

Intel® Server Manager 8.40 Server Guide for Windows

(This page intentionally left blank.)

Table of Contents

Introducing Intel Server Manager 8.40	1
Intel® Server Manager 8.40 (server installation)	1
System requirements	2
Security in Intel Server Manager	4
User rights	5
Intel Server Manager documentation	6
Managing computers	7
Using power options.....	7
Managing system inventory.....	9
Computer summary.....	9
Viewing system data	10
Asset management	12
BIOS.....	13
Chassis.....	14
CPU.....	14
Device drivers.....	15
Display.....	15
Drives	15
Environment variables.....	16
Fans	16
Field replaceable units	17
Installed applications.....	17
Keyboard and mouse	18
Memory	18
Modems.....	19
Motherboard.....	20
Multimedia	20
Network	21
Operating system	22
OS event log.....	23
PCI Hot Plug Devices.....	23
PCI Hot Plug Slots.....	23
Performance.....	25
Ports	26
Power supplies.....	27

Power supply management.....	27
Processes.....	28
Sensors	28
Services.....	29
Storage devices.....	30
Temperatures	30
Voltages	31
Reports	33
Monitoring configuration changes	33
Viewing hardware events	34
Exporting system data.....	36
Viewing the system log.....	36
Configuring and viewing alerts	39
Using alerts	39
Setting polling frequency	40
IPMI configuration	41
Monitoring computer health	45
Monitoring health.....	45
Using the taskbar icon.....	46
Selecting performance counters	46
Preferences	49
Alerts preferences	49
Reference information	53
Troubleshooting.....	53
IPMI	55
Intel Server Manager services	56
SNMP	57
Version information	57
Converting Celsius to Fahrenheit.....	57
Glossary	59
Copyright and trademark notice	69
Index	71

Introducing Intel® Server Manager 8.40

Intel® Server Manager 8.40 (server installation)

Intel Server Manager can help you manage your computer and troubleshoot common computer problems before they become serious. Use Intel Server Manager to:

- **View system inventory**—ISM provides extensive information about the computer's hardware and software configuration.
- **Monitor a computer's health**—ISM reports when the computer is in a warning or critical health state based on several health contributors such as temperature, voltage, free memory, and disk space.
- **Receive alerts for system events**—ISM can use various alert methods to notify you of problems.
- **Monitor real-time or historic performance**—ISM lets you monitor the performance of various system objects such as drives, processors, memory, and services. You can set alert actions to trigger notification when a specified counter crosses an upper or lower threshold a predetermined number of times.
- **Monitor current processes**—ISM lets you view current processes and statistics for each process, and shut down many processes.
- **Monitor current services**—ISM allows to view current services and their statuses, or to set alert actions to notify you of changes to service status.

Server and administrator installations

Intel Server Manager has the following modules that you can install:

- **Server**—The server installation enables an end user to view information and manage alerts for a local server computer. This installation allows an administrator to manage the server computer, but doesn't permit its end user to view or manage other computers.
- **Administrator**—The administrator installation enables an administrator to manage remote clients and servers on the network. This means you can view information, generate reports, receive alerts, and power on/off other managed computers remotely. To remotely reboot, power off, or power on computers, the administrator installation must be installed on at least one computer that is attached to the network.

Note—If you tried to run the console after installation and instead, Intel Server Manager launched this help file, you may not have a properly-configured IP address.

Running Intel Server Manager on multiple platforms

Intel Server Manager is available in versions for both Windows and Linux. Regardless of the platform on which it is installed, the administrator console can discover server computers running either Windows or Linux. An administrator console installed on a Windows platform can manage both Windows and Linux computers, but an administrator console installed on a Linux platform can manage only Linux computers. Intel Server Manager can also be viewed and run from a remote computer with a supported operating system and browser as shown in the table below.

Installation	Runs remotely in Internet Explorer on Windows	Runs remotely in Mozilla on Linux
Administrator for Windows	Yes	No
Server for Windows	Yes	No
Administrator for Linux	Yes	Yes
Server for Linux	Yes	Yes

System requirements

Note: Refer to your platform documentation to verify that the operating system versions listed below are supported on the computer you intend to install Intel Server Manager on. Some Intel Server Boards may not support the versions listed below.

Server computers

The following requirements are for servers running the Intel Server Manager server console, Primary Agents, and One-boot Flash Update (OFU).

For servers with only the Intel Server Manager Bridge Agent installed, OS requirements are the same, but only 10 MB disk space is required to install the Bridge Agent. TCP/IP must be properly configured, and a BMC is required.

To manage servers with a BMC but no Intel Server Manager software installed, software requirements do not apply.

- Windows 2000 Server SP4, Windows 2000 Advanced Server SP4, Windows 2003 Enterprise Server SP1, Windows XP Professional with SP2 (only on Intel Server Board SE7525GP2, Intel Server Board SE7525RP2, and Intel Server Platforms supported in-band by Intel Server Manager 8.40 with Intel® Pentium® 4 processors)
- 256 MB of RAM recommended
- 45 MB of available hard drive space to install
- 40-100 MB of available hard drive space to run (depending on cluster size)
- A network adapter with properly configured TCP/IP
- Internet Explorer 6.x SP1 or later (Windows), or Mozilla 1.5 or later (Linux only)
- Macromedia* Flash player is required for some graphic elements to display. Adobe Acrobat* Reader is needed to view documentation. If these are not previously installed they can be downloaded as needed via an Internet connection.

Note: Refer to the Getting Started with Intel Server Manager 8.40 manual for information on installing the packages, lm-sensors, and configuring the mysql and ftp users.

Red Hat Enterprise Linux 3 (32-bit Architecture)

- bash-2.05b-29
- mozilla-1.4 (1.7 preferred)
- mysql-3.23.58-2.3 (Intel Server Manager Administrator console only)

- mysql-server-3.23.58 (Intel Server Manager Administrator console only)
- net-snmp-5.0.8-11
- openssl-0.9.7a-22.1
- perl-5.8.0-88.4
- perl-CGI-2.81-88.4
- perl-DBD-MySQL-2.1021-3 (Intel Server Manager Administrator console only)
- perl-DBI-1.32-5
- perl-Filter-1.29-3
- pygtk2-1.99.16-8
- python-2.2.3-5
- sudo-1.6.7p5-1
- sysstat-4.0.7-4
- xinetd-2.3.12-2.3E
- w3c-libwww-5.4.0-5 (required for One-boot Flash Update utility)
- lm_sensors-2.9.1
- xorg-x11-deprecated-libs-6.8.2-1.FC3.13.i386.rpm

RHEL 3 ES Update 4 (Intel EM64T Edition)

- bash-2.05b-29
- mozilla-1.4 (1.7 preferred)
- mysql-3.23.58-2.3 (Intel Server Manager Administrator console only)
- mysql-server-3.23.58 (Intel Server Manager Administrator console only)
- net-snmp-5.0.8-11
- openssl-0.9.7a-22.1
- perl-5.8.0-88.4
- perl-CGI-2.81-88.4
- perl-DBD-MySQL-2.1021-3 (Intel Server Manager Administrator console only)
- perl-DBI-1.32-5
- perl-Filter-1.29-3
- pygtk2-1.99.16-8
- python-2.2.3-5
- sudo-1.6.7p5-1
- sysstat-4.0.7-4
- xinetd-2.3.12-2.3E
- lm_sensors-2.9.1
- w3c-libwww-5.4.0-5 (required for One-boot Flash Update utility)

- xorg-x11-deprecated-libs-6.8.2-1.FC3.13.i386.rpm

SuSE Enterprise Linux 9 SP1 (Intel EMT64)

- bash-2.05b-29
- mozilla-1.5 (1.7 preferred)
- mysql-client-4.0.18 (Intel Server Manager Administrator console only)
- mysql-4.0.18-32.1 (Intel Server Manager Administrator console only)
- net-snmp-5.1-80.3
- openssl-0.9.7a-22.1
- perl-5.8.0-88.4
- perl-DBD-mysql-2.9003-22.1 (Intel Server Manager Administrator console only)
- perl-DBI-1.41-28.1
- python-2.3.3
- python-gtk-2.0.0
- python-gnome-2.0.3-2
- sudo-1.6.7p5-1
- sysstat-5.0.1-35.1
- xinetd-2.3.13-39.3
- compat-gcc-32-3.2.3-47.3 & -c++-
- compat-glibc-2.3.2-95.30
- compat-libgcc-296-2.96-132.7.2
- compat-libstdc++-matching above
- mysql-shared-4.0.18-32.1 (Intel Server Manager Administrator console only)
- w3c-libwww-5.4.0-5 (required for One-boot Flash Update utility)
- xorg-x11-deprecated-libs-6.8.2-1.FC3.13.i386.rpm (required on Intel Compute Blades)
- libstdc++-3.2.3-47.i386.rpm (Disc 2 Update 4) (required on Intel Compute Blades)
- kernel source code (required for rebuilding OFU drivers)

Security in Intel Server Manager

This topic describes how security is implemented for privacy and authentication in Intel Server Manager. Three types of security are in force as the administrator console communicates with servers and clients:

- User rights as assigned in Windows user groups
- SSL encryption of data

- Digital certificates

The following sections describe security methods used for accessing the administrator console and for managing computers from the console.

Accessing the administrator console

The Intel Server Manager administrator console is accessed through a web browser, either on the same computer as the console or from another computer. To access the console, a user must log in to the OS with administrator or power user rights. (The user must be a member of the Windows Administrators or Power Users groups.) Users with power user rights have restricted administrator rights within Intel Server Manager. (See *User rights* for more information about user groups and rights to Intel Server Manager.)

Console access is also protected by SSL encryption. A temporary web server certificate and key pair is created at the beginning of each console session. After the session is completed this certificate and its private key are erased. This certificate/key pair is used for privacy (data encryption), but not authentication.

Remote access

When accessing the administrator console from a browser on another machine, the user can install a CBA8 root authority certificate as a trusted root certification authority in their browser's certificate store. This will enable the use of an SSL connection for console access.

If the trusted authority certificate has not been installed, a warning dialog will appear when the session is started indicating that the console's certificate chain cannot be verified. At this point the user can choose to ignore the warning or can install the root authority certificate. The root authority certificate should only be installed if the browser is to be used regularly for Intel Server Manager administrative purposes. If the administration is a one-time activity, it is simpler to ignore the warning. The CBA8 root authority certificate is used only to verify the temporary certificates of the Intel Server Manager Management Agent. To maintain the highest level of security, it should only be installed into browsers that are used regularly for Intel Server Manager administration.

User rights

Intel Server Manager uses operating system groups to define user rights. Windows user groups are listed below with a summary of user rights. Use the operating system's tools to add members to groups and manage group membership.

Administrators

Includes complete and unrestricted rights to the computer/domain, including complete and unrestricted administrator rights within Intel Server Manager

Power Users

Includes most administrative power with some restrictions, including restricted administrative rights within Intel Server Manager:

- The administrator console shows the My computers and Others computers lists and the Reports features; Management and Preferences features are not available

- Log files can be viewed but cannot be cleared or resized
- In the My computers list, user can filter and refresh the list, run reports, export data, and launch the Windows Explorer to connect to a computer
- In the Other computers list, user can filter and refresh the list only

Users

Includes read rights within Intel Server Manager, but does not include any administrative rights. Prevents users from making accidental or intentional system-wide changes.

Notes:

- Operating system level Administrator rights are required to enable ActiveX controls or install Flash on a computer (both of which are required to display portions of the Intel Server Manager user interface). User interface display problems can be avoided by making sure that the user is a member of the Administrator group on the computer from which he or she will run Intel Server Manager. Intel Server Manager group membership is useful for limiting rights on the computers which will be viewed from that computer.
- If you have configured membership in the domain-level Administrators group to automatically grant administrative rights on computers in the domain, then members of the domain-level Administrators group have rights to manage any Intel Server Manager computers on that domain.

Intel Server Manager documentation

After you have installed Intel Server Manager, documentation is available in two formats. Choose the format that is most convenient for you. The information is the same in each format.

- **HTML online help**—The online help (and the Intel Server Manager product) requires TCP/IP and Internet Explorer 6.0 or later. You can print selected topics from the online help by displaying the topic and clicking **File | Print**. If you want to print all of the documentation as a book, use the format listed below.
- **Adobe Acrobat .PDF format**—This is an electronic, printable format that requires Adobe Acrobat* Reader. (The latest free version of Adobe Acrobat Reader can be downloaded from <http://www.adobe.com>.) If Adobe Acrobat Reader is installed, you can access the guide from the Windows Start menu by clicking **Programs | Intel | ISM | User's Guide** (or **Administrator's Guide**).

Managing computers

Using power options

Rebooting or powering off a computer

The Intel Server Manager administrator can remotely power off or reboot computers on the network. The following events are part of this process.

Description of event	Example from log file or notification monitor
Intel Server Manager sends notification to all management stations that a reboot or shutdown was requested.	A system reboot or system shutdown command was issued by the Intel Server Manager user "administrator."
Each computer that you are attempting to reboot or shut down displays a message box indicating that it will be rebooted or shut down in 30 seconds. Users can cancel the reboot or shutdown command during that time if they are using the computer. If the user cancels, administrators receive notification.	A system reboot or system shutdown command issued by the Intel Server Manager user "administrator" was cancelled by the user Joe.
If the computer being rebooted or shut down is running Windows * XP with Fast User Switching enabled, all users currently logged on will receive notification that the administrator wants to reboot or shut down the computer. If any of the users cancels the reboot or shutdown within the countdown period, all users will receive the notification when they log on.	The Intel Server Manager user "administrator" attempted to reboot or shut down this computer. Because Joe cancelled that action, this computer will need to be rebooted before any changes take effect. Contact your system administrator immediately.

