Edition with SP2 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 click **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, complete the following steps:

1. Open Active Directory Users and Computers.

2. In the console tree, go to **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, go to the **Remote Install** tab and click **Advanced Settings**.
4. In the Advanced Settings dialog box, go to the **New Clients** tab.
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, complete the following 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 then click **Manage Authorized Servers**.
4. Click **Authorize**, enter the IP address or name of the WDS server, and then click **OK**. When prompted to ensure that this is the correct WDS server to authorize, click **Yes**.

The server will 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, complete the following steps:

1. On the Start menu, click **Run**.
2. Enter the cmd command.
3. At the command prompt, enter:


```
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 will be 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

Complete the following tasks 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. Make sure that the Z: drive is free because Windows Server 2003 creates the EFI partition there.

To set up the boot drive, complete the following steps:

1. Power off the server.
2. Make a note listing all device connections so 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 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, complete the following 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, HDD, a USB device, vMedia, or a DVD-ROM drive) is added to a system after it has booted to 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, complete the following 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 below 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`

You use this 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
<code>blkn</code>	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 <code>Partn</code> appears when a disk drive contains a partition.
<code>Acpi (Device,X)</code>	<code>Acpi</code> is Advanced Configuration and Power Interface. The device type is the first entry in parentheses. The second entry, <code>X</code> , is the PCI host number.
<code>Pci (D/F)</code>	This indicates PCI-related information. <code>D</code> is the PCI device/slot number and <code>F</code> is the PCI function number.
<code>Scsi (Pun,Lun)</code>	This denotes the physical characteristic of the SCSI disk. <code>Pun</code> is the SCSI number and <code>Lun</code> is the LUN number on the physical device.
<code>HD (Part,Sig)</code>	This indicates the partition <code>Part</code> and EFI signature <code>Sig</code> 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 it boots. For the server to boot to Windows Server 2003, 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 2003 without setting the ACPI flag to **windows**, the OS displays a blue screen error.

To set the ACPI flag, complete the following 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 `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.

Windows Server 2003 implements the ACPI 1.0b specification with some extensions from version 2.0, whereas HP-UX and Linux implement ACPI 2.0. As a result, the firmware must be prompted by this flag to recognize that the OS to be booted is Windows Server 2003.



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 set the cell local memory (CLM) parameter to 100% for optimal server performance. 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* on your Smart Setup media or see:

<http://docs.hp.com/en/windows.html>

To set the CLM parameter, complete the following 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 the Windows Server 2003 on the HP Integrity server.

To enable PXE on the HP Integrity server from the EFI Shell, complete the following steps:

1. From the EFI Boot Manager, select **EFI Shell**. The device mapping table appears.
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 2003. 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 operating system and security updates using the Smart Update media.



NOTE: HP Integrity servers must run Windows Server 2003 with Service Pack 2 (SP2). If you are running an earlier version of Windows Server 2003, upgrade your operating system to SP2. When updating to SP2, perform the update in the following order:

1. Install the latest HP Integrity Support Pack.
2. Reboot the machine.
3. Install the Windows Service Pack.
4. Reboot the machine again.
5. Use the Windows Update Service to ensure that you have the latest Microsoft updates.

If the Windows Server 2003 operating system is installed on your system, or if it was installed by HP before your system was delivered, you do not need to perform the steps in this chapter. Proceed to [Chapter 3 “Installing and Configuring the Management Tools”](#) and install your management tools software.

If your Windows Server 2003 OS is not installed, if you want to reinstall it, or if you want to migrate to Windows Server 2003 from another OS, install the OS and OS updates using the steps described in this chapter, in the following order:

- If you are installing your OS for the first time, or migrating from a different operating system:
 - If you are installing locally, choose one of the following options:
 - [“Install from a Headless Console”](#) (page 29)
 - [“Install from a GUI Console”](#) (page 34)
 - If you are not installing locally, choose one of the following options:
 - [“Install from PXE”](#) (page 37)
 - [“Using Integrated Remote Console to Install Windows on rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 Servers”](#) (page 46)
- If you are reinstalling your OS, choose one of the following options:
 - [“Reinstall from a Headless Console”](#) (page 38)
 - [“Reinstall from a GUI Console”](#) (page 40)
- After installing or reinstalling your OS, perform the following tasks:
 - [“Apply OS Updates Using the Smart Update Media”](#) (page 42)
 - [“Enable Windows Components”](#) (page 42)
 - [“Update Firmware, Drivers, and Software”](#) (page 44)
 - See if you need to perform any final tasks here: [“Miscellaneous Installation Issues”](#) (page 46)

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 then booting the server from the boot disk. You should 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 103).

Run EBSU

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.



NOTE: If you are installing an HP Virtual Machines (HPVM) Windows guest, you do not need to run EBSU as part of your setup. Skip this section and go directly to the next section: “Run Windows Setup” (page 33).

To run EBSU, complete the following steps:

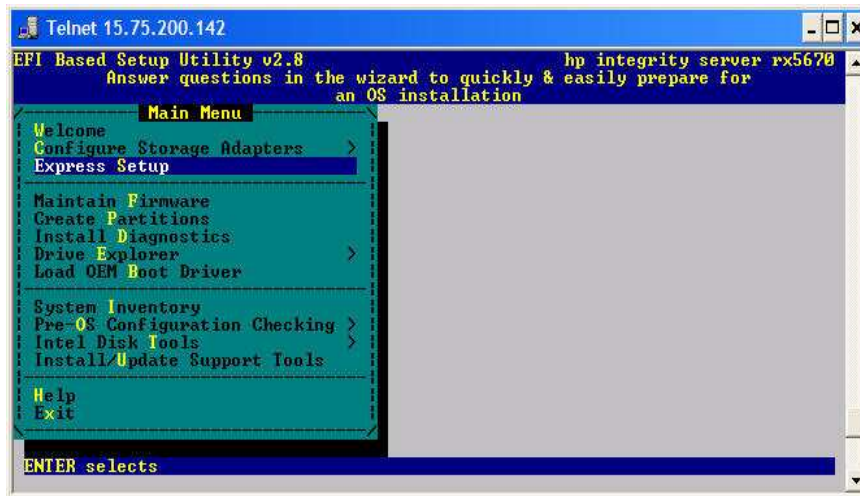
1. Power on the server. The server boots to EFI.
You can use the EFI Boot Manager from the Enhanced interface (gray background) or the Legacy interface (black background).
2. Load the HP Smart Setup media into the server DVD drive.
3. From the EFI Boot Menu, select **Internal Bootable DVD** and press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

Figure 2-1 Enter EBSU



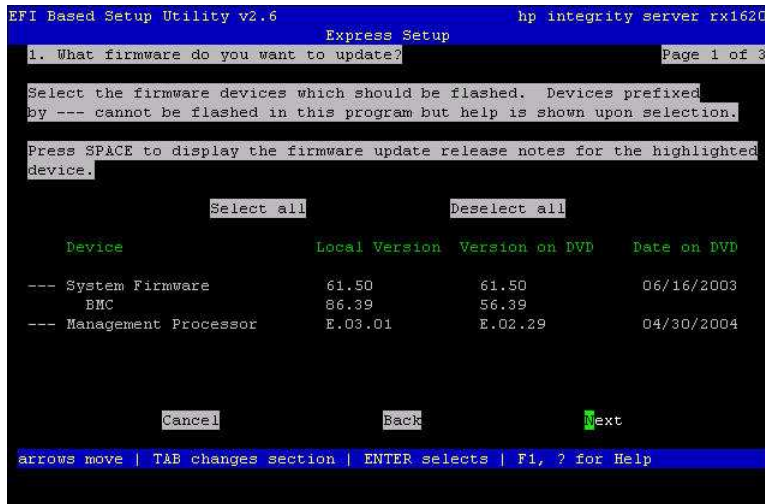
4. Click **OK** and press **Enter**.
5. From the Main Menu, select **Express Setup** and press **Enter**.

Figure 2-2 Select Express Setup



6. EBSU displays the Express Setup introduction. 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**.

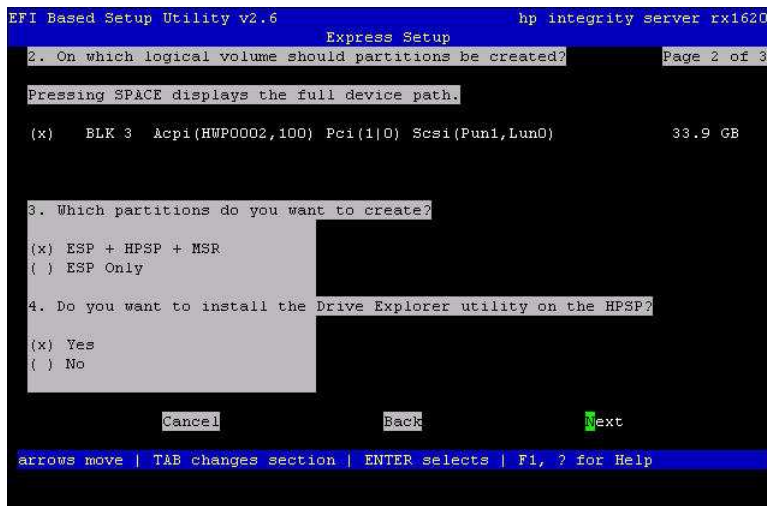
Figure 2-3 Firmware update



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. Also, you cannot use EBSU to flash the Management Processor (MP) firmware. You must download the latest MP firmware from the HP Integrity support site and flash it separately. See: <http://www.hp.com/support/itaniumservers/>.

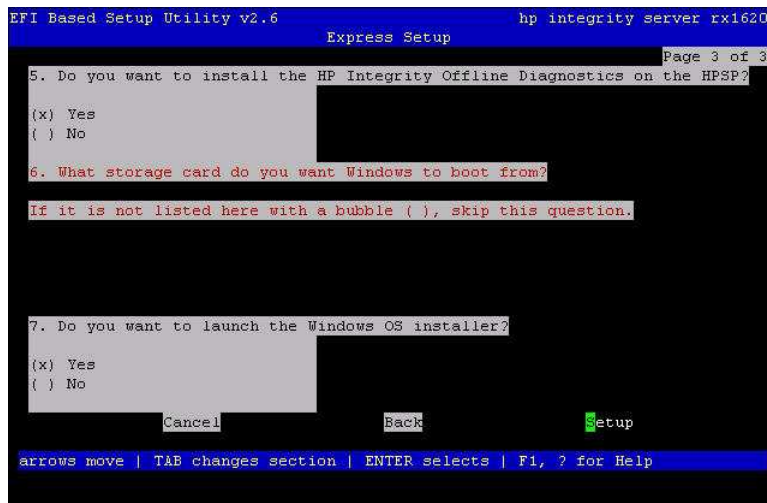
8. To specify the disk partitions you want to create, select **ESP Only** or **ESP + HPSP + MSR**. HP recommends the default — **ESP + HPSP + MSR** — as a means to simplify the maintenance of your server. Also select the option to install the Drive Explorer utility, which enables you to browse a drive in EFI. Select **Next** and press **Enter**.

Figure 2-4 Partition disk



9. Select the option to install offline diagnostic tools (from the HP Itanium Processor Family offline diagnostics and utilities CD).
10. Also select the option to launch the Windows OS installer, select **Setup**, and press **Enter**.

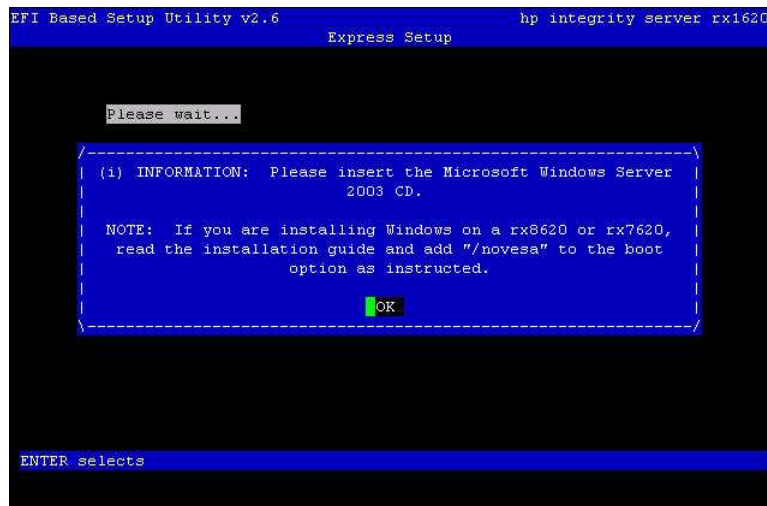
Figure 2-5 Install diagnostic tools



11. EBSU displays the partition confirmation window. Select **Continue** and press **Enter**.

12. EBSU prompts you to insert the Microsoft Windows Server 2003 CD in the DVD drive. Insert the CD and press **Enter**.

Figure 2-6 Insert the Microsoft Windows Server 2003 CD



Run Windows Setup

Windows Setup prompts you to create a system partition on the boot disk if needed, copies the OS files on to that partition, and attempts to reboot from the boot disk.

To run Windows Setup, complete the following steps:

1. Insert the Microsoft Windows Server 2003 CD in the DVD drive, and Windows Setup launches. Press **Enter** to start the installation.



NOTE: If you are installing an HPVM Windows guest, you must issue an **IN** command (for “insert”) from the HPVM console menu every time you insert a disc. If you do not issue the command, the server does not recognize the disc and appears to hang.

2. Windows Setup prompts you to select **Express Install**. Select **Express Install** by pressing **Enter**.
3. If Windows Setup cannot find a system partition, when you are prompted, press **Enter** to continue. Windows creates a partition and then prompts you to format it.
4. Select the partition to install the OS on and press **Enter**. Windows formats the partition if necessary, checks the partition for errors, and begins to copy the OS files.
5. Monitor the copy process until it completes. You can monitor installation progress from the SAC command prompt by using these three channels: `setuplog.txt`, `setupact.log`, and `setuperrlog`. For more information, see the *Windows Server 2003 and Windows Server 2008 Administration and User Guide*.

Upon completion, Windows Setup counts down to a reboot. Allow the system to reboot.

Enter the Product Key

To enter the product key, complete the following steps:

1. At the SAC prompt, press **Esc+Tab** to switch to a new command channel.
2. When prompted, type the product key (a volume license key or the key found on the COA label) and press **Enter**.

Install from a GUI Console

This section describes how to install the OS using a GUI console.

Run EBSU

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.



NOTE: If you are installing an HPVM Windows guest, you do not need to run EBSU as part of your setup. Skip this section and go to the next section: “Run Windows Setup” (page 36).

To run EBSU, complete the following steps:

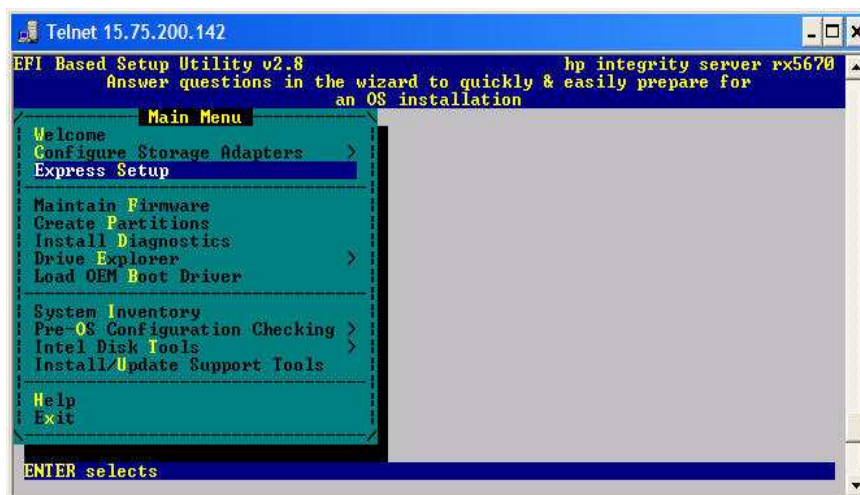
1. Power on the server. The server boots to EFI.
You can use the EFI Boot Manager from the Enhanced interface (grey background) or the Legacy interface (black background).
2. Load the HP Smart Setup media into the server DVD drive.
3. From the EFI Boot Menu, select **Internal Bootable DVD** and press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

Figure 2-7 Enter EBSU



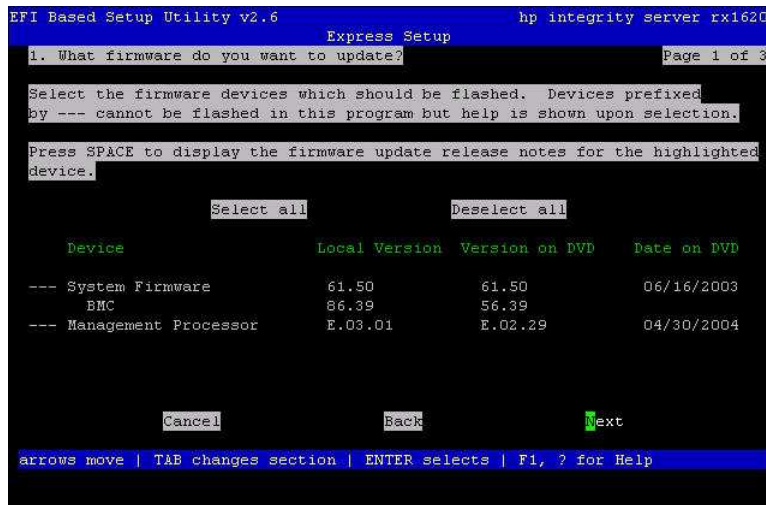
4. Click **OK** and press **Enter**
5. From the Main Menu, select **Express Setup** and press **Enter**.

Figure 2-8 Select Express Setup



6. EBSU displays the Express Setup introduction. 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**.

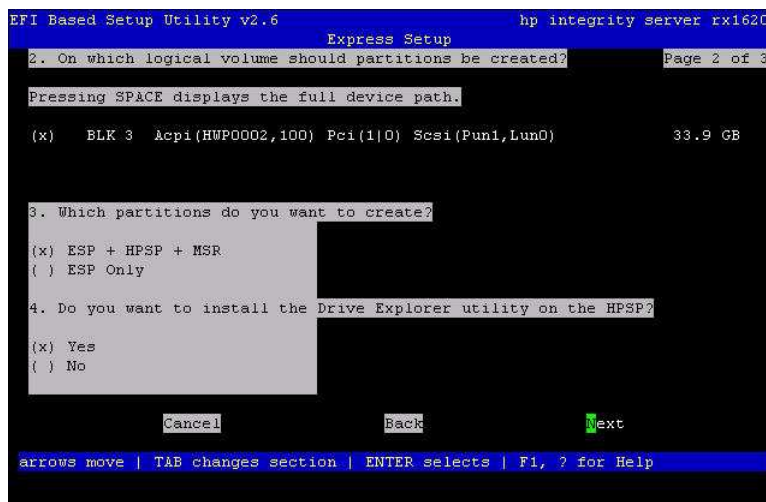
Figure 2-9 Firmware update



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. Also, you cannot use EBSU to flash the Management Processor (MP) firmware. You must download the latest MP firmware from the HP Integrity support site and flash it separately: <http://www.hp.com/support/itaniumservers/>.

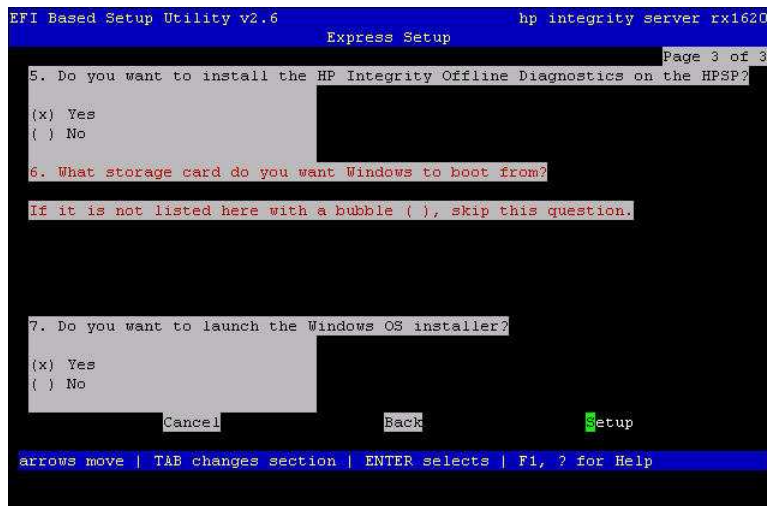
8. To specify the disk partitions you want to create, select **ESP Only** or **ESP + HPSP + MSR**. HP recommends the default — ESP + HPSP + MSR — as a means to simplify the maintenance of your server. Also select the option to install the Drive Explorer utility, which enables you to browse a drive in EFI. Select **Next** and press **Enter**.

Figure 2-10 Partition disk



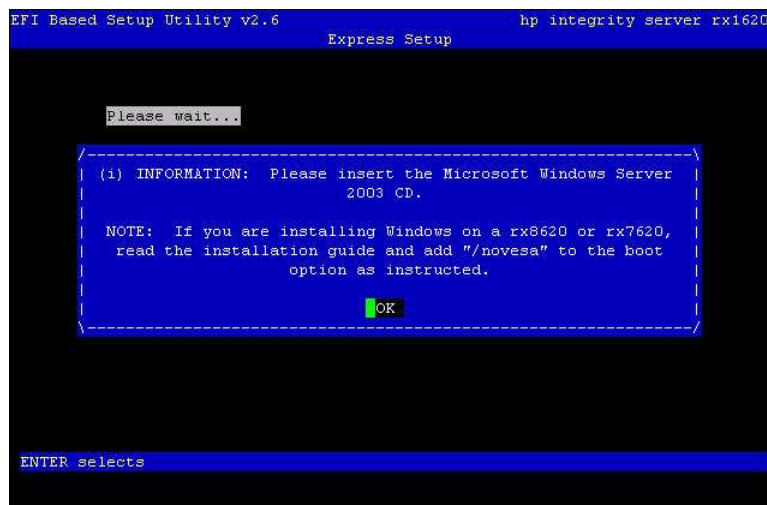
9. Select the option to install offline diagnostic tools (from the HP Itanium Processor Family offline diagnostics and utilities CD).
10. Also select the option to launch the Windows OS installer, select **Setup**, and press **Enter**.

Figure 2-11 Install diagnostic tools



11. EBSU displays the partition confirmation window. Select **Continue** and press **Enter**.
12. EBSU prompts you to insert the Microsoft Windows Server 2003 with SP2 CD in the DVD drive. Insert the CD and press **Enter**.

Figure 2-12 Insert the Microsoft Windows Server 2003 CD



Run Windows Setup

