lenovo

Integrated Management Module User Guide

ThinkThinkThinkServerThink

Integrated Management Module

lenovo

User Guide

Note: Before using this information and the product it supports, read the general information in Appendix B, "Notices," on page 99.

First Edition (July 2009)

Contents

Chapter 1. Introduction

The Integrated Management Module (IMM) consolidates the service processor functionality, Super I/O, video controller, and remote presence capabilities in a single chip on the server system board. The IMM replaces the baseboard management controller (BMC) and Remote Supervisor Adapter II in Lenovo® ThinkServer™ servers.

Before the IMM was used in Lenovo servers, the baseboard management controller (BMC) and basic input/output system (BIOS) were the standard systems-management hardware and firmware. ThinkServer servers used BMC service processors to manage the interface between systems-management software and platform hardware. The Remote Supervisor Adapter II and Remote Supervisor Adapter II Slimline were optional controllers for out-of-band server management.

The IMM offers several improvements over the combined functionality of the BMC and the Remote Supervisor Adapter II:

- Choice of dedicated or shared Ethernet connection.
- One IP address for both the Intelligent Platform Management Interface (IPMI) and the service processor interface.
- Embedded Dynamic System Analysis (DSA).
- Ability to locally or remotely update other entities without requiring a server restart to initiate the update process.
- Remote configuration with Advanced Settings Utility (ASU).
- Capability for applications and tools to access the IMM either in-band or out-of-band.
- Enhanced remote-presence capabilities.

Unified Extensible Firmware Interface (UEFI) replaces BIOS in ThinkServer servers. The basic input/output system (BIOS) was the standard firmware code that controlled basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard. The server firmware offers several features that BIOS does not, including UEFI 2.1 compliance, iSCSI compatibility, and enhanced reliability and service capabilities. The Setup Utility provides server information, server setup, customization compatibility, and establishes the boot device order.

Notes:

1. The server firmware is occasionally called UEFI in this document.
2. The server firmware is fully compatible with non-UEFI operating systems.

This document explains how to use the functions of the IMM in a Lenovo Thinkserver server. The IMM works with the server firmware to provide systems-management capability for ThinkServer servers.

This document does not contain explanations of errors or messages. IMM errors and messages are described in the *Hardware Maintenance Manual* that came with your server.

If firmware and documentation updates are available, you can download them from the Lenovo Support Web site. The IMM might have features that are not

described in the documentation, and the documentation might be updated occasionally to include information about those features, or technical updates might be available to provide additional information that is not included in the IMM documentation.

Note: Changes are made periodically to the Lenovo Support Web site. Procedures for locating firmware and documentation might vary slightly from what is described in this document.

To check for firmware updates, complete the following steps.

1. Go to http://www.lenovo.com/support.
2. Enter your product number (machine type and model number) or select **Servers and Storage** from the **Select your product** list.
3. Select **Servers and Storage** from the **Brand** list.
4. From the **Family** list, select the name of your server, and click **Continue**.
5. Click **Downloads and drivers** to download firmware and driver updates.

To check for documentation updates, complete the following steps:

1. Go to http://www.lenovo.com/support.
2. Enter your product number (machine type and model number) or select **Servers and Storage** from the **Select your product** list.
3. Select **Servers and Storage** from the **Brand** list.
4. From the **Family** list, select the name of your server, and click **Continue**.
5. Click **User's guides and manuals** for documentation.

IMM features

The IMM provides the following functions:

- Around-the-clock remote access and management of your server
- Remote management independent of the status of the managed server
- Remote control of hardware and operating systems
- Web-based management with standard Web browsers

There are two types of IMM functionality: IMM Standard and IMM Premium. For information about the type of IMM hardware in your server, see the documentation that came with the server.

IMM Standard has the following features:

- Access to critical server settings
- Access to server vital product data (VPD)
- Advanced Hardware Failure Prediction
- Automatic notification and alerts
- Continuous health monitoring and control
- Choice of a dedicated or shared Ethernet connection
- Domain Name System (DNS) server support
- Dynamic Host Configuration Protocol (DHCP) support
- E-mail alerts
- Embedded Dynamic System Analysis (DSA)
- Enhanced user authority levels

- LAN over USB for in-band communications to the IMM
- Event logs that are time stamped, saved on the IMM, and can be attached to e-mail alerts
- Industry-standard interfaces and protocols
- OS watchdogs
- Remote configuration through Advanced Settings Utility (ASU)
- Remote firmware updating
- Remote power control
- Seamless remote accelerated graphics
- Secure Web server user interface
- Serial over LAN
- Server console redirection
- Simple Network Management Protocol (SNMP) support
- User authentication using a secure connection to a Lightweight Directory Access Protocol (LDAP) server

IMM Premium has the following features:

- Remote presence, including the remote control of a server
- Operating-system failure screen capture and display through the Web interface
- Remote disk, which enables the attachment of a diskette drive, CD/DVD drive, USB flash drive, or disk image to a server

Note: The following features of the Remote Supervisor Adapter II are not in the IMM:

- Display of server MAC addresses
- Multiple NTP server entries
- Dynamic DNS support

Upgrading from IMM Standard to IMM Premium

If your server has IMM Standard functionality, you can upgrade to IMM Premium by purchasing and installing a virtual media key on your server system board. No new firmware is required.

Comparing the IMM to other systems-management hardware in ThinkServer servers

The following table compares IMM features with baseboard management controller (BMC) and Remote Supervisor Adapter II features in ThinkServer servers.

Note: Like the BMC, the IMM uses the standard Intelligent Platform Management Interface (IPMI) specification.

Table 1. Comparison of the IMM features and combined BMC and Remote Supervisor Adapter II features in ThinkServer servers

Description	BMC with Remote Supervisor Adapter II (TS100, TS100, TS100x, RS110, and RD120)	IMM(RD210, RD220, and later)
Network connections	BMC uses a network connection that is shared with a server and an IP address that is different from the Remote Supervisor Adapter II IP address. Remote Supervisor Adapter II uses a dedicated systems-management network connection and an IP address that is different from the BMC IP address.	The IMM provides both BMC and Remote Supervisor Adapter II functionality through the same network connection. One IP address is used for both. The user can choose either a dedicated or a shared network connection.
Update capabilities	Each server requires a unique update for BMC and Remote Supervisor Adapter II. BIOS and diagnostic tools can be updated in-band.	One IMM firmware image can be used for all of the applicable servers. The IMM firmware, server firmware, and Dynamic System Analysis (DSA) firmware can be updated both in-band and out-of-band. The IMM can update itself, the server firmware, and the DSA firmware either locally or remotely without requiring the server to be restarted to initiate the update process.
Configuration capabilities	Configuration changes with the Advanced Settings Utility (ASU) are available only in-band. The system requires separate configurations for BMC, Remote Supervisor Adapter II, and BIOS.	The ASU can run either in-band or out-of-band and can configure both the IMM and the server firmware. With the ASU, you can also modify the boot order, iSCSI, and VPD (machine type, serial number, UUID, and asset ID). The server firmware configuration settings are kept by the IMM. Therefore, you can make server firmware configuration changes while the server is turned off or while the operating system is running, and those changes are effective the next time the server is started. The IMM configuration settings can be configured in-band or out-of-band through the following IMM user interfaces: • Web interface • Command-line interface • SNMP
Operating-system screen capture	Screen captures are performed by the Remote Supervisor Adapter II when operating-system failures occur. The display of screen captures requires a Java™ applet.	This feature is available only with IMM Premium. Screen captures are displayed directly by the Web browser without the need for a Java applet.

Table 1. Comparison of the IMM features and combined BMC and Remote Supervisor Adapter II features in ThinkServer servers (continued)

Description	BMC with Remote Supervisor Adapter II (TS100, TS100, TS100x, RS110, and RD120)	IMM(RD210, RD220, and later)
Error logging	The BMC provides a BMC system-event log (IPMI event log). The Remote Supervisor Adapter II provides a text-based log that includes descriptions of events that are reported by the BMC. This log also contains any information or events detected by the Remote Supervisor Adapter II itself.	The IMM has two event logs: 1. The system-event log is available through the IPMI interface. 2. The chassis-event log is available through the other IMM interfaces. The chassis-event log displays text messages that are generated using the Distributed Management Task Force specifications DSP0244 and DSP8007. **Note:** For an explanation of a specific event or message, see the *Hardware Maintenance Manual* that is available on the Lenovo Support Web site at http://www.lenovo.com/support.
Monitoring	The BMC with Remote Supervisor Adapter II has the following monitoring capabilities: • Monitoring of server and battery voltage, server temperature, fans, power supplies, and processor and DIMM status • Fan speed control • Hardware Failure Prediction • System diagnostic LED control (power, hard disk drive, activity, alerts, heartbeat) • Automatic Server Restart (ASR) • Automatic BIOS Recovery (ABR)	The IMM provides the same monitoring capabilities as the BMC and Remote Supervisor Adapter II. When used in a RAID configuration, expanded hard disk drive status, including disk drive Hardware Failure Prediction, is supported by the IMM.

Table 1. Comparison of the IMM features and combined BMC and Remote Supervisor Adapter II features in ThinkServer servers (continued)

Description	BMC with Remote Supervisor Adapter II (TS100, TS100, TS100x, RS110, and RD120)	IMM(RD210, RD220, and later)
Remote presence	The BMC with Remote Supervisor Adapter II has the following remote presence capabilities: • Graphical console redirection over LAN • Remote virtual diskette and CD-ROM • High-speed remote redirection of PCI video, keyboard, and mouse • Video resolution up to 1024 x 768, at 70 Hz, is supported • Data encryption	This feature is available only with IMM Premium. In addition to the Remote Supervisor Adapter II remote presence features, the IMM also has the following capabilities. **Note:** The IMM requires Java Runtime Environment 1.5 or later. • Video resolution up to 1280 x 1024, at 75 Hz, is supported • USB 2.0 support for virtual keyboard, mouse, and mass storage devices • 15-bit color depth • Choice of either absolute or relative mouse mode • USB flash drive support • Server power and reset control on the Remote Control window • Video on the Remote Control window can be saved in a file The IMM provides two separate client windows. One is for video and keyboard and mouse interaction, and the other one is for virtual media. The IMM Web interface has a menu item that allows color depth adjustment to reduce the data transmitted in low-bandwidth situations. The Remote Supervisor Adapter II interface has a bandwidth slider.
Security	Remote Supervisor Adapter II has advanced security features, including Secure Sockets Layer (SSL) and encryption.	The IMM has the same security features as Remote Supervisor Adapter II.
Serial redirection	The IPMI Serial over LAN (SOL) function is a standard capability of the BMC. The Remote Supervisor Adapter II provides the ability to redirect server serial data to a Telnet or SSH session. **Note:** This feature is not available on some servers.	The COM1 port is used for SOL on ThinkServer servers. COM1 is configurable only through the IPMI interface. The COM2 port is used for serial redirection through Telnet or SSH. COM2 is configurable through all of the IMM interfaces except for the IPMI interface. Both COM port configurations are limited to 8 data bits, null parity, 1 stop bit, and a baud rate choice of 9600, 19200, 38400, 57600, 115200, or 230400. On rack-mounted and tower servers, the IMM COM2 port is an internal COM port with no external access.
SNMP	SNMP support is limited to SNMPv1.	The IMM supports SNMPv1 and SNMPv3.

Web browser and operating-system requirements

The IMM Web interface requires the Java Plug-in 1.5 or later (for the remote presence feature) and one of the following Web browsers:

- Microsoft® Internet Explorer® version 6.0 or later with the latest Service Pack
- Mozilla Firefox version 1.5 or later

The following server operating systems have USB support, which is required for the remote presence feature:

- Microsoft Windows® Server® 2008
- Microsoft Windows Server 2003
- Red Hat Enterprise Linux® versions 4.0 and 5.0
- SUSE Linux version 10.0

Note: The IMM Web interface does not support the double-byte character set (DBCS) languages.

Notices used in this book

The following notices are used in the documentation:

- **Note:** These notices provide important tips, guidance, or advice.
- **Important:** These notices provide information or advice that might help you avoid inconvenient or problem situations.
- **Attention:** These notices indicate potential damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage might occur.

Chapter 2. Opening and using the IMM Web interface

The IMM combines service processor functions, a video controller, and remote presence function (when an optional virtual media key is installed) in a single chip. To access the IMM remotely by using the IMM Web interface, you must first log in. This chapter describes the login procedures and the actions that you can perform from the IMM Web interface.

Accessing the IMM Web interface

The IMM supports both static and Dynamic Host Configuration Protocol (DHCP) IP addressing. The default static IP address assigned to the IMM is 192.168.70.125. The IMM is initially configured to attempt to obtain an address from a DHCP server, and if it cannot, it uses the static IP address.

The IMM provides the choice of using a dedicated systems-management network connection or one that is shared with the server. The default connection for rack-mounted and tower servers is to use the dedicated systems-management network connector.

Setting up the IMM network connection through the Server Firmware Setup Utility

After you start the server, you can use the Setup Utility to select an IMM network connection. The server with the IMM hardware must be connected to a Dynamic Host Configuration Protocol (DHCP) server, or the server network must be configured to use the IMM static IP address.

To set up the IMM network connection through the Setup Utility, complete the following steps:

1. Turn on the server.

   Note: Approximately 2 minutes after the server is connected to ac power, the power-control button becomes active.

   The welcome screen is displayed.
2. When the prompt `<F1> Setup` is displayed, press F1. If you have set both a power-on password and an administrator password, you must type the administrator password to access the full Setup Utility menu.
3. From the Setup Utility main menu, select **System Settings**.
4. On the next screen, select **Integrated Management Module**.
5. On the next screen, select **Network Configuration**.
6. Highlight **DHCP Control**. There are three IMM network connection choices in the **DHCP Control** field:
   - Static IP
   - DHCP Enabled
   - DHCP with Failover (default)
7. Select one of the network connection choices.

Notes:

a. If you choose to use a static IP address, you must specify the IP address, the subnet mask, and the default gateway.

b. You can also use the Setup Utility to select a dedicated or shared IMM network connection. On the **Network Configuration** screen, select **Dedicated** or **Shared** in the **Network Interface Port** field.

c. To find the locations of the Ethernet connectors on your server that are used by the IMM, see the documentation that came with your server.

8. Select **Save Network Settings**.
9. Exit from the Setup Utility.

Notes:

1. You must wait approximately 1 minute for changes to take effect before the server firmware is functional again.
2. You can also configure the IMM network connection through the IMM Web interface. For more information, see "Configuring network interfaces" on page 28.

Logging in to the IMM

Important: The IMM is set initially with a user name of `USERID` and password of `PASSW0RD` (with a zero, not the letter O). This default user setting has Supervisor access. Change this default password during your initial configuration for enhanced security.

To access the IMM through the IMM Web interface, complete the following steps:

1. Open a Web browser. In the address or URL field, type the IP address or host name of the IMM server to which you want to connect.
2. Type your user name and password in the IMM Login window. If you are using the IMM for the first time, you can obtain your user name and password from your system administrator. All login attempts are documented in the event log. Depending on how your system administrator configured the user ID, you might need to enter a new password.
3. On the Welcome Web page, select a timeout value from the drop-down list in the field that is provided. If your browser is inactive for that number of minutes, the IMM logs you off the Web interface.

   Note: Depending on how your system administrator configured the global login settings, the timeout value might be a fixed value.

4. Click **Continue** to start the session.

   The browser opens the System Status page, which gives you a quick view of the server status and the server health summary.

   For descriptions of the actions that you can perform from the links in the left navigation pane of the IMM Web interface, see "IMM action descriptions" on page 11. Then, go to Chapter 3, "Configuring the IMM," on page 15.

IMM action descriptions

Table 2 lists the actions that are available when you are logged in to the IMM.

Table 2. IMM actions

Link	Action	Description
System Status	View system health for a server, view the operating-system-failure screen capture, and view the users who are logged in to the IMM	You can monitor the server power and health state, and the temperature, voltage, and fan status of your server on the System Health page. You can also view the image of the last operating-system-failure screen capture and the users who are logged in to the IMM.
Easy LED Diagnostics	View the name, color, and status of every LED on the server light path	The Easy LED Diagnostics page displays the current status of the LEDs on the server.
Event Log	View event logs for remote servers	The Event Log page contains entries that are currently stored in the chassis-event log. The log includes a text description of events that are reported by the BMC, plus information about all remote access attempts and configuration changes. All events in the log are time stamped, using the IMM date and time settings. Some events also generate alerts, if they are configured to do so on the Alerts page. You can sort and filter events in the event log.
Vital Product Data	View the server vital product data (VPD)	The IMM collects server information, server firmware information, and server component VPD. This data is available from the Vital Product Data page.
Power/Restart	Remotely turn on or restart a server	The IMM provides full remote power control over your server with power-on, power-off, and restart actions. In addition, power-on and restart statistics are captured and displayed to show server hardware availability.
Remote Control	Redirect the server video console and use your computer disk drive or disk image as a drive on the server	From the Remote Control page, you can start the Remote Control feature. With Remote Control, you can view the server console from your computer, and you can mount one of your computer disk drives, such as the CD-ROM drive or the diskette drive, on the server. You can use your mouse and keyboard to interact with and control the server. When you have mounted a disk, you can use it to restart the server and to update firmware on the server. The mounted disk appears as a USB disk drive that is attached to the server.
PXE Network Boot	Change the host server startup (boot) sequence for the next restart to attempt a Preboot Execution Environment (PXE) / Dynamic Host Configuration Protocol (DHCP) network startup	If your server firmware and PXE boot agent utility are correctly defined, from the PXE Network Boot page you can change the host server startup (boot) sequence for the next restart to attempt a PXE / DHCP network startup. The host startup sequence will be altered only if the host is not under Privileged Access Protection (PAP). After the next restart occurs, the check box on the PXE Network Boot page will be cleared.
Firmware Update	Update firmware on the IMM	Use the options on the Firmware Update page to update the IMM firmware, server firmware, and DSA firmware.

Table 2. IMM actions (continued)

Link	Action	Description
System Settings	View and change the IMM server settings	You can configure the server location and general information, such as the name of the IMM, server timeout settings, and contact information for the IMM, from the System Settings page.
	Set the IMM clock	You can set the IMM clock that is used for time stamping the entries in the event log.
	Enable or disable the USB in-band interface	You can enable or disable the USB in-band (or LAN over USB) interface.
Login Profiles	Configure the IMM login profiles and global login settings	You can define up to 12 login profiles that enable access to the IMM. You can also define global login settings that apply to all login profiles, including enabling Lightweight Directory Access Protocol (LDAP) server authentication and customizing the account security level.
Alerts	Configure remote alerts and remote alert recipients	You can configure the IMM to generate and forward alerts for different events. On the Alerts page, you can configure the alerts that are monitored and the recipients that are notified.
	Configure Simple Network Management Protocol (SNMP) events	You can set the event categories for which SNMP traps are sent.
	Configure alert settings	You can establish global settings that apply to all remote alert recipients, such as the number of alert retries and the delay between the retries.
Serial Port	Configure the IMM serial port settings	From the Serial Port page, you can configure the serial port baud rate that is used by the serial redirection function. You can also configure the key sequence that is used to switch between the serial redirection and command-line interface (CLI) modes.
Port assignments	Change the port numbers of the IMM protocols	From the Port Assignments page, you can view and change the port numbers assigned to the IMM protocols (for example, HTTP, HTTPS, Telnet, and SNMP).
Network Interfaces	Configure the network interfaces of the IMM	From the Network Interfaces page, you can configure network-access settings for the Ethernet connection on the IMM.
Network Protocols	Configure the network protocols of the IMM	You can configure Simple Network Management Protocol (SNMP), Domain Name System (DNS), and Simple Mail Transfer Protocol (SMTP) settings that are used by the IMM from the Network Protocols page. You can also configure LDAP parameters.
Security	Configure the Secure Sockets Layer (SSL)	You can enable or disable SSL and manage the SSL certificates that are used. You can also enable or disable whether an SSL connection is used to connect to an LDAP server.
	Enable Secure Shell (SSH) access	You can enable SSH access to the IMM.
Configuration File	Back up and restore the IMM configuration	You can back up, modify, and restore the configuration of the IMM, and view a configuration summary, from the Configuration File page.

Table 2. IMM actions (continued)

Link	Action	Description
Restore Default Settings	Restore the IMM default settings	**Attention:** When you click **Restore Defaults**, all of the modifications that you made to the IMM are lost. You can reset the configuration of the IMM to the factory defaults.
Restart IMM	Restart the IMM	You can restart the IMM.
Log off	Log off the IMM	You can log off your connection to the IMM.

You can click the **View Configuration Summary** link, which is in the top-right corner on most pages, to quickly view the configuration of the IMM.

Chapter 3. Configuring the IMM

Use the links under **IMM Control** in the navigation pane to configure the IMM.