(This page intentionally left blank.)

Managing system inventory

Computer summary

Intel Server Manager instantly displays the overall health of the computer with an icon:

-  Normal
-  Critical
-  Warning

The summary page also displays information about the computer. Items displayed may vary depending on the type of computer and the technologies supported on the computer.

- **Computer name**—The name assigned to the computer.
- **Administrator**—The name of the computer hosting the administrator console that manages the computer.
- **Manufacturer**—The manufacturer of the computer.
- **Model**—The model number of the computer.
- **Version**—The version number of the computer.
- **Asset number**—The asset tracking number assigned to the computer. This number is sometimes assigned by the computer's manufacturer and stored in the computer's BIOS. This information is taken from the BIOS, and cannot be changed. If the field is blank, click **Asset number** and type an asset number.
- **Serial number**—The serial number of the computer.
- **BIOS version**—The version of the BIOS installed on the computer's motherboard.
- **Operating system**—The operating system currently running.
- **OS Version**—The operating system version, build number, and service pack release number.
- **CPU**—The type of processor installed on the motherboard.
- **Total physical memory**—The amount of total memory capacity of the computer's memory chips (not including virtual memory).
- **Total hard drive space**—The size of the installed hard disk, reported in megabytes.
- **Total free hard drive space**—The amount of available hard disk space, reported in megabytes or gigabytes.
- **TCP/IP address**—The address assigned to the computer for communicating on TCP/IP networks.

For IPMI systems only, the following information is displayed:

- **Hardware platform**—Description of the platform (such as IPMI).
- **IPMI version**—The version number of IPMI.
- **IPMI SDR version**—The version number of the SDR (sensor data record).

- **BMC firmware revision**—The revision number of BMC firmware.
- **ACPI power supply**—Information about ACPI-compliant power supplies is displayed when a server is out of band.

For blade chassis and blades, the following additional information is displayed:

- **Part number**—The part number of the component.
- **FRU number**—The identifying number if the component is a field replaceable unit.
- **FRU serial number**—The serial number if the component is a field replaceable unit.
- **Manufacture date**—The date of manufacture of the component.
- **Hardware revision**—The revision number of the component.
- **Type**—The identifying type of blade chassis.
- **Firmware summary**—In a box at the bottom of the summary information, details about various types of firmware are listed, including the firmware's build ID, date released, and revision number.

To open the summary page after viewing other information

- Click [**computer name**] **summary** at the top of the left pane.

Viewing system data

Intel Server Manager can display information about the hardware and software components on your computer. You can access this information with these methods:

- View all system data
- *Export all system data*

Server system data

The following list describes the information generally available for Intel Server Manager server systems.

Note: Some components may not be available for some computers, depending on the computer's motherboard, Operating System, and the manufacturer's configuration of Intel Server Manager.

- **Computer summary**—Displays a summary of the computer's hardware and software information.
- **Asset management**—Displays information about the computer's user, such as name, phone number, department, location, and position. Users with administrator rights on a computer can enter and modify this information. The computer name and an asset number may also be available.
- **BIOS**—Displays the *BIOS* manufacturer, version, date, and serial number; BIOS event log data; and allows alert configuration for POST error detection.
- **CPU**—Displays processor, speed, socket, and cache information; allows alert configuration for CPU changes.
- **Device drivers**—Displays the name, type, and status of each device driver.

- **Display**—Displays information about the computer's monitor, video adapter and driver, and supported video *resolutions*.
- **Drives**—Displays the computer's available and used disk space, and the configured thresholds that trigger alerts if disk space is running low. The partition, *file system*, cylinder, and sector information is also provided for each hard drive, as well as serial number and *S.M.A.R.T.* information, if applicable. Allows alert configuration for drive changes, drive space, and drive failure prediction.
- **Environment variables**—Displays the variable name, the user of the variable, and the variable's value.
- **Fans**—Displays status of cooling fans installed in the computer; allows alert configuration for fans.
- **Field replaceable units**—Displays modules or components of an IPMI system which can be replaced in its entirety as part of a field service repair operation.
- **Installed applications**—Displays a list of applications installed on the computer with version, date, filename, size, and path information. Allows alert configuration for applications being added or removed.
- **Keyboard and mouse**—Displays the type of keyboard and mouse attached to the computer.
- **Memory**—Displays the computer's available and used memory (physical and virtual), sockets, and the configured thresholds that trigger alerts if memory is running low. Allows alert configuration for ECC error detection, virtual memory, and changes to memory modules.
- **Modems**—Displays the names and types of modems on the system, and the ports they use.
- **Motherboard**—Displays motherboard manufacturer, model, and serial number, as well as *system slot* information.
- **Multimedia**—Displays information about the computer's multimedia devices.
- **Network**—Displays information about the computer's network adapters and drivers, *IP address* configuration, data statistics, and network connections. Allows alert configuration for addition or removal of NICs.
- **Operating system**—Displays operating system and version information, startup time, locale, registered user and organization, and serial number.
- **OS event log**—Displays the operating system logs of events from the selected computer.
- **Performance**—Displays current thresholds for specific parts of the system; lets you modify thresholds and select performance counters to monitor; allows alert configuration for performance.
- **Ports**—Displays the port name, *IRQ*, *I/O address*, and other information for the computer's *parallel* and *serial ports*.
- **Power supplies**—Displays the name and status of each power supply on the system.
- **Processes**—Displays a list of processes running on the system, and lets you terminate most processes.
- **Sensors**—Displays data for discrete and numeric sensors on IPMI systems.
- **Services**—Displays a list of services running on the system, and lets you select a service to generate an event should the service's status change. Also allows alert configuration.

- **Storage Devices**—Displays a list of storage devices on the system, including disk drives, tape drives, RAID arrays, DAT drives, etc.
- **Temperatures**—Displays a list of temperatures for key components of the system, and allows alert configuration for temperatures.
- **Voltages**—Displays a list of voltages for electrical components of the system, and allows alert configuration for voltages.

Blade and blade chassis data

The following list describes the information generally available for Intel Server Manager blade and blade chassis systems. Some components listed here may not be available for some systems, depending on the manufacturer's configuration.

- **Blade slots**—Lists the slots in a chassis and names of blades in the slots.
- **Blowers**—Displays status of blowers in blade chassis systems.
- **I/O modules**—Lists information about the I/O modules in a blade chassis.
- **Management modules**—Lists information about the management modules in a blade chassis.
- **Power domains**—Lists information about the power domains in a blade chassis.
- **Power modules**—Lists information about the power modules in a blade chassis.
- **Temperatures**—Displays a list of temperatures for key components of the blade or chassis.
- **Voltages**—Displays a list of voltages for electrical components of the blade or chassis.

To view system data

- In the left pane, click **System**, then click any of the items.

Asset management

Intel Server Manager enables you to manage and view the following user and asset information for the computer.

Contact

Contact information can be modified by a user with administrative rights.

- **Name**—The primary user's name.
- **Position**—The primary user's job position.
- **Phone number**—The primary user's phone number.
- **Location**—The primary user's location in the building.
- **Department**—The primary user's department.

System

- **Computer name**—The computer or host name.
- **Manufacturer**—The name of the company who made the computer.

- **Model**—The model number of the computer.
- **Version**—The computer system version.
- **Serial number**—A serial number assigned to the motherboard by its manufacturer.
- **Asset number**—The asset tracking number assigned to the computer. This is sometimes assigned by the computer's manufacturer and stored in the computer's *BIOS*. If it is not in the *BIOS*, this number can be added by a user with administrative rights.

To view and edit asset information

1. Click **System**, then click **Asset management**.
2. Type new information in any edit box.
3. Click **Apply**.

Note—The asset information fields can only be edited if you are logged in as a member of the Windows Administrators or Power Users groups.

BIOS

Intel Server Manager displays the following *BIOS* information for the computer:

- **Manufacturer**—The manufacturer of the *BIOS* installed on the motherboard.
- **Date**—The date of the *BIOS* installed on the motherboard.
- **Version**—The version of the *BIOS* installed on the motherboard.
- **Serial number**—The serial number of the *BIOS* installed on the motherboard.

You can also use this page to set alert actions for POST (power-on self test) errors that may occur when a computer boots. You can also view the *BIOS* event log.

BIOS event log

The log displays a list of events affecting the *BIOS*, including the date the event occurred and a description of the event.

To view BIOS information

- Click **System**, then click **BIOS**.

To set alert actions for POST errors

1. Click **Configure alert actions: POST error detection**.
2. Click the tab of the status type (OK or Warning) you want to set alerts for.
3. Click the types of alerts you want to send and click **Apply**.
4. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Chassis

Use Chassis to view whether the chassis of a computer is open or closed (supported on IPMI and some other systems). You can also turn on or off the LED indicator on an IPMI-enabled server. Turning the LED indicator on is helpful in identifying a machine among a row or rack of systems. You can also turn on the LED indicators of out-of-band IPMI computers from the administrator console.

Note: To view all available IPMI inventory information, you need SMBIOS 2.3.1 or higher.

To view chassis information

1. In the left pane, click **System**, then click **Chassis**.

To turn on the system identify LED

1. Specify the number of minutes you would like the LED turned on or off.
2. Click **On**.

To set alert actions for Chassis

1. Click **Management**, then click **Alerts**.
2. Click **Chassis** for non-IPMI enabled computers.

or

Click **Physical security/chassis intrusion** for IPMI-enabled computers.

3. Click the tab of the status type (OK or Warning) you want to set alerts for.
4. Click the types of alerts you want to send and click **Apply**.
5. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

CPU

ISM displays the following processor information for the computer:

CPU

- **Name**—The type of processor installed on the motherboard.
- **Description**—A specific description of the CPU.
- **Vendor ID**—A unique ID assigned to the processor which identifies its manufacturer.
- **Current speed**—The speed (measured in megahertz or gigahertz) at which the processor is currently running.
- **Maximum speed**—The maximum speed at which the CPU can run.
- **Bus speed**—The speed (in megahertz) of the bus.
- **Number of logical CPUs**—The number of installed logical microprocessors.
- **Number of physical CPUs**—The number of installed physical microprocessors.

Cache

- **Type**—Indicates whether the cache is internal (*primary*) or external (*secondary*) to the microprocessor.
- **Size**—The size of memory cache (measured in kilobytes) available to the processor.
- **Write policy**—The type of memory cache used, such as *write through* or *write back*.

To view processor information

- Click **System**, then click **CPU**.

To set alert actions for CPU

1. Click **Configure alert actions: CPU changes**.
2. Click the types of alerts you want to send and click **Apply**.
3. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Device drivers

Use Device drivers to view the name, type, and status of each device driver on the system.

To view device driver information

- Click **System**, then click **Device drivers**.

Display

Use Display to view monitor and video adapter information, and to view the supported resolutions of the monitor.

To view display information

- Click **System**, then click **Display**.

Drives

You can use Intel Server Manager to:

- Configure alert actions for drive space, drive failure prediction, and drive changes.
- Set warning and critical thresholds for disc space alerts.
- View information about the computer's drives.

To view drive information

- Click **System**, then click **Drives**.

To configure alert actions for disk space, drive failure prediction, or disk drive changes

1. Click the alert you want to configure.
2. Click the tab of the status type (Critical, Warning, OK, and Informational) you want to set alerts for.
3. Click the types of alerts you want to send and click **Apply**.
4. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

To set drive space thresholds

1. Click the drive for which you want to set thresholds.
2. Drag the colored arrows on the indicator bar or type Warning and Critical percent values in the appropriate boxes.
3. Click **Apply**.

Notes

- Used and available disk space are not updated dynamically. You can refresh them by clicking Apply or Refresh.
- You must have Macromedia* Flash installed to view the thresholds bar. You can download the Flash player at www.macromedia.com.

Environment variables

Use the Environment variables page to view a list of environment variables used by the current system. Information about user environment variables is available for computers running Windows* 2000, Windows 2003, or Windows XP. The following columns are displayed:

- **User**—The login name of the user that set the variable.
- **Variable**—User-specific variables that are initialized on startup and used by the operating system.
- **Value**—The value or text assigned to the variable.

To view environment variable information

- Click **System**, then click **Environment variables**.

Fans

Intel Server Manager can monitor the speed for cooling fans installed in the computer if the motherboard and fans support this feature. These can include:

- Processor fans for each microprocessor installed on the motherboard
- Rear chassis fans
- Front chassis fans

- Other fans included by the computer's manufacturer

The first time the computer boots after Intel Server Manager is installed, Intel Server Manager autodetects any fans installed in the computer. Intel Server Manager then monitors the fan's speed and generates an alert if the fan ever stops.

To view fans information

- Click **System**, then click **Fans**.

Note: Fan information is not updated dynamically. You can update it by refreshing the browser window view or by clicking Fans.

To set alert actions for fan problems

1. Click **Configure alert actions: Fans**.
2. Click the tab of the status type (OK or Critical) you want to set alerts for.
3. Click the types of alerts you want to send and click **Apply**.
4. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Field replaceable units

Intel Server Manager displays information about field replaceable units (FRUs) on managed IPMI-enabled computers.

A field replaceable unit is a module or component of the system which can be replaced in its entirety as part of a field service repair operation. Many organizations have FRU information for each major system board (such as processor board, memory board, I/O board, and so forth). The FRU data can include information such as model, asset tag, part number, and serial number. Field replaceable units can include the system board, memory devices, and drive backplanes.

To view Field replaceable unit information

- Click **System**, then click **Field replaceable units**.

Installed applications

Intel Server Manager provides a list of installed applications and their versions.

To view applications information

- Click **System**, then click **Installed applications**.

To set alert actions for installed applications

1. Click **Configure alert actions: Application added or removed**.
2. Click the types of alerts you want to send and click **Apply**.

3. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Keyboard and mouse

Intel Server Manager displays the following keyboard and mouse information for the computer:

Keyboard

- **Description**—The manufacturer and make of keyboard attached to the computer, including the type of connector used to attach the keyboard to the computer, such as PS/2, Micro-DIN, USB or DB-9.
- **Layout**—The keyboard layout selected in the operating system, such as US, French (Standard), or German (Standard).

Mouse

- **Manufacturer**—The manufacturer and make of pointing device attached to the computer.
- **Connector type**—The type of connector used to attach the keyboard to the computer, such as PS/2, Micro-DIN, USB or DB-9.
- **Number of buttons**—The number of buttons on the mouse.
- **Button configuration**—The configuration supporting the user's preferred hand for mouse usage.

To view keyboard/mouse information

- Click **System**, then click **Keyboard and mouse**.

Memory

You can use Intel Server Manager to:

- View information about available physical and virtual memory.
- View memory module information, such as socket type, size, and speed.
- Configure memory alerts
- Set thresholds for virtual memory alerts

To view memory or memory module information

1. Click **System**, then click **Memory**.
2. Open **Memory information** or **Memory modules**.

To set alert actions for memory

1. Click **Configure alert actions** for the type of alert you want to configure.

2. Click the tab of the status type (OK, Warning, Critical, or Informational) you want to set alerts for.
3. Click the types of alerts you want to send and click **Apply**.
4. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

To set virtual memory thresholds

1. Click **System**, then click **Memory**.
2. Open **Set thresholds: Virtual memory**.
3. Drag the colored arrows to adjust the Warning and Critical thresholds.

or

Type percentage numbers directly in the **Warning threshold** and **Critical threshold** boxes.

4. Click **Apply** to change the thresholds.

Notes

- Used and free space are not updated dynamically. You can refresh them by clicking Apply or Refresh.
- You must have Macromedia* Flash installed to view the thresholds bar. You can download the Flash player at www.macromedia.com.

Modems

Use Modems to view the names and types of modems on the system, and the ports they use. You can receive alerts when modems are added or removed from a computer. You can also enable Modem view when you want to monitor modem activity on a computer and receive alerts when modem activity is detected.

To view modem information

- Click **System**, then click **Modems**.

To detect modem activity on a computer

1. Click **Modem view**.
2. Check **Enable modem view**.
3. Click **Apply**.

To set alert actions for modems

1. Click **Configure alert actions** for the type of alert you want to configure.
2. Click the types of alerts you want to send and click **Apply**.
3. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Motherboard

Intel Server Manager displays information about a computer's motherboard and system slots.

Motherboard information

- **Manufacturer**—The manufacturer of the computer's motherboard.
- **Model**—The model of the computer's motherboard.
- **Serial number**—The serial number of the motherboard.

System slots

- **Description**—The type of expansion slots available on the computer's motherboard, such as *ISA*, *EISA*, *MCA*, *PCI*, *SCSI*, or *PCMCIA*.
- **Location**—The physical location of the system slot.
- **Label**—The label of the system slot.
- **Slot width**—The bus width of the expansion slot, such as 16-bit or 32-bit.
- **Status**—Indicates if the slot is available or currently in use.

Note—The computer may have two expansion slots (such as an ISA slot and a PCI slot) that share the same opening in the computer's case and can't be used at the same time.

To view motherboard information

- Click **System**, then click **Motherboard**.

Multimedia

Intel Server Manager displays multimedia information about installed sound devices, audio codecs, and video codecs. This information can include:

- **Filename**—The filename of the multimedia device.
- **Manufacturer**—The manufacturer of the multimedia device.
- **Description**—A description of the device (if available).
- **Size**—The size of the multimedia device file.
- **Install date**—The date the multimedia device was installed on the selected computer.
- **Version**—The multimedia device file version number.

To view multimedia information

- Click **System**, then click **Multimedia**.

Network

Intel Server Manager displays the following network information for a computer. Note that the information displayed may vary slightly depending on the computer and operating system.

Network information

- **Number of network adapters**—The number of network adapters on the selected computer.
- **Manufacturer**—The manufacturer of the network adapter.
- **Node (MAC) address**—The computer's unique six-byte hexadecimal *MAC address*.
- **Status—Connection status.**
- **TCP/IP address**—The four-byte address assigned to the computer for communicating on TCP/IP networks.
- **Subnet mask**—The four-octet number (such as 255.255.255.0) that is paired with an IP address. This number tells an IP router which octets in the IP address are the network ID and which octets are the node ID.
- **Default gateway**—The IP address of the router that is configured as a default gateway for *packets* leaving the network.
- **DHCP server**—The IP address of the Dynamic Host Configuration Protocol server.
- **DHCP lease obtained**—The date and time the DHCP lease was obtained.
- **DHCP lease expires**—The date and time the DHCP lease expires.
- **DNS servers**—The IP address for each Domain Name Service (DNS) server on your network. You may have more than one.
- **Primary WINS server**—The IP address of the primary Windows Internet Naming Service.
- **Secondary WINS server**—The IP address of the secondary Windows Internet Naming Service.

Data statistics since startup

- **Speed**—The connection speed in megabytes per second.
- **Bytes received**—The number of bytes received by the computer.
- **Bytes sent**—The number of bytes transmitted from the computer.
- **Packets received**—The total number of network packets received at the computer since startup. Because this number includes both unicast packets and broadcast packets, it will not match the number displayed by the operating system in the Local Area Connection Status dialog box.
- **Packets sent**—The number of network packets transmitted from the computer since startup.
- **Receive errors**—The number of times since startup that the computer was unable to receive a packet.

- **Send errors**—The number of times since startup that the computer was unable to transmit a packet.

Persistent network connections

- **User**—This applies only to Windows * XP, which supports Fast User Switching.
 - If you're logged on to Intel Server Manager as an administrator, you will see all active network connections for all logged on users.
 - If you're logged on to Intel Server Manager as a non-administrator (power user, for example), you will not see the drive mappings of other users. You will see your own drive mappings if your Intel Server Manager login name matches your Windows login name.
- **Drive**—The driver letter assigned to a particular network drive, such as F: or G:.
- **Connection name**—The *UNC* name of the network resource, such as \\server\sharename.

To view network information

- Click **System**, then click **Network**.

To set alert actions for NIC addition or removal

1. Click **Configure alert actions: NIC added or removed**.
2. Click the types of alerts you want to send and click **Apply**.
3. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Operating system

Intel Server Manager displays the following information about the computer's operating system:

- **Name**—The operating system currently running.
- **Startup time**—The date and time the operating system was started.
- **Locale**—The language of the operating system.
- **Version**—The operating system version, build number, and service pack release number.
- **Registered user**—The user the operating system is registered to.
- **Registered organization**—The organization the organization is registered to.
- **Serial number**—The serial number of the operating system.

To view operating system information

- Click **System**, then click **Operating system**.

OS event log

Use the OS event log page to view a log of the most recent operating system events from the selected computer. You can select one of the following three views:

- Application
- System
- Security

Each section has four columns of information.

- **Type**—The type of event that occurred. The four types are informational, warning, error, and critical.
- **Date**—The date and time the event occurred.
- **Source**—The application or service from which the event initiated.
- **Description**—A detailed description of the event. The description may include corrective action taken by the system or text to resolve the error.

To open the OS event log

- Click **System**, then click **OS event log**.

PCI Hot Plug Devices

Intel Server Manager allows you to check the status for devices installed into PCI Hot Plug Slots in the managed server.

Note: Currently, only Intel® Server Board SE7520AF2 and Intel Server Board Set SE8500HW4 running Microsoft Windows supports PCI Hot Plug slots. Check the Intel Server Manager Release Notes for the latest information on platform support.

PCI hot plug slot sensor information

You can view the following for devices installed into PCI hot plug slots:

- **Class Code**—The general name of the device (e.g. Ethernet Controller).
- **Manufacturer**—The organization responsible for creating the device.
- **Device Present**—Indicates whether the device is physically plugged into the slot.

To view information about devices in PCI hot plug slots (Microsoft Windows)

- In the left pane of the server console, click **System**, then click **PCI Hot Plug Devices**.

PCI Hot Plug Slots

Intel Server Manager allows you to check the status of PCI Hot Plug slots on the managed server.

Note: Currently, only Intel® Server Board SE7520AF2 and Intel Server Platforms SR4850HW4 and SR6850HW4 running Microsoft Windows supports PCI Hot Plug slots. Check the Intel Server Manager Release Notes for the latest information on platform support.

Note: To power on and off PCI slots for hot add and removal on SE7520AF2 systems, a special application called PCI Hot Plug Monitor is required. This application, and its installation and user's guide, are available on the SE7520AF2 System Resource CD. The Intel Server Platforms SR4850HW4 and SR6850HW4 have built-in hardware and do not require this utility (they do require an operating system that supports PCI hot-plug).

If you have the required hardware and software, you can determine both the status of the slot and the sensors associated with the slot. Additionally, you can configure alerts for the following:

- **Device installation or removal**—Generates alerts when a device has been installed or attached. You can also configure an alert for when the slot is ready for device installation or removal, or for when the slot requests device removal.
- **Slot powers off or becomes disabled**— Generates alerts when a slot has been powered off or if the slot has become disabled.
- **Interlock or Identity Status asserted**—Generates an alert when a slot interlock or Identity Status has been asserted.
- **Fault asserted**—Generates an alert when a fault has occurred on the device in the slot.

PCI hot plug slot sensor information

You can view the following for PCI hot plug slot sensor:

- **Sensor Name**—The name of the sensor associated with the slot.
- **Current Status**—The current status of the device as reported by the sensor.
- **Current Reading**—Information about the device (e.g. Installed and Attached).
- **Description**—A description of what the sensor monitors (e.g. Fan 1 presence).

To view PCI hot plug slot information (Microsoft Windows)

- In the left pane of the server console, click **System**, then click **PCI Hot Plug Slots**.

To set alert actions for PCI Hot Plug Slots

1. Perform the steps to view PCI Hot Plug Slot information.
2. Click the tab to configure alert actions. The alerts you set apply to all the slots.
3. Click the tab of the status type (Critical, OK, and Informational) for which you want to set alerts. Not all status types are available for each system component.
4. Click the type of alert you want to send.
5. If you want to set options for the alert (if applicable), click **Apply** to save your settings, then click Set preferences.
6. Click **Apply**.

Performance

The Intel Server Manager Performance page lets you monitor the performance of various system objects. You can monitor specific hardware components, such as drives, processors, and memory, or you can monitor OS components, such as processes or bytes/sec transferred by the system's Web server. The Performance page includes a graph that displays real-time or historical data for a counter. You can also acknowledge alerts received for a counter and stop monitoring a performance counter by deleting it from the list of monitored counters.

In order to monitor a performance counter you must first select the counter, which adds it to the list of *monitored counters*. When you do this you also specify the frequency for polling the item and set performance thresholds and the number of violations that are allowed before an alert is generated.

You can set alert actions to trigger notification when a performance counter crosses an upper or lower threshold a predetermined number of times.


To view a performance graph for a monitored counter

1. Click **System**, then click **Performance**.
2. Click **Performance graph**.
3. From the **Counters** drop-down list, select the counter you for which want to see a performance graph.
4. Select **View real-time data** to display a graph of real-time performance.

or

Select **View historical data** to display a graph showing performance over the period you specified (Keep history) when selecting the counter.

Notes

- The horizontal axis represents time that has passed.
- The vertical axis represents the units you are measuring, such as bytes/sec (when monitoring file transfers, for example), percentage (when monitoring percentage of the CPU that is in use), or bytes available (when monitoring hard drive space).
- The line height is not a fixed unit. The height of the line changes relative to the extremes in the data; for one counter the vertical axis might represent 1 to 100 and for another it might represent 1 to 500,000. When the data varies across a wide extreme, minimal changes can appear as a flat line.
- Selecting another counter refreshes the graph and resets the units of measurement.
- Click  to clear and restart the graph.
- Click **Reload counters** to refresh the list with any new objects, instances, or counters.

To stop monitoring a performance counter

1. Click **System**, then click **Performance**.
2. Click **Monitored performance counters**.

3. Check the counter(s) you want to stop.
or
Click **Select all** to select all current counters.
4. Click **Delete**.

To acknowledge an alert for a performance counter

1. Click **System**, then click **Performance**.
2. Click **Monitored performance counters**.
3. Check the counter for which you have received an alert.
4. Click **Acknowledge**.

To set a performance alert action

1. Click **Configure alert actions: Performance**.
2. Click the tab of the status type (OK or Warning) you want to set alerts for.
3. Click the types of alerts you want to send and click **Apply**.
4. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Note—You must *select a counter* or counters to monitor before alerting can take place.

Ports

Intel Server Manager displays the following port information for the computer.

Serial ports

- **Name**—The name of the *serial port*, such as *COM1* or *COM2*.
- **IRQ**—The *interrupt request* number assigned to the serial port, such as 3 or 4.
- **I/O address**—The starting memory address (represented in *hexadecimal*) designated for the input/output of data from the serial port.
- **Baud rate**—The default baud rate of data transfer for the serial port.
- **Bits per byte**—The number of data bits per byte (7 or 8 typically).
- **Parity**—The type of parity bit in use, if any (even, odd, none, mark, or space).
- **Stop bits**—The number of bits signaling the end of a unit of transmission on a serial line.

Parallel ports

- **Name**—The name of the *parallel port*, such as *LPT1*.
- **I/O address**—The starting memory address (represented in hexadecimal) designated for the input/output of data from the parallel port.

To view ports information

- Click **System**, then click **Ports**.

Power supplies

Use Power supplies to view the name and status of each power supply on a server. You can also set alert actions to trigger notification if a power cord is connected or disconnected, a power supply is added or removed, or a power supply fails.