Windows Setup prompts you to create a system partition on the boot disk if needed, copies the OS files on to that partition, and attempts to reboot from the boot disk.

To run Windows Setup, complete the following steps:

1. Insert the Microsoft Windows Server 2003 CD in the DVD drive, and Windows Setup launches. Press **Enter** to start the installation.



NOTE: If you are installing an HPVM Windows guest, you must issue an **IN** command (for “insert”) from the HPVM console menu every time you insert a disc. If you do not issue the command, the server does not recognize the disc and appears to hang.

2. Windows Setup prompts you to select **Express Install**. Select **Express Install** by pressing **Enter**.

3. If Windows Setup cannot find a system partition, when you are prompted, press **Enter** to continue. Windows creates a partition and then prompts you to format it.
4. Select the partition on which to install the OS and press **Enter**. Windows formats the partition if necessary, checks the partition for errors, and begins to copy the OS files.
5. Monitor the copy process until it completes. You can monitor installation progress from the SAC command prompt by using these three channels: `setuplog.txt`, `setupact.log`, and `setuperrlog`. For more information, see the *Windows Server 2003 and Windows Server 2008 Administration and User Guide*.

Upon completion, Windows Setup counts down to a reboot. Allow the system to reboot.

Specify Server Settings

When the system boots, Windows displays a screen indicating that an EMS channel (MP remote port) is present. It can take 2 to 15 minutes for the mouse and keyboard to start operating in this mode.

To set up Windows Server 2003 after initial boot from the local console, complete the following steps:

1. When prompted to enter server settings, click **OK**.
2. In the Windows Setup Wizard, enter the following setup information:
 - a. In the License Agreement window, click **Accept** and then click **Next**.
 - b. In the Regional and Language Options window, click **Next**.
 - c. In the Your Product Key window, enter the product key located on the label attached to the server.
 - d. In the Licensing Modes window, select the license you purchased.
 - e. In the Administrator Password window, enter the server name and a password.
 - f. In the Date and Time window, select the time zone, and click **Next**.

The server reboots to the EFI Boot Manager.

3. From the EFI Boot Menu, select **Windows Server 2003**. The server boots to Windows.
4. Log in to the system with the administrator password you specified earlier.
5. After installing the OS, install the HP Support Pack (from the HP Smart Setup media) and install the OS updates from Microsoft (from the HP Smart Update media).

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.

Support for PXE/WDS installations is limited to the HP Integrity servers listed in the following table.

Table 2-1 Integrity servers supporting PXE/WDS installations

Server	PXE/WDS support
rx2660, rx3600, rx6600, BL860c, BL870c, rx7620, rx7640, rx8620, rx8640	Yes — Enterprise edition only
Superdome (sx1000 and sx2000)	Yes — Enterprise edition only

To install Windows Server 2003 from PXE, complete the following 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 2003 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 2003 from a headless console, complete the following 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.



IMPORTANT: If you are installing an HPVM Windows guest, you must issue an **IN** command (for “insert”) from the HPVM console menu every time you insert a disc. If you do not issue the command, the server does not recognize the disc and appears to hang.



NOTE: With rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 servers, 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.
4. Type **co** and press **Enter**.
5. Because Windows Server 2003 cannot create a boot entry if one exists, delete all existing boot entries. 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: With rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 servers, 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. A Warning message appears stating that all data, including the partition table, will be lost upon reinstallation. Read the message and confirm the target drive (DRIVE 0) and controller. To continue, press **y** and then **Enter**. If you want to abort, press **n** and then **Enter** instead.
16. Select the partition size (33 GB is recommended) and press **Enter**. The maximum partition size is limited to the size of the drive.
17. Select **Y** to continue. The installation process copies files to the hard disk. Do not power off the server during the installation.
18. 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]`.
19. At the prompt, press any key to reboot the system. Then press **Enter** to get to the SAC prompt. The system should boot immediately to Windows.
20. When the SAC prompt appears (EVENT:), hold down the **Esc** key and press the **Tab** key one time. Release both keys, then press **Enter** to switch to the command prompt.
21. At the License Agreement screen, hold down the **Esc** key and press the number **8**. Then release both keys



NOTE: You have only a few seconds to press the **8** key, otherwise the system will reboot!

NOTE: Also, if you are using a terminal emulator configured for UTF8 support, then instead of pressing **Esc + 8**, you should press the **F8** key instead.

22. Type in your product activation key (**nnnn-nnnn-nnnn-nnnn-nnnn**), including the hyphens, found on your Certificate of Authenticity.
23. Type in the desired Administrator password and press **Enter**. The system boots immediately to Windows.
24. 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 2003 after the initial boot from a headless console, complete the following steps:

1. Open a terminal server client and log in to Windows Server 2003 by typing Administrator for the user name and Abcdef12 (case-sensitive) for the password.
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 51). 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 51).
 - 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 51) 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 51).
3. The system prompts you to reboot. Click **Yes** to reboot. To secure your server properly, HP strongly recommends that you change your Administrator password after the reboot.
4. Install any available operating system updates using your HP Smart Update media. For instructions, see: “Apply OS Updates Using the Smart Update Media” (page 42)
5. Your system is now ready to go online.

Reinstall from a GUI Console

HP Integrity servers that are factory-installed with Windows Server 2003 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 2003 from the local GUI console, complete the following 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. Because Windows Server 2003 cannot create a boot entry if one exists, delete all existing boot entries. 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.



IMPORTANT: If you are installing an HPVM Windows guest, you must issue an `IN` command (for “insert”) from the HPVM console menu every time you insert a disc. If you do not issue the command, the server does not recognize the disc and appears to hang.

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. A Warning message appears stating that all data, including the partition table, will be lost upon reinstallation. Read the message and confirm the target drive (DRIVE 0) and controller. To continue, press **y** and then **Enter**. If you want to abort, press **n** and then **Enter** instead.
9. Select the partition size (33 GB is recommended) and click **OK**. The maximum partition size is limited to the size of the drive.
10. At the Warning message, click **Yes** to continue. The installation process copies files to the hard disk. Do not power off the server during the installation.
11. 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 [OK]`.
12. At the command line message, press any key to reboot the system.
13. Select EULA, a user name, a password, and your network settings.
14. The system will reboot one or more times and then boot to Windows.
15. You are logged in automatically as Administrator the first time that Windows Server 2003 boots. However, after any period of inactivity, a timeout screen saver displays and you must log back in again using the default password `Abcdef12` (case-sensitive).
16. 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 2003 after the initial boot from the local console, complete the following 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 51). After you finish this reinstallation procedure, you should also perform the other configuration tasks outlined in “[Installing and Configuring the Management Tools](#)” (page 51).
 - 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 51) 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 51).

2. The system prompts you to reboot. Click **Yes** to reboot. To secure your server properly, HP strongly recommends that you change your Administrator password after the reboot.
3. Install any available operating system updates using your HP Smart Update media. For instructions, see: “[Apply OS Updates Using the Smart Update Media](#)” (page 42)
4. Your system is now ready to go online.

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 Integrity Essentials Foundation Pack kit with the Smart Setup media.

To apply the OS updates using the HP Smart Update media, complete the following steps:

1. Insert the HP Smart Update media. The Smart Update screen appears.
2. Click the **QFEs for WS2003 SP 2** 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. You can also run **QFE Check**, which is included with each Smart Component (when you extract the Smart Component bundle).



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.

Install TCP/IP



NOTE: Install TCP/IP before installing the HP management agents.

To install the TCP/IP driver, complete the following steps:

1. Select **Start > Settings > Control Panel > Network Connections**.
2. Right-click the **Local Area Connection** icon and select **Properties**.
3. Select **Internet Protocol TCP/IP** and click **Install**.
4. Click **OK**.

Install SNMP

SNMP support is included in Windows Server 2003. To install the SNMP Protocol, complete the following steps:

1. Select **Start > Settings > Control Panel**.
2. Click **Add or Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. In the **Windows Component** wizard, clear all components except **Management and Monitoring Tools**, then click **Next**.
5. From the Management and Monitoring Tools window, select **Simple Network Management Protocol**, then click **OK**. The Component Wizard page appears.
6. Click **OK** to start the installation.
7. Monitor the installation and click **Finish** to complete it.

Configure SNMP

To configure SNMP, complete the following steps:

1. From the Control Panel select **Administrative Tools > Services**, right-click **SNMP Service**, and select **Properties**. The SNMP Service Properties (Local Computer) dialog appears.
2. On the **Security** tab, click **Add** to add the community string.
3. Select a name for the string and access rights.
4. Click **Apply**, then click **OK**.

Set IP Addresses from a Headless Console

To set the MP IP from a headless console, complete the following 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, complete the following 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 2003 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, complete the following steps:

1. Right-click the **My Computer** icon and click **Properties**.
2. On the Remote tab, select **Enable Remote Desktop on this computer**.
3. Click **OK**.
4. On the Control Panel, double-click **Windows Firewall**.
5. Go to the **Exceptions** tab, select **Remote Desktop**, and click **OK**.

To enable remote desktop connections from a headless server, complete the following 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 Windows Server 2003 64-bit for Itanium Release to Manufacturing (RTM) with SP2 slipstream media, 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, complete the following steps:

1. Click **Start > Programs > Accessories > Communications > 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.

Update Firmware, Drivers, and Software

To update your system after installing the OS, install the Integrity Support Pack from the HP Smart Setup media.



IMPORTANT: HP Customer Engineers must perform firmware updates for Superdome, rx8620, and rx7620 servers in compliance with the support agreement.

You must install the Integrity Support Pack if you did not use the HP Reinstallation media to install the OS.

Update Firmware

To check the system firmware version and boot the server to EFI, complete the following steps:

1. Use the arrow key to select **EFI Shell**, and then press **Enter**.
2. At the EFI Shell prompt, enter `info fw`.
The EFI Shell lists the firmware version as follows:

```
FIRMWARE INFORMATION
Firmware Revision:
All CELLS - 1.12 Thu Oct 16 08:10:32 2003
```
3. Verify the installed version with the version present on the HP Smart Setup media or on the HP Integrity support site at:
<http://www.hp.com/support/itaniumservers/>



NOTE: For rx7620, rx7640, rx8620, rx8640, and Superdome servers, contact HP support or an HP Customer Engineer to obtain the latest firmware.

The EBSU on the Smart Setup media enables you to update the firmware. You can use this procedure without using Express Setup.

1. Download the latest firmware for your server from the HP website:
<http://www.hp.com/support/itaniumservers/>.
2. Copy the files to the EFI partition:
 - a. Open a command prompt window.
 - b. Enter the `mountvol z: /s` command to mount the EFI partition, where *z* is an available drive letter on your system.
 - c. Copy the files to the *z:* drive.
 - d. Reboot the system to EFI Boot Manager.
3. In EFI Boot Manager, select **EFI Shell[Built-in]**, then press **Enter**. The device mapping table appears.
4. Find the files in the EFI shell.
 - a. Enter `fsX:`, where *X* is a number from the device mapping table (for example, `fs0:`).
 - b. At the EFI Shell prompt, change to the directory where the firmware file was copied.
5. Enter the firmware executable file name, and press **Enter** to begin installation.

Update Device Drivers

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, complete the following steps:

1. From the Windows Desktop, right-click the **My Computer** icon.
2. Click the **Properties** button, displaying the System Properties window.
3. Go to the **Hardware** tab.
4. Click **Device Manager** to display the Device Manager window, and then select **View > Devices by Type** to list the system devices.
5. Expand the **Other Devices** entry.

6. Scan the listed devices, verifying that no device displays 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 Windows cannot find 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. HP Integrity rx8620 and rx7620 servers do not have legacy serial devices, so this error always occurs. The bang does not indicate faulty hardware in this case.

7. If a device is flagged with a fault indicator (a bang or question mark), insert the HP Smart Setup media in the server's drive and accept the End User Licensing Agreement.
8. Right-click the flagged device and select **Update Driver** from the context menu.
9. In the Hardware Update Wizard screen, select **Install the software automatically** and click **Next**.
10. If you see a warning dialog stating the driver is not digitally signed, ignore it by clicking **Next** to continue. This is not an issue.
11. 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 might 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 Windows 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 or features of the Windows-on-Integrity solution.

Using Integrated Remote Console to Install Windows on rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 Servers

If you are using the IRC to remotely install Windows Server 2003 on rx2660, rx3600, rx6600, BL860c, BL870c, rx7640, rx8640, and Superdome/sx2000 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 29).
- Disconnect the local graphics console before you install Windows using IRC, and then reconnect it afterwards. This method is easy and therefore recommended.
- Create a boot entry that includes the /NOVESA option.

If you select the last option, the Windows installation fails during plug-n-play detection of the system’s monitor and video controller. The failure occurs after you see the message `An EMS channel is detected` and click **OK** to continue. Symptoms of the failure include rapid resizing of the installation window, partial data display, and mouse input failure.

To recover and finish the installation, create a new boot entry that includes the /NOVESA option by completing the following steps:

1. From the EFI Shell, go to the MSUTIL directory:

```
fs1: cd msutil
```

2. Run the `nvrboot.efi` utility:

```
fs1: nvrboot
```

EFI displays the Boot Options menu:

```
NVRBOOT: OS Boot Options Maintenance Tool [Version 5.2.3683]
* 1. Windows Server 2003, Enterprise
2. EFI Shell [Built-in]
* = Windows OS boot option
(D)isplay (M)odify (C)opy E(x)port (I)mport (E)rase (P)ush (H)elp (Q)uit
```

3. Enter **c** to copy.

EFI prompts you to select which OS boot option to copy.

4. Select the first option, **Windows Server 2003, Enterprise**, by entering **1**. The first boot option is copied and should appear as a new item at the end of the list.
5. Enter **m** to modify. EFI prompts you to select the boot option to modify.
6. Select the new boot option by typing the number that represents its order in the list (the exact number can vary from system to system). EFI then prompts you to specify which loader variable you want to modify:

```
Enter VAR to modify: LoadIdentifier = Windows Server 2003, EnterpriseOsLoadOptions =
/redirectEfiOsLoaderFilePath = cf5f2ddc-b885-11d7-b831-000000000000 ::
\efi\microsoft\winnt50\ia64ldr.efiOsLoaderFilePath = e605a034-b885-11d7-b831-000000000000 :: \windows
```

7. Select the second option, **OsLoadOptions**, by entering **2**.
8. Enter the line as it currently appears, then add the /NOVESA option at the end. For example, for the example shown in step 6, you would enter `OsLoadOptions = /redirect /novesa` then press **Enter**. The EFI displays the boot loader options again (with the /NOVESA option):