- From the System Settings page, you can:
  - Set server information
  - Set server timeouts
  - Set IMM date and time
  - Enable or disable commands on the USB interface
- From the Login Profiles page, you can:
  - Set login profiles to control access to the IMM
  - Configure global login settings, such as the lockout period after unsuccessful login attempts
  - Configure the account security level
- From the Alerts page, you can:
  - Configure remote alert recipients
  - Set the number of remote alert attempts
  - Select the delay between alerts
  - Select which alerts are sent and how they are forwarded
- From the Serial Port page, you can:
  - Configure the baud rate of serial port 2 (COM2) for serial redirection
  - Specify the keystroke sequence that is used to switch between the serial redirection and the command-line interface (CLI)
- From the Port Assignments page, you can change the port numbers of IMM services.
- From the Network Interfaces page, you can set up the Ethernet connection for the IMM.
- From the Network Protocols page, you can configure:
  - SNMP setup
  - DNS setup
  - Telnet protocol
  - SMTP setup
  - LDAP setup
  - Service location protocol
- From the Security page, you can install and configure the Secure Sockets Layer (SSL) settings.
- From the Configuration File page, you can back up, modify, and restore the configuration of the IMM.
- From the Restore Defaults page, you can reset the IMM configuration to the factory defaults.
- From the Restart IMM page, you can restart the IMM.

Setting system information

To set the IMM system information, complete the following steps:

1. Log in to the IMM where you want to set the system information. For more information, see Chapter 2, “Opening and using the IMM Web interface,” on page 9.
2. In the navigation pane, click **System Settings**.

   Note: The available fields in the System Settings page are determined by the accessed remote server.
3. In the **Name** field in the **IMM Information** area, type the name of the IMM.

   Use the **Name** field to specify a name for the IMM in this server. The name is included with e-mail and SNMP alert notifications to identify the source of the alert.

   Note: Your IMM name (in the **Name** field) and the IP host name of the IMM (in the **Hostname** field on the Network Interfaces page) do not automatically share the same name because the **Name** field is limited to 16 characters. The **Hostname** field can contain up to 63 characters. To minimize confusion, set the **Name** field to the nonqualified portion of the IP host name. The nonqualified IP host name consists of up to the first period of a fully qualified IP host name. For example, for the fully qualified IP host name imm1.us.company.com, the nonqualified IP host name is imm1. For information about your host name, see “Configuring network interfaces” on page 28.
4. In the **Contact** field, type the contact information. For example, you can specify the name and phone number of the person to contact if there is a problem with this server. You can type a maximum of 47 characters in this field.
5. In the **Location** field, type the location of the server. Include in this field sufficient detail to quickly locate the server for maintenance or other purposes. You can type a maximum of 47 characters in this field.
6. Scroll to the bottom of the page and click **Save**.

Setting server timeouts

Note: Server timeouts require that the in-band USB interface (or LAN over USB) be enabled to allow commands. For more information about the enabling and disabling commands for the USB interface, see “Disabling the USB in-band interface” on page 19. For information regarding the installation of the required device drivers, see “Installing device drivers” on page 71.

To set the server timeout values, complete the following steps:

1. Log in to the IMM where you want to set the server timeouts. For more information, see Chapter 2, “Opening and using the IMM Web interface,” on page 9.
2. In the navigation pane, click **System Settings** and scroll down to the **Server Timeouts** area.

   You can set the IMM to respond automatically to the following events:

   - Halted operating system
   - Failure to load operating system
3. Enable the server timeouts that correspond to the events that you want the IMM to respond to automatically.

   OS watchdog

   Use the **OS watchdog** field to specify the number of minutes between checks of the operating system by the IMM. If the operating system

fails to respond to one of these checks, the IMM generates an OS timeout alert and restarts the server. After the server is restarted, the OS watchdog is disabled until the operating system is shut down and the server is power cycled.

To set the OS watchdog value, select a time interval from the menu. To turn off this watchdog, select **0.0** from the menu. To capture operating-system-failure screens, you must enable the watchdog in the **OS watchdog** field.

Loader watchdog
Use the **Loader watchdog** field to specify the number of minutes that the IMM waits between the completion of POST and the starting of the operating system. If this interval is exceeded, the IMM generates a loader timeout alert and automatically restarts the server. After the server is restarted, the loader timeout is automatically disabled until the operating system is shut down and the server is power cycled (or until the operating system starts and the software is successfully loaded).

To set the loader timeout value, select the time limit that the IMM waits for the operating-system startup to be completed. To turn off this watchdog, select **0.0** from the menu.

4. Scroll to the bottom of the page and click **Save**.

Setting the IMM date and time

The IMM uses its own real-time clock to time stamp all events that are logged in the event log.

Note: The IMM date and time setting affects only the IMM clock, not the server clock. The IMM real-time clock and the server clock are separate, independent clocks and can be set to different times. To synchronize the IMM clock with the server clock, go to the **Network Time Protocol** area of the page and set the NTP server host name or IP address to the same server host name or IP address that is used to set the server clock. See "Synchronizing clocks in a network" on page 18 for more information.

Alerts that are sent by e-mail and SNMP use the real-time clock setting to time stamp the alerts. The clock settings support Greenwich mean time (GMT) offsets and daylight saving time (DST) for added ease-of-use for administrators who are managing systems remotely over different time zones. You can remotely access the event log even if the server is turned off or disabled.

To verify the date and time settings of the IMM, complete the following steps:

1. Log in to the IMM where you want to set the IMM date and time values. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **System Settings** and scroll down to the **IMM Date and Time** area, which shows the date and time when the Web page was generated.
3. To override the date and time settings and to enable daylight saving time (DST) and Greenwich mean time (GMT) offsets, click **Set IMM Date and Time**.
4. In the **Date** field, type the numbers of the current month, day, and year.
5. In the **Time** field, type the numbers that correspond to the current hour, minutes, and seconds in the applicable entry fields. The hour (hh) must be a

number from 00 - 23 as represented on a 24-hour clock. The minutes (mm) and seconds (ss) must be numbers from 00 - 59.

6. In the **GMT offset** field, select the number that specifies the offset, in hours, from Greenwich mean time (GMT), corresponding to the time zone where the server is located.
7. Select or clear the **Automatically adjust for daylight saving changes** check box to specify whether the IMM clock automatically adjusts when the local time changes between standard time and daylight saving time.
8. Click **Save**.

Synchronizing clocks in a network

The Network Time Protocol (NTP) provides a way to synchronize clocks throughout a computer network, enabling any NTP client to obtain the correct time from an NTP server.

The IMM NTP feature provides a way to synchronize the IMM real-time clock with the time that is provided by an NTP server. You can specify the NTP server that is to be used, specify the frequency with which the IMM is synchronized, enable or disable the NTP feature, and request immediate time synchronization.

The NTP feature does not provide the extended security and authentication that are provided through encryption algorithms in NTP Version 3 and NTP Version 4. The IMM NTP feature supports only the Simple Network Time Protocol (SNTP) without authentication.

To set up the IMM NTP feature settings, complete the following steps:

1. Log in to the IMM on which you want to synchronize the clocks in the network. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **System Settings** and scroll down to the **IMM Date and Time** area.
3. Click **Set IMM Date and Time**.
4. Under **Network Time Protocol (NTP)**, you can select from the following settings:

   NTP auto-synchronization service
   Use this selection to enable or disable automatic synchronization of the IMM clock with an NTP server.

   NTP server host name or IP address
   Use this field to specify the name of the NTP server to be used for clock synchronization.

   NTP update frequency
   Use this field to specify the approximate interval (in minutes) between synchronization requests. Enter a value between 3 - 1440 minutes.

   Synchronize Clock Now
   Click this button to request an immediate synchronization instead of waiting for the interval time to lapse.
5. Click **Save**.

Disabling the USB in-band interface

Important: If you disable the USB in-band interface, you cannot perform an in-band update of the IMM firmware, server firmware, and DSA firmware by using the Linux or Windows flash utilities. If the USB in-band interface is disabled, use the Firmware Update option on the IMM Web interface to update the firmware. For more information, see "Updating firmware" on page 67.

If you disable the USB in-band interface, also disable the watchdog timeouts to prevent the server from restarting unexpectedly. For more information, see "Setting server timeouts" on page 16.

The USB in-band interface, or LAN over USB, is used for in-band communications to the IMM. To prevent any application that is running on the server from requesting the IMM to perform tasks, you must disable the USB in-band interface. For more information about LAN over USB, see Chapter 6, "LAN over USB," on page 71.

To disable the USB in-band interface, complete the following steps:

1. Log in to the IMM on which you want to disable the USB device driver interface. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **System Settings** and scroll down to the **Miscellaneous** area.
3. Select the **Do not allow commands on USB interface** check box to disable the USB in-band interface. Selecting this option does not affect the USB remote presence functions (for example, keyboard, mouse, and mass storage). When you disable the USB in-band interface, the in-band systems-management applications such as the Advanced Settings Utility (ASU) and firmware update package utilities might not work.

   Note: The ASU works with a disabled USB in-band interface if an IPMI device driver is installed.

   If you try to use systems-management applications while the in-band interface is disabled, they might not work.
4. Click **Save**.

To enable the USB device driver interface after it has been disabled, clear the **Do not allow commands on USB interface** check box and click **Save**.

Notes:

1. The USB in-band interface is also called "LAN over USB" and is described in more detail in Chapter 6, "LAN over USB," on page 71.
2. When you attempt a network installation of some Linux distributions, the installation might fail if the IMM USB in-band interface is enabled. For more information, see http://rhn.redhat.com/errata/RHBA-2009-0127.html.
3. If you are performing a network installation that does not contain the update on the Red Hat Web site described in the preceding note 2, you must disable the USB in-band interface before you perform the installation and enable it after the installation is complete.
4. For information about the configuration of the LAN over USB interface, see "Configuring the LAN over USB interface manually" on page 71.

Creating a login profile

Use the Login Profiles table to view, configure, or change individual login profiles. Use the links in the Login ID column to configure individual login profiles. You can define up to 12 unique profiles. Each link in the Login ID column is labeled with the configured login ID of the associated profile.

Certain login profiles are shared with the IPMI user IDs, providing a single set of local user accounts (username/password) that work with all of the IMM user interfaces, including IPMI. Rules that pertain to these shared login profiles are described in the following list:

- IPMI user ID 1 is always the null user.
- IPMI user ID 2 maps to login ID 1, IPMI user ID 3 maps to login ID 2, and so on.
- The IMM default user is set to `USERID` and `PASSW0RD` (with a zero, not the letter O) for IPMI user ID 2 and login ID 1.

For example, if a user is added through IPMI commands, that user information is also available for authentication through the Web, Telnet, SSH, and other interfaces. Conversely, if a user is added on the Web or other interfaces, that user information is available for starting an IPMI session.

Because the user accounts are shared with IPMI, certain restrictions are imposed to provide a common ground between the interfaces that use these accounts. The following list describes IMM and IPMI login profile restrictions:

- IPMI allows a maximum of 64 user IDs. The IMM IPMI implementation allows only 12 user accounts.
- IPMI allows anonymous logins (null user name and null password), but the IMM does not.
- IPMI allows multiple user IDs with the same user names, but the IMM does not.
- IPMI requests to change the user name from the current name to the same current name return an `invalid parameter` completion code because the requested user name is already in use.
- The maximum IPMI password length for the IMM is 16 bytes.
- The following words are restricted and are not available for use as local IMM user names:
  - immroot
  - nobody
  - ldap
  - lighttpd
  - sshd
  - daemon
  - immftp

To configure a login profile, complete the following steps:

1. Log in to the IMM where you want to create a login profile. For more information, see Chapter 2, “Opening and using the IMM Web interface,” on page 9.
2. In the navigation pane, click **Login Profiles**.

Note: If you have not configured a profile, it does not appear in the Login Profiles table.

The Login Profiles page displays each login ID, the login access level, and the password expiration information.

Important: By default, the IMM is configured with one login profile that enables remote access using a login user ID of USERID and a password of PASSW0RD (the 0 is a zero, not the letter O). To avoid a potential security exposure, change this default login profile during the initial setup of the IMM.

3. Click **Add User**. An individual profile is displayed.
4. In the **Login ID** field, type the name of the profile.

   You can type a maximum of 16 characters in the **Login ID** field. Valid characters are uppercase and lowercase letters, numbers, periods, and underscores.

   Note: This login ID is used to grant remote access to the IMM.
5. In the **Password** field, assign a password to the login ID.

   A password must contain a minimum of five characters, one of which must be a nonalphabetic character. Null or empty passwords are accepted.

   Note: This password is used with the login ID to grant remote access to the IMM.
6. In the **Confirm password** field, type the password again.
7. In the **Authority Level** area, select one of the following options to set the access rights for this login ID:

   Supervisor
   The user has no restrictions.

   Read Only
   The user has read-only access only and cannot perform actions such as file transfers, power and restart actions, or remote presence functions.

   Custom
   If you select the **Custom** option, you must select one or more of the following custom authority levels:
   - **User Account Management:** A user can add, modify, or delete users and change the global login settings in the Login Profiles page.
   - **Remote Console Access:** A user can access the remote console.
   - **Remote Console and Virtual Media Access:** A user can access both the remote console and the virtual media feature.
   - **Remote Server Power/Restart Access:** A user can access the power-on and restart functions for the remote server. These functions are available in the Power/Restart page.
   - **Ability to Clear Event Logs:** A user can clear the event logs. Everyone can look at the event logs, but this particular permission is required to clear the logs.
   - **Adapter Configuration - Basic:** A user can modify configuration parameters in the System Settings and Alerts pages.
   - **Adapter Configuration - Networking & Security:** A user can modify configuration parameters in the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port pages.

- **Adapter Configuration - Advanced:** A user has no restrictions when configuring the IMM. In addition, the user is said to have administrative access to the IMM, meaning that the user can also perform the following advanced functions: firmware updates, PXE network boot, restore IMM factory defaults, modify and restore IMM configuration from a configuration file, and restart and reset the IMM.

When a user sets the authority level of an IMM login ID, the resulting IPMI privilege level of the corresponding IPMI User ID is set according to these priorities:

- If the user sets the IMM login ID authority level to Supervisor, the IPMI privilege level is set to Administrator.
- If the user sets the IMM login ID authority level to Read Only, the IPMI privilege level is set to User.
- If the user sets the IMM login ID authority level to have any of the following types of access, the IPMI privilege level is set to Administrator:
  - User Account Management Access
  - Remote Console Access
  - Remote Console and Remote Disk Access
  - Adapter Configuration - Networking & Security
  - Adapter Configuration - Advanced
- If the user sets the IMM login ID authority level to have Remote Server Power/Restart Access or Ability to Clear Event Logs, the IPMI privilege level is set to Operator.
- If the user sets the IMM login ID authority level to have Adapter Configuration (Basic), the IPMI privilege level is set to User.

Note: To return the login profiles to the factory defaults, click **Clear Login Profiles**.

8. In the **Configure SNMPv3 User** area, select the check box if the user should have access to the IMM by using the SNMPv3 protocol. After you click the check box, the configuration settings for SNMPv3 appear. Use following fields to configure the SNMPv3 settings for the user profile:

Authentication Protocol
Use this field to specify either **HMAC-MD5** or **HMAC-SHA** as the authentication protocol. These are hash algorithms used by the SNMPv3 security model for the authentication. The password for the Linux account will be used for authentication. If you choose **None**, authentication protocol is not used.

Privacy Protocol
Data transfer between the SNMP client and the agent can be protected using encryption. The supported methods are **DES** and **AES**. Privacy protocol is valid only if the authentication protocol is set to either **HMAC-MD5** or **HMAC-SHA**.

Privacy Password
Use this field to specify the encryption password.

Confirm Privacy Password
Use this field to confirm the encryption password.

Access Type

Use this field to specify either **Get** or **Set** as the access type. SNMPv3 users with the access type Get can perform only query operations. With the access type Set, SNMPv3 users can both perform query operations and modify settings (for example, setting the password for an user).

Hostname/IP address for traps

Use this field to specify the trap destination for the user. This can be an IP address or hostname. Using traps, the SNMP agent notifies the management station about events (for example, when a processor temperature exceeds the limit).

9. Click **Save** to save your login ID settings.

Deleting a login profile

To delete a login profile, complete the following steps:

1. Log in to the IMM for which you want to create a login profile. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Login Profiles**. The Login Profiles page displays each login ID, the login access level, and the password expiration information.
3. Click the login profile that you want to delete. The Login Profile page for that user is displayed
4. Click **Clear Login Profile**.

Configuring the global login settings

Complete the following steps to set conditions that apply to all login profiles for the IMM:

1. Log in to the IMM for which you want to set the global login settings. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Login Profiles**.
3. Scroll down to the **Global Login Settings** area.
4. In the **User authentication method** field, specify how users who are attempting to log in are authenticated. Select one of the following authentication methods:
   - **Local only:** Users are authenticated by a search of a table that is local to the IMM. If there is no match on the user ID and password, access is denied. Users who are successfully authenticated are assigned the authority level that is configured in "Creating a login profile" on page 20.
   - **LDAP only:** The IMM attempts to authenticate the user by using the LDAP server. Local user tables on the IMM are never searched with this authentication method.
   - **Local first, then LDAP:** Local authentication is attempted first. If local authentication fails, LDAP authentication is attempted.
   - **LDAP first, then Local:** LDAP authentication is attempted first. If LDAP authentication fails, local authentication is attempted.

   Notes:

   a. Only locally administered accounts are shared with the IPMI interface because IPMI does not support LDAP authentication.

   b. Even if the **User authentication method** field is set to **LDAP only**, users can log in to the IPMI interface by using the locally administered accounts.

5. In the **Lockout period after 5 login failures** field, specify how long, in minutes, the IMM prohibits remote login attempts if more than five sequential failures to log in remotely are detected. The lockout of one user does not prevent other users from logging in.
6. In the **Web inactivity session timeout** field, specify how long, in minutes, the IMM waits before it disconnects an inactive Web session. Select **No timeout** to disable this feature. Select **User picks timeout** if the user will select the timeout period during the login process.
7. (Optional) In the **Account security level** area, select a password security level. The **Legacy security settings** and **High security settings** set the default values as indicated in the requirement list.
8. To customize the security setting, select **Custom security settings** to view and change the account security management configuration.

   User login password required
   Use this field to indicate whether a login ID with no password is allowed.

   Number of previous passwords that cannot be used
   Use this field to indicate the number of previous passwords that cannot be reused. Up to five previous passwords can be compared. Select **0** to allow the reuse of all previous passwords.

   Maximum Password Age
   Use this field to indicate the maximum password age that is allowed before the password must be changed. Values of 0 - 365 days are supported. Select **0** to disable the password expiration checking.
9. Click **Save**.

Configuring remote alert settings

You can configure remote alert recipients, the number of alert attempts, incidents that trigger remote alerts, and local alerts from the **Alerts** link on the navigation pane.

After you configure a remote alert recipient, the IMM sends an alert to that recipient through a network connection when any event selected from the Monitored Alerts group occurs. The alert contains information about the nature of the event, the time and date of the event, and the name of the system that generated the alert.

Note: If the **SNMP Agent** or **SNMP Traps** fields are not set to **Enabled**, no SNMP traps are sent. For information about these fields, see "Configuring SNMP" on page 31.

Configuring remote alert recipients

You can define up to 12 unique remote alert recipients. Each link for an alert recipient is labeled with the recipient name and alert status.

Note: If you have not configured an alert recipient profile, the profile does not appear in the remote alert recipients list.

To configure a remote alert recipient, complete the following steps:

1. Log in to the IMM for which you want to configure remote alert settings. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.

2. In the navigation pane, click **Alerts**. The Remote Alert Recipients page is displayed. You can see the notification method and alert status for each recipient, if they are set.
3. Click one of the remote alert recipient links or click **Add Recipient**. An individual recipient window opens.
4. In the **Status** field, click **Enabled** to activate the remote alert recipient.
5. In the **Name** field, type the name of the recipient or other identifier. The name that you type appears as the link for the recipient on the Alerts page.
6. In the **E-mail address** field, enter the alert recipient's e-mail address.
7. Use the check box to include event logs with e-mail alerts.
8. In the **Monitored Alerts** field, select the type of alerts that are sent to the alert recipient.

   The remote alerts are categorized by the following levels of severity:

   Critical alerts
   Critical alerts are generated for events that signal that a server component is no longer functioning.

   Warning alerts
   Warning alerts are generated for events that might progress to a critical level.

   System alerts
   System alerts are generated for events that occur as a result of system errors or for events that occur as a result of configuration changes.

   All alerts are stored in the event log and sent to all configured remote alert recipients.
9. Click **Save**.

Configuring global remote alert settings

The global remote alert settings apply only to forwarded alerts.

Complete the following steps to set the number of times that the IMM attempts to send an alert:

1. Log in to the IMM on which you want to set remote alert attempts. For more information, see Chapter 2, “Opening and using the IMM Web interface,” on page 9.
2. In the navigation pane, click **Alerts** and scroll down to the **Global Remote Alert Settings** area.

   Use these settings to define the number of remote alert attempts and the length of time between the attempts. The settings apply to all configured remote alert recipients.

   Remote alert retry limit
   Use the **Remote alert retry limit** field to specify the number of additional times that the IMM attempts to send an alert to a recipient. The IMM does not send multiple alerts; additional alert attempts occur only if there is a failure when the IMM attempts to send the initial alert.

   Note: This alert setting does not apply to SNMP alerts.

Delay between entries
Use the **Delay between entries** field to specify the time interval (in minutes) that the IMM waits before sending an alert to the next recipient in the list.

