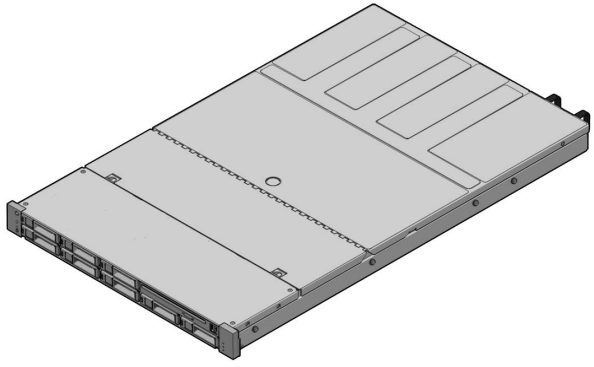
Sun Fire™ X4150 Server Embedded Lights Out Manager Administration Guide



Sun Microsystems, Inc.
www.sun.com

Part No. 820-1855-10
September 2007, Revision A

Submit comments about this document at: `http://www.sun.com/hwdocs/feedback`

Contents

Preface xiii

1. Sun Fire X4150 server ELOM Overview 1

Sun Fire X4150 server ELOM Features 2

Embedded Lights Out Manager Common Tasks 2

Sun Fire X4150 server Default Settings 3

About the Preconfigured Administrator Account 4

About the Indicator and Fault LEDs 4

2. Connecting to the ELOM 5

About Connection Tasks 6

Connecting Using a Serial Connection 6

- To Connect Using a Serial Connection 6

Connecting Using Ethernet 7

3. Monitoring the Server System Using the Web-Based Interface 11

Using the Web-Based Interface 11

Browser and Software Requirements 12

Users and Privileges 12

Web-Based Interface Tasks 12

Accessing the ELOM Using a Web Browser 13

▼ To Access the ELOM Using a Web Browser 13
Viewing the System From the Web Browser 14
Viewing System and Component Information 16
▼ To View System Information 16
Viewing Version Information 16
▼ To View SP Version Information 16
Viewing Server Board Information 17
▼ To View Server Board Information 17
Viewing Component Information 17
▼ To View CPU Information 17
Viewing Memory Information 19
▼ To View Memory Information 19
Monitoring the System Sensors 19
▼ To Monitor the System Sensors 20
Reading Sensors 20
▼ To Read Sensors 20
Viewing a Sensor Summary 21
▼ To View a Sensor Summary 21
Monitoring Fans 23
▼ To Monitor Fans 23
Monitoring Temperatures 23
▼ To Monitor Temperatures 23
Monitoring Voltages 24
▼ To Monitor Voltage 24
Viewing and Managing the Event Log 24
▼ To Display the Event Log 25
▼ To View the Event Logs 25
▼ To Save the Event Log 25

▼ To Clear the Event Log 26

4. Configuring, Managing and Maintaining the Server Using the Web-Based Interface 27

Configuring the System 28

▼ To Configure the System 29

Configuring Network Settings 30

▼ To Configure the Network Settings 30

Configuring E-mail Notification 30

▼ To Configure E-mail Notification 30

Configuring Platform Event Filters 30

▼ To Configure a Platform Event Filter 31

Configuring System Management Access 33

▼ To access the System Management Access Submenus 33

Configuring the SSL Certificate 34

▼ To Configure the SSL Certificate 34

Configuring SNMP 34

▼ To Configure SNMP 35

▼ To Add an SNMP Community 35

▼ To Delete an SNMP Community 36

▼ To Modify an SNMP Community 36

▼ To Add an SNMP User 36

▼ To Delete an SNMP User 37

▼ To Edit an SNMP User 37

Configuring Active Directory Service 37

▼ To Configure Active Directory Service 38

Managing and Maintaining the System 38

Managing Users and Accounts 38

▼ To Add a User 39

▼ To Change a User Password or Privilege 41
▼ To Delete a User Account 41
▼ To Disable or Enable a User 41
Managing the System Locator Indicator LED 42
▼ To Control the State of the System Indicator LED 42
Managing the Front Panel and On-Board Fault LEDs 42
▼ To View the State of the Fault LEDs 43
▼ To Turn the Fault LEDs Off 43
Setting Power Control 44
▼ To Set Power Control 44
Resetting the Service Processor 44
▼ To Reset the Service Processor 44
Updating the Firmware 45
Updating the Firmware Using a Web Browser 45
▼ To Update the Firmware Using a Web Browser 46
Recovering from a Corrupt SP 46
▼ To Recover From a Corrupt SP 47
Managing Session Timeout 48
▼ To Set the Session Timeout 48
▼ To Disable the Session Timeout 48
Setting the Time 49
▼ To Set the Time 49

5. Using the Remote Console Application 51

Accessing the Remote Console 51
Requirements 51
CD and Diskette Redirection Operational Model 52
Starting the Remote Console Application 54
▼ To Start the Remote Console Application 54