```
Enter VAR to modify:
LoadIdentifier = Windows Server 2003, Enterprise
OsLoadOptions = /redirect /novesa
EfiOsLoaderFilePath = cf5f2ddc-b885-11d7-b831-000000000000 :: \efi\microsoft\winnt50\ia64ldr.efi
OsLoaderFilePath = e605a034-b885-11d7-b831-000000000000 :: \windows
```

9. Enter **q** (to quit), then choose **Exit** to return to the Boot Manager.
10. In the new list of boot options, scroll down to the new entry and press **Enter** to reboot the system using the modified boot entry.

Installing a Windows Guest on an HPVM Host

HPVM is a soft-partitioning and virtualization technology that provides OS isolation with CPU allocation and shared I/O. HPVM enables a single Integrity server to emulate multiple virtual machines running distinct operating systems and environments. The Virtual Machines solution consists of two components:

- A VM host (the physical system where the virtual machines reside)
- Virtual machines, also known as guests

Virtual machines, or guests, are abstractions of real, physical machines. They are fully loaded operational systems, complete with OS, system management utilities, applications, and networks, all running in the virtual machine environment that you set up for them. You boot and manage guests using the same storage media and procedures that you would if the guest OS was running on its own dedicated physical hardware platform.

It is beyond the scope of this document to describe the installation and use of HPVM on Integrity servers. These topics are covered in detail in *HP Integrity Virtual Machines Installation, Configuration, and Administration* found here:

<http://docs.hp.com/en/hplex.html#HP%20Integrity%20Virtual%20Machines>

If you are interested in implementing HPVM, see this document first. It explains how to install and configure the host OS, HPVM software, and guests.

Be aware of the following peculiarities regarding installation of Windows guests on Integrity servers serving as HPVM hosts:

- When you insert or eject a disc, such as the Smart Setup or Smart Update media, or the HP Reinstall or Microsoft OS media, you must issue an **IN** (insert) or **EJ** (eject) command from the HPVM console menu. If you forget to do this, the server does not recognize the inserted disc and does not eject the disc when you push the Eject button. In addition, if you do not issue these commands, the server appears to be unresponsive.
- You must create a boot option for the guest after you insert the Reinstall or Microsoft OS media to load the Windows OS by using the **Internal Bootable DVD** option.
- You must install the HP Integrity Baseboard Management Controller Device Driver on guests for HPVM to function on these systems. The Baseboard Management Controller driver (also known as the HP Health Driver) is installed from the Support Pack and Reinstall Media. You can install it manually from the Smart Setup media. You can verify the installation and status of this driver using the Windows Device Manager.

Enabling Hyperthreading on HP Integrity Servers

HP Integrity servers now support Intel® Dual-Core Itanium® 2 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.

Enable Hyperthreading Using EFI

To enable hyperthreading on partitionable and nonpartitionable HP Integrity servers using the Extensible Firmware Interface (EFI), complete the following 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.

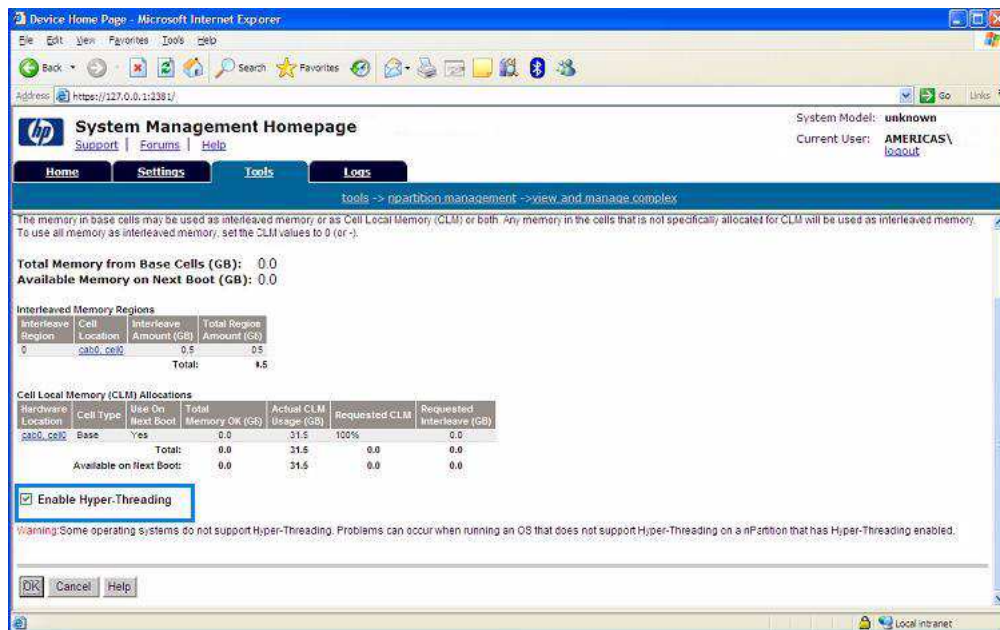
Enable Hyperthreading Using Partition Manager

Another way to enable hyperthreading (on partitionable servers only) is to use the Partition Manager partitioning tool. Partition Manager is a Web-based application for system administrators that provides a convenient GUI for creating, configuring, and managing hard partitions (nPartitions) on an HP Integrity server.

To enable hyperthreading on partitionable HP Integrity servers where the OS and system management tools are installed and upgraded to their latest versions, complete the following steps:

1. On the management station or local nPartition desktop, double-click the **HP System Management Homepage (SMH)** icon. This icon is added to the desktop by the SMH installer. It is a link to the System Management Homepage on the local system. You do not need administrative access (normal Windows login accounts should allow access to SMH). If the icon is not on the desktop, or has been deleted, you can access SMH using the following URL: `https://localhost:2381`
2. When you are logged in to SMH, go to the Tools tab and click **View and Manage Complex** in the “nPartition Management” category. If Partition Manager is running on the partitionable system being managed, you are immediately logged into the local complex, and all views displayed are of that local complex. If Partition Manager is running on a management station used to access the server remotely, a screen for logging into a remote partition appears, and you must enter an IP address and password to continue. For context-sensitive help at any time, click the **Help** button.

Figure 2-13 Enabling hyperthreading in the Partition Manager



3. In the lower left corner of the screen, select **Enable hyperthreading** and click **OK**.

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) or using the Integrated Remote Console method. If you want to install the Support Pack onto multiple systems remotely, see the procedures found in the *HP Smart Update Manager (HPSUM) User Guide* found at: <http://docs.hp.com/en/windows.html>. Also, you must install the Integrity Support Pack if you did not use the HP Reinstallation media to install the OS.

To install the Integrity Support Pack, complete the following steps:

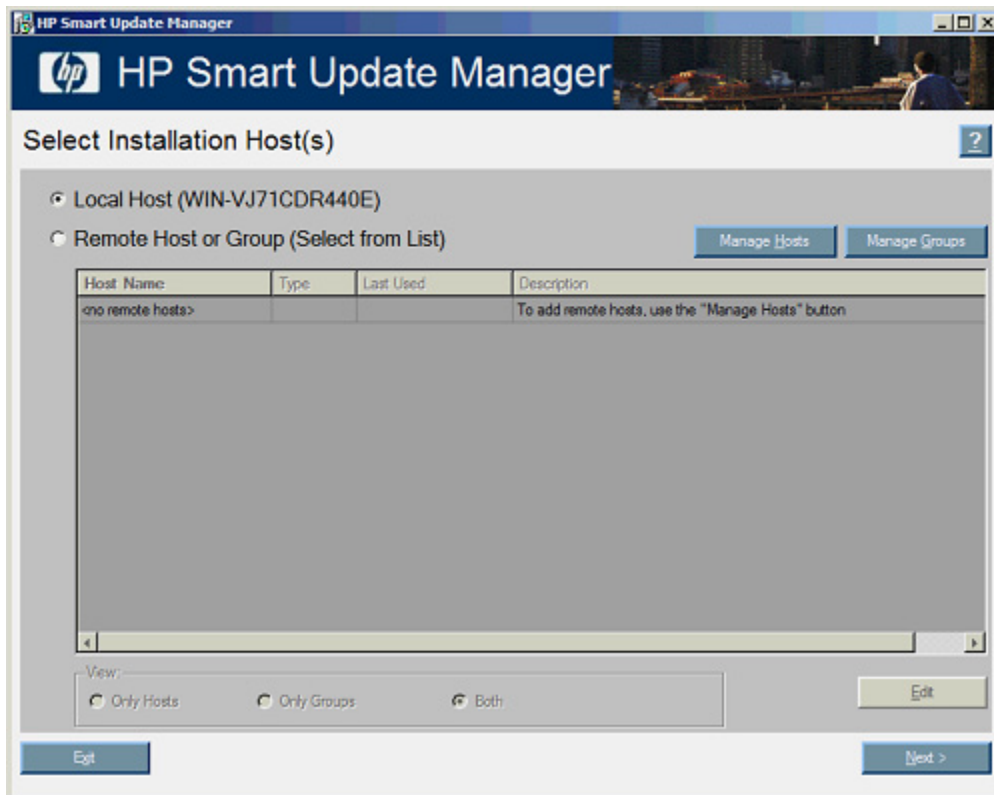
1. Insert the HP Smart Setup media into the DVD drive of the target machine. The Smart Setup media starts running and the License Agreement screen appears.



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 now.

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 screen, click **Run**.
6. At the second Security Warning pop-up screen, click **Run** again.
7. HP Smart Update Manager (HPSUM) starts running and the Select Installation Host(s) screen appears. Select the **Local Host** button and click **Next**.

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



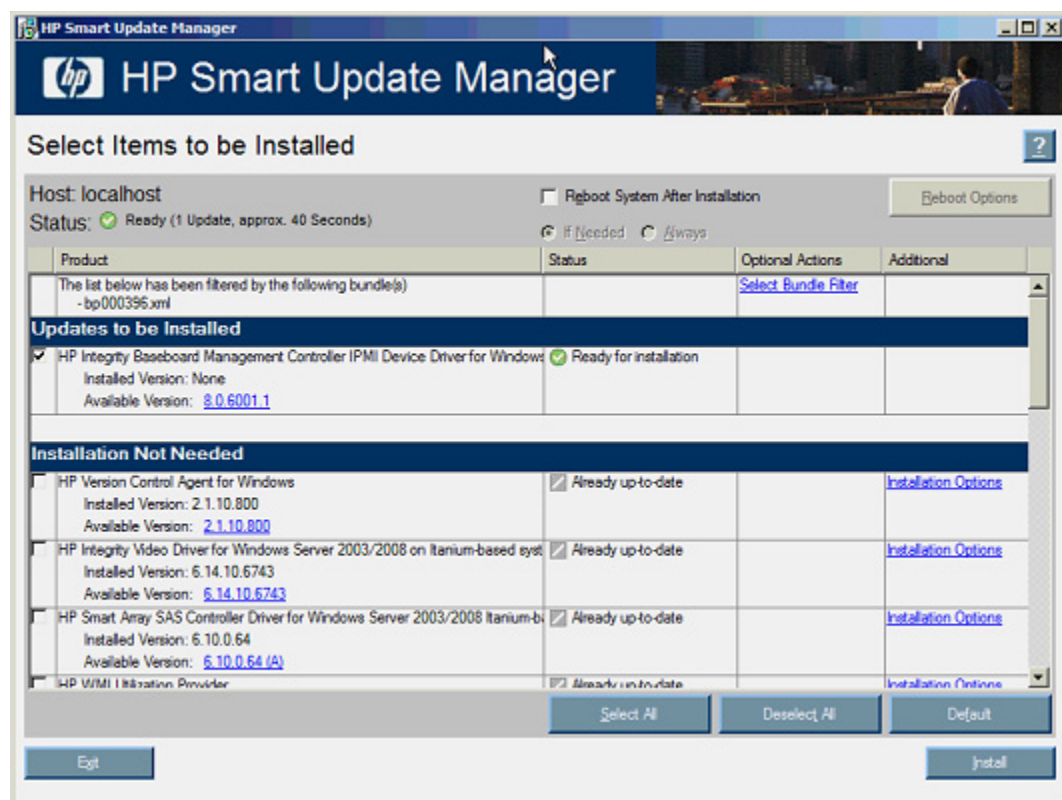
8. The Discovery Progress screen appears as HPSUM checks the local system to see which components are installed.
9. When the discovery process finishes, the Select Bundle Filter screen appears and lists the Integrity Support Packs that were found on the Smart Setup media. Select **HP Integrity Support Pack for Windows Server 2003 on Itanium-based Systems** (if multiple Integrity Support Packs are available, you **must** select the one marked “2003”). 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 component updates contained in the Integrity Support Pack, with a check mark next to each, by default. Click **Install** to install all items. Installation will take a minimum of 15 minutes.

Figure 3-3 HPSUM Select Items to be Installed screen



11. 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 System Management Homepage

This section describes the configuration of SMH on Integrity servers. After configuring SMH you can use [Appendix D “SMH and Management Agents”](#) 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 SNMP 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.

Configure the Management Agents

This section describes the configuration of the HP Insight Management Agents on Integrity servers. The management agents are a collection of services that report system information and status to the SMH application. After configuring the agents you can use [Appendix D “SMH and Management Agents”](#) to see what each agent does.



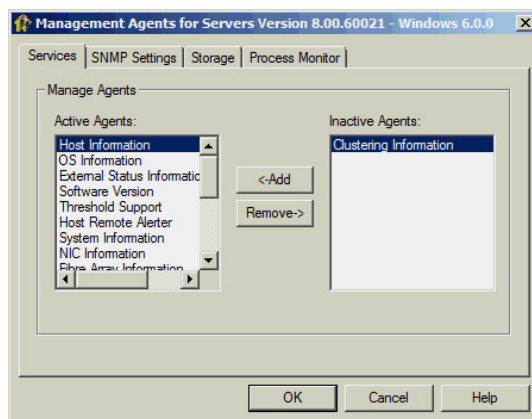
NOTE: HP management agents require TCP/IP and SNMP on the system.

Activate and Deactivate Agents

Agents are activated when they are installed (except for Clustering Information agents). Inactive agents remain installed but are dormant until you reactivate them. To activate or deactivate an agent, complete the following steps:

1. Log in with Administrator rights. You must have Admin rights to access the management agents from the Windows Control Panel.
2. Open the Windows Control Panel and select **HP Management Agents for Integrity Servers**.
The installed agents are listed in the window. All agents except clustering information are activated at installation.

Figure 3-5 Services tab



3. From the Services tab, select an agent from either column to change the active or inactive status.
4. Click **Add** or **Remove** to change the status of the selected agent.
5. Click **OK** when you have made all required status changes.

Configure the Event Notifier

The event notifier monitors agent events and sends email notifications when designated events occur. Use the event notifier configuration wizard to configure email addresses, entity types, and events triggers.