Delay between retries
Use the **Delay between retries** field to specify the time interval (in minutes) that the IMM waits between retries to send an alert to a recipient.

3. Scroll to the bottom of the page and click **Save**.

Configuring SNMP alert settings

The SNMP agent notifies the IMM about events through SNMP traps. You can configure the SNMP to filter the events based on the event type. Event categories that are available for filtering are Critical, Warning and System. The SNMP alert settings are global for all SNMP traps.

Notes:

1. The IMM provides two Management Information Base (MIB) files for use with SNMP applications. The MIB files are included in the IMM firmware update packages.
2. IMM supports the SNMPv1 and SNMPv3 standards.

Complete the following steps to select the type or types of alerts that are sent to SNMP:

1. Log in to the IMM on which you want to set remote alert attempts. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Alerts** and scroll down to the **SNMP Alerts Settings** area.
3. Select the type or types of alerts. The remote alerts are categorized by the following levels of severity:
   - Critical
   - Warning
   - System
4. Scroll to the bottom of the page and click **Save**.

Configuring serial port settings

The IMM provides two serial ports that are used for serial redirection.

Serial port 1 (COM1) is used for IPMI Serial over LAN (SOL). COM1 is configurable only through the IPMI interface.

COM2 is used for serial redirection through Telnet or SSH. COM2 is not configurable through the IPMI interface. On rack-mounted and tower servers, COM2 is an internal COM port with no external access.

Both serial ports use 8 data bits, null parity, and 1 stop bit. A baud rate choice of 9600, 19200, 38400, 57600, 115200, and 230400 is available.

You can configure the serial redirection and command-line interface for the COM2 port in the IMM.

To configure the serial data-transfer rate and redirection, complete the following steps:

1. Log in to the IMM on which you want to configure the serial port. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Serial Port**.
3. In the **Baud rate** field, select the data-transfer rate to match the rate of the server COM port that you want to use for serial redirection.

   Use the **Baud rate** field to specify the data-transfer rate of your serial port connection. To set the baud rate, select the data-transfer rate, in bits per second, that corresponds to your serial port connection.
4. In the **CLI mode** field in the **Serial Redirect/CLI Settings** area, select **CLI with EMS compatible keystroke sequences** if you want to use the Microsoft Windows Server 2003 Emergency Management Services (EMS) compatible key sequence to exit the serial redirection operation, or select **CLI with user defined keystroke sequences** if you want to use your own key sequence.

   Note: If you select **CLI with user defined keystroke sequences**, you must define the key sequence.

   After the serial redirection starts, it continues until the user types the exit key sequence. When the exit key sequence is typed, serial redirection stops and the user is returned to command mode in the Telnet or SSH session. Use this field to specify the exit key sequence.
5. Click **Save**.

Serial-to-Telnet or SSH redirection

Serial-to-Telnet or SSH redirection enables a system administrator to use the IMM as a serial terminal server. A server serial port can be accessed from a Telnet or SSH connection when serial redirection is enabled.

Notes:

1. The IMM allows a maximum of two open Telnet sessions. The Telnet sessions can access the serial ports independently so that multiple users can have a concurrent view of a redirected serial port.
2. The command-line interface **console 1** command is used to start a serial redirection session with the COM port.

Example session

```
telnet 192.168.70.125 (Press Enter.)
Connecting to 192.168.70.125...
username: USERID (Press Enter.)
password: ******** (Press Enter.)
system> console 1 (Press Enter.)
```

All traffic from COM2 is now routed to the Telnet session. All traffic from the Telnet or SSH session is routed to COM2.

```
ESC Q
```

Type the exit key sequence to return to the command-line interface. In this example, press Esc and then type `q`.

```
Back to LegacyCLI console....
```

Configuring port assignments

To change the port numbers of IMM services, complete the following steps:

1. Log in to the IMM where you want to configure the port assignments. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Port Assignments**.
3. Use the following information to assign values for the fields:

   HTTP This is the port number for the HTTP server of the IMM. The default port number is 80. Other valid values are in the range 1 - 65535. If you change this port number, you must add this port number, preceded by a colon, at the end of the Web address. For example, if the HTTP port is changed to 8500, type `http://hostname:8500/` to open the IMM Web interface. Note that you must type the prefix `http://` before the IP address and port number.

   HTTPS
   This is the port number that is used for Web interface HTTPS (SSL) traffic. The default value is 443. Other valid values are in the range 1 - 65535.

   Telnet Legacy CLI
   This is the port number for Legacy CLI to log in through the Telnet service. The default value is 23. Other valid values are in the range 1 - 65535.

   SSH Legacy CLI
   This is the port number that is configured for Legacy CLI to log in through SSH. The default is 22.

   SNMP Agent
   This is the port number for the SNMP agent that runs on the IMM. The default value is 161. Other valid values are in the range 1 - 65535.

   SNMP Traps
   This is the port number that is used for SNMP traps. The default value is 162. Other valid values are in the range 1 - 65535.

   Remote Presence
   This is the port number that the remote control feature uses to view and interact with the server console. The default is 3900 for rack-mounted and tower servers.

   The following port numbers are reserved and can be used only for the corresponding services.

Table 3. Reserved port numbers

Port number	Services used for
427	SLP
7070 through 7077	Partition management

4. Click **Save**.

Configuring network interfaces

On the Network Interfaces page, you can set access to the IMM by configuring an Ethernet connection to the IMM. To configure the Ethernet setup for the IMM, complete the following steps:

1. Log in to the IMM where you want to set up the configuration. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Network Interfaces**.
3. If you want to use an Ethernet connection, select **Enabled** in the **Interface** field. Ethernet is enabled by default.

   Note: Disabling the Ethernet interface prevents all access to the IMM from the external network.
4. If you want to use a Dynamic Host Configuration Protocol (DHCP) server connection, enable it by clicking either of the following choices in the DHCP field:
   - **Enabled - Obtain IP config from DHCP server**
   - **Try DHCP server. If it fails, use static IP config.**

   The default setting is **Try DHCP server. If it fails, use static IP config.**

   Note: Do not enable DHCP unless you have an accessible, active, and configured DHCP server on your network. When DHCP is used, the automatic configuration overrides any manual settings.

   If you want to assign a static IP address to the IMM, select **Disabled - Use static IP configuration**.

   If DHCP is enabled, the host name is assigned as follows:
   - If the **Hostname** field contains an entry, the IMM DHCP support requests that the DHCP server use this host name.
   - If the **Hostname** field does not contain an entry, the IMM DHCP support requests that the DHCP server assigns a unique host name to the IMM.
5. Type the IP host name of the IMM in the **Hostname** field.

   You can enter a maximum of 63 characters in this field, which represents the IP host name of the IMM. The host name defaults to IMMA, followed by the IMM burned-in media access control (MAC) address.

   Note: The IP host name of the IMM (the **Hostname** field) and IMM name (the **Name** field on the System page) do not automatically share the same name, because the **Name** field is limited to 15 characters but the **Hostname** field can contain up to 63 characters. To minimize confusion, set the **Name** field to the nonqualified portion of the IP host name. The nonqualified IP host name consists of up to the first period of a fully qualified IP host name. For example, for the fully qualified IP host name imm1.us.company.com, the nonqualified IP host name is imm1. For information about your host name, see "Setting system information" on page 15.

   If you enabled DHCP, go to step 12 on page 30.

   If you have not enabled DHCP, continue with step 6.
6. In the **IP address** field, type the IP address of the IMM. The IP address must contain four integers from 0 - 255 with no spaces and separated by periods.
7. In the **Subnet mask** field, type the subnet mask that is used by the IMM. The subnet mask must contain four integers from 0 - 255 with no spaces or consecutive periods and separated by periods.

   The default setting is 255.255.255.0.

8. In the **Gateway address** field, type your network gateway router. The gateway address must contain four integers from 0 - 255 with no spaces or consecutive periods and separated by periods.
9. Scroll to the bottom of the page and click **Save**.
10. Click **Advanced Ethernet Setup** if you need to set additional Ethernet settings.

    The following table describes the functions on the Advanced Ethernet Setup page.

Table 4. Functions on the Advanced Ethernet Setup page

Field	Function
Auto Negotiate	The IMM determines the data rate and duplex settings automatically, according to your switch capabilities.
Data rate	Use the **Data Rate** field to specify the amount of data that is to be transferred per second over your LAN connection. To set the data rate, click the menu and select the data-transfer rate, in Mb[1], that corresponds to the capability of your network. To automatically detect the data-transfer rate, set the **Auto Negotiate** field to **Yes**, which is the default value.
Duplex	Use the **Duplex** field to specify the type of communication channel that is used in your network. To set the duplex mode, select one of the following choices: • **Full** enables data to be carried in both directions at once. • **Half** enables data to be carried in either one direction or the other, but not both at the same time. To automatically detect the duplex type, set the **Auto Negotiate** field to **Yes**, which is the default value.
Maximum transmission unit	Use the **Maximum transmission unit** field to specify the maximum size of a packet (in bytes) for your network interface. For Ethernet, the valid maximum transmission unit (MTU) range is 60 - 1500. The default value for this field is 1500.
Locally administered MAC address	Enter a physical address for the IMM in the **Locally administered MAC address** field. If a value is specified, the locally administered address overrides the burned-in MAC address. The locally administered address must be a hexadecimal value from 000000000000 through FFFFFFFFFFFF. This value must be in the form *xx*:*xx*:*xx*:*xx*:*xx*:*xx* where *x* is a number 0 - 9. The IMM does not support the use of a multicast address. The first byte of a multicast address is an odd number (the least significant bit is set to 1). Therefore, the first byte must be an even number.
Burned-in MAC address	The burned-in MAC address is a unique physical address that is assigned to this IMM by the manufacturer. The address is a read-only field.
[1]Mb equals approximately 1 000 000 bits.	

11. Modify the advanced Ethernet settings as necessary.
12. Scroll to the bottom of the page and click **Save**.
13. Click **Cancel** to return to the Network Interfaces page. If DHCP is enabled, the server automatically assigns the host name, IP address, gateway address, subnet mask, domain name, DHCP server IP address, and up to three DNS server IP addresses.
14. If DHCP is enabled, to view the DHCP server assigned setting, click **IP Configuration Assigned by DHCP Server**.

15. Click **Save**.
16. Click **View Configuration Summary** to see a summary of all current configuration settings.
17. In the navigation pane, click **Restart IMM** to activate the changes.

Note: You can also configure the IMM network connection through the Setup Utility. For more information, see "Setting up the IMM network connection through the Server Firmware Setup Utility" on page 9.

Configuring network protocols

On the Network Protocols page, you can perform the following functions:

- Configure Simple Network Management Protocol (SNMP)
- Configure Domain Name System (DNS)
- Configure Telnet Protocol
- Configure Simple Mail Transfer Protocol (SMTP)
- Configure Lightweight Directory Access Protocol (LDAP)
- Configure Service Location Protocol (SLP)

Changes to the network protocol settings require that the IMM be restarted for the changes to take effect. If you are changing more than one protocol, you can wait until all of the protocol changes have been made and saved before you restart the IMM.

Configuring SNMP

You can use the SNMP agent to collect information and to control the server. The IMM can also be configured to send SNMP alerts to the configured host names or IP addresses.

Notes:

1. The IMM provides two Management Information Base (MIB) files for use with SNMP applications. The MIB files are included in the IMM firmware update packages.
2. IMM supports the SNMPv1 and SNMPv3 standards.

To configure SNMP, complete the following steps:

1. Log in to the IMM where you want to configure SNMP. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Network Protocols**.
3. Select **Enabled** in either the **SNMPv1 agent** or the **SNMPv3 agent** field.

   Note: If you enabled the SNMPv3 agent, you must configure SNMPv3 settings for active login profiles for the interaction between the SNMPv3 manager and SNMPv3 agent to work correctly. You can configure these settings at the bottom of the individual login profile settings on the Login Profiles page (see "Creating a login profile" on page 20 for more information). Click the link for the login profile to configure, scroll to the bottom of the page and then click the **Configure SNMPv3 User** check box.
4. Select **Enabled** in the **SNMP traps** field to forward alerts to SNMP communities on your network. To enable the SNMP agent, the following criteria must be met:

- A system contact must be specified on the System Settings page. For information about the System Settings page settings, see "Setting system information" on page 15.
- System location must be specified on the System Settings page.
- At least one community name must be specified.
- At least one valid IP address or host name (if DNS is enabled) must be specified for that community.

Note: Alert recipients whose notification method is SNMP cannot receive alerts unless the **SNMPv1 agent** or **SNMPv3 agent** and the **SNMP traps** fields are set to **Enabled**.

5. Set up a community to define the administrative relationship between SNMP agents and SNMP managers. You must define at least one community. Each community definition consists of the following parameters:
   - Community Name
   - Access Type
   - IP address

   If any of these parameters is not correct, SNMP management access is not granted.

   Note: If an error message window opens, make the necessary adjustments to the fields that are listed in the error window. Then, scroll to the bottom of the page and click **Save** to save your corrected information. You must configure at least one community to enable this SNMP agent.
6. In the **Community Name** field, enter a name or authentication string to specify the community.
7. In the **Access Type** field, select an access type. Select **Trap** to allow all hosts in the community to receive traps; select **Get** to allow all hosts in the community to receive traps and query MIB objects; select **Set** to allow all hosts in the community to receive traps, query, and set MIB objects.
8. In the corresponding **Host Name or IP Address** field, enter the host name or IP address of each community manager.
9. Scroll to the bottom of the page and click **Save**.
10. In the navigation pane, click **Restart IMM** to activate the changes.

Configuring DNS

To configure the Domain Name System (DNS), complete the following steps:

1. Log in to the IMM where you want to configure DNS. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Network Protocols** and scroll down to the **Domain Name System (DNS)** area of the page.
3. If a DNS server (or servers) is available on your network, select **Enabled** in the **DNS** field. The **DNS** field specifies whether you use a DNS server on your network to translate host names into IP addresses.
4. If you enabled DNS, in the **DNS server IP address** fields, specify the IP addresses of up to three DNS servers on your network. Each IP address must contain integers from 0 - 255, separated by periods.
5. Scroll to the bottom of the page and click **Save**.
6. In the navigation pane, click **Restart IMM** to activate the changes.

Configuring Telnet

To configure Telnet, complete the following steps:

1. Log in to the IMM where you want to configure Telnet. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Network Protocols** and scroll down to the **Telnet Protocol** area of the page. You can set the maximum number of concurrent Telnet users, or you can disable Telnet access.
3. Scroll to the bottom of the page and click **Save**.
4. In the navigation pane, click **Restart IMM** to activate the changes.

Configuring SMTP

To specify the IP address or host name of the Simple Mail Transfer Protocol (SMTP) server, complete the following steps:

1. Log in to the IMM where you want to configure SMTP. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Network Protocols** and scroll down to the **SMTP** area of the page.
3. In the **SMTP Server Host Name or IP address** field, type the host name of the SMTP server. Use this field to specify the IP address or, if DNS is enabled and configured, the host name of the SMTP server.
4. Scroll to the bottom of the page and click **Save**.
5. In the navigation pane, click **Restart IMM** to activate the changes.

Configuring LDAP

Using a Lightweight Directory Access Protocol (LDAP) server, the IMM can authenticate a user by querying or searching an LDAP directory on an LDAP server, instead of going through its local user database. Then, the IMM can remotely authenticate any user access through a central LDAP server. This requires LDAP client support on the IMM. You can also assign authority levels according to information that is found on the LDAP server.

You can also use LDAP to assign users and IMMs to groups and perform group authentication, in addition to the normal user (password check) authentication. For example, an IMM can be associated with one or more groups, and a user would pass group authentication only if the user belongs to at least one group that is associated with the IMM.

Setting up a client to use the LDAP server

To set up a client to use the LDAP server, complete the following steps:

1. Log in to the IMM on which you want to set up the client. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Network protocols** and scroll down to the **Lightweight Directory Access Protocol (LDAP) Client** area of the page.

   The IMM contains a Version 2.0 LDAP client that you can configure to provide user authentication through one or more LDAP servers. The LDAP server that is to be used for authentication can be discovered dynamically or manually preconfigured.
3. Choose one of the following methods to configure the LDAP client:

- To dynamically discover the LDAP server, select **Use DNS to Find LDAP Servers**.

  If you choose to discover the LDAP server dynamically, the mechanisms that are described by RFC2782 (a DNS RR for specifying the location of services) are applied to find the server. This is known as DNS SRV. The parameters are described in the following list:

  Domain Source
  The DNS SRV request that is sent to the DNS server must specify a domain name. The LDAP client determines where to get this domain name according to which option is selected. There are three options:
  - **Extract search domain from login id**. The LDAP client uses the domain name in the login ID. For example, if the login ID is joesmith@mycompany.com, the domain name is mycompany.com. If the domain name cannot be extracted, the DNS SRV fails, causing the user authentication to fail automatically.
  - **Use only configured search domain below**. The LDAP client uses the domain name that is configured in the **Search Domain** parameter.
  - **Try login id first, then configured value**. The LDAP client first attempts to extract the domain name from the login ID. If this is successful, this domain name is used in the DNS SRV request. If no domain name is present in the login ID, the LDAP client uses the configured **Search Domain** parameter as the domain name in the DNS SRV request. If nothing is configured, user authentication fails immediately.

  Search Domain
  This parameter can be used as the domain name in the DNS SRV request, depending on how the **Domain Source** parameter is configured.

  Service Name
  The DNS SRV request that is sent to the DNS server must also specify a service name. The configured value is used. If this field is left blank, the default value is **ldap**. The DNS SRV request must also specify a protocol name. The default is **tcp** and is not configurable.
- To use a preconfigured LDAP server, select **Use Pre-Configured LDAP Server**.

  Note: The port number for each server is optional. If the field is left blank, the default value of 389 is used for nonsecured LDAP connections. For secured connections, the default is 636. You must configure at least one LDAP server.

  You can configure the following parameters:

  Root DN
  This is the distinguished name (DN) of the root entry of the directory tree on the LDAP server (for example, dn=mycompany,dc=com). This DN is used as the base object for all searches.

  UID Search Attribute
  When the selected binding method is **Anonymously** or **w/ Configured Credentials**, the initial bind to the LDAP server is followed by a search request that is aimed at retrieving specific information about the user, including the user's DN, login permissions, and group membership. This search request must specify the attribute name that is used to represent user IDs on that server. This attribute name is configured here.

On Active Directory servers, this attribute name is usually **sAMAccountName**. On Novell eDirectory and OpenLDAP servers, it is usually **uid**. If this field is left blank, it defaults to **uid**.

Group Filter

This field is used for group authentication. Group authentication is attempted after the user's credentials are successfully verified. If group authentication fails, the user's attempt to log on is denied. When the group filter is configured, it is used to specify to which groups the service processor belongs. This means that the user must belong to at least one of the groups that are configured for group authentication to succeed.

If the **Group Filter** field is left blank, group authentication automatically succeeds. If the group filter is configured, an attempt is made to match at least one group in the list to a group to which the user belongs. If there is no match, the user fails authentication and is denied access. If there is at least one match, group authentication is successful. The comparisons are case sensitive.

The filter is limited to 511 characters and can consist of one or more group names. The colon (:) character must be used to delimit multiple group names. Leading and trailing spaces are ignored, but any other space is treated as part of the group name. A selection to allow or not allow the use of wildcards in the group name is provided. The filter can be a specific group name (for example, IMMWest), a wildcard (*) that matches everything, or a wildcard with a prefix (for example, IMM*). The default filter is IMM*. If security policies in your installation prohibit the use of wildcards, you can choose to not allow the use of wildcards, and the wildcard character (*) is treated as a normal character instead of the wildcard.

A group name can be specified as a full DN or using only the cn portion. For example, a group with a DN of cn=adminGroup,dc=mycompany,dc=com can be specified using the actual DN or with adminGroup.

For Active Directory environments only, nested group membership is supported. For example, if a user is a member of GroupA and GroupB and GroupA is a member of GroupC, the user is said to be a member of GroupC also. Nested searches stop if 128 groups have been searched. Groups in one level are searched before groups in a lower level. Loops are not detected.

Binding Method

Before the LDAP server can be searched or queried, a bind request must be sent. This parameter controls how this initial bind to the LDAP server is performed. Choose from the following three options:

- **Anonymously**. Bind without a DN or password. This option is strongly discouraged because most servers are configured to not allow search requests on specific user records.
- **w/ Configured Credentials**. Bind with configured client DN and password.
- **w/ Login Credentials**. Bind with the credentials that are supplied during the login process. The user ID can be provided through a Distinguished Name, a fully qualified domain name, or a user ID that matches the UID Search Attribute that is configured on the IMM.

If the initial bind is successful, a search is performed to find an entry on the LDAP server that belongs to the user who is logging in. If necessary,

a second attempt to bind is attempted, this time with the DN that is retrieved from the user's LDAP record and the password that was entered during the login process. If this fails, the user is denied access. The second bind is performed only when the Anonymously or Configured Credentials binding methods are used.

Configuring LDAP client authentication

To configure the LDAP client authentication, complete the following steps:

1. In the navigation pane, click **Network protocols**.
2. Scroll down to the **Lightweight Directory Access Protocol (LDAP) Client** area of the page and click **Set DN and password only if Binding Method used is w/ Configured Credentials**.
3. To use client-based authentication, in the **Client DN** field, type a client distinguished name. Type a password in the **Password** field or leave it blank.