To view power supply information

- Click **System**, then click **Power supplies**.

To set alert actions for power supplies

1. Click **Configure alert actions: Power supplies**.
2. Click the tab of the status type (Informational, OK, Warning, or Critical) you want to set alerts for.
3. Click the types of alerts you want to send and click **Apply**.
4. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Power supply management

Use the Power supply management page to view power usage information for the system as a whole, and for each individual power supply unit. You can also set alert actions to trigger notification when power usage crosses configured sensor thresholds. Note that these thresholds are configured in the BMC, and are not configurable by ISM. When power usage crosses sensor thresholds, events are generated. For power usage, you can set actions for events that have a status of Critical or OK.

To view power supply management information

- Click **System**, then click **Power supply management**.

To set alert actions for power usage

1. Click **Management**, then click **Alerts**.
2. Click **Power supply management**.
3. Click the tab of the status type (Critical, Warning, OK, and Informational) you want to set alerts for
4. Click the types of alerts you want to send and click **Apply**.
5. If you want to set options for an alert (if applicable), click **Apply** to save your settings, then click **Set preferences**.

Processes

Use the Processes page to view a list of current processes on the selected machine, view statistics on each process, and shut down one or more processes.

Note: Terminating a process can cause undesired results including loss of data and system instability. The process will not be given the chance to save its state or data before it is terminated.

Information about processes is listed in the following columns:

- **Name**—The name of the executable file of the process.
- **CPU Time**—The percentage or amount of time used by the process.
- **Memory usage**—The amount of memory the process is using.
- **Virtual size**—The size of virtual memory taken by the process on the hard disk.
- **Handles**—The number of object handles in a process's object table.
- **Threads**—Single uses of a program that execute independently of other threads in the program.

To view current processes

- Click **System**, then click **Processes**.

To terminate a process

1. Click **System**, then click **Processes**.
2. Check the process you want to terminate.
3. Click **End process**, then click **OK**.

Sensors

Use the Sensors page to view data on all the sensors of an IPMI system. Each sensor's information is taken from a Sensor Data Record (SDR), which is stored in the Sensor Data Repository. An SDR defines and completely describes a sensor, including the sensor's default initialization settings that the Baseboard Management Controller (BMC) uses at system initialization. The sensor data for many components is also displayed on the component's System page (such as Fans, Temperatures, and so forth).

Two types of sensors are displayed: *discrete sensors*, which can contain up to 15 possible states; and *numeric sensors* that return a numeric reading. Sensor data can include:

- **Type**—The classification of the sensor.
- **Description**—Additional information about the sensor.
- **Status**—The current operating state of the sensor.
- **Value**—The quantity and measurement of the type.

Notes

- The Intel Server Manager administrator database must have the correct BMC password to retrieve information from an out-of-band node. If the BMC password is not correct, the status for the node's sensors will display as "Unavailable."
- You may be prompted for the BMC password when you change thresholds or restore default thresholds for a numeric sensor. Some BMCs require that the password be supplied before making this change.

To view sensor information

1. Click **System**, then click **Sensors**.
2. Click the sensor for which you want more detailed information.

To change thresholds for a numeric sensor

1. Click **System**, then click **Sensors**.
2. Click the sensor for which you want to change thresholds.
3. Change upper and lower thresholds.
4. Click **Apply**.

Services



You can use Intel Server Manager to view the services on your computer and their statuses, or to set alert actions to notify you of changes to service status.

For each service on your computer, Intel Server Manager displays the service name, its startup type, and its current status. The check box beside each service indicates whether you're monitoring that service. If a monitored service stops or starts, an alert event is generated.

To view the currently running services

- Click **System**, then click **Services**.

To start or stop a service

1. Click the icon at the far right of the service you want to start/stop, then click **OK**.
Click  to stop the service.
Click  to start the service.

To set a service alert action

1. Click **Configure alert actions: Services**.
2. Click the tab of the status type (OK or Warning) you want to set alerts for.
3. Click the types of alerts you want to send and click **Apply**.
4. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Storage devices

Use Storage to view information about storage devices on a server, such as hard drives, tape drives, media changers, DAT drives, SCSI enclosures, and *RAID* devices.

Devices are listed by *SCSI* controller type. You can view the status of individual devices under a *SCSI* type, and for some device types you can view individual components (for example, for a device with multiple slots, you can view the status of each slot in more detail).

Device information can include safety-related physical sensor readings for items such as fans, temperature, power supplies, alarms, and doors (open or closed).

RAID arrays are treated as one device but the status page contains information about individual drives. If one drive fails or is removed, the *RAID* array shows failed; it then can be rebuilt as a new *RAID* array

Events such as disk failure generate pop-up alert windows with details that identify the device, controller, and channel for quick identification of the device.

Note: IDE and SATA drives which are run on add-in controller cards will appear as *SCSI* devices.

To view storage device information

- Click **System**, then click **Storage devices**.

Temperatures

Use Temperatures to monitor the temperature of vital components in your system. The data comes from the location of the temperature sensor inside the computer. The data is represented numerically and visually with a thermometer image. The columns of data are as follows:

- **Name**—The name of the component being monitored.
- **Maximum**—The maximum temperature the component can have before its performance is compromised (as determined by the manufacturer).
- **Last**—The temperature reading of the component taken from the last background scan. If this column has a substantially different value than the Current column, there may be a sudden change in the computer's health.
- **Current**—The current temperature of the component. If this column shows a value of zero, the computer is out of band (IPMI servers only).

To view temperature information

1. Click **System**, then click **Temperatures**.
2. Click the component for which you want more detailed information.

Note: Temperature information is not updated dynamically. You can update it by refreshing the browser window view or by clicking **Temperatures**.

To change temperature thresholds

1. Click **System**, then click **Temperatures**.
2. Click the component for which you want to change thresholds.

3. Change upper and lower thresholds.
4. Click **Apply**.

To set alert actions for temperatures

1. Click **Configure alert actions: Temperatures**.
2. Click the tab of the status type (OK or Critical) you want to set alerts for.
3. Click the types of alerts you want to send and click **Apply**.
4. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

Voltages

On motherboards that support voltage monitoring, Intel Server Manager monitors the power voltages on the computer's power supply lines. When the voltage on a given power supply line exceeds a threshold defined by the manufacturer, Intel Server Manager can notify you of a potential problem with the computer's power supply. The monitored voltages vary depending on the computer's motherboard. Also, the voltage thresholds that trigger an alert can vary across voltage lines, and can also be adjusted by the motherboard manufacturer.

To view voltage information

1. Click **System**, then click **Voltages**.
2. Click the component for which you want more detailed information.

Notes

- Voltage information is not updated dynamically. You can update it by refreshing the browser window view or by clicking **Voltages**.
- You must have Macromedia* Flash installed to view the voltage status graphics. You can download the Flash player at www.macromedia.com.

To change voltage thresholds

1. Click **System**, then click **Voltages**.
2. Click the component for which you want to change thresholds.
3. Change upper and lower thresholds (values are in millivolts).
4. Click **Apply**.

To set alert actions for voltages

1. Click **Configure alert actions: Voltages**.
2. Click the tab of the status type (OK or Critical) you want to set alerts for.
3. Click the types of alerts you want to send and click **Apply**.
4. To set general options for an alert type, click **Set preferences**. This link opens the *Alerts preferences* page.

(This page intentionally left blank.)

Reports

Monitoring configuration changes

Configuration changes on a managed computer can generate alerts and are also logged. Computers running the administrator console can display configuration changes as pop-up alerts.

Note: Configuration change reports are not available for computers with the Intel Server Manager bridge agent installed (rather than the full server installation) or for out-of-band computers.

To view configuration changes

1. Click **Reports**, then click **Configuration changes**.
2. Click **Next** and **Previous** to scroll through the pages of the log.
3. To display changes for a range of dates, click **Filter by date range**, clear the **Show events for all dates** checkbox, enter a start date and an end date, then click **Filter**.

Alerts for configuration changes

Intel Server Manager can generate alerts if a computer's hardware or software configuration changes. These changes may affect a computer's performance and stability or cause problems with a standard installation. By monitoring vital pieces of the computer, Intel Server Manager can help you reduce the total cost of ownership (TCO).

The computer configuration changes that will generate alerts are:

- **Application installed or uninstalled**—You can see which users installed or removed applications. This may be helpful in tracking licenses or employee productivity. Intel Server Manager monitors applications that are registered in the Windows Add/Remove Programs area of the Control Panel. Other applications are ignored. The application name that is used in the Windows Add/Remove Programs is the application name that appears in the notification log or alert pop-ups window.
- **Memory added or removed**—ISM detects and monitors the quantity and type of memory installed. If the configuration changes, Intel Server Manager generates an alert.
- **Hard drives added or removed**—ISM detects and monitors the type and size of the drives installed on computers. If the configuration changes, Intel Server Manager generates an alert. Intel Server Manager does not monitor disk configuration changes on laptop computers because the administrator would constantly be getting alerts from drives that are designed to be temporarily plugged in and then removed. Drives in docking stations could also generate excessive alerts as the laptop is docked and undocked.
- **Processor (or processors) added, removed, or modified**—ISM detects and monitors the number, type, and speed of the processor(s). If the configuration changes, Intel Server Manager generates an alert. Intel Server Manager does not monitor processor changes on laptop computers.

To set alert actions for configuration changes

1. Click **Management**, then click **Alerts**.
2. Click **Configuration changes**.
3. Click the types of alerts you want to send and click **Apply**.
4. To set options for an alert (if applicable), click **Apply** to save your settings, then click **Set preferences**.

Viewing hardware events

Use Hardware events to view a list of events occurring on the hardware components of an IPMI system. This log captures system-generated hardware events, rather than the BIOS or OS data captured in the *BIOS event log* or *OS event viewer*. Log entries can be filtered by date range, generator, or sensor type.

- **Date**—The date and time the event occurred.
- **Generator**—The component that originated the event.
- **Sensor type**—The type of sensor on which the event occurred.
- **Details**—A description of what occurred on the sensor to produce the event.

To view the hardware events log

1. Click **Reports**, then click **Hardware events**.
2. Click the **Next** and **Previous** buttons to scroll through the pages of notifications in the log.
3. To filter by date range, clear the **Show events for all dates** checkbox, enter a start date, enter an end date, then click **Filter**.
4. To filter by generator or sensor type, select a generator type, select a sensor type, then click **Filter**.

Hardware events log backup

The Hardware events log displays information from the System Events Log (SEL) that is created and stored on the BMC. Because event data is not purged from the log, when the SEL reaches its storage limit, no new entries will be created as new system events are generated. You can configure Intel Server Manager to back up the SEL when it reaches a certain percentage of its capacity. The backup action performed depends on the status of the computer:

Computer status	Backup action
Unmanaged and in-band	Backup files are created in the local system temporary folder. Filenames are IPM#.tmp, where # is a number that increments with each new backup file. After creation, these files are not managed by Intel Server Manager, but may be manually viewed or deleted.
Unmanaged and out-of-band	The SEL cannot be backed up. When it becomes full, new events will not be added to it.
Managed and in-band	Backup information is sent to the administrator computer, where it is stored in the AutoSELBackup table in the database. If the

Computer status	Backup action
	administrator computer is not on when the server needs to back up, the server computer will hold the information until the administrator is powered on.
Managed and out-of-band, administrator powered on	The administrator computer retrieves backup information and stores it in the AutoSELBackup table in the database.
Managed and out-of-band, administrator powered off	The SEL cannot be backed up. When it becomes full, new events will not be added to it.

To configure hardware events log backup options

1. Click **Reports**, then click **Hardware events**.
2. Click **Configure the log file backup**.
3. Check **Turn on hardware event backup**.
4. Specify the frequency to check the log and the percentage at which it should be backed up.
5. Click **Apply**.

To back up or clear the hardware events log immediately

1. Click **Reports**, then click **Hardware events**.
2. Click **Configure the log file backup**.
3. To back up the log contents and then clear the log, click **Back up now**.
4. To clear the log without backing up its contents, click **Clear now**.

Notes:

- The backup process saves only information that is contained in the SEL. Anything cleared from the SEL before backup will not be saved.
- When an administrator begins managing a computer by adding it to the My computers list, any backup files that already exist in that computer's temporary folder will not be sent to the administrator for backup in the database. All new backups will be sent to the administrator.
- You can manually delete data from the SEL backup using a third-party SQL query analyzer.
- Be aware that while individual backup files may not be large, if you have turned on automatic hardware event backup the disk space required for storing backup files may be substantial over time. Some systems log many hardware events and may store backup files frequently. On an unmanaged server, if you do not regularly monitor the size of the temporary files directory it may eventually take up excessive amounts of disk space. On a managed server, the backup data saved to the administrator computer's database may likewise take up excessive space.

Exporting system data

Using Intel Server Manager, you can export information about the hardware and software components on your computer. The type of data that is available is described in *Viewing system data*.

Because Intel Server Manager gathers all of a computer's system information during an export, the export process can sometimes take up to a minute or more.

To export data

1. Click **Reports**, then click **Run export**.
2. Type a name for the export, then click **Run**.

The .XML output is saved in the Intel\ServerManager\server\wwwroot\ISM\exports folder.

To view exported data

1. Click **Reports**, then click **System exports**.
2. Click the name of the export you want to view.

Viewing the system log

When an event occurs on a Intel Server Manager computer, Intel Server Manager records the event details in a log.

You can filter log files to view only certain categories of events or view events that occurred within a date range. This may be useful if the log file is large and contains many entries. About 50 categories of log entries are available, including configuration changes, processor missing, and disk space.