Use the configuration wizard to completely configure the notification service.

To configure the event notifier, complete the following steps:

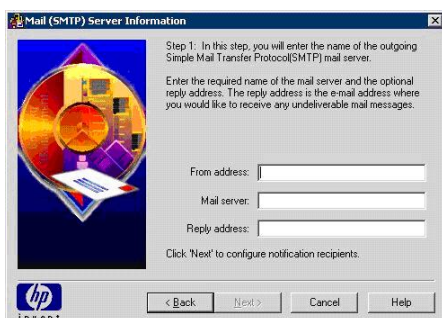
1. From Windows, select **Start > HP Insight Management Agents > Event Notifier Configuration Wizard**. A Welcome screen appears.

Figure 3-6 Welcome message



2. Click **Next** to access the SMTP information window. The following screen appears.

Figure 3-7 Mail (SMTP) server information



3. In the From address field enter a valid email address or leave it blank.
4. In the Mail server field, enter the name of the SMTP mail server you are using.

You must enter a valid server address to continue with the setup process. The wizard checks the SMTP mail server address you entered to see if it can be accessed. If the wizard cannot access the mail server address, it displays a warning message and returns you to the SMTP server address window.

5. Click **Next**. The Events recipients information window appears.

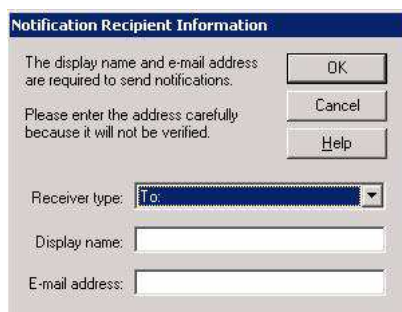
Figure 3-8 Event recipients information



In this window, you add users to receive event messages.

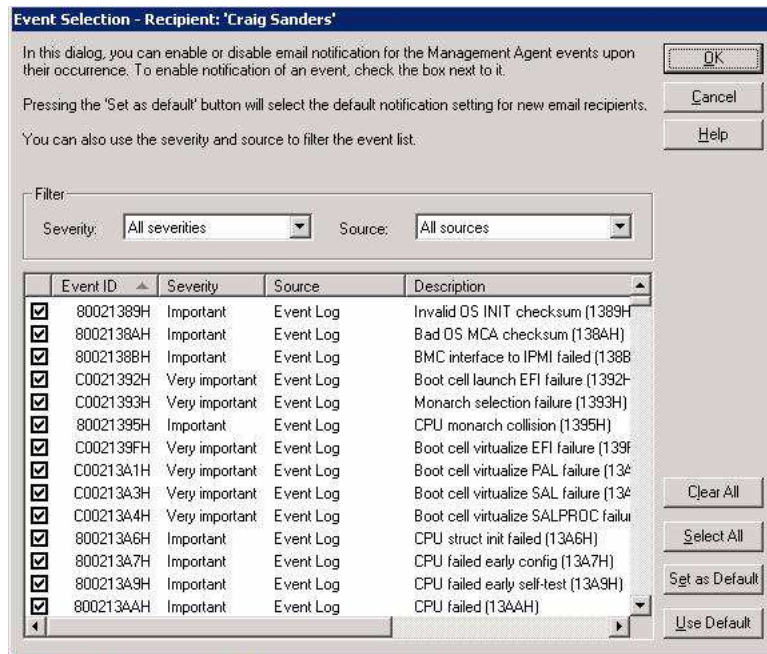
6. Click **Add** to add a user or click **Edit** to edit the properties for an existing user. The following screen appears.

Figure 3-9 Adding a new user



7. From the Receiver type drop-down list, select the email recipient type.
8. Click **OK** to return to the recipient information window.
9. Select a user name and click **Edit** to edit user properties, or select a user name and click **Delete** to remove a user.
10. Click **Events** to display the Event Selection window. A screen similar to the following appears.

Figure 3-10 Event selection window



11. Use the Severity and Source filter fields to view selected events only. The event severity levels, source, and message are not user-configurable.
12. Click the check box to enable an event or disable email notification for an event.
13. Click **Use Default** to load the current default event notification settings.
14. Click **Set Default** to set and save the current notification settings as the default values.
15. Click **OK** when you are done to return to the Event Recipient Information window.
16. Click **Finish** to close the window.

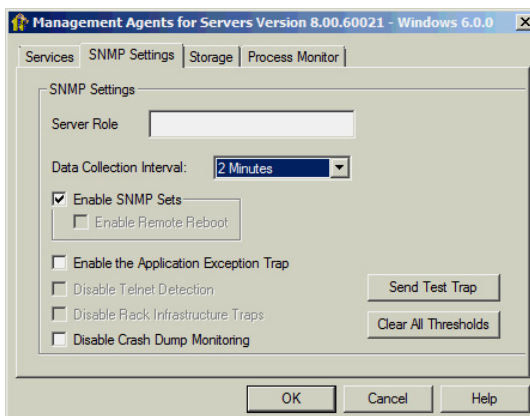
Set the SNMP Data Collection Interval

Active agents poll server devices at preset intervals, collecting management SNMP data.

To set the agent SNMP data collection interval, complete the following steps:

1. Open the Windows Control Panel and double-click **HP Management Agents**.
The installed agents are listed in the window. All agents except clustering information are activated at time of installation.
2. Click the **SNMP Settings** tab. The following screen appears.

Figure 3-11 SNMP Settings tab



3. From the **Data Collection Interval** list box, select a time interval for SNMP data collection.
4. Click the **Send Test Trap** button (available only if the HP host agent is active) to send a test trap.
5. Click **Clear All Thresholds** to clear current SNMP trap threshold values.
6. Click **OK**.



NOTE: Windows Server 2003 on the HP Integrity server does not support the following SNMP operations:

- Enable Remote Reboot
- Enable the Application Exception Trap
- Disable Telnet Detection
- Disable Rack Infrastructure Traps

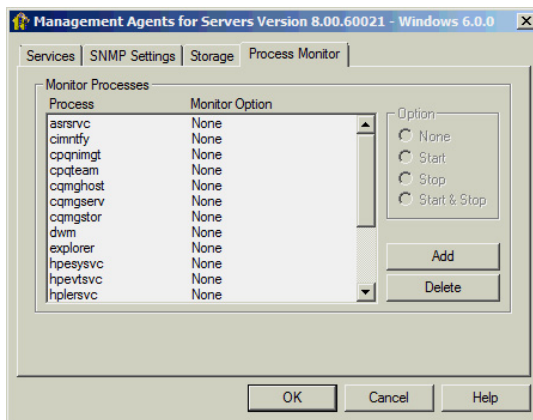
Monitor Server Processes

Use the Process Monitor tab to set up SNMP traps generated when a process starts, stops, or both.

To enable agent process monitoring, complete the following steps:

1. Open the Windows Control Panel and select **Start Menu > Control Panel > HP Insight Management Agents**. The Management Agents for Servers Version Number window appears.
2. Click the **Process Monitor** tab. A screen similar to the following appears.

Figure 3-12 Process Monitor tab



This tab displays all active (running) server processes. The Monitor Option column displays the monitoring status for each process listed.

3. Select the desired process.
4. Change its monitoring status by clicking one of these radio buttons:
 - **None** — No SNMP traps are generated for this process.
 - **Start** — An SNMP trap is generated when this process starts.
 - **Stop** — An SNMP trap is generated when this process stops.
 - **Start & Stop** — An SNMP trap is generated when this process starts or stops.
 - **Add** — Add a process to the monitor. Enter the name of the process, then click **Apply** to add the process.
 - **Delete** — Highlight a process in the list, and select Delete to delete the process.
5. Click **Add** to add a process, then enter the name of the process.

6. Click **Delete** to delete a process selected from the list. You can only delete processes that a user has created. The **Delete** button is disabled for system default processes.
7. Click **OK** to confirm.
8. Click **OK** when you finish configuring process monitoring.

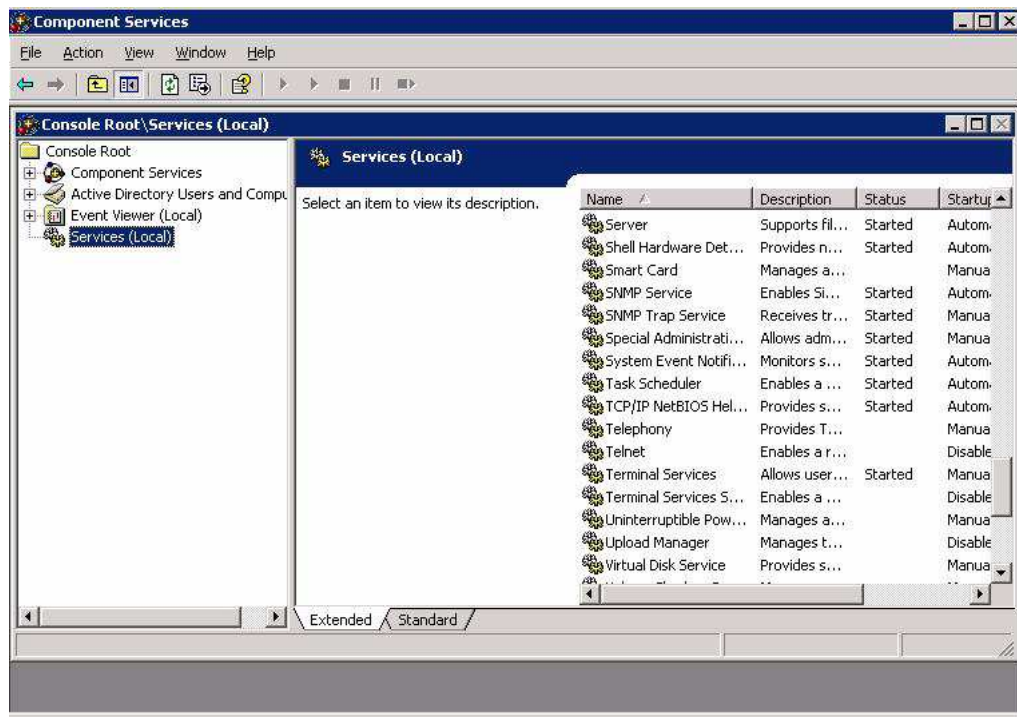
Send SNMP Traps to Management Applications by IP Address

Configure SNMP services with specific IP addresses to send SNMP traps to an SNMP management application with an IP address.

To configure management agents with a management console IP, complete the following steps:

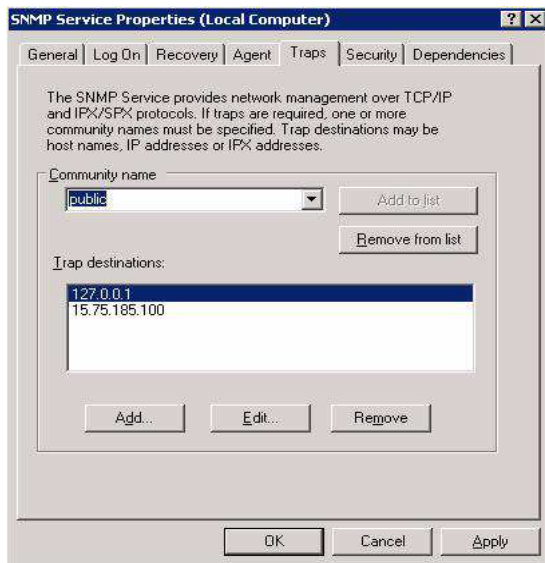
1. From the Start menu, select **Start > Settings > Control Panel > Administrative Tools > Component Services**. The Component Services window appears.

Figure 3-13 Component Services window



2. Click **Services (Local)**.
3. From the list of services, double-click **SNMP Service**. The SNMP Service Properties (Local Computer) window appears.
4. Click the **Security** tab.
5. Click the **Traps** tab. A screen similar to the following appears.

Figure 3-14 SNMP traps tab



6. In the Community name field, if a community name exists, select it; if not, enter a community name and click **Add to List**.

The default community string for HP Insight Manager is **public**. If you enter a different community string here, enter the same string on the management console that is responsible for the system. HP recommends not using the string **public** because it is the default value, commonly used, and can present a security risk.

7. Under the **Traps Destinations** list, click **Add**. The SNMP Service Configuration window appears.

Figure 3-15 SNMP service configuration



8. In the Host name, IP or IPX Address field, enter the IP address of the management console. This address identifies the management console to receive the alert when the server agents detect a significant event.
9. Add **127.0.0.1** as a trap destination if it is not already listed. You must do this to enable the loopback service.
10. Click **Add** and then **OK**.

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 77). For a description of nPartitioning and associated tools and concepts, see the *nPartition Administrator's Guide* found at:

- <http://docs.hp.com/en/5991-1247B/> (for the HTML version)
- <http://docs.hp.com/en/5991-1247B/5991-1247B.pdf> (for the PDF version)

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, complete the following 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

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 Emulex driver options set in LPutil are equal to or greater than the number of physical drives (default = 20).
 - b. Maximum queue depth: For 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:

<http://docs.hp.com/en/8875/WIE-SQLTuning-1006-00.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, complete the following 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.

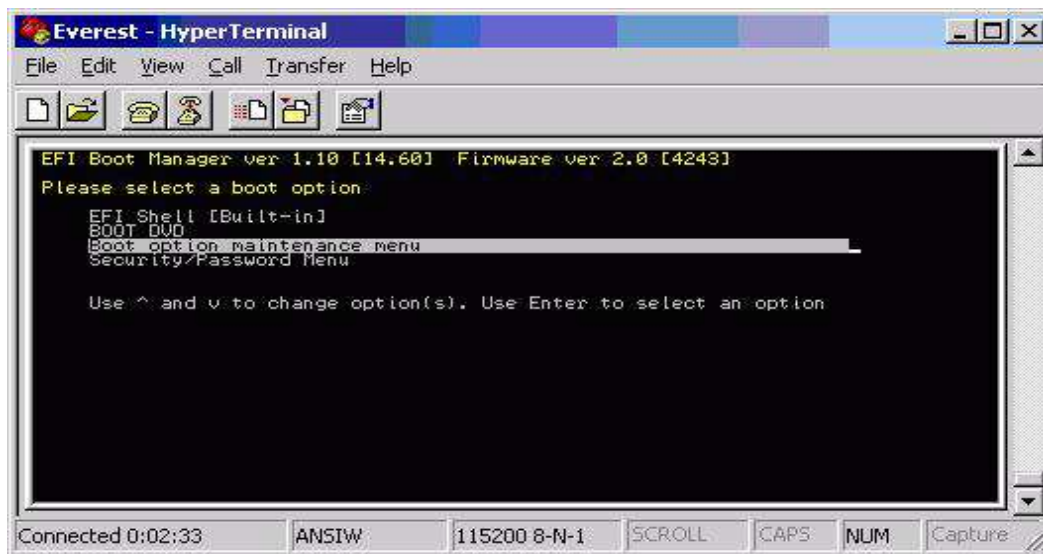
HP Integrity servers use EFI to initialize the platform firmware and load the OS. After the system is initialized, EFI provides two interfaces that you can interact with:

- 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. For detailed information on using Express Setup, see “Run EBSU” (page 34). 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 management processor (MP) firmware. You must download the latest MP firmware from the HP Integrity support site at <http://www.hp.com/support/itaniumservers/> and flash it separately.

- **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
- **Load OEM Boot Driver** — Loads OEM drivers for boot devices into memory. Ordinarily, boot drivers not on the Windows CD are installed using the floppy drive. Because Integrity servers do not have floppy drives, the drivers must be loaded into memory and then installed. EBSU shows detected devices that have a virtual floppy image available. To load the virtual floppy image manually, follow these steps:
 1. At the EFI Shell prompt, enter `fs0:.`
 2. Navigate to the `\efi\io_cards\vfloppy` directory.
 3. Enter the following:

```
set -v VirtualFloppySourcePath \efi\io_cards\vfloppy\SA6400.img
```
 4. Enter the following:

```
set -v VirtualFloppyHandleNumber 0
```
 5. Enter the following:

```
load vfloppy.efi
```
 6. Enter the following:

```
map -r
```

You cannot unload or change the virtual floppy file system unless you reset the computer.



CAUTION: When Windows installation begins, you are prompted to press F6 to install a third-party SCSI or RAID driver. Do not press F6. Pressing F6 forces Windows to look for the driver on a physical floppy drive, which does not exist. The driver is loaded into memory and installed automatically.

- **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 is available only 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.
- **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.

Creating a Boot File Using the EFI Shell

If the `boot000x` file is missing after you install Windows Server 2003, use the following procedure to create a boot file.

1. Remove all media from the DVD drive.
2. From the EFI Boot Manager, select **EFI Shell[Built-in]**.
3. At the EFI Shell prompt, enter `fs0:.`
4. At the `fs0:>` prompt, enter `cd MSUTIL`.
5. At the `fs0:\MSUTIL>` prompt, execute the `NVRBOOT.EFI` boot utility.
6. Enter X to export the current EFI boot content to the boot file.
7. Select the first entry with the text Windows Server 2003.
8. At the prompt, enter the following path:

```
EFI\Microsoft\Winnt50\boot0001
```

This creates the Windows boot file `boot0001`.

Verify Successful Boot File Creation

To verify that the boot file was created successfully, use the following procedure:

1. From the EFI Boot Manager, select **EFI Shell[Built-in]**.
2. At the EFI Shell prompt, enter `fs0:.`

3. At the `fs0:>` prompt, enter `cd MSUTIL`.
4. At the `fs0:\MSUTIL>` prompt, execute the `NVRBOOT.EFI` boot utility.
5. Enter `I` to Import.
6. Enter the following path:
`EFI\Microsoft\Winnt50\boot0001`
7. Click **Exit** to return to the EFI Boot Manager utility.
8. Boot the server using the new Windows entry.

C nPartitioning

This appendix introduces node partitions (nPartitions) on cell-based HP Integrity servers running Microsoft® Windows® Server 2003 and describes the tools to manage them.

A cell-based HP Integrity server (such as the rx7620, the rx7640, the rx8620, the rx8640, or Superdome) can be configured as a single system or partitioned into several independent systems. Partitioning provides hardware and software isolation, in which each partition is assigned memory, processors, and I/O resources for its exclusive use, and executes its own operating system image.

For a description of nPartitioning on HP Integrity servers, see the *nPartition Administrator's Guide*:

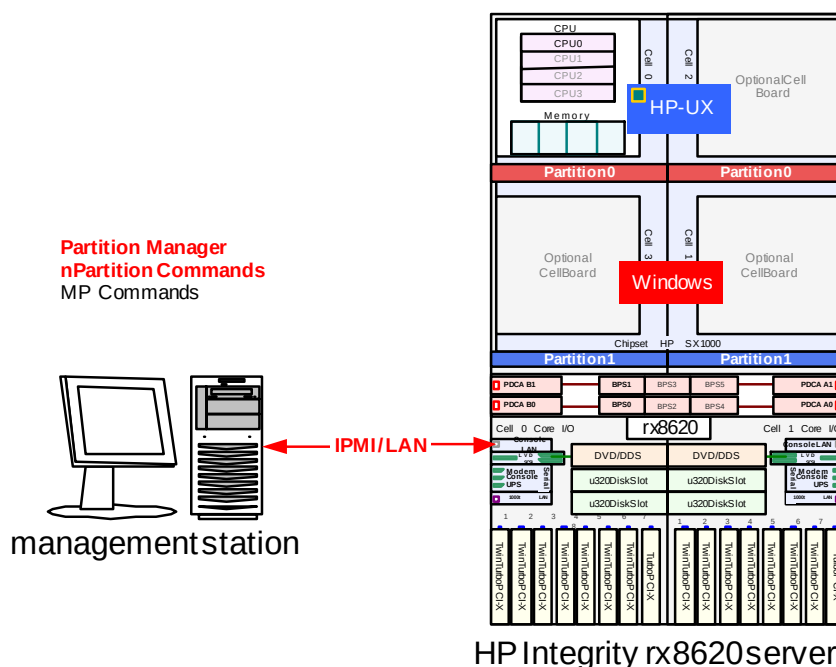
- <http://docs.hp.com/en/5991-1247B/> (for the HTML version)
- <http://docs.hp.com/en/5991-1247B/5991-1247B.pdf> (for the PDF version)

Quick Start

This section provides an overview of the installation and configuration steps needed to get you up and running as quickly as possible.

Figure C-1 shows the hardware, software, and most commonly used connection method. All components are described later in this chapter.

Figure C-1 System overview



The most common setup for nPartition management of HP Integrity servers running Windows involves a remote management station. This dedicated management station hosts the 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.

To set up and configure the management station:

1. Establish a dedicated management station for the HP Integrity server. See: “[Setting up the Management Station](#)” (page 88).
2. Install the nPartition tools using the HP Smart Update Manager utility on your Smart Setup media.
3. Verify installation of the nPartition tools. See: “[Verify Installation of the nPartition Management Tools](#)” (page 62).

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.

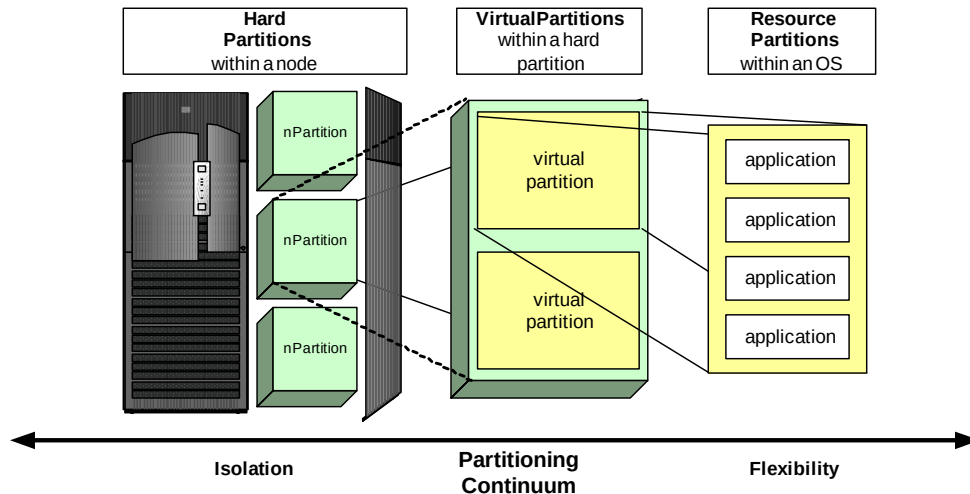
Partitioning Continuum

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. *Windows Server 2003 does not support virtual partitions.*

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. *Windows Server 2003 does not support resource partitions.*

This document focuses on nPartitions running Microsoft Windows Server 2003.

Cell Structure of nPartitions

HP Integrity mid-range and high-end servers (rx7620/rx7640, rx8620/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 rx7260 and rx8620 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 rx8620 or 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 rx7620 or 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: |
- Retrieving information about the server, including everything displayed by Partition Manager and the `parstatus` 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

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 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

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.

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)

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 2003, use third-party remote control software such as the free VNC (www.realvnc.com) or the Symantec pcAnywhere software.

Terminal Services

Windows Server 2000 and Windows Server 2003 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 2003. 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**.

To connect to the management station from the remote terminal:

- On Windows XP, select **Start > All Programs > Accessories > Communications > Remote Desktop Connection**.
- On Windows Server 2003, select **Start > Administrative > Tools > Remote Desktops**. To connect to a Windows 2003 console, use the `/console` switch with the Remote Desktop Connection application. This is present on the latest version available at www.microsoft.com and on Windows Server 2003. (This version is a 32-bit program available on the 32-bit and 64-bit Windows Server 2003 operating systems.)

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 WBE or the IPMI-over-LAN method. For remote administration using WBE, the tool accesses the nPar Provider running on an nPartition in the target |

complex (for example, with the `-u . . . -h . . .` options). For remote administration using IPMI over LAN, the tool accesses the MP (for example, with the `-g . . . -h . . .` 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:

- | | |
|---|---|
| <code>bcfg</code> | Lists and configures boot options list for the local nPartition. |
| <code>autoboot</code> | Lists, enables, or disables the nPartition autoboot configuration value. |
| <code>acpiconfig</code> | 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 2003, you must set the ACPI configuration setting for the nPartition to windows. |
| <code>acpiconfig enable
softpowerdown</code> | 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. |
| <code>acpiconfig disable
softpowerdown</code> | 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. |
| <code>reset</code> | Resets the local nPartition, resetting cells and proceeding with the nPartition boot phase. |
| <code>reconfigreset</code> | 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:

- | | |
|--------------------------|--|
| <code>shutdown /r</code> | 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. |
| <code>shutdown /s</code> | 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, <code>shutdown /s</code> 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 Management Agents

System Management Homepage (SMH), combined with HP Insight Management Agents, enable you to view subsystem and status information from a Web browser, locally or remotely. You can access HP Insight Management Agents from 32-bit systems and Integrity servers. To do this, you must have completed the following tasks, described earlier in this document:

- Installed TCP/IP
- Installed SNMP
- Configured SNMP
- Installed HP System Management Homepage
- Installed the HP Insight Management Agents

As part of the HP Insight Management Agent installation, the HP Management Agents Control Panel applet and WebAgents are installed that enable access to Management Agent information using HP System Management Homepage (SMH).

HP Insight Management Agents

HP Insight Management Agents comprise the following:

- HP Insight Foundation Agents
- HP Insight Server Agents
- HP Insight Network Interface Card (NIC) Agents
- HP Insight Storage Agents
- HP Insight Management Services

You can deactivate and activate the management agents from the HP Management Agents Control Panel, accessible from **Start>Control Panel>HP management Agents**.

The following sections describe the components of each agent.

HP Insight Foundation Agents

HP Insight Foundation Agents comprise the following:

Host Information	Enables a subservice that captures general information about the host such as OS description, OS version, OS type, crash dump state, CPU utilization, file system, physical hardware mapping, software running, system status, physical memory, platform type, and host GUID.
OS Information	Enables a subservice that captures OS information such as running processes, physical memory, logical and physical disks, cache, paging file, processors, and networking.
External Status Information	Enables a sub-service that captures information about external MIB.
Software Version	Displays the version numbers of HP system software installed on the machine.
Threshold Support	Allows a management application, such as HPSIM, to set user-definable alarms on monitored items (for example, system processor utilization or file system utilization).
Host Remote Alert	Enables a subservice that monitors registry keys updated by Cluster, Performance, and Host information to verify and notify when thresholds are reached.
Clustering Information	Enables a subservice that captures information about a configured cluster in the machine.

HP Insight Server Agents

HP Insight Server Agents comprise the following:

System configuration information	Collects configuration information of server hardware-related devices such as CPU, Memory, I/O, cooling, power supply, and cabinets.
System Devices Status	Provides dynamic status of monitored devices in the server (for example, cooling devices, temperature sensors, and power supplies) and of the watchdog timer used for automatic server recovery.
Device Settings	Enables you to set server device settings (for example, asset tag, unit identification, and attention LED states) and watchdog timer (automatic server recovery) parameters.

HP Insight NIC Agents

HP Insight NIC Agents support logical HP Network Interface Cards (NICs) configured on the system you are managing, including virtual NICs, team NICs, and single NICs. It also collects Ethernet statistics.

HP Insight Storage Agents

HP Insight Storage Agents comprise the following:

Fibre Array information	Enables a service that provides support for Fibre Channel connected Storage Management. This service is not supported on HP Virtual Machines (HPVM).
Drive Array information	For a physical drive: Each physical drive is listed as a separate entry in the Mass Storage submenu. The information displayed next to the physical drive includes the condition of the drive, the location of the drive (port and drive number), and drive size. For a logical drive: Each logical drive in the list displays the condition, logical drive number, and the fault tolerance of that logical drive. This service is not supported on HP Virtual Machines (HPVM).
SCSI information	Provides the module name, module version, and the date the agent was created. This service is not supported on HP Virtual Machines (HPVM).
Storage Remote Alert	Enables a service that provides support for SNMP Traps for all SCSI, Smart Array, and Fiber Channel Storage Agents. This service is not supported on HP Virtual Machines (HPVM).

HP Insight Management Services

Management Processor (MP) information	Enables a <code>telnet</code> connection to the MP through a browser and captures information about the MP.
HP Loop-Back Event Service	Enables a service that monitors trap-generating events in SEL when specific traps are received. The service monitors traps that do not have a corresponding event in SEL, such as events generated by Storage, Cluster, and Foundation.
Predictive Failure Monitor	Enables a service that monitors failures in the system and generates events when thresholds are reached. Monitored failures include memory errors, internal cache errors, external cache for MX2 processor errors, fabric errors, Enhanced Thermal Management, Front Side Bus, and Intel Cache Safe Technology performance errors.

Event subsystem information	Enables a service that monitors events from System Events Log (SEL), Forward Progress Log (FPL), and the MP, and generates traps when events are found.
Automatic Server Recovery	Enables a service that checks if the system is frozen and if so, reboots the system.

Using SMH

SMH enables you to administer systems locally via a web-based GUI. It provides a single, hierarchical menu interface that enables you to quickly find and invoke applications to perform common system tasks.



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*:

<http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&usecc=us&docId=6417&taskId=101&prodTypeId=1864&prodSeriesId=34313#3>

Accessing WebAgents

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

1. From a system connected to the server through the network, 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, the Security Alert dialog box appears asking you to indicate whether to trust the server.



NOTE: The Security Alert dialog box shown is specific to Internet Explorer.

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 this is implemented, a Security Alert dialog box does not appear. If the alert appears when you do not expect it, 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. Click **Yes**.



NOTE: If you have enabled Anonymous access, the **System Management Homepage** appears.

4. Select the account from the **User** dropdown list. The choices include administrator, operator, or user.
5. Enter the correct password in the **Password** field.
6. Click **OK**. The **System Management Homepage** appears.

In reference to the HP Version Control Repository Manager, the Anonymous login, if enabled, and the User login allow you to access all pages, but you cannot configure a repository, delete/copy/create Support Paqs, install components, or clear the log. The Anonymous login is disabled by default.

The first time you log in to the SMH, you are granted anonymous access and can read system management data, but you cannot execute SNMP sets (writes). For instructions on preventing anonymous login and limiting write capability for specific user classes, see the *System Management Homepage Installation Guide*.

7. Click a specific device name to see current status for that device.
The window that appears depends on the configuration of your server. All SNMP devices are displayed.

Navigating SMH

SMH displays HP Web-enabled System Management software. In addition, SMH displays the status of the items grouped by category. For more information, see the online help.

The SMH interface is separated into the following two frames:

Header frame	The header frame is constantly visible regardless of the page you are viewing. A navigation vector, located in the top section, displays the path you are viewing.
Data frame	The data frame displays the status for HP Management software and utilities on the system.

The following information areas appear in the header or data frames:

- SMH Pages
 - The Home page
 - The Settings page
 - The Tasks page
 - The Logs page
- Support

The Support link provides you with links to HP support areas.
- Forums

The Forums link provides you with links to HP forums.
- Help

The Help link launches help files in a separate browser window. The help contents can contain a combination of help files related to the HP Web-enabled System Management Software and utilities.
- System Model

The System Model displays the model of the system. In some cases, the System Model might display Unknown if no HP Web-enabled System Management Agents are installed on the system.
- Current User

The Current User displays the user who is logged in. If the user is Administrator, Operator, or User, there is a Logout link. If you have Anonymous access enabled and you are accessing the page anonymously, the Current User appears as Anonymous, and the Login link appears. If Local Access is enabled and you are accessing the HP Web-enabled System Management software from a local machine, the Current User appears as Administrator or Anonymous (depending on the level of access enabled) and Local Access.

The SMH Home Page

The SMH Home page provides the system, subsystem, and status view of the server. It displays groupings of systems and their status. Information on the Home page is provided by integrated agents or management utilities (for example, integrated version control, server, and storage agents). The Home page contains the following:

- Organizational Menu

The organizational menu appears in the left side of the Home page. It contains links to the HP Web-enabled System Management Software to include:

- Integrated agents
Contains participants and links to entry points if applicable. You can click an agent link to access the agent.
- Other agents
Lists the visible HP Web-enabled System Management Software that does not participate in HP SMH.
- Management processor
Displays a link to the Integrated Lights-Out (iLO) board.
- Other software
Can provide links to Integrity, Support, and Forums.
- Key
Displays a list of status icons and a brief description of each.
- Software Status Categories
 - Overall System Status
 - System Report
 - Network
 - Storage
 - Operating System
 - System
 - System Configuration

System Status

The System Status icon indicates the health of the system and HP Web-enabled System Management software.

Icon	Key Word
	Unknown
	OK
	Degraded
	Failed

Overall System Status

The Overall System Status category displays links to subsystems that have a failed or degraded status, as provided by the integrated HP Web-enabled System Management Software. If there are no agents installed or no failed or degraded items, the Overall System Status category displays no failed or degraded items.

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.

Network

The NIC Management Agents display logical HP NICs that are configured on the system you are viewing. This can be a virtual NIC, single NIC, or teams of NICs. The information displayed depends on the type of NIC, and can include the following:

- NIC controller information
- NIC interface information
- Ethernet statistics
- Logical adapter information

Storage

The Storage section provides an overview of the selected server's mass storage subsystem. The mass storage controllers being used by the server are listed in the Navigation frame on the left side of the screen. The colored ball next to each controller indicates the status of that controller.



NOTE: EMC, EVA, VA, and XP storage systems are not supported by WebAgents.

The 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

Operating System

The Operating System category displays the following information:

- Logical disks
Information includes volume, free space, queue length, and disk busy time.
- Memory
Information includes available KBytes, pages/second, pages input/second, pages output/second, pages reads/second, cache bytes, cache faults, and pool non-paged bytes.
- Network
Information includes TCP information, including active connections, established connections, segments/second, segments retransmitted/second, and connection failures. Also includes controller information, including total bytes/second, packets/second, output queue length, packet errors, current bandwidth, bytes sent and received, and packets sent and received.
- Physical disks
Information includes volume name, queue length, and disk busy time.
- Processes
Information includes process name, number of active threads, private bytes, page file bytes, working set, page faults, % CPU time, and % privileged CPU time.
- Processor
Information includes CPU name, interrupts/second, % user CPU time, % privileged CPU time, % DPC time, % interrupt time, and % CPU time with thresholds supported.
- Server
Information includes system health (system up time, total threads, context switches/second, processor queue length, total processes, and % registry usage), security (access permission errors, access granted errors, server logon errors, and server sessions errored out), and server

utilization (network utilization in total bytes/second, server sessions, context block queue/second, and % total page file usage).

- **File System Space Used**
Information includes volume name, used space, unused space, and percentage of space used.
- **HP Insight Agents Processes**
Information includes process name and status (started or stopped).

System

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.

System Configuration

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, HPVM 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 description information that includes 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.

E Headless Windows Installations

Users of Microsoft Windows Server 2003 and Windows Server 2008 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 A6869A 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 A6869A, 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

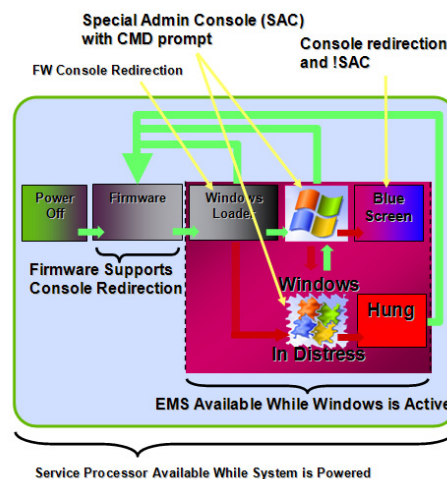
When the server powers on, the system firmware is responsible for configuring all hardware and loading EFI. This phase is also called FW or BIOS console redirection. EFI can be used to prepare the system for OS install or to choose an OS to boot.

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), shown below, 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.