Configuring LDAP search attributes

To configure the LDAP search attributes, complete the following steps:

1. In the navigation pane, click **Network protocols**.
2. Scroll down to the **Lightweight Directory Access Protocol (LDAP) Client** area and click **Set attribute names for LDAP client search algorithm**.
3. To configure the search attributes, use the following information.

UID Search Attribute

When the selected binding method is **Anonymously** or **w/ Configured Credentials**, the initial bind to the LDAP server is followed by a search request that is directed at retrieving specific information about the user, including the distinguished name, login permissions, and group membership. To retrieve this information, the search request must specify the attribute name that is used to represent user IDs on that server. Specifically, this name is used as a search filter against the login ID that is entered by the user. This attribute name is configured here. For example, on Active Directory servers, the attribute name that is used for user IDs is usually sAMAccoutName. On Novell eDirectory and OpenLDAP servers, it is usually uid. If this field is left blank, a default of UID is used during user authentication.

Group Search Attribute

In an Active Directory or Novell eDirectory environment, this parameter specifies the attribute name that is used to identify the groups to which a user belongs. In Active Directory, this is usually memberOf, and with eDirectory, this is usually groupMembership.

In an OpenLDAP server environment, users are usually assigned to groups whose objectClass equals PosixGroup. In that context, this parameter specifies the attribute name that is used to identify the members of a particular PosixGroup. This is usually memberUid.

If this field is left blank, the attribute name in the filter defaults to memberOf.

Login Permission Attribute

When a user is authenticated through an LDAP server successfully, the login permissions for this user must be retrieved. To retrieve these permissions, the search filter that is sent to the server must specify the attribute name that is associated with login permissions. This field specifies this attribute name.

If this field is left blank, the user is assigned a default of read-only permissions, assuming that the user passes the user and group authentication.

The attribute value that is returned by the LDAP server is searched for the keyword string IBMRBSPermission=. This keyword must be immediately followed by a bit string that is entered as 12 consecutive 0's or 1's. Each bit represents a set of functions. The bits are numbered according to their positions. The leftmost bit is bit position 0, and the rightmost bit is bit position 11. A value of 1 at a position enables the function that is associated with that position. A value of 0 disables that function. The string IBMRBSPermission=010000000000 is a valid example.

The IBMRBSPermission= keyword is used to allow it to be placed anywhere in the attribute field. This enables the LDAP administrator to reuse an existing attribute, therefore preventing an extension to the LDAP schema. This also enables the attribute to be used for its original purpose. You can add the keyword string anywhere in the attribute field. The attribute that you use should allow for a free-formatted string.

When the attribute is retrieved successfully, the value that is returned by the LDAP server is interpreted according to the following information:

- **Deny Always (bit position 0):** If this bit is set, the user always fails authentication. This function can be used to block a user or users who are associated with a particular group.
- **Supervisor Access (bit position 1):** If this bit is set, the user is given administrator privileges. The user has read and write access to every function. When this bit is set, bits 2 through 11 do not have to be set individually.
- **Read Only Access (bit position 2):** If this bit is set, the user has read-only access and cannot perform any maintenance procedures (for example, restart, remote actions, and firmware updates) or modify anything (using the save, clear, or restore functions). The Read Only Access bit and all other bits are mutually exclusive, with the Read Only Access bit having the lowest precedence. If any other bit is set, the Read Only Access bit is ignored.
- **Networking and Security (bit position 3):** If this bit is set, the user can modify the configuration on the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port pages.
- **User Account Management (bit position 4):** If this bit is set, the user can add, modify, and delete users and change the Global Login Settings in the Login Profiles page.
- **Remote Console Access (bit position 5):** If this bit is set, the user can access the remote server console.
- **Remote Console and Remote Disk (bit position 6):** If this bit is set, the user can access the remote server console and the remote disk functions for the remote server.
- **Remote Server Power/Restart Access (bit position 7):** If this bit is set, the user can access the power-on and restart functions for the remote server. These functions are available in the Power/Restart page.
- **Basic Adapter Configuration (bit position 8):** If this bit is set, the user can modify configuration parameters on the System Settings and Alerts pages.

- **Ability to Clear Event Logs (bit position 9):** If this bit is set, the user can clear the event logs. All users can view the event logs, but this particular permission is required to clear the logs.
- **Advanced Adapter Configuration (bit position 10):** If this bit is set, the user has no restrictions when configuring the IMM. In addition, the user is said to have administrative access to the IMM, meaning that the user can also perform the following advanced functions: firmware upgrades, PXE network boot, restoring IMM factory defaults, modifying and restoring IMM configuration from a configuration file, and restarting and resetting the IMM.
- **Reserved (bit position 11):** This bit is reserved for future use.

If none of the bits are set, the user has read-only authority.

Priority is given to login permissions that are retrieved directly from the user record. If the login permission attribute is not in the user's record, an attempt is made to retrieve the permissions from the groups to which the user belongs. This is done as part of the group authentication phase. The user is assigned the inclusive OR of all the bits for all of the groups. The Read Only bit is set only if all the other bits are zero. If the Deny Always bit is set for any of the groups, the user is refused access. The Deny Always bit always has precedence over every other bit.

Important: If you give a user the ability to modify basic, networking, and security-related IMM configuration parameters, consider giving this same user the ability to restart the IMM (bit position 10). Otherwise, a user might be able to change parameters (for example, the IP address of the IMM) but cannot make them take effect.

Service Location Protocol (SLP)

To view the SLP setting, complete the following steps:

1. In the navigation pane, click **Network protocols**.
2. Scroll down to the **Service Location Protocol (SLP)** area. The multicast address, which is the IP address that the IMM SLP server listens on, is displayed.

Configuring security

Use the general procedure in this section to configure security for the IMM Web server, for the connection between the IMM and an LDAP server. If you are not familiar with the use of SSL certificates, read the information in "SSL certificate overview" on page 39.

Use the following general tasks list to configure the security for the IMM:

1. Configure the Secure Web server:
   a. Disable the SSL server. Use the **HTTPS Server Configuration for Web Server** area on the Security page.
   b. Generate or import a certificate. Use the **HTTPS Server Certificate Management** area on the Security page (see "SSL server certificate management" on page 40).
   c. Enable the SSL server. Use the **HTTPS Server Configuration for Web Server** area on the Security page (see "Enabling SSL for the secure Web server" on page 43).
2. Configure SSL security for LDAP connections:

a. Disable the SSL client. Use the **SSL Client Configuration for LDAP Client** area on the Security page.
b. Generate or import a certificate. Use the **SSL Client Certificate Management** area on the Security page (see "SSL client certificate management" on page 43).
c. Import one or more trusted certificates. Use the **SSL Client Trusted Certificate Management** area on the Security page (see "SSL client trusted certificate management" on page 43).
d. Enable the SSL client. Use the **SSL Client Configuration for LDAP Client** area on the Security page (see "Enabling SSL for the LDAP client" on page 44).

3. Restart the IMM for SSL server configuration changes to take effect. For more information, see "Restarting IMM" on page 47.

   Note: Changes to the SSL client configuration take effect immediately and do not require a restart of the IMM.

Secure Web server and secure LDAP

Secure Sockets Layer (SSL) is a security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

You can configure the IMM to use SSL support for two types of connections: secure server (HTTPS) and secure LDAP connection (LDAPS). The IMM takes on the role of SSL client or SSL server depending on the type of connection. The following table shows that the IMM acts as an SSL server for secure Web server connections. The IMM acts as an SSL client for secure LDAP connections.

Table 5. IMM SSL connection support

Connection type	SSL client	SSL server
Secure Web server (HTTPS)	Web browser of the user (For example: Microsoft Internet Explorer)	IMM Web server
Secure LDAP connection (LDAPS)	IMM LDAP client	An LDAP server

You can view or change the SSL settings from the Security page. You can enable or disable SSL and manage the certificates that are required for SSL.

SSL certificate overview

You can use SSL with either a self-signed certificate or with a certificate that is signed by a third-party certificate authority. Using a self-signed certificate is the simplest method for using SSL, but it does create a small security risk. The risk arises because the SSL client has no way of validating the identity of the SSL server for the first connection that is attempted between the client and server. It is possible that a third party might impersonate the server and intercept data that is flowing between the IMM and the Web browser. If, at the time of the initial connection between the browser and the IMM, the self-signed certificate is imported into the certificate store of the browser, all future communications will be secure for that browser (assuming that the initial connection was not compromised by an attack).

For more complete security, you can use a certificate that is signed by a certificate authority. To obtain a signed certificate, use the SSL Certificate Management page

to generate a certificate-signing request. You must then send the certificate-signing request to a certificate authority and make arrangements to procure a certificate. When the certificate is received, it is then imported into the IMM through the **Import a Signed Certificate** link, and you can enable SSL.

The function of the certificate authority is to verify the identity of the IMM. A certificate contains digital signatures for the certificate authority and the IMM. If a well-known certificate authority issues the certificate or if the certificate of the certificate authority has already been imported into the Web browser, the browser can validate the certificate and positively identify the IMM Web server.

The IMM requires a certificate for the secure Web server and one for the secure LDAP client. Also, the secure LDAP client requires one or more trusted certificates. The trusted certificate is used by the secure LDAP client to positively identify the LDAP server. The trusted certificate is the certificate of the certificate authority that signed the certificate of the LDAP server. If the LDAP server uses self-signed certificates, the trusted certificate can be the certificate of the LDAP server itself. Additional trusted certificates must be imported if more than one LDAP server is used in your configuration.

SSL server certificate management

The SSL server requires that a valid certificate and corresponding private encryption key be installed before SSL is enabled. Two methods are available for generating the private key and required certificate: using a self-signed certificate and using a certificate that is signed by a certificate authority. If you want to use a self-signed certificate for the SSL server, see "Generating a self-signed certificate." If you want to use a certificate-authority-signed certificate for the SSL server, see "Generating a certificate-signing request."

Generating a self-signed certificate

To generate a new private encryption key and self-signed certificate, complete the following steps:

1. In the navigation plane, click **Security**.
2. In the **SSL Server Configuration for Web Server** area, make sure that the setting is **Disabled**. If it is not disabled, select **Disabled** and then click **Save**.

   Notes:

   a. The IMM must be restarted before the selected value (**Enabled** or **Disabled**) takes effect.

   b. Before you can enable SSL, a valid SSL certificate must be in place.

   c. To use SSL, you must configure a client Web browser to use SSL3 or TLS. Older export-grade browsers with only SSL2 support cannot be used.
3. In the **SSL Server Certificate Management** area, select **Generate a New Key and a Self-signed Certificate**.
4. Type the information in the required fields and any optional fields that apply to your configuration. For a description of the fields, see "Required certificate data" on page 41. After you finish typing the information, click **Generate Certificate**. Your new encryption keys and certificate are generated. This process might take several minutes. You see confirmation if a self-signed certificate is installed.

Generating a certificate-signing request

To generate a new private encryption key and certificate-signing request, complete the following steps:

1. In the navigation pane, click **Security**.
2. In the **SSL Server Configuration for Web Server** area, make sure that the SSL server is disabled. If it is not disabled, select **Disabled** in the **SSL Server** field and then click **Save**.
3. In the **SSL Server Certificate Management** area, select **Generate a New Key and a Certificate-Signing Request**.
4. Type the information in the required fields and any optional fields that apply to your configuration. The fields are the same as for the self-signed certificate, with some additional fields.

   Read the information in the following sections for a description of each of the common fields.

   Required certificate data
   The following user-input fields are required for generating a self-signed certificate or a certificate-signing request:

   Country
   Use this field to indicate the country where the IMM is physically located. This field must contain the 2-character country code.

   State or Province
   Use this field to indicate the state or province where the IMM is physically located. This field can contain a maximum of 30 characters.

   City or Locality
   Use this field to indicate the city or locality where the IMM is physically located. This field can contain a maximum of 50 characters.

   Organization Name
   Use this field to indicate the company or organization that owns the IMM. When this is used to generate a certificate-signing request, the issuing certificate authority can verify that the organization that is requesting the certificate is legally entitled to claim ownership of the given company or organization name. This field can contain a maximum of 60 characters.

   IMM Host Name
   Use this field to indicate the IMM host name that currently appears in the browser Web address bar.

   Make sure that the value that you typed in this field exactly matches the host name as it is known by the Web browser. The browser compares the host name in the resolved Web address to the name that appears in the certificate. To prevent certificate warnings from the browser, the value that is used in this field must match the host name that is used by the browser to connect to the IMM. For example, if the address in the Web address bar is http://mm11.xyz.com/private/main.ssi, the value that is used for the IMM Host Name field must be mm11.xyz.com. If the Web address is http://mm11/private/main.ssi, the value that is used must be mm11. If the Web address is http://192.168.70.2/private/main.ssi, the value that is used must be 192.168.70.2.

   This certificate attribute is generally referred to as the common name.

   This field can contain a maximum of 60 characters.

Contact Person
Use this field to indicate the name of a contact person who is responsible for the IMM. This field can contain a maximum of 60 characters.

Email Address
Use this field to indicate the e-mail address of a contact person who is responsible for the IMM. This field can contain a maximum of 60 characters.

Optional certificate data
The following user-input fields are optional for generating a self-signed certificate or a certificate-signing request:

Organizational Unit
Use this field to indicate the unit within the company or organization that owns the IMM. This field can contain a maximum of 60 characters.

Surname
Use this field for additional information, such as the surname of a person who is responsible for the IMM. This field can contain a maximum of 60 characters

Given Name
Use this field for additional information, such as the given name of a person who is responsible for the IMM. This field can contain a maximum of 60 characters.

Initials
Use this field for additional information, such as the initials of a person who is responsible for the IMM. This field can contain a maximum of 20 characters.

DN Qualifier
Use this field for additional information, such as a distinguished name qualifier for the IMM. This field can contain a maximum of 60 characters.

Certificate-Signing request attributes
The following fields are optional unless they are required by your selected certificate authority:

Challenge Password
Use this field to assign a password to the certificate-signing request. This field can contain a maximum of 30 characters.

Unstructured Name
Use this field for additional information, such as an unstructured name that is assigned to the IMM. This field can contain a maximum of 60 characters.

5. After you complete the information, click **Generate CSR**. The new encryption keys and certificate are generated. This process might take several minutes.
6. Click **Download CSR** and then click **Save** to save the file to your workstation. The file that is produced when you create a certificate-signing request is in DER format. If your certificate authority expects the data in some other format, such as PEM, you can convert the file by using a tool such as OpenSSL (http://www.openssl.org). If the certificate authority asks you to copy the contents of the certificate-signing request file into a Web browser window, PEM format is usually expected.

   The command for converting a certificate-signing request from DER to PEM format using OpenSSL is similar to the following example:

```
openssl req -in csr.der -inform DER -out csr.pem -outform PEM
```

7. Send the certificate-signing request to your certificate authority. When the certificate authority returns your signed certificate, you might have to convert the certificate to DER format. (If you received the certificate as text in an e-mail or a Web page, it is probably in PEM format.) You can change the format using a tool that is provided by your certificate authority or using a tool such as OpenSSL (http://www.openssl.org). The command for converting a certificate from PEM to DER format is similar to the following example:

   ```
   openssl x509 -in cert.pem -inform PEM -out cert.der -outform DER
   ```

   Go to step 8 after the signed certificate is returned from the certificate authority.
8. In the navigation pane, click **Security**. Scroll to the **SSL Server Certificate Management** area.
9. Click **Import a Signed Certificate**.
10. Click **Browse**.
11. Click the certificate file that you want and then click **Open**. The file name (including the full path) is displayed in the field next to the **Browse** button.
12. Click **Import Server Certificate** to begin the process. A progress indicator is displayed as the file is transferred to storage on the IMM. Continue to display this page until the transfer is completed.

Enabling SSL for the secure Web server

Note: To enable SSL, a valid SSL certificate must be installed.

Complete the following steps to enable the secure Web server:

1. In the navigation pane, click **Security**. The page that is displayed shows that a valid SSL server certificate is installed. If the SSL server certificate status does not show that a valid SSL certificate is installed, go to "SSL server certificate management" on page 40.
2. Scroll to the **SSL Server Configuration for Web Server** area, select **Enabled** in the **SSL Client** field, and then click **Save**. The selected value takes effect the next time the IMM is restarted.

SSL client certificate management

The SSL client requires that a valid certificate and corresponding private encryption key be installed before SSL is enabled. Two methods are available for generating the private key and required certificate: using a self-signed certificate, or using a certificate signed by a certificate authority.

The procedure for generating the private encryption key and certificate for the SSL client is the same as the procedure for the SSL server, except that you use the **SSL Client Certificate Management** area of the Security Web page instead of the **SSL Server Certificate Management** area. If you want to use a self-signed certificate for the SSL client, see "Generating a self-signed certificate" on page 40. If you want to use a certificate authority signed certificate for the SSL client, see "Generating a certificate-signing request" on page 40.

SSL client trusted certificate management

The secure SSL client (LDAP client) uses trusted certificates to positively identify the LDAP server. A trusted certificate can be the certificate of the certificate authority that signed the certificate of the LDAP server, or it can be the actual

certificate of the LDAP server. At least one certificate must be imported to the IMM before the SSL client is enabled. You can import up to three trusted certificates.

To import a trusted certificate, complete the following steps:

1. In the navigation pane, select **Security**.
2. In the **SSL Client Configuration for LDAP Client** area, make sure that the SSL client is disabled. If it is not disabled, select **Disabled** in the **SSL Client** field and then click **Save**.
3. Scroll to the **SSL Client Trusted Certificate Management** area.
4. Click **Import** next to one of the **Trusted CA Certificate 1** fields.
5. Click **Browse**.
6. Select the certificate file that you want and click **Open**. The file name (including the full path) is displayed in the box next to the **Browse** button.
7. To begin the import process, click **Import Certificate**. A progress indicator is displayed as the file is transferred to storage on the IMM. Continue displaying this page until the transfer is completed.

   The **Remove** button is now available for the Trusted CA Certificate 1 option. If you want to remove a trusted certificate, click the corresponding **Remove** button.

   You can import other trusted certificates by using the Trusted CA Certificate 2 and the Trusted CA Certificate 3 **Import** buttons.

Enabling SSL for the LDAP client

Use the **SSL Client Configuration for LDAP Client** area of the Security page to enable or disable SSL for the LDAP Client. To enable SSL, a valid SSL client certificate and at least one trusted certificate must first be installed.

To enable SSL for the client, complete the following steps:

1. In the navigation pane, click **Security**.

   The Security page shows an installed SSL client certificate and Trusted CA Certificate 1.
2. On the SSL Client Configuration for LDAP Client page, select **Enabled** in the **SSL Client** field.

   Notes:

   a. The selected value (Enabled or Disabled) takes effect immediately.
   b. Before you can enable SSL, a valid SSL certificate must be in place.
   c. Your LDAP server must support SSL3 or TLS to be compatible with the SSL implementation that the LDAP client uses.
3. Click **Save**. The selected value takes effect immediately.

Configuring the Secure Shell server

The Secure Shell (SSH) feature provides secure access to the command-line interface and the serial (text console) redirect features of the IMM.

Secure Shell users are authenticated by exchanging user ID and password. The password and user ID are sent after the encryption channel is established. The user ID and password pair can be one of the 12 locally stored user IDs and passwords, or they can be stored on an LDAP server. Public key authentication is not supported.

Generating a Secure Shell server key

A Secure Shell server key is used to authenticate the identity of the Secure Shell server to the client. Secure shell must be disabled before you create a new Secure Shell server private key. You must create a server key before you enable the Secure Shell server.

When you request a new server key, both a Rivest, Shamir, and Adelman key and a DSA key are created to allow access to the IMM from an SSH version 2 client. For security, the Secure Shell server private key is not backed up during a configuration save and restore operation.

To create a new Secure Shell server key, complete the following steps:

1. In the navigation pane, click **Security**.
2. Scroll to the **Secure Shell (SSH) Server** area and make sure that the Secure Shell server is disabled. If it is not disabled, select **Disabled** in the **SSH Server** field and then click **Save**.
3. Scroll to the **SSH Server Key Management** area.
4. Click **Generate SSH Server Private Key**. A progress window opens. Wait for the operation to be completed.

Enabling the Secure Shell server

From the Security page you can enable or disable the Secure Shell server. The selection that you make takes effect only after the IMM is restarted. The value that is displayed on the screen (Enabled or Disabled) is the last selected value and is the value that is used when the IMM is restarted.

Note: You can enable the Secure Shell server only if a valid Secure Shell server private key is installed.

To enable the Secure Shell server, complete the following steps:

1. In the navigation pane, click **Security**.
2. Scroll to the **Secure Shell (SSH) Server** area.
3. Click **Enabled** in the **SSH Server** field.
4. In the navigation pane, click **Restart IMM** to restart the IMM.

Using the Secure Shell server

If you are using the Secure Shell client that is included in Red Hat Linux version 7.3, to start a Secure Shell session to an IMM with network address 192.168.70.132, type a command similar to the following example:

```
ssh -x -l userid 192.168.70.132
```

where -x indicates no X Window System forwarding and -l indicates that the session should use the user ID *userid*.