Notes



- Date/time information is listed as UTC/Greenwich Mean Time.
- The log continues to store events until you empty the log or until it reaches maximum size. When the log reaches its maximum size, the older entries are removed as new entries are added. You can set the local log size to be 1 MB to 5 MB. Resizing clears the log.

To view the local system log

1. Click **Reports**, then click **System log**.
2. Use the View drop-down list in the log file toolbar to view all events or to select a particular type of event to view.
3. To filter by date range, click **Filter by date range**, clear the **Show events for all dates** checkbox, enter a start date, enter an end date, then click **Filter**.
4. Click **Next** and **Previous** to scroll through the pages in the log.

To delete or resize a log file

1. Display the local log file as described above.

2. To resize the log, click , enter a new size, then click **Resize**. This will copy the previous entries to the newly sized log. (Note that if the new log size is smaller, old entries will be deleted.)
3. To delete the log, click .

To copy log contents to another application

1. Select the log entries you want to copy. (Use the Ctrl and Shift keys to select multiple entries.)
2. Click **Edit | Copy** to copy the selection to the Windows clipboard.
3. In the application where you want to copy the log entries, click **Edit | Paste**.

(This page intentionally left blank.)

Configuring and viewing alerts

Using alerts

When a problem or other event occurs on a computer (for example, the computer is running low on disk space), Intel Server Manager can send an alert. You can customize these alerts by choosing the severity level or threshold that will trigger the alert. Alerts are sent to the administrator console and can be configured to perform specific actions or notify the local machine.

- *How do I see alerts?*
- *What kinds of computer problems can generate alerts?*
- *Configuring severity levels for events*
- *Example: Configuring an individual alert for a disk space problem*

How do I see alerts?

Intel Server Manager can notify you of problems or other computer events by:

- Adding information to the *log*.
- *E-mailing* a notice.
- Running a program.
- *Shutting down or rebooting* a computer.
- Sending an SNMP trap to an SNMP management console on the network.
- Playing a *sound*.
- Displaying information in the *Pop-up alerts window*.
- Forwarding information to the Alert Management System (AMS), available with other LANDesk products such as LANDesk Management Suite..

Notes:

- The SNMP option is only available if the SNMP software is installed on the Intel Server Manager computer. This software is not included on the Intel Server Manager CD. SNMP is available as part of each supported Windows* platform. If Intel Server Manager doesn't detect the SNMP components when it loads, these options aren't available to select when configuring alert actions.
- To dismiss multiple pop-up alerts at one time, right-click one of the alerts and select an **Acknowledge all** option.

What kinds of computer problems can generate alerts?

Intel Server Manager monitors computers differently depending on the hardware and chipset that is installed. For example, chassis intrusion detection might not be available for all computers. Some of the events that Intel Server Manager can monitor are listed below:

- Applications or packages are added or removed on a computer.

- Hardware components (such as NICs, modems, drives, and memory) are added or removed on a computer.
- Errors in ECC memory have been detected.
- A system has been powered on, powered off, or rebooted remotely.
- Thresholds for system performance (such as virtual memory, drive space, voltages, temperatures, etc.) have been exceeded.
- Modem activity has been detected.

Configuring severity levels for events

Computer problems or events have some or all of the severity levels shown below. You can choose the severity level or threshold that will trigger the alert.

- **Informational**—Is available to support configuration changes, *BSA* events, discovery information, or computer events that manufacturers may include with their systems.
- **OK**—Notifies you when a problem has been resolved and returned to an acceptable level.
- **Warning**—Provides some advance warning of a problem before it reaches a critical point.
- **Critical**—Probably needs your immediate attention.

Depending on the nature of the event or computer problem, some severity levels don't apply and aren't included. For example, with the chassis intrusion event, the computer's chassis is either open or closed. If it is open, this can trigger an alert action with a severity of warning. Other events, such as Disk space and Virtual memory, include three severity levels (OK, Warning, and Critical).

Example: Configuring an individual alert for a local drive space

1. From the console of the managed computer, click **Management**, then click **Alerts**.
2. Click **Drive Space**.
3. Click the types of alerts you want to send and click **Apply**.
4. To set options for an alert (if applicable), click **Apply** to save your settings, then click **Set preferences**.

Setting polling frequency

Intel Server Manager uses the Microsoft Windows registry to store application options and state information. Several registry keys specify how often Intel Server Manager will poll, or check, for information relevant to alerts.

Important—Exercise extreme caution when editing the registry. The following steps are recommended only if you are knowledgeable about the process and implications of editing registry settings. We recommend that you make a backup copy of the registry file prior to making changes.

To set the polling frequency

1. Access the Windows Registry Editor.

The polling timers are located under HKLM\Software\Intel\Server Manager\CurrentVersion\CCS and HKLM\Software\Intel\Server Manager\CurrentVersion\conf\Thresholds.

2. Browse to the value PollingFrequency in any of the polling timers listed in the table below.

Polling timer	Default frequency
Services	3 min (180 sec)
Disk change	1 min (60 sec)
SMART check	10 min (600 sec)
Disk space	1 min (60 sec)
Memory usage	1 min (60 sec)
ECC memory error check	10 min (600 sec)
Application change	10 min (600 sec)
NIC change	3 min (180 sec)
Modem change	3 min (180 sec)
Power supply change	1 min (60 sec)

3. Enter a new frequency in number of seconds.
4. Reboot your computer for the changes to take effect.

Note—If the polling is set to occur at too frequent of an interval, it may increase CPU usage and impact performance.

IPMI configuration

Use the IPMI configuration page to customize settings for communicating with *IPMI*-enabled systems. The features described below are available for in-band servers; if a server is out of band, only the power configuration and BMC user settings are available.

NOTE: It is strongly recommended that you do not change IPMI settings unless you are familiar with the *IPMI specification* and understand the related technologies involved in these settings. Improper use of these configuration options may prevent Intel Server Manager from successfully communicating with IPMI-enabled computers.

The following configuration options are available:

- *Restore default BMC settings*
- *LAN and serial configuration*
- *Watchdog timer settings*
- *Power configuration settings*
- *BMC username/password settings*

Restoring default BMC settings

If you have customized the BMC settings for a computer, you can restore them to the settings that Intel Server Manager uses when the product is installed, which include the following:

- IP synchronization is re-enabled
- LAN and serial channel configuration is reset to automatic settings:
 - All LAN and serial channels are enabled with an administrative privilege limit and no session limit
 - Per-message authentication is enabled, with MD5, MD2, straight password, and RMCP+ (IPMI 2.0 only) authentication methods
- Power configuration is restored to the recommended setting (restore computer to the state it was in when power was lost)
- The PEF (Platform Event Filtering) table is restored to Intel Server Manager defaults, which includes the Event destination in the LAN Configuration

Notes:

- BMC user name settings are not reset when BMC settings are restored.
- When a server is out of band, the Restore recommended settings option is not available.

To restore default BMC settings

1. Click **Management**, then click **IPMI configuration**.
2. Click **IPMI configuration**, then click **Restore recommended settings**.

Changing LAN and serial configurations

IPMI messages can be carried directly from the BMC over LAN and serial interfaces in addition to the computer's System Interface. Enabling LAN or serial communication allows the Intel Server Manager administrator console to receive IPMI-specific alerts even if the computer is powered down. The administrator console maintains this communication as long as the computer has a physical network connection with a valid network address, and as long as the computer's main power remains connected.

To change LAN and serial configuration settings

1. Click **Management**, then click **IPMI configuration**.
2. Click **LAN and serial configuration**.
3. Select an access method for LAN and for serial access.

4. Click **Apply**.

Notes:

- If you select custom configuration, click the **Customize** option to specify configuration details.
- For serial modem operation, you may need to configure the server board's BIOS and jumper settings. See the documentation that same the particular server for details

Changing watchdog timer settings

IPMI provides an interface for the BMC watchdog timer. This timer can be set to expire periodically, and is configured to initiate certain actions if it expires (such as power cycling). Intel Server Manager is configured to reset the timer periodically so it does not expire; if the computer becomes unavailable (for example, it is powered down or hangs), the timer is not reset and it then expires, which initiates the action.

You can specify how much time to allow before the timer expires and select an action to perform if it does expire.

To change watchdog timer settings

1. Click **Management**, then click **IPMI configuration**.
2. Click **Watchdog timer settings**.
3. Check **Turn on the watchdog timer** to enable the timer.
4. Specify the frequency of checking the timer (number of minutes or seconds).
5. Select an action to initiate when the watchdog timer expires.
6. Click **Apply**.

Changing power configuration settings

When power is lost on an IPMI-enabled computer, you can specify what action should be taken when power is restored. It is recommended to restore the computer to whatever state it was in at the time power was lost, but you can also choose to keep it powered off or always power up the computer.

To change power configuration settings

1. Click **Management**, then click **IPMI configuration**.
2. Click **Power configuration**.
3. Select an option for when power is restored.
4. Click **Apply**.

Changing BMC user settings

Intel Server Manager authenticates to a BMC with a user name/password combination that is unique to the BMC (separate from any other Intel Server Manager user names). Intel Server Manager reserves the first user name so it can always communicate with the BMC. If the BMC

allows other user names to be defined, you can define user names with passwords for BMC authentication.

To change BMC user settings



1. Click **Management**, then click **IPMI configuration**.
2. Click **BMC user settings**.
3. To add or change a username, click **Edit**.
4. To clear the data for a user name, click **Clear**.

Monitoring computer health

Monitoring health

Intel Server Manager monitors important computer functions and resources so it can alert you to problems as soon as it becomes aware of them. Depending on the computer's hardware, resources and functions, Intel Server Manager can monitor any of the following:

- **Chassis intrusion**—Monitors when the system's chassis is opened.
- **Drive failure prediction**—Monitors a *S.M.A.R.T.* drive for potential disk failure.
- **Drive space**—Monitors how much drive space remains on each logical drive. *Thresholds* are configurable for each logical drive.
- **ECC error detection**—Monitors the detection of ECC (error-correcting code) memory.
- **Fan speeds**—Monitors the speed for cooling fans installed in the computer.
- **Performance**—Monitors performance data of counters you specify (for components such as drives, memory, network traffic, and so forth).
- **Power supplies**—Monitors the status of each power supply on the system.
- **Services**—Monitors the system services you have selected.
- **Temperatures**—Monitors the temperature of vital components in your system.
- **Virtual memory**—Monitors how much virtual memory remains available to the computer. Thresholds are configurable.
- **Voltages**—Monitors the power voltages on the computer's power supply lines.

When a problem occurs in one of the areas listed above, the computer's health status changes from Normal to either Warning or Critical, depending on the event and its severity. (The status icon for the computer will include a Warning  or Critical  icon.) You can observe a computer's health change using one of the following Intel Server Manager tools:

- **Summary**—The computer summary page displays a description of the problem.
- **System**—Under the System link in the left pane, click the item generating the health status change (such as Drives or Memory). The page for the item includes a description of the problem and steps you can take to resolve the problem.
- **Alerts**—ISM includes five different *alert actions* you can select to notify you of health changes.

You can select the health contributors that determine the computer's health status. By default all health contributors are selected. If you deselect an item it no longer contributes to the overall health, but you will still receive alerts for that item. For example, if you decide that Performance counters do not need to be included in overall health warnings for a server, you can deselect Performance. You will, however, receive any alerts you have selected for Performance counters.

For an out-of-band IPMI server, a limited number of health contributors can be monitored through the server's BMC. These are indicated with "(IPMI)" in the list of health contributors. These are not configurable, so they are monitored when the server is out of band whether or not you have deselected them on the list of health contributors.

When you receive health status notifications for a blade server or chassis management module (MM), you can view the details in the management module's web interface provided by the

manufacturer. On the summary page for the server or MM, click the health status notification to open the manufacturer's user interface.

To select health contributors

1. Click **Management**, then click **Health**.
2. On the Health page, select the items you want contributing to overall system health, then click **Apply**.

Using the taskbar icon

The Windows *taskbar* displays an icon you can use to launch Intel Server Manager. The taskbar icon also indicates the health status of your computer or other computers on the network. Placing the mouse pointer over the icon displays the health status and number of unacknowledged alerts received.

The taskbar icon indicates that the computer's health is currently in one of these three states:



Normal



Warning



Critical

The taskbar icon flashes when the system receives a new alert. It continues flashing until you acknowledge the alert. See *Configuring and using pop-up alerts* for more information.

To run Intel Server Manager from the taskbar

1. Right-click or double-click the taskbar icon.
2. Click **Manage this Computer**.

Selecting performance counters

The Intel Server Manager Performance counters page lets you select performance items that you want to monitor. You can monitor specific hardware components, such as drives, processors, and memory, or you can monitor OS components, such as processes or bytes/sec transferred by the system's Web server. When you select a performance counter you also specify the frequency for polling the item, as well as specify the performance thresholds and number of violations that are allowed before an alert is generated.

When a performance counter has been selected you can then *monitor performance* on the Performance page by viewing a graph with real time or historical data.

You can also set alert actions to trigger notification when a performance counter crosses an upper or lower threshold a predetermined number of times.

To select a performance counter to monitor

1. Click **Management**, then click **Performance counters**.
2. Click **Select performance counters to monitor**.

3. From the Objects column, select the object you want to monitor.
4. From the Instances column, select the instance of the object you want to monitor, if applicable.
5. From the Counters column, select the specific counter you want to monitor.
6. Specify polling interval and days to keep history.
7. In the **Alert after counter is out of range** drop-down list, specify the number of times the counter will be allowed to cross the thresholds before an alert is generated.
8. Specify upper and/or lower thresholds.
9. Click **Apply**.