Setting Parameters for the Remote Console 55

▼ To Set Parameters for the Remote Console 55

Redirecting Keyboard, Video, Mouse, or Storage Devices 56

▼ To Redirect Keyboard and Mouse Devices 56

▼ To Redirect Storage Devices 57

Installing an Operating System on a Remote Server 58

▼ To Install an OS on a Remote Server Using a Virtual CD-ROM 58

Other Remote Options 59

6. Using IPMI 61

About IPMI 61

IPMItool 62

Sensors 62

Supported IPMI 2.0 Commands 63

7. Using the Command-Line Interface 69

Logging In to the CLI 69

Command Syntax 70

Managing the Host 72

Managing the Host State 72

Managing the Host Console 73

Viewing Host Sensors 73

Managing ELOM Network Settings 74

▼ To Display Network Settings 74

▼ To Configure Network Settings 74

Managing Local User Accounts With the CLI 75

Adding a User Account Using the CLI 76

▼ To Add a User Account Using the CLI 76

To Delete a User Account Using the CLI 76

▼ To Display User Accounts Using the CLI 76
Configuring User Accounts 77
Managing Alerts 78
Displaying Alerts 78
▼ To Display Alerts 78
Displaying PET Target Properties 80
▼ To Display PET Target Properties 80
Configuring Alerts 80
Configuring the PET IP Address 81
▼ To Configure the PET IP Address 81
Configuring the PEF Global Controls 81
▼ To Configure the PEF Global Controls 82
Configuring the Event Filter Tables 82
▼ To Configure the Event Filter Tables 83
Displaying Version Information 85
To Display the Current SP Version Information 85
Updating the Firmware 86
▼ To Update the Firmware 86

8. Using Simple Network Management Protocol 89

About SNMP 89
How SNMP Works 89
SNMP MIB Files 90
MIBs Integration 90
SNMP Messages 91
Configuring SNMP on the ELOM 92
Adding Your Server to Your SNMP Environment 92
Configuring Receipt of SNMP Traps 92
Managing SNMP User Accounts 92

Adding a User Account 92
Deleting a User Account 93
Configuring User Accounts 93

A. Command-Line Interface Reference 95

CLI Command Quick Reference 95
CLI Command Reference 99

Glossary 109

Index 131

Figures

FIGURE 3-1 ELOM System Information Screen 14

FIGURE 3-2 An Excerpt of the View Event Logs Screen 25

FIGURE 4-1 The Configuration Screen 29

FIGURE 4-2 The Platform Event Filter Screen 32

FIGURE 4-3 The User Management Screen 40

FIGURE 4-4 The Fault LED Screen 43

FIGURE 5-1 Keyboard, Video, and Mouse Selections 57

FIGURE 8-1 Sun Server MIB Tree 91

Preface

The *Sun Fire X4150 Server Embedded Lights Out Manager Administration Guide* provides instructions for managing Sun servers using the Sun Fire X4150 server (ELOM) with the service processor.

How This Document Is Organized

Chapter 1 describes the Embedded Lights Out Manager from an architectural standpoint and indicates tasks that can be accomplished with the management software.

Chapter 2 details the physical connections and how to communicate with your Sun Fire X4150 server.

Chapter 3 describes how to use the web-based interface to monitor your server with the embedded system management software.

Chapter 4 provides information about configuring, managing and maintaining the server system with a web browser.

Chapter 5 describes how to use the remote console through the web-based interface.

Chapter 6 describes the Intelligent Platform Interface (IPMI) and how it can be used to manage field replaceable units (FRUs) and system health independently of the operating system.

Chapter 7 provides an alternative method of managing your server—through the command-line interface (CLI).

Chapter 8 helps you understand the basics of the Simple Network Management Protocol (SNMP) and how it is important to your server management.

Appendix A gives you a quick reference to the commands you can use with Embedded Lights Out Manager.

Glossary is a list of words and phrases and their definitions.

Using UNIX Commands

This document might not contain information about basic UNIX® commands and procedures such as shutting down the system, booting the system, and configuring devices. Refer to the following for this information:

- Software documentation that you received with your system
- Solaris™ Operating System documentation, which is at `http://docs.sun.com.`

Typographic Conventions

Typeface*	Meaning	Examples
`AaBbCc123`	The names of commands, files, and directories; onscreen computer output.	Edit your `.login` file. Use `ls -a` to list all files. `% You have mail.`
`AaBbCc123`	What you type, when contrasted with onscreen computer output.	`% su` `Password:`
AaBbCc123	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the *User's Guide*. These are called *class* options. You *must* be a superuser to do this. To delete a file, enter `rm` *filename*.

* The settings on your web browser might differ from these settings.

Related Documentation

For the most up-to-date information about the Sun Fire X4150 server, navigate to your server at http://docs.sun.com/app/docs/prod/sf.x4150.

Translated versions of some of these documents are also available at http://docs.sun.com. Select a language from the drop-down list and navigate to the Sun Fire X4150 server document collection using the High-End Servers product category link. Available translations for the Sun Fire X4150 server include Simplified Chinese, Traditional Chinese, French, Japanese, and Korean.

English documentation is revised more frequently and might be more up-to-date than the translated documentation.