Using the configuration file

Select **Configuration File** in the navigation pane to back up and restore the IMM configuration.

Important: Security page settings are not saved with the backup operation and cannot be restored with the restore operation.

Backing up your current configuration

You can download a copy of your current IMM configuration to the client computer that is running the IMM Web interface. Use this backup copy to restore your IMM configuration if it is accidentally changed or damaged. Use it as a base that you can modify to configure multiple IMMs with similar configurations.

The configuration information that is saved under this procedure does not include the server firmware configuration settings or any IPMI settings that are not common with the non-IMPI user interfaces.

To back up your current configuration, complete the following steps:

1. Log in to the IMM where you want to back up your current configuration. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Configuration File**.
3. In the **Backup IMM Configuration** area, click **view the current configuration summary**.
4. Verify the settings and then click **Close**.
5. To back up this configuration, click **Backup**.
6. Type a name for the backup, select the location where the file will be saved, and then click **Save**.

   In Mozilla Firefox, click **Save File**, then click **OK**.

   In Microsoft Internet Explorer, click **Save this file to disk**, then click **OK**.

Restoring and modifying your IMM configuration

You can restore a saved configuration in full, or you can modify key fields in the saved configuration before you restore the configuration to your IMM. By modifying the configuration file before you restore it, you can set up multiple IMMs with similar configurations. You can quickly specify parameters that require unique values such as names and IP addresses, without having to enter common, shared information.

To restore or modify your current configuration, complete the following steps:

1. Log in to the IMM where you want to restore the configuration. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Configuration File**.
3. In the **Restore IMM Configuration** area, click **Browse**.
4. Click the configuration file that you want; then, click **Open**. The file (including the full path) appears in the box next to **Browse**.
5. If you do not want to make changes to the configuration file, click **Restore**. A new window opens with the IMM configuration information. Make sure that this is the configuration that you want to restore. If it is not the correct configuration, click **Cancel**.

   If you want to make changes to the configuration file before you restore the configuration, click **Modify and Restore** to open an editable configuration summary window. Initially, only the fields that allow changes are displayed. To change between this view and the complete configuration summary view, click the **Toggle View** button at the top or bottom of the window. To modify the contents of a field, click the corresponding text box and enter the data.

Note: When you click **Restore** or **Modify and Restore**, an alert window might open if the configuration file that you are attempting to restore was created by a different type of service processor or was created by the same type of service processor with older firmware (and therefore, with less functionality). This alert message includes a list of systems-management functions that you must configure after the restoration is complete. Some functions require configurations on more than one window.

6. To continue restoring this file to the IMM, click **Restore Configuration**. A progress indicator is displayed as the firmware on the IMM is updated. A confirmation window opens to verify whether the update was successful.

   Note: The security settings on the Security page are not restored by the restore operation. To modify security settings, see "Secure Web server and secure LDAP" on page 39.

7. After you receive a confirmation that the restore process is complete, in the navigation pane, click **Restart IMM**; then, click **Restart**.
8. Click **OK** to confirm that you want to restart the IMM.
9. Click **OK** to close the current browser window.
10. To log in to the IMM again, start the browser, and follow your regular login process.

Restoring defaults

Use the **Restore Defaults** link to restore the default configuration of the IMM, if you have Supervisor access.

Attention: When you click **Restore Defaults**, you will lose all the modifications that you made to the IMM.

To restore the IMM defaults, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Restore Defaults** to restore default settings of the IMM. If this is a local server, your TCP/IP connection will be broken, and you must reconfigure the network interface to restore connectivity.
3. Log in again to use the IMM Web interface.
4. Reconfigure the network interface to restore connectivity. For information about the network interface, see "Configuring network interfaces" on page 28.

Restarting IMM

Use the **Restart IMM** link to restart the IMM. You can perform this function only if you have Supervisor access. Any Ethernet connections are temporarily dropped. You must log in again to use the IMM Web interface.

To restart the IMM, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Restart IMM** to restart the IMM. Your TCP/IP or modem connections are broken.
3. Log in again to use the IMM Web interface.

Logging off

To log off the IMM or another remote server, click **Log Off** in the navigation pane.

Chapter 4. Monitoring server status

Use the links under the **Monitors** heading of the navigation pane to view the status of the server that you are accessing.

From the System Status pages, you can:

- Monitor the power status of the server and view the state of the operating system
- View the server temperature readings, voltage thresholds, and fan speeds
- View the latest server operating-system-failure screen capture
- View the list of users who are logged in to the IMM

From the Easy LED Diagnostics page, you can view the name, color, and status of any LEDs that are lit on a server.

From the Event Log page, you can:

- View certain events that are recorded in the event log of the IMM
- View the severity of events

From the Vital Product Data (VPD) page, you can view the vital product data.

Viewing system status

On the System Status page, you can monitor the temperature readings, voltage thresholds, and fan status of your server. You can also view the latest operating-system-failure screen, the users who are logged in to the IMM, and the system locator LED.

To view the system health and environmental information of the server, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **System Status** to view a dynamically-generated update of the overall health of the server.

   The status of your server determines the message that is shown at the top of the System Health Summary page. One of the following symbols is displayed:

   - A solid green circle and the phrase `Server is operating normally`
   - Either a red circle that contains an X or a yellow triangle that contains an exclamation point and the phrase `One or more monitored parameters are abnormal`

   If the monitored parameters are operating outside normal ranges, a list of the specific abnormal parameters is displayed on the System Health Summary page.
3. Scroll down to the **Temperature** area in the **Environmentals** section of the page, which includes temperature, voltage, and fan speed information.

   The IMM tracks the current temperature readings and threshold levels for system components such as microprocessors, system board, and hard disk drive backplane. When you click a temperature reading, a new window opens.

The Temperature Thresholds page displays the temperature levels at which the IMM reacts. The temperature threshold values are preset on the remote server and cannot be changed.

The reported temperatures are measured against the following threshold ranges:

Non-Critical
When the temperature reaches a specified value, a temperature alert is sent to the configured remote alert recipients. You must select the **Warning Alerts** check box in the **SNMP Alerts Settings** area of the Alerts page or the **Warning Alerts** check box on the Remote Alert Recipient page for the alert to be sent.

For more information about selecting alert options, see "Configuring SNMP alert settings" on page 26 or "Configuring remote alert recipients" on page 24.

Critical
When the temperature reaches a specified value higher than the warning value (the soft shutdown threshold), a second temperature alert is sent to configured remote alert recipients, and the server begins the shutdown process with an orderly operating-system shutdown. The server then turns itself off. You must select the **Critical Alerts** check box in the **SNMP Alerts Settings** area of the Alerts page or the **Critical Alerts** check box on the Remote Alert Recipient page for the alert to be sent.

For more information about selecting alert options, see "Configuring SNMP alert settings" on page 26 or "Configuring remote alert recipients" on page 24.

Fatal When the temperature reaches a specified value higher than the soft shutdown value (the hard shutdown threshold), the server immediately shuts down and sends an alert to configured remote alert recipients. You must select the **Critical Alerts** check box in the **SNMP Alerts Settings** area of the Alerts page or the **Critical Alerts** check box on the Remote Alert Recipient page for the alert to be sent.

For more information about selecting alert options, see "Configuring SNMP alert settings" on page 26 or "Configuring remote alert recipients" on page 24.

The IMM generates a non-critical, critical, or fatal event when the threshold is reached and initiates shutdown actions, if they are required.

4. Scroll down to the **Voltages** area. The IMM will send an alert if any monitored power source voltage falls outside its specified operational ranges.

   If you click a voltage reading, a new window opens.

   The Voltage Thresholds page displays the voltage ranges at which the IMM reacts. The voltage threshold values are preset on the remote server and cannot be changed.

   The IMM Web interface displays the voltage readings of the system board and the voltage regulator modules (VRM). The system sets a voltage range at which the following actions are taken:

   Non-Critical
   When the voltage drops below or exceeds a specified voltage range, a voltage alert is sent to configured remote alert recipients. You must

select the **Warning Alerts** check box in the **SNMP Alerts Settings** area of the Alerts page for the alert to be sent.

For more information about selecting alert options, see "Configuring SNMP alert settings" on page 26.

Critical
When the voltage drops below or exceeds a specified voltage range, a voltage alert is sent to configured remote alert recipients, and the server begins the shutdown process with an orderly operating-system shutdown. The server then turns itself off. You must select the **Critical Alerts** check box in the **SNMP Alerts Settings** area of the Alerts page for the alert to be sent.

For more information about selecting alert options, see "Configuring SNMP alert settings" on page 26.

Fatal When the voltage drops below or exceeds a specified voltage range, the server immediately shuts down and sends an alert to configured remote alert recipients. You must select the **Fatal Alerts** check box in the **SNMP Alerts Settings** area of the Alerts page for the alert to be sent.

Note: The hard shutdown alert is sent only if a soft shutdown alert has not yet been sent.

For more information about selecting alert options, see "Configuring SNMP alert settings" on page 26.

The IMM generates a non-critical, critical, or fatal event when the threshold is reached, and generates any shutdown actions, if they are required.

Non-critical
If the IMM indicates that this threshold has been reached, a warning event is generated.

Critical
If the IMM indicates that this threshold has been reached, a critical event is generated.

Fatal If the IMM indicates that this threshold has been reached, a critical event is generated.

5. Scroll down to the **Fan Speeds (% of max)** area. The IMM Web interface displays the running speed of the server fans (expressed in a percentage of the maximum fan speed). If you click a fan reading, a new window opens.

   You receive a fan alert when the fan speeds drop to an unacceptable level or when the fans stop. You must select the **Critical Alerts** check box in the **SNMP Alerts Settings** area of the Alerts page for the alert to be sent.

   For more information about selecting alert options, see "Configuring SNMP alert settings" on page 26.

6. Scroll down to the **View Latest OS Failure Screen** area. Click **View OS Failure Screen** to access an image of the operating-system-failure screen that was captured when the server stopped functioning.

   Note:

   The operating-system-failure screen capture feature is available only with IMM Premium. For information about upgrading from IMM Standard to IMM Premium, see "Upgrading from IMM Standard to IMM Premium" on page 3.

If an event occurs that causes the operating system to stop running, the operating-system watchdog is triggered, which causes the IMM to capture the operating-system-failure screen data and store it. The IMM stores only the most recent error event information, overwriting older operating-system-failure screen data when a new error event occurs.

To remotely access a server operating-system-failure screen image, complete the following steps:

a. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
b. In the navigation pane, click **System Health**, and then scroll down to the **View Latest OS Failure Screen** area.
c. Click **View OS Failure Screen**. The operating-system-failure screen image is displayed on your screen.

7. Scroll down to the **Users Currently Logged in** area. The IMM Web interface displays the login ID and access method of each user who is logged in to the IMM.
8. Scroll down to the **System Locator LED** area. The IMM Web interface displays the status of the system locator LED. It also provides buttons to change the state of the LED. For the meaning of the graphics that are displayed in this area, see the online help.

Viewing the Easy LED Diagnostics

The Easy LED Diagnostics screen displays the name, color, and status of any LEDs that are lit on the server.

To access and view the Easy LED Diagnostics, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Easy LED Diagnostics** to view the recent history of events on the server.
3. Scroll down to view the complete contents of the Easy LED Diagnostics.

Note: If an LED is not lit on the server, the Color column of the Easy LED Diagnostics table indicates that the LED Color is Not Applicable.

Viewing the event logs

Note: For an explanation of a specific event or message, see the *Hardware Maintenance Manual* that is available on the Lenovo Support Web site at http://www.lenovo.com/support.

Error codes and messages are displayed in the following types of event logs:

- **System-event log:** This log contains POST and system management interrupt (SMI) events and all events that are generated by the BMC that is embedded in the IMM. You can view the system-event log through the Setup Utility and through the Dynamic System Analysis (DSA) program (as the IPMI event log).

  The system-event log is limited in size. When it is full, new entries will not overwrite existing entries; therefore, you must periodically save and then clear the system-event log through the Setup Utility. When you are troubleshooting, you might have to save and then clear the system-event log to make the most recent events available for analysis.

Messages are listed on the left side of the screen, and details about the selected message are displayed on the right side of the screen. To move from one entry to the next, use the Up Arrow (↑) and Down Arrow (↓) keys.

The system-event log indicates an assertion event when an event has occurred. It indicates a deassertion event when the event is no longer occurring.

Some IMM sensors cause assertion events to be logged when their setpoints are reached. When a setpoint condition no longer exists, a corresponding deassertion event is logged. However, not all events are assertion-type events.

- **Integrated Management Module (IMM) event log:** This log contains a filtered subset of all IMM, POST, and system management interrupt (SMI) events. You can view the IMM event log through the IMM Web interface and through the Dynamic System Analysis (DSA) program (as the ASM event log).
- **DSA log:** This log is generated by the Dynamic System Analysis (DSA) program, and it is a chronologically ordered merge of the system-event log (as the IPMI event log), the IMM chassis-event log (as the ASM event log), and the operating-system event logs. You can view the DSA log through the DSA program.
- **Chassis event log:** The IMM generates text messages for the IPMI assertion and deassertion events and creates entries for them in the chassis-event log. The text is generated for these events through the Distributed Management Task Force (DMTF) specifications DSP0244 and DSP8007. This log also contains entries for events other than IPMI sensor assertions and deassertions. For example, the chassis-event log includes entries when a user changes a network setting or when a user logs into the Web interface. This log can be viewed from the IMM Web interface.

Viewing the system-event log from the Web interface

Note: The system-event log has a limited capacity. When that limit is reached, the older events are deleted in a first-in, first-out order.

To access and view the event log, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, “Opening and using the IMM Web interface,” on page 9.
2. In the navigation pane, click **Event Log** to view the recent history of events on the server.
3. Scroll down to view the complete contents of the event log. The events are given the following levels of severity:

   Informational
   This severity level is assigned to an event of which you should take note.

   Warning
   This severity level is assigned to an event that might affect server performance.

   Error This severity level is assigned to an event that needs immediate attention.

   The IMM Web interface distinguishes warning events with the letter W on a yellow background in the severity column and error events with the letter E on a red background.
4. Click **Save Log as Text File** to save the contents of the event log as a text file. Click **Reload Log** to refresh the display of the event log. Click **Clear Log** to delete the contents of the event log.

Viewing event logs from the Setup Utility

For complete information about using the Setup Utility, see the documentation that came with your server.

To view the POST event log or system-event log, complete the following steps:

1. Turn on the server.

   Note: Approximately 2 minutes after the server is connected to ac power, the power-control button becomes active.

2. When the prompt `<F1> Setup` is displayed, press F1. If you have set both a power-on password and an administrator password, you must type the administrator password to view the event logs.
3. Select **System Event Logs** and use one of the following procedures:
   - To view the POST event log, select **POST Event Viewer**.
   - To view the system-event log, select **System Event Log**.

Viewing event logs without restarting the server

If the server is not hung, methods are available for you to view one or more event logs without having to restart the server.

If you have installed Portable or Installable Dynamic System Analysis (DSA), you can use it to view the system-event log (as the IPMI event log), the IMM event log (as the ASM event log), the operating-system event logs, or the merged DSA log. You can also use DSA Preboot to view these logs, although you must restart the server to use DSA Preboot. To install Portable DSA, Installable DSA, or DSA Preboot or to download a DSA Preboot CD image, go to http://www.lenovo.com/support or complete the following steps:

Note: Changes are made periodically to the Lenovo Web site. The actual procedure might vary slightly from what is described in this document.

1. steps.

If IPMItool is installed in the server, you can use it to view the system-event log. Most recent versions of the Linux operating system come with a current version of IPMItool.

You can view the IMM event log through the **Event Log** link in the IMM Web interface.

The following table describes the methods that you can use to view the event logs, depending on the condition of the server. The first two conditions generally do not require that you restart the server.

Table 6. Methods for viewing event logs

Condition	Action
The server is not hung and is connected to a network.	Use any of the following methods: • Run Portable or Installable DSA to view the event logs or create an output file that you can send to Lenovo service and support. • Type the IP address of the IMM and go to the Event Log page. • Use IPMItool to view the system-event log.
The server is not hung and is not connected to a network.	Use IPMItool locally to view the system-event log.
The server is hung.	• If DSA Preboot is installed, restart the server and press F2 to start DSA Preboot and view the event logs. • If DSA Preboot is not installed, insert the DSA Preboot CD and restart the server to start DSA Preboot and view the event logs. • Alternatively, you can restart the server and press F1 to start the Setup Utility and view the POST event log or system-event log. For more information, see "Viewing event logs from the Setup Utility" on page 54.

Viewing vital product data

When the server starts, the IMM collects server information, server firmware information, and server component vital product data (VPD) and stores it in nonvolatile memory. You can access this information at any time from almost any computer. The Vital Product Data page contains key information about the remote managed server that the IMM is monitoring.

To view the server component vital product data, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Vital Product Data** to view the status of the hardware and software components on the server.
3. Scroll down to view the following VPD readings:

   Machine level VPD

   The vital product data for the server appears in this area. For viewing VPD, the machine-level VPD includes a universal unique identifier (UUID).

   Note: The machine-level VPD, component-level VPD, and component activity log provide information only when the server is turned on.

Table 7. Machine-level vital product data

Field	Function
Machine type and model	Identifies the server type and model number that the IMM is monitoring.
Serial number	Identifies the serial number of the server that the IMM is monitoring.
UUID	Identifies the universal unique identifier (UUID), a 32-digit hexadecimal number, of the server that the IMM is monitoring.

Component Level VPD

The vital product data for the components of the remote managed server is displayed in this area.

Table 8. Component-level vital product data

Field	Function
FRU name	Identifies the field replaceable units (FRUs) for each component.
Serial number	Identifies the serial number of each component.
Mfg ID	Identifies the manufacturer ID for each component.

Component Activity Log

You can view a record of component activity in this area.

Table 9. Component activity log

Field	Function
FRU name	Identifies the field replaceable units (FRUs) name of the component.
Serial number	Identifies the serial number of the component.
Mfg ID	Identifies the manufacturer of the component.
Action	Identifies the action taken for each component.
Timestamp	Identifies the date and time of the component action. The date is displayed in the *mm/dd/yy* format. The time is displayed in the *hh:mm:ss* format.

IMM VPD

You can view the IMM firmware, server firmware, and Dynamic System Analysis firmware VPD for the remote-managed server in this area.

Table 10. IMM, UEFI, and DSA firmware vital product data

Field	Function
Firmware type	Indicates the type of firmware code.
Version string	Indicates the version of the firmware code.
Release date	Indicates when the firmware was released.

Chapter 5. Performing IMM tasks

Use the functions under the **Tasks** heading in the navigation pane to directly control the actions of the IMM and your server. The tasks that you can perform depend on the server in which the IMM is installed.

You can perform the following tasks:

- View server power and restart activity
- Remotely control the power status of the server
- Remotely access the server console
- Remotely attach a disk or disk image to the server
- Update the IMM firmware

Note: Some features are available only on servers running a supported Microsoft Windows operating system.

Viewing server power and restart activity

The **Server Power/Restart Activity** area displays the power status of the server when the Web page was generated.

Power This field shows the power status of the server when the current Web page was generated.

State This field shows the state of the server when the current Web page was generated. The following states are possible:

- System power off / State unknown
- System on / starting UEFI
- System stopped in UEFI (Error detected)
- System running in UEFI
- Booting OS or in unsupported OS (might be in the operating system if the operating system is not configured to support the in-band interface to the IMM)
- OS booted

Restart count
This field shows the number of times that the server has been restarted.

Note: The counter is reset to zero each time the IMM subsystem is cleared to factory defaults.

Power-on hours
This field shows the total number of hours that the server has been turned on.

Controlling the power status of a server

The IMM provides full power control over your server with power-on, power-off, and restart actions. In addition, power-on and restart statistics are captured and displayed to show server hardware availability. To perform the actions in the **Server Power/Restart Control** area, you must have Supervisor access to the IMM.

To perform server power and restart actions, complete the following steps.

Note: Select the following options only in case of an emergency, or if you are offsite and the server is nonresponsive.

1. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Power/Restart**. Scroll down to the **Server Power/Restart Control** area.
3. Click one of the following options:

Power on server immediately
Turn on the server and start the operating system.

Power on server at specified time
Turn on the server at a specified time and start the operating system.

Power off server immediately
Turn off the server without shutting down the operating system.

Shut down OS and then power off server
Shut down the operating system and then turn off the server.

Shut down OS and then restart server
Restart the operating system.

Restart the server immediately
Turn off and then turn on the server immediately without first shutting down the operating system.

Schedule Daily/Weekly Power and Restart Actions
Shut down the operating system, turn off the server at a specified daily or weekly time (with or without restarting the server), and turn on the server at a specified daily or weekly time.

A confirmation message is displayed if you select any of these options, and you can cancel the operation if it was selected accidentally.

Remote presence

Notes:

1. The IMM remote presence function is available only in IMM Premium.
2. The remote control feature available only through the IMM Web interface. You must log in to the IMM with a user ID that has Supervisor access to use any of the remote control features.