Notes

- Performance log files can quickly grow in size; polling a single counter at a two second interval adds 2.5MB of information to the performance log daily.
- Changing the **Alert after counter is out of range** number lets you choose to focus on an issue when it is a persistent problem or when it is an isolated event. For example, if you are monitoring the bytes sent from a Web server, Intel Server Manager can alert you when the bytes/sec consistently runs high. Or, you can specify a low number such as 1 or 2 to get alerted whenever your anonymous FTP connections exceeds a certain number of users.

To set a performance alert action

1. Click **Management**, then click **Alerts**.
2. Click **Performance**.
3. Click the tab of the status type (OK or Warning) you want to set alerts for.
4. Click the types of alerts you want to send and click **Apply**.
5. To set options for an alert (if applicable), click **Apply** to save your settings, then click **Set preferences**.

Note—You must select a counter or counters to monitor before alerting can take place.

(This page intentionally left blank.)

Preferences

Alerts preferences

Use Alerts preferences for the following:

- *Configuring audio alerts*
- *Configuring e-mail and pager alerts*
- *Configuring and using pop-up alerts*
- *Configuring power cycle alerts*

Configuring audio alerts

Use the Audio alerts page to set audio notifications to play when certain events occur. The audio notification is played with a .WAV file that you specify in this page.

You can play an audio notification for Informational, OK, Warning, or Critical events.

To set an audio notification to play for specific events

1. Click **Preferences**, then click **Alerts**.
2. Click **Preferences: Audio alerts**, then check **Play audio alerts (.wav files)**.
3. In the text box of the event for which you want to play an audio notification, type the path and filename of the .WAV file. For example, C:\WINDOWS\Media\notify.wav. Repeat for other notifications.
4. When finished, click **Apply**.

Configuring e-mail and pager alerts

Use the E-mail alerts page to configure how you want Intel Server Manager to format and send alert-action e-mail messages. If you don't have access to an SMTP Internet mail server, this alert action won't work.

For information on configuring which events and severity levels trigger e-mail notices, see *Using alerts*.

Notes:

- In the event of a failed connection to the SMTP Internet mail server, Intel Server Manager will make continued attempts according to the delivery options you've specified. When Intel Server Manager successfully passes an e-mail notice to the SMTP server, it no longer has control of delivery for that notice.
- Intel Server Manager does not set e-mail alerts on SMTP servers that require authentication.

You can change these Intel Server Manager e-mail settings:

- **Outgoing mail server (SMTP)**—The SMTP Internet mail server that the alert action will send the message through.

- **To**—The e-mail address that will receive the alerts. Use a comma-separated list of e-mail addresses to notify multiple e-mail accounts. You can also send the message to a pager address such as 5551234567@ mobile.att.net.
- **From**—The e-mail address that will appear in the message's From field. This must be a valid e-mail address.
- **Subject**—The message's subject text.
- **Body**—The message's body text
- **Parameter language**—The language of the parameters.
- **Delivery attempts**—How often Intel Server Manager should retry failed connections to the SMTP mail server you specified.
- **Minutes between attempts**—How long Intel Server Manager should wait to retry failed connections to the SMTP mail server you specified.

The subject and body can contain dynamic parameters that get replaced when the e-mail message is sent. You can use up to 10 of these parameters in your message:

- %% = %
- %D = Description
- %N = Computer name
- %S = Severity
- %T = Time (UTC/Greenwich Mean Time)

To set e-mail and pager alerts preferences

1. Click **Preferences**, then click **Alerts**.
2. Click **Preferences: E-mail alerts**, then check **Send e-mail alerts**.
3. Configure the e-mail options.
4. Click **Apply**.

Configuring and using pop-up alerts

The pop-up alerts window displays information about events that have occurred on your computer. You can configure which events and which severity levels trigger the pop-up alerts window to open. See *Using alerts* for more information.

Notifications are cleared from the pop-up alerts window each time you log out or the computer shuts down. However, notifications are not deleted from the *notification log* when the computer boots.

Note—If you're running Windows * XP with Fast User Switching enabled:

- The pop-up alerts window appears for the current user who is logged on to the computer. Other users will see a flashing Intel Server Manager icon in the taskbar as described in *Using the taskbar icon*. These users can display the pop-up alerts window by clicking the Intel Server Manager icon.
- If multiple users are logged on and the current user dismisses the pop-up alerts window, other users will still see the notification when they switch back.

Setting pop-up alerts preferences



You can change the settings for pop-up alert display.

1. Click **Preferences**, then click **Alerts**.
2. Click **Preferences: Pop-up alerts**, then check **Display pop-up alerts**.
3. Configure the limit and hotkey options.
4. Click **Apply**.

Using options within the pop-up alerts window

In addition to the computer name and event details, the pop-up alerts window includes the following options:

- **More info**—Connects you to the computer that generated the notification, displays a more detailed description of the problem, or provides suggestions for corrective action.
- **Acknowledge**—Clears the current notification from the pop-up alerts window and displays the next notification. The pop-up alerts window closes when the last notification has been cleared.
- **Do not display new notifications**—Prevents the pop-up alerts window from appearing when new notifications are received. However, the system tray icon flashes to notify you when new alerts have been received.
- **Advanced options**—Right-click in the pop-up alerts window message box to access these advanced options:
 - **Acknowledge all**—Clears all notifications and closes the pop-up alerts window.
 - **Copy**—Copies the current notification to the clipboard.

Use the Page-Up  and Page-Down  arrows to cycle through a circular list of accumulated unacknowledged notifications.

Note—If you aren't logged in, notifications from your computer are stored in the log file.

Displaying the pop-up alerts window

You can display the pop-up alerts window at any time by pressing the notification hotkey combination on the keyboard (**Ctrl+Alt+N** by default).

Configuring power cycle alerts

Use the Power cycle alerts page to cause the computer to shutdown or reboot when certain configured events occur.

To configure which events and which severity levels trigger power cycle alerts, see *Using alerts*.

Note—Power cycles may cause data loss on unattended machines.

To set power cycle alerts

1. Click **Preferences**, then click **Alerts**.
2. Click **Preferences: Power cycle alerts**, then check **Allow power cycle alerts**.

3. Configure power cycle options.
4. When finished, click **Apply**.

Use the options below to configure power cycle alerts.

- **When an event is received: Shut down/reboot**—The type of power cycle (shutdown or reboot) to occur when a configured event is received.
- **Seconds before the power cycle is initiated**—The amount of time between when an event is received and when the power cycle take place. A warning appears on the computer's screen showing the number of seconds until shutdown or reboot; this allows time to save data and close applications. If this option is set to 0 no warning is given.
- **Number of power cycles alerts before you must acknowledge**—How many times the computer will be shut down or rebooted before requiring you to acknowledge that you want it to continue power cycling when an event occurs. This is useful in cases where the power cycle is triggered by an event that will not be corrected by reboot. For example, it is possible to set an alert to cause a power cycle when a drive space threshold is crossed. Because a power cycle will not affect drive space usage, when the computer is powered on again, drive space usage will still exceed the threshold and will generate another event, causing another power cycle. Requiring acknowledgement after a certain number of power cycles before proceeding with another power cycle prevents the computer from continuously shutting down without allowing you to fix the problem.
- **Current number of alerts that caused a power cycle**—The number of alert-driven power cycles that have occurred since the last acknowledgement.
- **Acknowledge**—Resets the current number of alert-driven power cycles to zero.

Reference information

Troubleshooting

Installing Intel Server Manager on computers with a bridge agent

If you install Intel Server Manager on clients or servers that have a previously installed Intel Server Manager bridge agent, be aware that the Intel Server Manager agent removes the existing bridge agent during installation. Any custom BMC configurations that may have been defined on the computer are lost.

IPMI not detected on Linux server with OpenIPMI

If Intel Server Manager is installed on a Linux server that has the OpenIPMI device driver installed, the Intel Server Manager IPMI driver (LDIPMI) will not load and IPMI functionality for that server will not be detected. Intel Server Manager currently does not support OpenIPMI.

System information not available on Windows Server 2003 servers

When you use the Intel Server Manager administrator console to manage a server running Windows Server 2003, you may see a message that information is not available for some system inventory items (such as fans, voltages, storage devices, etc.). This can be due to problems in the WMI repository (also called the CIM repository) for that machine. In this case the problem cannot be resolved in Intel Server Manager because the ability to manage the machine depends on the presence of an existing CIMV2 schema in the repository. This can only be resolved by restoring the WMI repository (refer to Windows Server 2003 support documentation for details).



"Connection failed" error message

Problem: IPMI server on Other computers list cannot be managed

In rare cases an IPMI server may be displayed on the Other computers list but cannot be added to the My computers list. This occurs if the server was in band at the time it was last discovered but then changes to out-of-band status and is out of band when you attempt to add it to My computers.

If this happens you will receive a "Connection failed" error message when you try to manage the computer.

If this occurs, you need to discover the computer again. This will list the computer with "out of band" status on the Other computers list, and you can then add the computer to the My computers list and manage it as you would any other out-of-band computer.

1. Click  to clear the Other computers list.
2. Click  to discover computers.
3. If needed, refresh the Other computers list.

4. Select the computer and click  to add it to My computers.

"The computer(s) could not be managed (general failure)" error message

General errors are generated by the manage/add computer system and are formatted as "The computer(s) could not be managed (general failure %s)" where %s is replaced with a number identifying the specific error.

Number	Meaning
0	A general catastrophic error occurred (possibly dealing with Windows Sockets).
1	An invalid network was found. The computer may have been attached to a network without a DNS.
2	Reserved for future use.
3	Invalid command line.
4	No computers selected to be managed.
5	Memory allocation error.

Windows Internet Connection Firewall conflicts with port settings

If you install Intel Server Manager on a computer running Windows Server 2003 SP1 and have Internet Connection Firewall (ICF) enabled, you may experience problems due to ICF blocking ports used by Intel Server Manager. To allow Intel Server Manager to function with ICF enabled, make the following changes to the advanced settings in Windows Network Connections.

1. Open **Network Connections** from the Windows **Start** menu.
2. Right-click **Local Area Connections** and select **Properties**.
3. Click the **Advanced** tab, then click **Settings**.
4. Click **Add** to enter each of the following port settings. Enter the IP address of the computer on which the administrator console is installed.

Description	External Port	Port Type
LANDesk Management (BCP1)	31770	TCP
LANDesk Management (BCP2)	6787	TCP
LANDesk Management Agent	9593	TCP
LANDesk Management Agent (Certificate)	9594	TCP
LANDesk Discovery (PDS2)	9595	UDP
LANDesk Discovery (IPMI)	623	UDP
LANDesk Discovery (CBA8)	9595	TCP

Blade chassis cannot be managed due to failed DNS resolution

For Intel Server Manager to manage a blade chassis management module (MM), your network must have a properly configured method for DNS resolution and reverse DNS lookup must be available. In addition, there must be unrestricted SNMP access to the MM. If you are unable to

manage a management module, review the following settings. After changing any of these settings, restart the MM to ensure that the new settings are in effect.

- **The DNS protocol must be enabled on the MM.** On the web interface for the MM, make sure that DNS is enabled and that a valid DNS server IP address is referenced. On the MM's web interface, click **MM Control | Network Protocols | Domain Name System (DNS)** to make this change.
- **There must be one available SNMP community name on the MM.** Management modules are typically configured with one unassigned community name, but if you have changed this configuration Intel Server Manager may be unable to assign a community name for its own use. On the MM's web interface, click **MM Control | Network Protocols | Simple Network Management Protocol (SNMP)** to verify this setting.
- **SNMP access must be unrestricted across the network.** If the MM is behind a router, make sure there is no SNMP filter on the router. (See your router documentation for more information.)

IPMI

Intel Server Manager includes support for Intelligent Platform Management Interface (IPMI). IPMI is a specification developed by Intel, *H-P, *NEC, * and Dell* to define the message and system interface for management-enabled hardware. IPMI contains monitoring and recovery features that let you access many features regardless of whether the machine is turned on or not, or what state the OS may be in. For an overview of IPMI from Intel, see the *IPMI Overview Guide*.

IPMI monitoring is based on the BMC (Baseboard Management Controller). The BMC operates on standby power and autonomously polls system health status. If the BMC detects that any elements are out of range, you can configure the resulting actions IPMI can take, such as logging the event, generating alerts, or performing automatic recovery actions such as system power-down or reset.

You must have SMBIOS 2.3.1 or higher installed in order for the BMC to be detected on the system. If the BMC is not detected, you may not see some IPMI information in reports, exports, and so forth.

IPMI defines common interfaces to the hardware used to monitor server physical health characteristics, such as temperature, voltage, fans, power supplies, and chassis intrusion. In addition to health monitoring, IPMI includes other system management capabilities including automatic alerting, automatic system shutdown and restart, remote restart and power control capabilities, and asset tracking.

Intel Server Manager supports IPMI versions 1.5 and 2.0 (which is backward-compatible with version 1.5). New features in version 2.0 include integrated Serial Over LAN management (SOL) and serial redirection over LAN, enhanced RMCP+ packet formats (authentication and encryption algorithms), enhanced discovery and support for new OEM payload types, firmware firewall (which restricts the execution of certain commands from a given interface), and continued support for OEM value-added feature integration.

The Intel Server Manager menu choices vary slightly for an IPMI-enabled system, depending on the state of the operating system.

Management features for IPMI-enabled systems

Monitoring capabilities depend on what has been installed on the server being monitored. Any IPMI-enabled system with a baseboard management controller (BMC) can be monitored by the administrator console in limited ways. Additional monitoring features are added when the Intel

Server Manager bridge agent is installed, and full-featured management is available when the Intel Server Manager server console is installed. In addition, the server console can be installed on a server that is not IPMI-enabled. The table below compares the functionality of these four options.