You can use the remote presence function, or remote control feature in the IMM Web interface, to view and interact with the server console. You can also assign to the server a CD or DVD drive, diskette drive, USB flash drive, or disk image that is on your computer.

The remote control feature provides the following functions:

- Remotely viewing video with graphics resolutions up to 1280 x 1024 at 75 Hz, regardless of the server state
- Remotely accessing the server, using the keyboard and mouse from a remote client
- Mapping the CD or DVD drive, diskette drive, and USB flash drive on a remote client, and mapping ISO and diskette image files as virtual drives that are available for use by the server

- Uploading a diskette image to the IMM memory and mapping it to the server as a virtual drive

Updating your IMM firmware and Java applet

Important: The IMM uses a Java applet to perform the remote presence function. When the IMM is updated to the latest firmware level, the Java applet is also updated to the latest level. By default, Java caches (stores locally) applets that were previously used. After a flash update of the IMM firmware, the Java applet that the server uses might not be at the latest level.

To correct this problem, complete the following steps:

1. Click **Start → Settings → Control Panel**.
2. Double-click **Java Plug-in 1.5**. The Java Plug-in Control Panel window opens.
3. Click the **Cache** tab.
4. Choose one of the following options:
   - Clear the **Enable Caching** check box so that Java caching is always disabled.
   - Click **Clear Caching**. If you choose this option, you must click **Clear Caching** after each IMM firmware update.

For more information about updating IMM firmware, see "Updating firmware" on page 67.

Enabling the remote presence function

Note: The IMM remote presence function is available only in IMM Premium. For more information about upgrading from IMM Standard to IMM Premium, see "Upgrading from IMM Standard to IMM Premium" on page 3.

To enable the remote presence feature, complete the following steps:

1. Disconnect power from the server by unplugging the power cord.
2. Install the virtual media key into the dedicated slot on the system board.
3. Reconnect power to the server.

   Note: Approximately 2 minutes after the server is connected to ac power, the power-control button becomes active.
4. Turn on the server.

Remote control

The remote control feature of IMM consists of two Java applications in two separate windows:

Video Viewer
The Video Viewer uses a remote console for remote systems management. A remote console is an interactive graphical user interface (GUI) display of the server, viewed on your computer. You see on your monitor exactly what is on the server console, and you have keyboard and mouse control of the console.

Virtual Media Session
The Virtual Media Session window lists all of the drives on the client that can be mapped as remote drives. It allows you to map ISO and diskette image files as virtual drives. Each mapped drive can be marked as read-only. The CD and DVD drives and ISO images are always read-only.

To remotely access a server console, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, “Opening and using the IMM Web interface,” on page 9.
2. In the navigation pane, click **Remote Control**.
3. To control the server remotely, use one of the links at the bottom of the Remote Control page. If you want exclusive remote access during your session, click **Start Remote Control in Single User Mode**. If you want to allow other users remote console (KVM) access during your session, click **Start Remote Control in Multi-user Mode**. New windows open that provide access to the Remote Disk and Remote Console functionality.

   If the **Encrypt disk and KVM data during transmission** check box was selected before the Remote Control window was opened, the disk data is encrypted with 3DES encryption.

Close both the Video Viewer window and the Virtual Media Session window when you are finished using the Remote Control feature.

Notes:

1. Do not close the Virtual Media Session window if a remote disk is currently mapped. See “Remote disk” on page 64 for instructions about closing and unmapping a remote disk.
2. If you have mouse or keyboard problems when you use Remote Control, see the help that is available from the Remote Control page in the Web interface.
3. If you use the remote console to change settings for the IMM in the Setup Utility program, the server might restart the IMM and you lose the remote console and the login session. After a short delay, you can log in to the IMM again with a new session, start the remote console again, and exit the Setup Utility program.

Remote control screen capture

The screen capture feature in the Video Viewer window captures the video display contents of the server. To capture and save a screen image, complete the following steps:

1. In the Video Viewer window, click **File**.
2. Select **Capture to File** from the menu.
3. When you are prompted, name the image file and save it to the location that you choose on the local client.

   Note: Screen capture images are saved as JPG or JPEG file types.

Remote control Video Viewer view modes

To change the view of the Video Viewer window, click **View**. The following menu options are available:

Refresh
The Video Viewer redraws the video display with the video data from the server.

Full Screen
The Video Viewer fills the client desktop with the video display. This option is available only when the Video Viewer is not in full screen mode.

Windowed
The Video Viewer switches out of full screen mode into windowed mode. This option is available only while the Video Viewer is in full screen mode.

Fit The Video Viewer resizes to completely display the target desktop without an extra border or scrollbars. This requires that the client desktop be large enough to display the resized window.

Remote control video color mode

If your connection to the remote server has limited bandwidth, you can reduce the bandwidth demand of the Video Viewer by adjusting the color settings in the Video Viewer window.

Note: Instead of the bandwidth slider in the Remote Supervisor Adapter II interface, the IMM has a menu item that allows color depth adjustment to reduce the data that is transmitted in low-bandwidth situations.

To change the video color mode, complete the following steps:

1. In the Video Viewer window, click **View**.
2. When you move the mouse pointer over **Color Mode** in the menu, two color-mode choices are displayed:
   - Color: 7, 9, 12, and 15-bit
   - Grayscale: 16, 32, 64, 128 shades
3. Select the color or grayscale setting.

Remote control keyboard support

The operating system on the client server that you are using traps certain key combinations, such as Ctrl+Alt+Del in Microsoft Windows, instead of transmitting them to the server. Other keys, such as F1, might cause an action on your computer as well as on the server. To use key combinations that affect the remote server, and not the local client, complete the following steps:

1. In the Video Viewer window, click **Macros**.
2. Select one of the predefined key combinations from the menu, or select **Soft Key** to choose or add a user-defined key combinations.

Use the Video Viewer **Macros** menu item to create and edit customized buttons that can be used to send key strokes to the server.

To create and edit customized buttons, complete the following steps:

1. In the Video Viewer window, click **Macros**.
2. Select **Soft Key** and then **Add**. A new window opens.
3. Click **New** to add a new key combination, or select a key combination and click **Delete** to remove an existing key combination.
4. If you are adding a new combination, type the key combination that you want to define in the pop-up window and then click **OK**.
5. When you are finished defining or removing key combinations, click **OK**.

International keyboard support

The Video Viewer uses platform-specific native code to intercept key events to access the physical key information directly. The client detects the physical key events and passes them along to the server. The server detects the same physical keystrokes that the client experienced and supports all standard keyboard layouts with the only limitation that the target and client use the same keyboard layout. If

a remote user has a different keyboard layout from the server, the user can switch the server layout while it is being accessed remotely and then switch back again.

Keyboard pass-through mode

The keyboard pass-through feature disables the handling of most special key combinations on the client so that they can be passed directly to the server. This provides an alternative to using the macros.

Some operating systems define certain keystrokes to be outside the control of an application, so the behavior of the pass-through mechanism operates independently of the server. For example, in a Linux X session, the Ctrl+Alt+F2 keystroke combination switches to virtual console 2. There is no mechanism to intercept this keystroke sequence and, therefore, no way for the client to pass these keystrokes directly to the target. The only option in this case is to use the keyboard macros defined for this purpose.

To enable or disable keyboard pass-through mode, complete the following steps:

1. In the Video Viewer window, click **Tools**.
2. Select **Session Options** from the menu.
3. When the Session Options window is displayed, click the **General** tab.
4. Select the **Pass all keystrokes to target** check box to enable or disable the feature.
5. Click **OK** to save the choice.

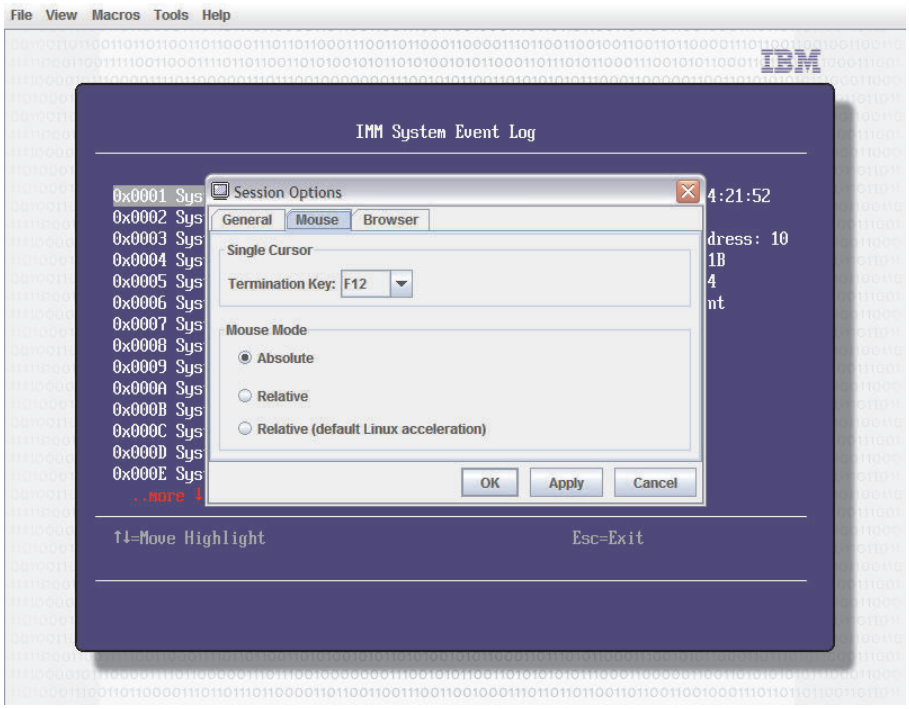
Remote control mouse support

The Video Viewer window offers several options for mouse control, including absolute mouse control, relative mouse control, and single cursor mode.

Absolute and relative mouse control

To access the absolute and relative options for controlling the mouse, complete the following steps:

1. In the Remote Control window, click **Tools**.
2. Select **Session Options** from the menu.
3. When the Session Options window is displayed, click the **Mouse** tab.



4. Select one of the following mouse modes:

   Absolute
   The client sends mouse location messages to the server that are always relative to the origin (top left) of the viewing area.

   Relative
   The client sends the mouse location as an offset from the previous location.

   Relative (default Linux acceleration)
   The client applies an acceleration factor to align the mouse better on Linux targets. The acceleration settings have been selected to maximize compatibility with Linux distributions.

Single cursor mode

Some operating systems do not align the local and remote cursors, which results in offsets between the local and remote mouse cursors. Single cursor mode hides the local client cursor while the mouse is within the Video Viewer window. When single cursor mode is activated, the user sees only the remote cursor.

To enable single cursor mode, complete the following steps:

1. In the Video Viewer window, click **Tools**.
2. Select **Single Cursor**.

When the Video Viewer is in single cursor mode, you cannot use the mouse to switch to another window or otherwise click outside the KVM client window, because there is no local cursor. To disable single cursor mode, press the defined termination key. To view the defined termination key, or change the termination key, click **Tools** → **Session Options** → **Mouse**.

Remote power control

You can send server power and restart commands from the Video Viewer window without returning to the Web browser. To control the server power with the Video Viewer, complete the following steps:

1. In the Video Viewer window, click **Tools**.
2. When you move the mouse pointer over **Power** in the menu, these choices are displayed:

   On Turns on the server power.

   Off Turns off the server power.

   Reboot
   Restarts the server.

   Cycle Turns the server power off, then back on.

Viewing performance statistics

To view the Video Viewer performance statistics, complete the following steps:

1. In the Video Viewer window, click **Tools**.
2. Click **Stats**. The following information is displayed:

   Frame Rate
   A running average of the number of frames, decoded per second by the client.

   Bandwidth
   A running average of the total number of kilobytes per second received by the client.

   Compression
   A running average of the bandwidth reduction due to video compression. This value often is displayed as 100.0%. It is rounded to the tenth of a percent.

   Packet Rate
   A running average of the number of video packets received per second.

Starting Remote Desktop Protocol

If the Windows-based Remote Desktop Protocol (RDP) client is installed, you can switch over to using an RDP client instead of the KVM client. The remote server must be configured to receive RDP connections.

Remote disk

From the Virtual Media Session window, you can assign to the server a CD or DVD drive, a diskette drive, or a USB flash drive that is on your computer, or you can specify a disk image on your computer for the server to use. You can use the drive for functions such as restarting (booting) the server, updating code, installing new software on the server, and installing or updating the operating system on the server. You can use the Remote Control feature to access the remote disk. Drives and disk images are displayed as USB drives on the server.

Notes:

1. The following server operating systems have USB support, which is required for the Remote Disk feature:
   - Microsoft Windows Server 2008
   - Microsoft Windows Server 2003

- Red Hat Linux versions 4.0 and 5.0
- SUSE Linux version 10.0
- Novell NetWare 6.5

2. The client server requires the Java 1.5 Plug-in or later.
3. The client server must have an Intel® Pentium® III microprocessor or later, operating at 700 MHz or faster, or equivalent.

Accessing the Remote Control

To begin a remote control session and access the remote disk, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
2. In the navigation pane, click **Remote Control**.
3. On the Remote Control page, click one of the **Start Remote Control** options:
   - If you want exclusive remote access during your session, click **Start Remote Control in Single User Mode**.
   - If you want to allow other users to have remote console (KVM) access during your session, click **Start Remote Control in Multi-user Mode**.

   The Video Viewer and Virtual Media Session windows open.

   Note: If the **Encrypt disk and KVM data during transmission** check box was selected before the Remote Control window was opened, the disk data is encrypted with 3DES encryption.

   The Virtual Media Session window is separate from the Video Viewer window. The Virtual Media Session window lists all of the drives on the client that can be mapped as remote drives. The Virtual Media Session window also allows you to map ISO and diskette image files as virtual drives. Each mapped drive can be marked as read-only. The CD and DVD drives and ISO images are always read-only.

Mapping and unmapping drives with IMM firmware version 1.03 and later

To map a drive, select the **Select** check box next to the drive that you want to map.

Note: A CD or DVD drive must contain media before it is mapped. If the drive is empty, you are prompted to insert a CD or DVD into the drive.

Click the **Mount Selected** button to mount and map the selected drive or drives.

If you click **Add Image**, diskette image files and ISO image files can be added to the list of available drives. After the diskette or ISO image file is listed in the Virtual Media Session window, it can be mapped just like the other drives.

To unmap the drives, click the **Unmount All** button. Before the drives are unmapped, you must confirm that you want the drives to be unmapped.

Note: After you confirm that you want the drives to be unmapped, all of the drives are unmounted. You cannot unmount drives individually.

You can select a diskette image file and save the diskette image in IMM memory. This enables the disk to remain mounted on the server so that you can access the disk later, even after the IMM Web interface session has ended. A maximum of one drive image can be stored on the IMM card. The drive or image contents must be 1.44 MB or smaller. To upload a diskette image file, complete the following steps:

1. Click **RDOC**.
2. When the new window opens, click **Upload**.
3. Click **Browse** to select the image file that you want to use.
4. In the **Name** field, enter a name for the image and click **OK** to upload the file.

   Note: To unload the image file from memory, select the name in the RDOC Setup window and click **Delete**.

Mapping and unmapping drives with IMM firmware version 1.02 and earlier

To map a drive, select the **Mapped** check box next to the drive that you want to map.

Note: A CD or DVD drive must contain media before it is mapped. If the drive is empty, you are prompted to insert a CD or DVD into the drive.

If you click **Add Image**, diskette image files and ISO image files can be added to the list of available drives. After the diskette or ISO image file is listed in the Virtual Media Session window, it can be mapped just like the other drives.

To unmap a drive, clear the **Mapped** check box for the drive. Before the drive is unmapped, you must confirm that you want the drive to be unmapped.

You can select a diskette image file and save the diskette image in IMM memory. This enables the disk to remain mounted on the server so that you can access the disk later, even after the IMM Web interface session has ended. A maximum of one drive image can be stored on the IMM card. The drive or image contents must be 1.44 MB or smaller. To upload a diskette image file, complete the following steps:

1. Click **RDOC**.
2. When the new window opens, click **Upload**.
3. Click **Browse** to select the image file that you want to use.
4. In the **Name** field, enter a name for the image and click **OK** to upload the file.

   Note: To unload the image file from memory, select the name in the RDOC Setup window and click **Delete**.

Exiting Remote Control

Close both the Video Viewer window and the Virtual Media Session window when you have finished using the Remote Control feature.

Setting up PXE network boot

To set up your server to attempt a Preboot Execution Environment (PXE) network boot at the next server restart, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, “Opening and using the IMM Web interface,” on page 9.
2. In the navigation pane, click **PXE Network Boot**.
3. Select the **Attempt PXE network boot at next server restart** check box.
4. Click **Save**.

Updating firmware

Use the **Firmware Update** option on the navigation pane to update the IMM firmware, the server firmware, and Dynamic System Analysis (DSA) firmware.

To update the firmware, complete the following steps.

Note: Changes are made periodically to the Lenovo Support Web site. The actual procedure might vary slightly from what is described in this document.

1. Download the latest firmware update applicable for the server in which the IMM is installed:
   a. Steps - Lenovo support and Downloads and Drivers
2. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface," on page 9.
3. In the navigation pane, click **Firmware Update**.
4. Click **Browse**.
5. Navigate to the update package that you want to update.

   Notes:

   a. The server firmware cannot be updated while the server is turned off or while the server is starting.
   b. To determine the type of firmware file to use, see the update package readme file. In most cases, the IMM can use either the EXE or BIN file to perform the update.
6. Click **Open**. The file (including the full path) is displayed in the box next to **Browse**.
7. To begin the update process, click **Update**.

   A progress indicator opens as the file is transferred to temporary storage on the IMM. A confirmation window opens when the file transfer is completed.
8. Verify that the file that is shown on the Confirm Firmware Update window is what you intend to update. If it is not, click **Cancel**.
9. To complete the update process, click **Continue**. A progress indicator opens as the firmware is updated. A confirmation window opens to verify that the update was successful.
10. If you are updating the IMM firmware, click **Restart IMM** in the navigation pane and then click **Restart**. The server firmware and DSA updates do not require that the IMM be restarted. These updates take effect the next time that the server is started.
11. Click **OK** to confirm that you want to restart the IMM.
12. Click **OK** to close the current browser window.
13. After the IMM restarts, log in to the IMM again to access the Web interface.

Resetting the IMM with the Setup Utility

To reset the IMM through the Setup Utility, complete the following steps:

1. Turn on the server.

   Note: Approximately 2 minutes after the server is connected to ac power, the power-control button becomes active.
2. When the prompt `F1 Setup` is displayed, press F1. If you have set both a power-on password and an administrator password, you must type the administrator password to access the full Setup Utility menu.

3. From the Setup Utility main menu, select **System Settings**.
4. On the next screen, select **Integrated Management Module**.
5. Select **Reset IMM**.

Note: After you reset the IMM, this confirmation message is displayed immediately:

```
IMM reset command has been sent successfully!! Press ENTER to continue.
```

The IMM reset process is not yet complete. You must wait approximately 4 minutes for the IMM to reset before the IMM is functional again. If you attempt to access sever firmware information while the server is resetting, `Unknown` is displayed in the fields, and the description is `Error retrieving information from IMM`.

Managing tools and utilities with IMM and the server firmware

This section describes the tools and utilities that are supported by IMM and the server firmware. The tools that you use to manage the IMM in-band do not require you to install device drivers. However, if you choose to use certain tools such as IPMItool in-band, you must install the OpenIPMI drivers.

Updates and downloads for systems-management tools and utilities are available on the Lenovo Support Web site at http://www.lenovo.com/support. To check for updates to tools and utilities, complete the following steps.

Note: Changes are made periodically to the Lenovo Support Web site. Procedures for locating firmware and documentation might vary slightly from what is described in this document.

1. Steps

Using IPMItool

IPMItool provides various tools that you can use to manage and configure an IPMI system. You can use IPMItool in-band or out-of-band to manage and configure the IMM.

For more information about IPMItool, or to download IPMItool, go to http://sourceforge.net/.

Using Advanced Settings Utility (ASU)

Advanced Settings Utility (ASU) version 3.0.0 or later is required to manage IMM. ASU is a tool that you can use to modify firmware settings from the command-line interface on multiple operating-system platforms. It also enables you to issue selected IMM setup commands. You can use ASU in-band or out-of-band to manage and configure the IMM.

Note: If the USB in-band interface (LAN over USB) is disabled, ASU requires the installation of IPMI device drivers.

Other methods for managing the IMM

You can use the following user interfaces to manage, configure, and update the IMM:

- IMM Web interface
- SNMPv1

- SNMPv3
- Telnet CLI
- SSH CLI

Chapter 6. LAN over USB

Unlike the BMC and Remote Supervisor Adapter II, the IMM does not require IPMI device drivers or USB daemons for in-band IMM communication. Instead, a LAN over USB interface enables in-band communications to the IMM; the IMM hardware on the system board presents an internal Ethernet NIC from the IMM to the operating system.

Note: LAN over USB is also called the "USB in-band interface" in the IMM Web interface.

Typically, the IMM IP address for the LAN over USB interface is set to a static address of 169.254.95.118 with a subnet mask of 255.255.0.0. In the event of an IP address collision on the network, the IMM might obtain a different IP address in the 169.254.*xxx.xxx* range. The IMM first attempts to use the default static address, 169.254.95.118. If that IP address is already in use, the IMM attempts to randomly obtain an address until it finds one that is not in use.

Because the IMM might obtain a random IP address for the LAN over USB interface, the ASU, and DSA use the Service Location Protocol (SLP) to discover the IMM IP address. These tools perform an SLP multicast discovery on the LAN over USB interface. When they receive a response from the IMM, they obtain the attributes that contain the IP address that the IMM is using for the LAN over USB interface.

Potential conflicts with the LAN over USB interface

In some situations, the IMM LAN over USB interface can conflict with certain network configurations, applications, or both. For example, Open MPI attempts to use all of the available network interfaces on a server. Open MPI detects the IMM LAN over USB interface and attempts to use it to communicate with other systems in a clustered environment. The LAN over USB interface is an internal interface, so this interface does not work for external communications with other systems in the cluster.

Configuring the LAN over USB interface manually

For the IMM to use the LAN over USB interface, you might have to complete other configuration tasks if the automatic setup fails or if you prefer to set up the LAN over USB manually. The firmware update package or Advanced Settings Utility attempts to perform the setup automatically.

Installing device drivers

For the IMM to use the LAN over USB interface, you might have to install operating-system drivers. If the automatic setup fails or if you prefer to set up the LAN over USB manually, use one of the following procedures.

Installing the Windows IPMI device driver

The Microsoft IPMI device driver is not installed by default on Microsoft Windows Server 2003 R2 operating systems. To install the Microsoft IPMI device driver, complete the following steps:

1. From the Windows desktop, click **Start → Control Panel → Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. From the component list, select **Management and Monitoring Tools**, and then click **Details**.
4. Select **Hardware Management**.
5. Click **Next**. The installation wizard opens and guides you through the installation.

   Note: The Windows installation CD might be required.

Installing the LAN over USB Windows device driver

When you install Windows, an unknown RNDIS device is shown in the Device Manager. You must install a Windows INF file that identifies this device and is required by Windows operating system to detect and use the LAN over USB functionality. The signed version of the INF is included in all of the Windows versions of the IMM, UEFI, and DSA update packages. The file needs to be installed only once. To install the Windows INF file, complete the following steps:

1. Obtain a Windows version of the IMM, server firmware, or DSA update package (see "Updating firmware" on page 67 for more information).
2. Extract the `ibm_rndis_server_os.inf` and `device.cat` files from the firmware update package and copy them to the `\WINDOWS\inf` subdirectory.
3. For Windows 2003: Install the `ibm_rndis_server_os.inf` file by right-clicking the file and selecting **Install**. This generates a PNF file of the same name in `\WINDOWS\inf`.

   For Windows 2008: Go to **Computer Management**, then **Device Manager** and locate the RNDIS Device. Select **Properties → Driver → Reinstall driver**. Point the server to the `\Windows\inf` directory, where it can locate the `ibm_rndis_server_os.inf` file and install the device.
4. Go to **Computer Management**, then **Device Manager**, right-click **Network adapters**, and select **Scan for hardware changes**. A message confirms that the Ethernet device is found and installed. The New Hardware Wizard starts automatically.
5. When you are prompted `Can Windows connect to Windows Update to search for software?`, click **No, not this time**. Click **Next** to continue.
6. When you are prompted `What do you want the wizard to do?`, click **Install from a list or specific location (Advanced)**. Click **Next** to continue.
7. When you are prompted `Please choose your search and installation options`, click **Don't search. I will choose the driver to install**. Click **Next** to continue.
8. When you are prompted `Select a hardware type, and then click Next`, click **Network adapters**. Click **Next** to continue.
9. When you are prompted `Completing the Found New Hardware Wizard`, click **Finish**.

   Note: A new local area connection is displayed and might state `This connection has limited or no connectivity`. Ignore this message.
10. Go back to the Device Manager. Verify that **Lenovo USB Remote NDIS Network Device** appears under **Network Adapters**.

11. Open a command prompt, type `ipconfig`, and press Enter. The local area connection for the IBM USB RNDIS is displayed with an IP address in the range of 169.254.*xxx.xxx* with a subnet mask set to 255.255.0.0.

Installing the LAN over USB Linux device driver

Current versions of Linux, such as RHEL5 Update 2 and SLES10 Service Pack 2, support the LAN over USB interface by default. This interface is detected and displayed during the installation of these operating systems. When you configure the device, use a static IP address of 169.254.95.130 with a subnet mask of 255.255.0.0.

Note: Older Linux distributions might not detect the LAN over USB interface and might require manual configuration.

The IMM LAN over USB interface requires that the `usbnet` and `cdc_ether` device drivers be loaded. If the device drivers have not been installed, use the `modprobe` command to install them. When these device drivers are installed, the IMM USB network interface is shown as a network device in the operating system. To discover the name that the operating system has assigned to the IMM USB network interface, type:

```
dmesg | grep -i cdc ether
```

Use the `ifconfig` command to configure the interface to have an IP address in the range 169.254.*xxx.xxx*. For example:

```
ifconfig IMM_device_name 169.254.1.102 netmask 255.255.0.0
```

This interface is configured to have an IP address in the 169.254.*xxx.xxx* range each time that the operating system is started.

Chapter 7. Command-line interface

Use the IMM command-line interface (CLI) to access the IMM without having to use the Web interface. It provides a subset of the management functions that are provided by the Web interface.

You can access the CLI through a Telnet or SSH session. You must be authenticated by the IMM before you can issue any CLI commands.

Managing the IMM using IPMI

The IMM comes with User ID 2 set initially to a user name of USERID and password of PASSW0RD (with a zero, not the letter O). This user has Supervisor access.

Important: Change this default password during your initial configuration for enhanced security.

The IMM also provides the following IPMI remote server management capabilities:

Command-line interface
The command-line interface provides direct access to server-management functions through the IPMI 2.0 protocol. You can use IPMItool to issue commands to control server power, view server information, and identify the server. For more information about IPMItool, see "Using IPMItool" on page 68.

Serial over LAN
To manage servers from a remote location, use IPMItool to establish a Serial over LAN (SOL) connection. For more information about IPMItool, see "Using IPMItool" on page 68.

Accessing the command line

To access the command line, start a Telnet or SSH session to the IMM IP address (see "Serial-to-Telnet or SSH redirection" on page 27 for more information).

Logging in to the command-line session

To log in to the command line, complete the following steps:

1. Establish a connection with the IMM.
2. At the user name prompt, type the user ID.
3. At the password prompt, type the password that you use to log in to the IMM.

   You are logged in to the command line. The command-line prompt is `system>`. The command-line session continues until you type `exit` at the command line. Then you are logged off and the session is ended.

Command syntax

Read the following guidelines before you use the commands:

- Each command has the following format:

  `command [arguments] [-options]`
- The command syntax is case sensitive.
- The command name is all lowercase.
- All arguments must immediately follow the command. The options immediately follow the arguments.
- Each option is always preceded by a hyphen (-). An option can be a short option (single letter) or a long option (multiple letters).
- If an option has an argument, the argument is mandatory, for example:

  `ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0`

  where **ifconfig** is the command, eth0 is an argument, and -i, -g, and -s are options. In this example, all three options have arguments.
- Brackets indicate that an argument or option is optional. Brackets are not part of the command that you type.

Features and limitations

The CLI has the following features and limitations:

- Multiple concurrent CLI sessions are allowed with different access methods (Telnet or SSH). At most, two Telnet command-line sessions can be active at any time.

  Note: The number of Telnet sessions is configurable; valid values are 0, 1, and 2. The value 0 means that the Telnet interface is disabled.
- One command is allowed per line (160-character limit, including spaces).
- There is no continuation character for long commands. The only editing function is the Backspace key to erase the character that you just typed.
- The Up Arrow and Down Arrow keys can be used to browse through the last eight commands. The **history** command displays a list of the last eight commands, which you can then use as a shortcut to execute a command, as in the following example:

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

- In the command-line interface, the output buffer limit is 2 KB. There is no buffering. The output of an individual command cannot exceed 2048 characters. This limit does not apply in serial redirect mode (the data is buffered during serial redirect).
- The output of a command is displayed on the screen after the command has completed execution. This makes it impossible for commands to report real-time execution status. For example, in the verbose mode of the **flashing** command, the flashing progress is not shown in real time. It is shown after the command completes execution.
- Simple text messages are used to denote command execution status, as in the following example:

```
system> power on
ok
system> power state
Power: On
State: System power off/State unknown
system>
```

- The command syntax is case sensitive.
- There must be at least one space between an option and its argument. For example, `ifconfig eth0 -i192.168.70.133` is incorrect syntax. The correct syntax is `ifconfig eth0 -i 192.168.70.133`.
- All commands have the `-h`, `-help`, and `?` options, which give syntax help. All of the following examples will give the same result:

```
system> power -h
system> power -help
system> power ?
```

- Some of the commands that are described in the following sections might not be available. To see a list of the commands that are supported, use the help or ? option, as shown in the following examples:

```
system> help
system> ?
```

Utility commands

The utility commands are as follows:

- exit
- help
- history

exit command

Description

Use the **exit** command to log off and end the command-line interface session.

help command

Description

Use the **help** command to display a list of all commands with a short description for each. You can also type ? at the command prompt.

history command

Description

Use the **history** command to display an indexed history list of the last eight commands that were issued. The indexes can then be used as shortcuts (preceded by !) to reissue commands from this history list.

Example

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

Monitor commands

The monitor commands are as follows:

- clearlog
- fans
- readlog
- syshealth
- temps
- volts

clearlog command

Description

Use the **clearlog** command to clear the event log of the IMM or IMM. You must have the authority to clear event logs to use this command.

fans command

Description

Use the **fans** command to display the speed for each of the server fans.

Example

```
system> fans
fan1 75%
fan2 80%
fan3 90%
system>
```

readlog command

Syntax

```
readlog [options]
option:
-f
```

Description

Use the **readlog** command to display the IMM event log entries, five at a time. The entries are displayed from the most recent to the oldest.

readlog displays the first five entries in the event log, starting with the most recent, on its first execution, and then the next five for each subsequent call.

readlog -f resets the counter and displays the first 5 entries in the event log, starting with the most recent.

Example

```
system> readlog -f
1 I SERVPROC 12/18/03 10:18:58 Remote Login Successful.
Login ID:''USERID' CLI authenticated from 192.168.70.231 (Telnet).'
2 I SERVPROC 12/18/03 10:12:22 Remote Login successful.
Login ID: ''USERID' from web browser at IP@=192.168.70.231'
3 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
4 E SERVPROC 12/18/03 10:10:37 Environmental monitor not responding.
5 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

syshealth command

Description

Use the **syshealth** command to display a summary of the health of the server. The power state, system state, restart count, and IMM software status are displayed.

Example

```
system> syshealth
Power On
State System on/starting UEFI
Restarts 71
system>
```

temps command

Description

Use the **temps** command to display all the temperatures and temperature thresholds. The same set of temperatures are displayed as in the Web interface.

Example

```
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius
        WR      W      T     SS     HS
---------------------------------------
CPU1   65/18  72/22  80/27  85/29  90/32
```

```
CPU2   58/14  72/22  80/27  85/29  9/320
DASD1  66/19  73/23  82/28  88/31  9/332
Amb    59/15  70/21  83/28  90/32  9/355
system>
```

Notes:

1. The output has the following column headings:
   - WR: warning reset
   - W: warning
   - T: temperature (current value)
   - SS: soft shutdown
   - HS: hard shutdown
2. All temperature values are in degrees Fahrenheit/Celsius.

volts command

Description

Use the **volts** command to display all the voltages and voltage thresholds. The same set of voltages are displayed as in the Web interface.

Example

```
system> volts
      HSL   SSL   WL    WRL   V     WRH   WH   SSH    HSH
-------------------------------------------------------------
5v    5.02  4.00  4.15  4.50  4.60  5.25  5.50  5.75  6.00
3.3v  3.35  2.80  2.95  3.05  3.10  3.50  3.65  3.70  3.85
12v   12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40 12.65
-5v   -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40 -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80 -2.70
VRM1                        3.45
VRM2                        5.45
system>
```

Note: The output has the following column headings:

- HSL: hard shutdown low
- SSL: soft shutdown low
- WL: warning low
- WRL: warning reset low
- V: voltage (current value)
- WRH: warning reset high
- WH: warning high
- SSH: soft shutdown high
- HSH: hard shutdown high

vpd command

Syntax

```
vpd sys
vpd IMM
vpd biosvpd dsa
```

Description

Use the **vpd** command to display vital product data for the system (sys), IMM, server firmware (bios), and Dynamic System Analysis Preboot (dsa). The same information is displayed as in the Web interface.

Example

```
system> vpd dsa
Type     Version      ReleaseDate
----     -------      -----------
dsa      D6YT19AUS    02/27/2009
system>
```

Server power and restart control commands

The server power and restart commands are as follows:

- power
- reset

power command

Syntax

```
power on
power off [-s]
power state
power cycle [-s]
```

Description

Use the **power** command to control the server power. To issue the **power** commands, you must have power and restart access authority.

power on turns on the server power.

power off turns off the server power. The **-s** option shuts down the operating system before the server is turned off.

power state displays the server power state (on or off) and the current state of the server.

power cycle turns off the server power and then turns on the power. The **-s** option shuts down the operating system before the server is turned off.

reset command

Syntax

```
reset [option]
option:
-s
```

Description

Use the **reset** command to restart the server. To use this command, you must have power and restart access authority. The **-s** option shuts down the operating system before the server is restarted.

Serial redirect command

There is one serial redirect command: console.

console command

Syntax

```
console 1
```

Description

Use the **console** command to start a serial redirect console session to the designated serial port of the IMM.

Configuration commands

The configuration commands are as follows:

- dhcpinfo
- ifconfig
- ldap
- ntp
- passwordcfg
- portcfg
- slp
- srcfg
- ssl
- tcpcmdmode
- timeouts
- usbeth
- users

dhcpinfo command

Syntax

```
dhcpinfo eth0
```

Description

Use the **dhcpinfo** command to view the DHCP server-assigned IP configuration for eth0, if the interface is configured automatically by a DHCP server. You can use the **ifconfig** command to enable or disable DHCP.

Example

```
system> dhcpinfo eth0
-server 192.168.70.29
-n IMMA00096B9E003A
-i 192.168.70.202
-g 192.168.70.29
-s 255.255.255.0
-d linux-sp.raleigh.lenovo.com
-dns1 192.168.70.29
-dns2 0.0.0.0
-dns3 0.0.0.0
system>
```

The following table describes the output from the example.

Option	Description
-server	DHCP server that assigned the configuration
-n	Assigned host name
-i	Assigned IP address
-g	Assigned gateway address
-s	Assigned subnet mask

Option	Description
-d	Assigned domain name
-dns1	Primary DNS server IP address
-dns2	Secondary DNS IP address
-dns3	Tertiary DNS server IP address

ifconfig command

Syntax

```
ifconfig eth0 [options]
options:
-state interface_state
-c config_method
-i static_ip_address
-g gateway_address
-s subnet_mask
-n hostname
-r data_rate
-d duplex_mode
-m max_transmission_unit
-l locally_administered_MAC
```

Description

Use the **ifconfig** command to configure the Ethernet interface. Type `ifconfig eth0` to display the current Ethernet interface configuration. To change the Ethernet interface configuration, type the options, followed by the values. To change the interface configuration, you must have at least Adapter Networking and Security Configuration authority.

The following table shows the arguments for the options.

Option	Description	Values
-state	Interface state	disabled, enabled
-c	Configuration method	dhcp, static, dthens (dthens corresponds to the **try dhcp server, if it fails use static config** option on the Web interface)
-i	Static IP address	Valid IP address format
-g	Gateway address	Valid IP address format
-s	Subnet mask	Valid IP address format
-n	Host name	String of up to 63 characters. Can include letters, digits, periods, underscores, and hyphens.
-r	Data rate	10, 100, auto
-d	Duplex mode	full, half, auto
-m	MTU	Numeric between 60 and 1500
-l	LAA	MAC address format. Multicast addresses are not allowed (the first byte must be even).

Example

```
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
```

```
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
system>
```

Note: The **-b** option in the ifconfig display is for the burned-in MAC address. The burned-in MAC address is read-only and is not configurable.

ldap command

Syntax

```
ldap [options]
options:
   -a loc|ldap|locId|Idloc
   -b anon|client|login
   -c client_dn
   -d search_domain
   -f group_filter
   -g group_search_attr
   -l string
   -m login|cfg|lthenc
   -n service_name
   -p client_pw
   -pc confirm_pw
   -r root_dn
   -s1ip host name/ip_addr
   -s2ip host name/ip_addr
   -s3ip host name/ip_addr
   -s1pn port_number
   -s2pn port_number
   -s3pn port_number
   -u search_attrib
   -v off|on
   -w on|off
   -h
```

Description

Use the **ldap** command to display and configure the LDAP protocol configuration parameters.

The following table shows the arguments for the options.

Option	Description	Values
-a	User authentication method	Local only, LDAP only, local first then LDAP, LDAP first then local
-b	Binding method	Anonymous, bind with ClientDN and password, user principal bind (UPN)
-c	Client distinguished name	String of up to 63 characters for *client_dn*
-d	Search domain	String of up to 31 characters for *search_domain*
-f	Group filter	String of up to 63 characters for *group_filter*
-g	Group search attribute	String of up to 63 characters for *group_search_attr*

Option	Description	Values
-l	Login permission attribute	String of up to 63 characters for *string*
-m	Domain source	Extract search domain from login ID, use only configured search domain, try login first then configured value
-n	Service name	String of up to 15 characters for *service_name*
-p	Client password	String of up to 15 characters for *client_pw*
-pc	Confirm client password	String of up to 15 characters for *confirm_pw* Command usage is: ldap -p *client_pw* -pc *confirm_pw* This option is required when you change the client password. It compares the *confirm_pw* argument with the *client_pw* argument, and the command will fail if they do not match.
-r	Root entry distinguished name (DN)	String of up to 63 characters for *root_dn*
s1ip	Server 1 host name/IP address	String of up to 63 characters or an IP address for *host name/ip_addr*
s2ip	Server 2 host name/IP address	String of up to 63 characters or an IP address for *host name/ip_addr*
s3ip	Server 3 host name/IP address	String of up to 63 characters or an IP address for *host name/ip_addr*
s1pn	Server 1 port number	A numeric port number of up to 5 digits for *port_number.*
s2pn	Server 2 port number	A numeric port number of up to 5 digits for *port_number.*
s3pn	Server 3 port number	A numeric port number of up to 5 digits for *port_number.*
-u	UID search attribute	String of up to 23 characters for *search_attrib*
-v	Get LDAP server address through DNS	Off, on
-w	Allows wildcards in the group name	Off, on
-h	Displays the command usage and options	

ntp command

Syntax

```
ntp [options]
options:
-en state
-i  hostname
-f  frequency
-synch
```

Description

Use the **ntp** command to display and configure the Network Time Protocol (NTP).

The following table shows the arguments for the options.

Option	Description	Values
-en	Enables or disables the Network Time Protocol	Enabled, disabled
-i	Name or IP address of the Network Time Protocol server	The name of the NTP server to be used for clock synchronization.
-f	The frequency (in minutes) that the IMMclock is synchronized with the Network Time Protocol server	3 - 1440 minutes
-synch	Requests an immediate synchronization with the Network Time Protocol server	No values are used with this parameter.

Example

```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

passwordcfg command

Syntax

```
passwordcfg [options]
options: {-high}|{-legacy}|{-exp|-cnt|-nul}
-legacy
-high
-exp:
-cnt:
-nul:
-h
```

Description

Use the **passwordcfg** command to display and configure the password parameters.

Option	Description
-legacy	Sets account security to a predefined legacy set of defaults
-high	Sets account security to a predefined high set of defaults
-exp	Maximum password age (0 - 365 days). Set to 0 for no expiration.
-cnt	Number of previous passwords that cannot be reused (0 - 5)
-nul	Allows accounts with no password (yes | no)
-h	Displays the command usage and options

Example

```
system> passwordcfg
Security Level: Legacy
system> passwordcfg -exp 365
ok
system> passwordcfg -nul yes
ok
system> passwordcfg -cnt 5
```

```
ok
system> passwordcfg
Security Level: Customize
-exp: 365
-cnt: 5
-nul: allowed
```

portcfg command

Syntax

```
portcfg [options]
portcfg [options]
options:
-b baud_rate
-climode cli_mode
-cliauth cli_auth
```

Description

Use the **portcfg** command to configure the serial port. To change the serial port configuration, type the options, followed by the values. To change the serial port configuration, you must have at least Adapter Networking and Security Configuration authority.

The parameters are set in the hardware and cannot be changed:

- 8 data bits
- no parity
- 1 stop bit

The following table shows the arguments for the options.

Option	Description	Values
-b	Baud rate	9600, 19200, 38400, 57600, 115200, 230400
-climode	CLI mode	none, cliems, cliuser • none: The command-line interface is disabled. • cliems: The command-line interface is enabled with EMS-compatible keystroke sequences. • cliuser: The command-line interface is enabled with user-defined keystroke sequences.