	BMC*	BMC + bridge agent	BMC + server console	Server console (non-IPMI)
Out of band management enabled	X	X	X	
In band management enabled			X	X
Server can be discovered	X	X	X	X
Read environment sensors	X	X	X	ASIC only
Power on/off remotely	X	X	X	X
Read & clear event log	X	X	X	
Configure alerts	X	X	X	X
Read OS information		X	X	X
Graceful shutdown		X	X	X
Read SMBIOS information (processor, slots, memory)		X	X	X
IP syncing (OS to BMC)		X	X	
Watchdog timer		X	X	
BMC communicates with admin console	X	X	Out of band only	
Local Intel Server Manager components communicate with admin console			X	X
Full range of Intel Server Manager management features			X	

*Standard BMC. The mini BMC (mBMC) is a scaled-down version of a baseboard management controller. It has the functionality listed above, with limitations such as the following:

- Does not support serial over LAN (SOL) redirection
- Has only one username for BMC management
- Uses only one channel for communicating with the BMC
- Has a smaller system event log (SEL) repository
- The bridge agent is not supported on mini BMC platforms

Intel Server Manager services

On Windows * 2000, Windows 2003, and Windows XP, Intel Server Manager runs a number of services, depending on the components installed:

- **SSM**—Intel System Space Manager. Loads and unloads Intel Server Manager components (such as the *HTTP server*, node discovery engine, node log file, health manager, store and forward, and *SNMP*) as they are needed by Intel Server Manager.

- **BSA**—Intel Bootstrap Agent. Enables the discovery of Intel Server Manager computers and provides a secure mechanism to transfer packages, mainly BIOS and driver updates.
- **LSM_WBA**—ISM WinBridge Agent.
- **LANDesk Message Handler Service**—Monitors for modem calls made and received, and triggers alert events.
- **Intel Server Manager SNMP Service**—Receives SNMP platform event traps directly from the BMC and relays them to the Intel Server Manager event system.
- **USM**—User Space Manager. Although not a service, USM starts for each user at log on. It houses tray icons and pop-up alerts.
- **Resident Agent**—Enables security features in Intel Server Manager. This service will appear in the Windows Firewall Exceptions list on Windows XP SP2.
- **Intel Intel Server Manager WDT**—Watchdog timer reset service (IPMI-enabled computers only).

SNMP

Intel Server Manager uses Simple Network Management Protocol (SNMP) to provide support for:

- Alerting via SNMP. Intel Server Manager can directly forward *SNMP traps*.
- An administrator performing SNMP gets on managed computers.

Version information

Use Version information to view a list of files installed during the Intel Server Manager installation, and to view the availability of those files.

To view version information

1. In the top-right of the browser window, click **About**.
2. Click **Version Info**.
3. To exit, click **Back to about** or **Close** at the bottom of the screen.

Converting Celsius to Fahrenheit

Because temperature-monitoring computer hardware reports the temperature in degrees Celsius, users in the United States may want to convert the reported temperature to Fahrenheit. The table below lists the Fahrenheit equivalents to the Celsius values reported by Intel Server Manager. (The conversion formula is: $^{\circ}\text{F} = 9/5(^{\circ}\text{C}) + 32$)

$^{\circ}\text{C}$	$^{\circ}\text{F}$	$^{\circ}\text{C}$	$^{\circ}\text{F}$	$^{\circ}\text{C}$	$^{\circ}\text{F}$	$^{\circ}\text{C}$	$^{\circ}\text{F}$
0 $^{\circ}$	32.0 $^{\circ}$	26 $^{\circ}$	78.8 $^{\circ}$	51 $^{\circ}$	123.8 $^{\circ}$	76 $^{\circ}$	168.8 $^{\circ}$

1°	33.8°	27°	80.6°	52°	125.6°	77°	170.6°
2°	35.6°	28°	82.4°	53°	127.4°	78°	172.4°
3°	37.4°	29°	84.2°	54°	129.2°	79°	174.2°
4°	39.2°	30°	86.0°	55°	131.0°	80°	176.0°
5°	41.0°	31°	87.8°	56°	132.8°	81°	177.8°
6°	42.8°	32°	89.6°	57°	134.6°	82°	179.6°
7°	44.6°	33°	91.4°	58°	136.4°	83°	181.4°
8°	46.4°	34°	93.2°	59°	138.2°	84°	183.2°
9°	48.2°	35°	95.0°	60°	140°	85°	185.0°
10°	50.0°	36°	96.8°	61°	141.8°	86°	186.8°
11°	51.8°	37°	98.6°	62°	143.6°	87°	188.6°
12°	53.6°	38°	100.4°	63°	145.4°	88°	190.4°
13°	55.4°	39°	102.2°	64°	147.2°	89°	192.2°
14°	57.2°	40°	104.0°	65°	149.0°	90°	194.0°
15°	59.0°	41°	105.8°	66°	150.8°	91°	195.8°
16°	60.8°	42°	107.6°	67°	152.6°	92°	197.6°
17°	62.6°	43°	109.4°	68°	154.4°	93°	199.4°
18°	64.4°	44°	111.2°	69°	156.2°	94°	201.2°
19°	66.2°	45°	113.0°	70°	158.0°	95°	203.0°
20°	68.0°	46°	114.8°	71°	159.8°	96°	204.8°
21°	69.8°	47°	116.6°	72°	161.6°	97°	206.6°
22°	71.6°	48°	118.4°	73°	163.4°	98°	208.4°

23°	73.4°	49°	120.2°	74°	165.2°	99°	210.2°
24°	75.2°	50°	122.0°	75°	167.0°	100°	212.0°
25°	77.0°						

Glossary

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

A

AGP

Advanced Graphics Port. A high-performance bus type that uses short expansion slots for AGP video cards. AGP buses are targeted at 3D graphics applications and based on a set of performance enhancements to *PCI*.

AMS

Alert Management System. A component of Intel management products that provides various alerting capabilities, such as paging, Internet mail, and broadcasts.

ASF

Alert Standard Format. A standard which defines alerting and remote control interfaces to proactively manage networked devices when their operating system is absent.

ASIC

Application-Specific Integrated Circuit. A customized microchip which is designed for a specific application.

B

BIOS

Basic Input/Output System. A set of software routines generally stored in a firmware chip located on the motherboard. The BIOS is responsible for your computer's input/output activities, such as interpreting keystrokes and mouse clicks, displaying images and characters on the screen, and sending data to the printer.

blade server

A server designed for use in a space-saving rack with multiple servers that share power management, cooling systems, and other management features for improved efficiency. Blade servers are typically stored in a blade *chassis* that contains one or more chassis *management modules*.

BMC

Baseboard Management Controller. A microchip that autonomously polls system health status. The BMC operates on standby power and can take several actions should any elements go out of range.

BSA

Bootstrap Agent. A set of modules installed onto computers that securely enable the bootstrapping (loading and executing) and configuration of other software packages from a remote console application.

C

cache

A block of fast memory that holds data or instructions the processor is most likely to use next. A primary cache is built into the microprocessor. A secondary cache is external to the microprocessor and uses its own memory chips. The write policy of a memory cache can be implemented in two ways: a *write-through cache* and a *write-back cache*.

chassis

The frame or structure of a computer. A blade chassis is the frame that holds multiple *blade servers* and typically includes a chassis *management module* (MM) that enables integrated management of multiple blade servers.

CIM

Common Information Model. An industry standard for managing a computer's components. CIM is also sponsored by the Desktop management Task Force (DMTF). Intel Server Manager uses CIM to gather information about a computer's components.

CMM

Chassis *management module*.

COM1

First communications port (Communications 1). Because serial ports are often used for connecting long-distance communications devices (such as modems) to a computer, the serial ports on a computer are named "COM1" (Communications 1) and "COM2" (Communications 2).

CRC

Cyclical Redundancy Check. A network error-checking procedure that calculates a checksum of a *packet's* contents before sending the packet, then stores that checksum in the trailer of the packet to be delivered. When the packet arrives at its destination on the network, the checksum is recalculated to verify the data integrity. If a discrepancy exists, the originating computer receives a request to resend the packet.

D

DHCP

Dynamic Host Configuration Protocol. A communication protocol for managing *IP address* assignments within a network. IP addresses for nodes on the network can be static (one address for one node) or can be assigned dynamically (for example, if there are more computers than available IP addresses).

DIMM

Dual In-line Memory Module. A small circuit board that contains memory chips on both sides of the module. Like the *SIMM*, the DIMM is easily inserted into a socket on the motherboard to

increase the amount of RAM available to the computer. The DIMM connector tabs use 168 pins with separate contacts on each side of the circuit board. The dual contacts allow twice as much data to pass in and out of the DIMM. (DIMM also refers to the socket type designed to receive the DIMM circuit board.)

discover

Searching specified networks for computers.

DMA

Direct Memory Access. The process of moving data from devices (such as a hard drive) directly into memory. This process frees up the processor substantially so it can focus on other tasks.

DMA channel

One of seven channels (numbered 0-6) used to move data from devices (such as a hard drive) directly into memory.

DNS server

Domain Name Service server. Maintains a dynamic database of computers on the Internet with a network address (usually an IP address) and a meaningful domain name, such as "www.Intel.com." When you type a domain name in a browser to find an Internet resource, a DNS server finds the associated IP address of that resource.

E**ECC**

Error Correction Code. An advanced error detection protocol for system memory on a computer. This code can detect both single-bit and multi-bit errors and correct single-bit errors on the fly.

EDO

Extended Data Output. A type of memory chip technology that can increase the CPU's memory access time by 10 to 15 percent over a non-EDO chip. To achieve the performance increase, however, the computer must be designed to take advantage of the speed benefit EDO memory offers.

EISA

Enhanced Industry Standard Architecture. One of two immediate successors to the *ISA* bus standard. The EISA bus was developed by a consortium of IBM competitors to challenge IBM's *MCA* bus.

environment variables

Variables related to the user environment that are initialized on computer startup and used by the operating system and applications running on the environment.

expansion slots

Long, narrow sockets on a motherboard used to install custom expansion cards into a computer for extended functionality. For example, you can plug a network adapter into an expansion slot so the computer can connect to a network. Other examples of expansion cards include video cards, sound cards, and modems.

F**FAT**

File Allocation Table. A common file system supported by most operating systems. FAT is widely used and requires little overhead, but does not offer many of the features available in more advanced file systems, such as *NTFS* or *FAT32*.

FAT32

File Allocation Table 32-bit. *FAT32* supports larger disk sizes (up to 2 terabytes) than the original *FAT*. It also uses a smaller cluster size, which reduces the amount of slack space (unused space) in each cluster.

file system

The portion of an operating system responsible for managing, saving, and retrieving files on a hard drive or other media. Common file systems include *FAT*, *FAT32*, *NTFS*, *ext2*, *ext3*, and *ReiserFS*.

FRU

Field Replaceable Unit. On an IPMI-enabled system, a module or component which is typically replaced in its entirety as part of a field service repair operation.

G

gigahertz (GHz)

One billion cycles per second. A microprocessor's speed (also known as its clock speed), is measured in gigahertz. Because each computer instruction requires a fixed number of cycles, the clock speed determines how many instructions the microprocessor can execute in one second. A microprocessor that runs at 10 GHz executes 10 billion cycles per second.

H

hexadecimal

A base-16 system of counting used to enumerate and provide addresses for many aspects of computer circuitry, such as memory, *IRQs*, and network adapter addresses. The hexadecimal digits are: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F. These digits represent the decimal numbers 0 through 15. After counting to the digit F in hexadecimal, you continue counting in double digits from 10 to 1F (16–31 in decimal), 20 to 2F (32–47 in decimal), and so forth.

HTTP server

Hypertext Transfer Protocol server. A server computer that stores files, such as HTML Web pages, and serves those files to HTTP client computers as they are requested.

I

I/O address

A hexadecimal address in base memory used for input and output.

in-band

When a network element (such as a firewall, router, server, and so forth) is being managed by a wide area or local area network management tool (such as *SNMP*), it is considered to be “in-band.” See also *out-of-band*.

instrumentation

The executable code that provides CIM management functionality for a particular component. The instrumentation code is provided by the component manufacturer.

Interrupt Request (IRQ)

A prioritized signal line used by hardware devices to interrupt the processor and request processing attention. Each hardware device generally requires its own IRQ address--a number from 0 to 15 (0 to F in *hexadecimal*).

IP address

A number that identifies the location of a network and a local computer on a network. It is composed of four octets separated by decimals, such as 127.17.5.12. IP addresses are used exclusively with the *TCP/IP* network protocols.

IPMB

Intelligent Platform Management Bus. Name for the architecture, protocol, and implementation of a special bus that interconnects the baseboard and chassis electronics and provides a communications media for system platform management information.

IPMI

Intelligent Platform Management Interface. A specification developed to define the message and system interface for management-enabled hardware. IPMI contains monitoring and recovery features that allow management of the hardware regardless of whether the machine is turned on or not, or what state the OS may be in.

ISA

Industry Standard Architecture. The original bus standard used in IBM and compatible computers. ISA was later superseded by more technologically advanced bus architectures, such as *EISA*, *MCA*, *PCI*, and *SCSI*.

J**JBOD**

Just a Bunch Of Disks. Used to refer to hard disks that aren't configured according to RAID -- a subsystem of disk drives that improves performance and fault tolerance.

K

None

L**LIF socket**

Low Insertion Force socket. An older socket type used on early motherboards for processors and other chips. Unlike its successor, the *ZIF socket*, you must use considerable force when inserting a chip into a LIF socket, and a special tool or screwdriver is generally required to remove a chip from a LIF socket.

LPT1

First parallel printer port (Line Printer 1). Because parallel ports are typically used for connecting printers to a computer, the parallel port names LPT1 and LPT2 were named after the early "line printers" that connected to them (line printer 1, line printer 2, and so forth).