Example

```
system> portcfg
-b       : 115200
-climode : 2 (CLI with user defined keystroke sequences) system>
system>
```

srcfg command

Syntax

```
srcfg [options]
options:
-exitcliseq exitcli_keyseq
```

Description

Use the **srcfg** command to configure the serial redirection. Type `srcfg` to display the current configuration. To change the serial redirect configuration, type the

options, followed by the values. To change the serial redirect configuration, you must have at least Adapter Networking and Security Configuration authority.

The following table shows the arguments for the `-exitcliseq` option.

Option	Description	Values
-exitcliseq	Exit a command-line interface keystroke sequence	User-defined keystroke sequence to exit the CLI. For details, see the values for the -entercliseq option in this table.

Example

```
system> srcfg
-exitcliseq ^[Q
system>
```

ssl command

Syntax

```
ssl [options]
options:
-ce on | off
-se on | off
-h
```

Description

Note: Before you can enable an SSL client, a client certificate must be installed.

Use the **ssl** command to display and configure the Secure Sockets Layer (SSL) parameters.

Option	Description
-ce	Enables or disables an SSL client
-se	Enables or disables an SSL server
-h	Lists usage and options

Parameters

The following parameters are presented in the option status display for the **ssl** command and are output only from the command-line interface:

Server secure transport enable
This status display is read-only and cannot be set directly.

Server Web/CMD key status
This status display is read-only and cannot be set directly. Possible command line output values are as follows:

```
Private Key and Cert/CSR not available
Private Key and CA-signed cert installed
Private Key and Auto-gen self-signed cert installed
Private Key and Self-signed cert installed
Private Key stored, CSR available for download
```

SSL server CSR key status

This status display is read-only and cannot be set directly. Possible command line output values are as follows:

```
Private Key and Cert/CSR not available
Private Key and CA-signed cert installed
Private Key and Auto-gen self-signed cert installed
Private Key and Self-signed cert installed
Private Key stored, CSR available for download
```

SSL client LDAP key status

This status display is read-only and cannot be set directly. Possible command line output values are as follows as follows:

```
Private Key and Cert/CSR not available
Private Key and CA-signed cert installed
Private Key and Auto-gen self-signed cert installed
Private Key and Self-signed cert installed
Private Key stored, CSR available for download
```

SSL client CSR key status

This status display is read-only and cannot be set directly. Possible command line output values are as follows:

```
Private Key and Cert/CSR not available
Private Key and CA-signed cert installed
Private Key and Auto-gen self-signed cert installed
Private Key and Self-signed cert installed
Private Key stored, CSR available for download
```

timeouts command

Syntax

```
timeouts [options]
options:
-o OS_watchdog_option
-l loader_watchdog_option
```

Description

Use the **timeouts** command to display the timeout values or change them. To display the timeouts, type `timeouts`. To change timeout values, type the options followed by the values. To change timeout values, you must have at least Adapter Configuration authority.

The following table shows the arguments for the timeout values. These values match the graduated scale pull-down options for server timeouts on the Web interface.

Option	Timeout	Units	Values
-o	Operating system timeout	minutes	disabled, 2.5, 3, 3.5, 4
-l	Loader timeout	minutes	disabled, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120

Example

```
system> timeouts
-o disabled
-l 3.5
system> timeouts -o 2.5
```

```
ok
system> timeouts
-o 2.5
-l 3.5
```

usbeth command

Syntax

```
usbeth [options]
options:
-en <enabled|disabled>
```

Description

Use the **usbeth** command to enable or disable the in-band LAN over USB interface. For more information about enabling or disabling this interface, see "Disabling the USB in-band interface" on page 19.

Example

```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

users command

Syntax

```
users [options]
options:
-user number
-n username
-p password
-a authority level
```

Description

Use the **users** command to access all user accounts and their authority levels and to create new user accounts and modify existing accounts.

Read the following guidelines about the **users** command:

- User numbers must be from 1 to 12, inclusive.
- User names must be less than 16 characters and can contain only numbers, letters, periods, and underscores.
- Passwords must be more than 5 and fewer than 16 characters long and must contain at least one alphabetic and one nonalphabetic character.
- The authority level can be one of the following levels:
  - super (supervisor)
  - ro (read only)
  - Any combination of the following values, separated by |:
    - am (User account management access)
    - rca (Remote console access)
    - rcvma (Remote console and virtual media access)
    - pr (Remote server power/restart access)
    - cel (Ability to clear event logs)
    - bc (Adapter configuration [basic])

nsc (Adapter configuration [network and security])
ac (Adapter configuration [advanced])

Example

```
system> users
1. USERID Read/Write
Password Expires: no expiration
2. manu Read Only
Password Expires: no expiration
3. eliflippen Read Only
Password Expires: no expiration
4.  <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
system> users -7 -n sptest -p PASSW0RD -a custom:am|rca|cel|nsc|ac
ok
system> users
1. USERID  Read/Write
Password Expires: no expiration
2. test    Read/Write
Password Expires: no expiration
3. test2   Read/Write
Password Expires: no expiration
4. <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
6. <not used>
7. sptest  custom:am|rca|cel|nsc|ac
Password Expires: no expiration
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
system>
```

IMM control commands

The IMM control commands are as follows:

- clearcfg
- clock
- identify
- resetsp
- update

clearcfg command

Description

Use the **clearcfg** command to set the IMM configuration to its factory defaults. You must have at least Advanced Adapter Configuration authority to issue this command. After the configuration of the IMM is cleared, the IMM is restarted.

clock command

Syntax

```
clock [options]
options:
-d mm/dd/yyyy
-t hh:mm:ss
-g gmt offset
-dst on/off/special case
```

Description

Use the **clock** command to display the current date and time according to the IMM clock and the GMT offset. You can set the date, time, GMT offset, and daylight saving time settings.

Note the following information:

- For a GMT offset of +2 or +10, special daylight saving time settings are required.
- For +2, the daylight saving time options are as follows: off, ee (Eastern Europe), gtb (Great Britain), egt (Egypt), fle (finland).
- For +10, the daylight saving time settings are as follows: off, ea (Eastern Australia), tas (Tasmania), vlad (Vladivostok).
- The year must be from 2000 to 2089, inclusive.
- The month, date, hours, minutes, and seconds can be single-digit values (for example, 9:50:25 instead of 09:50:25).
- GMT offset can be in the format of +2:00, +2, or 2 for positive offsets, and -5:00 or -5 for negative offsets.

Example

```
system> clock
12/12/2003 13:15:23 GMT-5:00 dst on
system> clock -d 12/31/2004
ok
system> clock
12/31/2004 13:15:30 GMT-5:00 dst on
```

identify command

Syntax

```
identify [options]
options:
-s on/off/blink
-d seconds
```

Description

Use the **identify** command to turn the chassis identify LED on or off, or to have it flash. The -d option can be used with -s on to turn the LED on for only for the number of seconds specified with the -d parameter. The LED then turns off after the number of seconds elapses.

Example

```
system> identify
-s off
system> identify -s on -d 30
ok
system>
```

resetsp command

Description

Use the **resetsp** command to restart the IMM or IMM. You must have at least Advanced Adapter Configuration authority to be able to issue this command.

update command

Syntax

```
update -i TFTP_server_IP_address -l filename
```

Description

Use the **update** command to update the firmware on the IMM or IMM. To use this command, you must have at least Advanced Adapter Configuration authority. The firmware file (specified by *filename*) is first transferred from the TFTP server (specified by its IP address) to the IMM or IMM and then flashed. The **-v** option specifies verbose mode.

Note: Make sure that the TFTP server is running on the server from which the file will be downloaded.

Option	Description
-i	TFTP server IP address
-l	File name (to be flashed)
-v	Verbose mode

Example

In the verbose mode, the flashing progress is displayed in real time in the percentage of completion.

```
system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Downloading image - 66%

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.
Flashing image - 45%

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.
Flash operation completed.
system>
```

If the flashing is not in the verbose mode, progress is displayed in consecutive # characters.

```
system>update -i 192.168.70.200 -l dsa_d6yt28a_68608_2.upd
Firmware update is in progress. Please wait..
Downloading image: ################################################
Flashing image: ################################################
Flash operation completed.
```

Appendix A. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you. This section contains information about where to go for additional information about Lenovo and Lenovo products, what to do if you experience a problem with your system, and whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Use the troubleshooting information in your system documentation, and use the diagnostic tools that come with your system. Information about diagnostic tools is in the *Hardware Maintenance Manual*.
- Go to the Lenovo Support Web site at http://www.lenovo.com/support to check for technical information, hints, tips, and new device drivers or to submit a request for information.

You can solve many problems without outside assistance by using the information available on the Lenovo support site at http://www.lenovo.com/support or by following the troubleshooting procedures that Lenovo provides in the documentation that is provided with your Lenovo product. The documentation that comes with Lenovo systems also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the documentation

Information about your Lenovo system and preinstalled software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, readme files, and help files. Most of the documentation for your server is on the *ThinkServer Documentation* DVD provided with your server. See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. Lenovo maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.lenovo.com/support and follow the instructions.

Getting help and information from the World Wide Web

On the World Wide Web, the Lenovo Web site has up-to-date information about Lenovo systems, optional devices, services, and support. For general information about Lenovo products or to purchase Lenovo products, go to http://www.lenovo.com. For support on Lenovo products, go to http://www.lenovo.com/support.

Calling for service

During the warranty period, you can get help and information by telephone through the Customer Support Center.

These services are available during the warranty period:

- **Problem determination -** Trained personnel are available to assist you with determining a hardware problem and deciding what action is necessary to fix the problem.
- **Hardware repair -** If the problem is caused by hardware under warranty, trained service personnel are available to provide the applicable level of service.
- **Engineering Change management -** There might be changes that are required after a product has been sold. Lenovo or your reseller will make selected Engineering Changes (ECs) available that apply to your hardware.

These items are not covered by the warranty:

- Replacement or use of parts not manufactured for or by Lenovo or non-warranted Lenovo parts
- Identification of software problem sources
- Configuration of BIOS as part of an installation or upgrade
- Changes, modifications, or upgrades to device drivers
- Installation and maintenance of network operating systems (NOS)
- Installation and maintenance of application programs

Refer to the safety and warranty information that is provided with your computer for a complete explanation of warranty terms. You must retain your proof of purchase to obtain warranty service.

For a list of service and support phone numbers for your country or region, go to http://www.lenovo.com/support and click **Support phone list** or refer to the safety and warranty information provided with your computer.

Note: Phone numbers are subject to change without notice. If the number for your country or region is not provided, contact your Lenovo reseller or Lenovo marketing representative.

If possible, be at your computer when you call. Have the following information available:

- Machine type and model
- Serial numbers of your hardware products
- Description of the problem
- Exact working of any error messages
- Hardware and software configuration information

Using other services

If you travel with a Lenovo notebook computer or relocate your computer to a country where your desktop, notebook, or server machine type is sold, your computer might be eligible for International Warranty Service, which automatically entitles you to obtain warranty service throughout the warranty period. Service will be performed by service providers authorized to perform warranty service.

Service methods and procedures vary by country, and some services might not be available in all countries. International Warranty Service is delivered through the method of service (such as depot, carry-in, or on-site service) that is provided in the servicing country. Service centers in certain countries might not be able to service all models of a particular machine type. In some countries, fees and restrictions might apply at the time of service.

To determine whether your computer is eligible for International Warranty Service and to view a list of the countries where service is available, go to http://www.lenovo.com/support, click **Warranty**, and follow the instructions on the screen.

For technical assistance with the installation of, or questions related to, Service Packs for your preinstalled Microsoft Windows product, refer to the Microsoft Product Support Services Web site at http://www.support.microsoft.com/directory/, or you can contact the Customer Support Center. Some fees might apply.

Purchasing additional services

During and after the warranty period, you can purchase additional services, such as support for hardware, operating systems, and application programs; network setup and configuration; upgraded or extended hardware repair services; and custom installations. Service availability and service name might vary by country or region. For more information about these services, go to the Lenovo Web site at http://www.lenovo.com/.

Lenovo product service

台灣 Lenovo 產品服務資訊如下：
荷蘭商聯想股份有限公司台灣分公司
台北市信義區信義路五段七號十九樓之一
服務電話：0800-000-700

Appendix B. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may

vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

The following terms are trademarks of Lenovo in the United States, other countries, or both:

Lenovo
The Lenovo logo
ThinkServer

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM

Intel and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows Server are trademarks of the Microsoft group of companies.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Red Hat, the Red Hat "Shadow Man" logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

Sun and Java are trademarks of Sun Microsystems, Inc. in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Important notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives that are available from Lenovo.

Maximum memory might require replacement of the standard memory with an optional memory module.

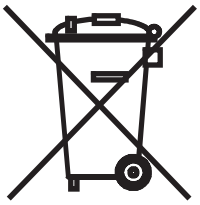
Lenovo makes no representation or warranties regarding non-Lenovo products and services, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Product recycling and disposal

This unit must be recycled or discarded according to applicable local and national regulations. Lenovo encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. Lenovo offers a variety of programs and services to assist equipment owners in recycling their IT products. Information on Lenovo product recycling offerings can be found on Lenovo's Internet site at
http://www.lenovo.com/lenovo/environment/recycling.

Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. Lenovo recomienda a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstos ya no les sean útiles. Lenovo dispone de una serie de programas y servicios de devolución de productos, a fin de ayudar a los propietarios de equipos a reciclar sus productos de TI. Se puede encontrar información sobre las ofertas de reciclado de productos de Lenovo en el sitio web de Lenovo
http://www.lenovo.com/lenovo/environment/recycling.



Notice: This mark applies only to countries within the European Union (EU) and Norway.

This appliance is labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable throughout the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

注意：このマークは EU 諸国およびノルウェーにおいてのみ適用されます。

この機器には、EU 諸国に対する廃電気電子機器指令 2002/96/EC(WEEE) のラベルが貼られています。この指令は、EU 諸国に適用する使用済み機器の回収とリサイクルの骨子を定めています。このラベルは、使用済みになった時に指令に従って適正な処理をする必要があることを知らせるために種々の製品に貼られています。

Remarque : Cette marque s'applique uniquement aux pays de l'Union Européenne et à la Norvège.

L'etiquette du système respecte la Directive européenne 2002/96/EC en matière de Déchets des Equipements Electriques et Electroniques (DEEE), qui détermine les dispositions de retour et de recyclage applicables aux systèmes utilisés à travers l'Union européenne. Conformément à la directive, ladite étiquette précise que le produit sur lequel elle est apposée ne doit pas être jeté mais être récupéré en fin de vie.

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local Lenovo representative.

Compliance with Republic of Turkey Directive on the Restriction of Hazardous Substances

Meets requirements of the Republic of Turkey Directive on the Restriction of the Use of Certain Hazardous Substances In Electrical and Electronic Equipment (EEE).

Türkiye EEE Yönetmeliğine Uygunluk Beyanı

Bu Lenovo ürünü, T.C. Çevre ve Orman Bakanlığı'nın "Elektrik ve Elektronik Eşyalarda Bazı Zararlı Maddelerin Kullanımının Sınırlandırılmasına Dair Yönetmelik (EEE)" direktiflerine uygundur.

EEE Yönetmeliğine Uygundur.

Recycling statements for Japan

日本のリサイクルに関して

本機器またはモニターの回収リサイクルについて

企業のお客様が、本機が使用済みとなり廃棄される場合は、廃棄物処理法の規定により、産業廃棄物として、地域を管轄する県知事あるいは、政令市長の許可を持った産業廃棄物処理業者に適正処理を委託する必要があります。また、弊社では資源有効利用促進法に基づき使用済みパソコンの回収および再利用・再資源化を行う「PC 回収リサイクル・サービス」を提供しています。詳細については、以下のURL にアクセスしてください。
http://www.ibm.com/jp/pc/service/recycle/pcrecycle

また、同法により、家庭で使用済みとなったパソコンのメーカー等による回収再資源化が2003 年10 月1 日よりスタートしました。詳細については、以下のURL にアクセスしてください。
http://www.ibm.com/jp/pc/service/recycle/personal

重金属を含む内部部品の廃棄処理について

本機器のプリント基板等には微量の重金属(鉛など) が使用されています。使用後は適切な処理を行うため、上記「本機器またはモニターの回収リサイクルについて」に従って廃棄してください。

リチウム電池交換後の廃棄処理について

本機器には、ボタン型のリチウム電池がシステム・ボード上に取り付けられています。この電池を交換する場合には、お買い上げいただいた販売店にお問い合わせいただくか、弊社の修理サービスをご利用ください。万一お客様が交換された場合の古い電池を廃棄する際は、ビニール・テープなどで絶縁処理をして、お買い上げいただいた販売店にお問い合わせいただくか、もしくは産業廃棄物処理業者に処理をご依頼ください。また一般家庭などから、一般廃棄物として自治体に廃棄を依頼するときは、地方自治体の条例・規則に従って廃棄してください。

Battery return program

This product may contain a lithium or lithium ion battery. Consult your user manual or service manual for specific battery information. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal or batteries outside the United States, go to http://www.lenovo.com/lenovo/environment or contact your local waste disposal facility.

For Taiwan: Please recycle batteries.

For the European Union:

Notice: This mark applies only to countries within the European Union (EU).

Batteries or packaging for batteries are labeled in accordance with European Directive 2006/66/EC concerning batteries and accumulators and waste batteries and accumulators. The Directive determines the framework for the return and recycling of used batteries and accumulators as applicable throughout the European Union. This label is applied to various batteries to indicate that the battery is not to be thrown away, but rather reclaimed upon end of life per this Directive.

Les batteries ou emballages pour batteries sont étiquetés conformément aux directives européennes 2006/66/EC, norme relative aux batteries et accumulateurs en usage et aux batteries et accumulateurs usés. Les directives déterminent la marche à suivre en vigueue dans l'Union Européenne pour le retour et le recyclage des batteries et accumulateurs usés. Cette étiquette est appliquée sur diverses batteries pour indiquer que la batterie ne doit pas être mise au rebut mais plutôt récupérée en fin de cycle de vie selon cette norme.

In accordance with the European Directive 2006/66/EC, batteries and accumulators are labeled to indicate that they are to be collected separately and recycled at end of life. The label on the battery may also include a chemical symbol for the metal concerned in the battery (Pb for lead, Hg for mercury, and Cd for cadmium). Users of batteries and accumulators must not dispose of batteries and accumulators as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and treatment of batteries and accumulators. Customer participation is important to minimize any potential effects of batteries and accumulators on the environment and human health due to the potential presence of hazardous substances. For proper collection and treatment, go to http://www.lenovo.com/lenovo/environment.

For California:

Perchlorate material - special handling may apply. See http://www.dtsc.ca.gov/hazardouswaste/perchlorate/.

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5 Chapter 33. Best Management Practices for Perchlorate Materials. This product/part may include a lithium manganese dioxide battery which contains a perchlorate substance.

German Ordinance for Work gloss statement

The product is not suitable for use with visual display work place devices according to clause 2 of the German Ordinance for Work with Visual Display Units.

Das Produkt ist nicht für den Einsatz an Bildschirmarbeitsplätzen im Sinne § 2 der Bildschirmarbeitsverordnung geeignet.

Electronic emission notices

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Lenovo is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

United Kingdom telecommunications safety requirement

Notice to Customers

This apparatus is approved under approval number NS/G/1234/J/100003 for indirect connection to public telecommunication systems in the United Kingdom.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. Lenovo cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-Lenovo option cards

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Germany Class A compliance statement

Deutschsprachiger EU Hinweis:

Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG (früher 89/336/EWG) zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der Lenovo empfohlene Kabel angeschlossen werden. Lenovo übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der Lenovo verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der Lenovo gesteckt/eingebaut werden.

Deutschland:

Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmittein

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln” EMVG (früher “Gesetz über die elektromagnetische Verträglichkeit von Geräten”). Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG (früher 89/336/EWG) in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln, EMVG vom 20. Juli 2007 (früher Gesetz über die elektromagnetische Verträglichkeit von Geräten), bzw. der EMV EG Richtlinie 2004/108/EC (früher 89/336/EWG), für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen. Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die Lenovo (Deutschland) GmbH, Gropiusplatz 10, D-70563 Stuttgart.

Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Nach der EN 55022: "Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen."

Nach dem EMVG: "Geräte dürfen an Orten, für die sie nicht ausreichend entstört sind, nur mit besonderer Genehmigung des Bundesministers für Post und Telekommunikation oder des Bundesamtes für Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind." (Auszug aus dem EMVG, Paragraph 3, Abs. 4). Dieses Genehmigungsverfahren ist nach Paragraph 9 EMVG in Verbindung mit der entsprechenden Kostenverordnung (Amtsblatt 14/93) kostenpflichtig.

Anmerkung: Um die Einhaltung des EMVG sicherzustellen sind die Geräte, wie in den Handbüchern angegeben, zu installieren und zu betreiben.

Japan Voluntary Control Council for Interference (VCCI) statement

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Taiwan Class A warning statement

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

People's Republic of China Class A warning statement

声　　明
此为 A 级产品。在生活环境中，
该产品可能会造成无线电干扰。
在这种情况下，可能需要用户对其
干扰采取切实可行的措施。

Korea Class A warning statement

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자
또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 판매 또는
구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Index

J

K

L

M

N

O

P

R

S

T

U

V

W

Printed in USA