M**MAC address**

Media Access Control address (also known as the hardware address or node address). A unique six-byte hexadecimal address (such as 00AA00C778F7) that is permanently coded into the network adapter and can be used to identify a specific computer on a network.

management module (MM)

A special-use, single-board computer with processor, bus, memory, and peripherals that facilitates the management of multiple blade servers housed in a blade chassis. An MM typically monitors IPMI components, provides power and temperature management, and allows for out-of-band management. In Intel Server Manager the MM is managed as a unique system and individual blade servers are also managed individually as well as being part of an MM group.

MCA

Microchannel Architecture. A bus architecture developed by IBM as a successor to the ISA bus.

megahertz (MHz)

One million cycles per second. A microprocessor's speed (also known as its clock speed), is measured in megahertz. Because each computer instruction requires a fixed number of cycles, the clock speed determines how many instructions the microprocessor can execute in one second. A microprocessor that runs at 450 MHz executes 450 million cycles per second.

MIB file

Management Information Base. A text file that describes a component. MIB files are generally organized in a hierarchy of components, groups, attributes, and attribute values.

MM

See *management module*.

MOF

Managed Object Format. The file format used by CIM to describe components. MOF files are text files generally organized in a hierarchy of classes, instances, properties, and values.

N**NDIS**

Network Device Interface Specification. A standard that defines how the MAC sublayer (in the OSI model) communicates with the various protocol drivers. This interface is used to enable different protocols (such as TCP/IP, IPX*/SPX*, and NetBEUI) running in the same computer to communicate with the network adapter.

NTFS

New Technology File System. A proprietary, feature-rich file system developed by Microsoft and used in Windows NT*. Among other things, NTFS supports long filenames, file level security, and file compression.

O**out-of-band**

When a network goes down or is severely disrupted, a network management tool (such as SNMP) is rendered useless and network elements (such as a firewall, router, server, and so forth) cannot be managed by the tool. These out-of-band network elements can be managed by IPMI. See also *in-band*.

P**packets**

Discrete chunks of data, packaged with control and addressing information, that travel over a network cable between sending and receiving computers.

parallel port

A hardware port that is used to connect printers or other devices using parallel communication. Parallel ports and cables are generally used over short distances because "cross talk" (data from one wire bleeding over onto another) is a problem with parallel cables over long distances.

parity errors

Parity errors occur when a memory error-checking procedure finds that some data stored in memory has become flawed. Parity errors are generally caused by a physical problem in the memory chips and often signal that a memory chip is going bad.

PCI

Peripheral Component Interconnect. A bus architecture developed by Intel that has wide support as a successor to the original *ISA* bus.

PCMCIA

Personal Computer Memory Card International Association, also known as PC Card. An expansion card about the size of a credit card, originally developed for the portable computer market.

plug and play

A computer's ability to automatically detect and configure new hardware components when they are plugged in, without requiring you to first complete an installation procedure. With plug and play, you can use a new peripheral as soon as it is plugged in.

POST

Power-On Self-Test. A series of diagnostic tests run by a computer's BIOS when power is turned on. The POST determines whether system hardware is functioning properly; if any essential hardware is not functional, the boot process does not continue.

primary cache

Memory cache that is built into the microprocessor. The close proximity of a primary cache to the microprocessor's circuitry gives a primary cache more speed-up potential than a secondary cache.

primary gateway

In a TCP/IP network, the router that all network packets are sent to if their ultimate destination is not on the local network.

provider

The CIM instrumentation that collects and manages data from CIM components.

proxy server

A server that resides on the network between an application (such as a Web browser), and another server (such as an HTTP server). Proxy servers improve performance by caching and fulfilling requests for files that have been previously accessed by the proxy server. Proxy servers also provide security for the network by filtering requests made to the server.

Q

None

R

RAID

Redundant Array of Independent (or Inexpensive) Disks, a category of disk drives that employ two or more drives in combination for fault tolerance and performance. RAID disk drives are used frequently on servers but aren't generally necessary for personal computers.

resolution

The number of tiny individual picture elements ("pixels") of a screen that combine to make up a screen display. A high resolution (1280 x 1024) uses many more pixels than a low resolution (640 x 480) and yields a sharper screen image. Higher resolutions are generally selected by users with larger monitors to achieve a more economical use of the large screen's viewing area.

S

SCSI

Small Computer Systems Interface. A bus type that allows up to seven SCSI devices to be chained together and share a common bus. Without processor intervention, SCSI devices can arbitrate which device in the chain has access to the bus at any given time. Two SCSI devices (such as a SCSI hard drive and a SCSI tape drive) can even relay data directly between each other without processor intervention.

SDR

Sensor Data Record. A data record that provides platform management sensor type, locations, event generation, and access information.

secondary cache

Memory cache that uses a cache controller and memory chips that are external to the microprocessor. Secondary cache does not offer the same degree of speed-up potential as primary cache. However, it can be considerably larger than a primary cache and therefore hold more instructions and data.

serial port

A hardware port that is used to connect serial devices (modem, mouse, and keyboard) to the computer. Serial ports convert the computer's parallel data into serial data that can be sent over a serial cable one bit (or voltage pulse) at a time. Serial ports and cables are used for long-distance communication to eliminate the "cross talk" (data from one wire bleeding over onto another) that can occur with parallel communication over long distances. Serial ports are also used to connect the mouse and keyboard to a computer. These devices don't send much data and therefore don't require the extra bandwidth of a parallel cable.

SIMM

Single In-line Memory Module. A small circuit board that contains usually eight or nine memory chips in a single bank. The SIMM is easily inserted into a socket on the motherboard to increase the amount of memory available to the computer.

Slot 1

The processor socket type used for some Intel® Pentium® processors. Slot 1 uses a 242-contact slot that accepts a processor packaged as a Single Edge Contact (SEC) cartridge. A

motherboard has one or two Slot 1s. Slot 1 only supports communication between the L2 cache and processor at half the processor's clock speed.

Slot 2

The processor socket type used for the Intel® Pentium® II Xeon™ processors. Slot 2 uses a 330-contact slot that accepts a processor packaged as a Single Edge Contact (SEC) cartridge. The Slot 2 design allows the processor to communicate with the L2 cache at the processor's full clock speed.

slot type

The type of expansion slots available on the computer's motherboard, such as *ISA*, *EISA*, *MCA*, *PCI*, *SCSI*, or *AGP*. (Not to be confused with the processor's socket types: Slot 1 and Slot 2.)

S.M.A.R.T.

Self Monitoring Analysis and reporting Technology. A drive technology that monitors its own health and reports potential problems before they occur.

SNMP

Simple Network management Protocol. A network management protocol that is part of the standard TCP/IP protocol suite. Intel Server Manager can snap in to an SNMP management console, which can receive and manage SNMP traps to monitor network devices and notify of extraordinary events or problems that occur on the network.

SNMP management console

A computer on the network that has software installed to receive and manage SNMP traps. Some products commonly used for this purpose include Microsoft Systems management Server, HP OpenView Network Node Manager*, CA Unicenter Frameworks*, and IBM/Tivoli NetView*.

SNMP trap

A notification of some network event that SNMP sends to a specified destination, usually an SNMP management console.

SSL

Secure Sockets Layer. The most commonly used protocol for secure message transfer on the Internet. When establishing an HTTP connection that requires SSL security, the URL begins with "https" to indicate that the message is transmitted over the secure layer.

subnet mask

A 32-bit number composed of four octets separated by decimals, such as 255.255.255.0. The subnet mask is paired with an *IP address*, such as 127.17.5.12, to tell an IP router which octets in the IP address are the network ID and which octets are the node ID. A subnet mask of 255.255.255.0, for example, would indicate that the first three octets of an IP address (such as 127.17.5) are the network ID, and the last octet of the IP address (such as .12) is a node ID. (The valid numbers that can be used in a subnet mask are 255, 254, 252, 248, 240, 224, 192, 128, and 0.)

T**taskbar**

A Windows toolbar that usually appears at the bottom of the screen (although it can be moved to the top or either side of the screen). The taskbar includes the Windows Start menu, buttons representing the running applications, and a system tray (on the far right side of the taskbar) which includes the current time and icons for various tools and programs.

TCP/IP

Transmission Control Protocol/Internet Protocol. The basic protocol used for Internet (and network) communication.

threshold

A configurable value that, if passed, can trigger an alert action. You can set the thresholds for some system events, such as available disk space and memory.

U**UDP**

User Datagram Protocol. A connectionless transport-layer protocol commonly used in the TCP/IP protocol family. Unlike TCP, when a UDP packet is sent over the network, UDP makes no effort to verify that the packet was successfully received on the other end.

UNC

Universal Naming Convention or Uniform Naming Convention. A format for specifying the location of resources (such as computers and printers) on a network. A UNC name uses this format:

`\\computer name\shared resource pathname.`

Example: `\\My computer\My documents\file.txt`

V

None

W**write-back cache**

A write-back cache writes data into the cache, then periodically checks for discrepancies between cache data and memory data. (Discrepancies can occur, for example, from a hard drive transferring data directly into memory via *DMA*). Write-back cache is faster than write-through cache, but the overhead to monitor discrepancies between memory and cache makes write-back cache more expensive.

write-through cache

A write-through cache writes the same data into memory and cache in a single operation. A write-through cache is slower than a write-back cache, but potentially safer because it guarantees that cache data and corresponding memory data are always the same.

X

None

Y

None

Z**ZIF socket**

Zero Insertion Force (ZIF) socket is a socket type used on motherboards for processors and other chips. Unlike the *LIF socket*, little pressure is needed to seat a chip into a ZIF socket, and a special tool or screwdriver is not required to remove a chip from a ZIF socket. The ZIF socket was designed to reduce the risk of accidentally bending a pin (or whole row of pins) on an expensive processor when seating the chip into a socket.

Copyright and trademark notice

This *Intel® Server Manager 8.40 Server Guide for Windows*, as well as the software described in it is furnished under license and may only be used or copied in accordance with the terms of the license. The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document.

Except as permitted by such license, no part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means without the express written consent of Intel Corporation.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. Intel products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

Intel may make changes to specifications and product descriptions at any time, without notice.

Intel, Pentium, Xeon, and Celeron are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2004, 2005 Intel Corporation.

Copyright © 2004, 2005 LANDesk Software, Ltd. All rights reserved.

Index

A	
adapter information.....	18
Administrator system requirements	2
alert actions, drives.....	18
alert actions, memory	21
alert actions, operating systems	26
alert actions, performance	28
alert actions, sensors.....	32
alert actions, voltage.....	35
applications, installed on a computer	20
asset management	15
asset number of computer.....	15
audio device.....	23
B	
Baseboard Management Controller.....	59
BIOS	16
BIOS, manufacturer	16
BIOS, serial number	16
BIOS, version.....	16
BMC	59
BMC configuration	46
C	
Celsius, converting to Fahrenheit.....	62
certificate, security	5
chassis fans	19
client system requirements.....	2
computer memory.....	21
computer motherboard	23
computer name.....	15
computer summary	11
computer, asset number.....	11
computer, serial number.....	11
configuration changes	37
console redirection	9
contact information.....	15
control, assets	15
copyright notice.....	73
D	
default gateway.....	24
desktop summary.....	11
device drivers.....	18
device, multimedia	23
DHCP server	24
dictionary of terms.....	63
discrete sensors.....	32
display	18
documentation	7
drive space, setting thresholds for	18
drivers	18
drives	18
E	
encryption of data	5
environment variables.....	19
events, hardware	38
F	
Fahrenheit--converting from Celsius.....	62
fans	19
field replaceable unit.....	20
frequency of polling.....	44
FRUs.....	20, 59
G	
glossary of terms.....	63
H	
hardware events	38
I	
I/O ports	30
information, motherboard.....	23
installation, troubleshooting	57

installed applications	20	physical memory	21
installing.....	20, 37	polling timers.....	44
Intelligent Platform Management Interface	59	ports	30
Internet Explorer	2	power configuration, IPMI	46
IPMI	59	power off a computer remotely	9
IPMI configuration.....	46	power on a computer remotely	9
K		power options.....	9
keyboards/mouse	21	processes.....	32
L		processor fans	19
LAN and serial connection, IPMI	46	programs installed on a computer	20
laptop summary	11	R	
Linux system requirements.....	2	reboot a computer remotely.....	9
list of applications on computer	20	remotely power off, power on, or reboot computers.....	9
log, hardware events	38	resolutions, supported monitor	18
M		routers.....	2
management of assets	15	S	
memory.....	21	security.....	5
MIDI device.....	23	sensors	32
mixer device.....	23	serial number, operating system.....	26
model, motherboard	23	serial over LAN (SOL) connection	9
monitor information	18	serial ports	30
monitoring configuration changes.....	37	server summary	11
motherboard	23	server system requirements	2
mouse/keyboards	21	services, Windows	61
multimedia	23	set thresholds for drives.....	18
N		set thresholds, memory	21
network	24	SNMP.....	61
number of network adapters.....	24	software	20, 37
numeric sensors	32	start process	32
O		stop process.....	32
operating system on computer	11	subnet mask.....	24
operating systems.....	26	subnets	2
OS.....	26	summary of computer	11
P		system requirements	2
parallel ports	30	T	
PCI hot-plug.....	27	TCP/IP address.....	24
performance.....	28		

terminating a process	32	video device	23
terms	63	viewing configuration changes.....	37
thresholds, memory	21	viewing fan information	19
thresholds, setting for drive space.....	18	viewing motherboard information.....	23
trademark notice	73	viewing statistics for processes	32
troubleshooting	57	virtual memory	21
turning off a computer remotely.....	9	voltages.....	35
turning on a computer remotely.....	9	W	
V		watchdog timer, BMC	46
variables, environment	19	Windows services	61
version information	62	Windows System Monitor information	28
version, operating system.....	26	WINS server.....	24