For all Sun hardware documentation, go to http://docs.sun.com/.

Sun Documentation, Support, and Training

Sun Function	URL
Documentation	http://www.sun.com/documentation/
Support	http://www.sun.com/support/
Training	http://www.sun.com/training/

Third-Party Web Sites

Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions, which you can submit at http://www.sun.com/hwdocs/feedback.

Please include the title and part number of this document with your feedback:

Sun Fire X4150 Server Embedded Lights Out Manager Administration Guide, 820-2705

CHAPTER 1

Sun Fire X4150 server ELOM Overview

This chapter serves as an overview of the capabilities of the Sun Fire X4150 server Embedded Lights Out Manager (ELOM), and contains the following sections:

- "Sun Fire X4150 server ELOM Features" on page 2
- "Embedded Lights Out Manager Common Tasks" on page 2
- "Sun Fire X4150 server Default Settings" on page 3
- "About the Preconfigured Administrator Account" on page 4
- "About the Indicator and Fault LEDs" on page 4

Sun Fire X4150 server ELOM Features

The ELOM provides a dedicated system of hardware and supporting software that enables you to manage your server independent of an operating system, and in low-power situations. ELOM is composed of four components:

- Web-based interface (requires JavaR v5 or later)
- Command-line Interface (accessed via serial or ethernet using `ssh`)
- IPMI v2
- SNMP v3

You can access the ELOM using a web browser, secure shell (SSH), or via the Sun Fire X4150 server's serial port. Your server's default network setting is configured as DHCP for easy access via a web browser or SSH, and the ELOM output is directed by default to the serial port.

Embedded Lights Out Manager Common Tasks

The following table shows common tasks and the management interfaces used to perform each task.

TABLE 1-1 ELOM Common Tasks

Task	IPMI	Web-Based Interface	CLI	SNMP
Redirect the system graphical console to a remote client web browser.	-	Yes	-	-
Connect a remote diskette drive to the system as a virtual diskette drive.	-	Yes	-	-
Connect a remote CD-ROM drive to the system as a virtual CD-ROM drive.	-	Yes	-	-
Monitor system fans, temperatures, and voltages remotely.	Yes	Yes	Yes	Yes
Monitor system BIOS messages remotely.	Yes	Yes	Yes	-
Monitor system operating system messages remotely.	Yes	Yes	Yes	-

TABLE 1-1 ELOM Common Tasks *(Continued)*

Task	IPMI	Web-Based Interface	CLI	SNMP
Interrogate system components for their IDs and serial numbers.	Yes	-	Yes	Yes
Redirect the system serial console to a remote client.	Yes	-	Yes	-
Monitor system status (health check) remotely.	Yes	Yes	Yes	Yes
Interrogate system network interface cards remotely for MAC addresses.	Yes	Yes	Yes	-
Manage user accounts remotely.	Yes	Yes	Yes	-
Manage system power status remotely (power on, power off, power reset).	Yes	Yes	Yes	-
Monitor and manage environmental settings for key system components (CPUs, motherboards, fans).	Yes	Yes	Yes	Monitor only

Sun Fire X4150 server Default Settings

Sun has configured the SP controller and SP firmware on your server to use the most common default settings. It is unlikely that you will need to change any of these defaults.

TABLE 1-2 SP Controller and Firmware Default Settings

System Component	Default Status	Action Required
Service processor card	Preinstalled	None
Service processor firmware	Preinstalled	None
IPMI interface	Enabled	None
Web-based interface	Enabled	None
Command-line interface (CLI)	Enabled	None
SNMP interface	Enabled	None

About the Preconfigured Administrator Account

The ELOM is shipped with one preconfigured administrator account:

User name: **root**
Password: **changeme**

The preconfigured administrator account, root, is the default account. It cannot be deleted or modified. You can only change the password for the root account. This default account contains administrator privileges (read and write access) to all service processor features and commands. For security reasons you should change the root password and create an alternate user account that also has administrator privileges. To change a user password or to create a new user, see Chapter 4.

If you've changed the root password, but have not created an alternate account, and the new root password is lost or forgotten, you will have to reset the SP to return the ELOM to its default settings. For information about how to do this, see"Resetting the Service Processor" on page 44.

About the Indicator and Fault LEDs

The LEDs on the front and rear panel of your server allow you to manage the server at a rudimentary level. The LEDs are helpful for indicating when a problem has occurred, and you can use these LEDs in combination with the internal fault indicator LEDs and buttons to troubleshoot and repair component failure issues. However, using the ELOM it is possible not only to troubleshoot component failure issues, but also to configure, manage, and maintain the server remotely and to implement an effective preventative maintenance program. Using the ELOM as part of a regular maintenance regimen allows you to take a proactive approach to server repair. This can improve system performance and minimize downtime.

For information about the Indicator and Fault LEDs, see the *Sun Fire X4150 Server Service Manual*.

For information about managing, maintaining, and configuring your server, see Chapter 4 of this guide.

CHAPTER 2

Connecting to the ELOM

This chapter details the ways to connect to and communicate with your Sun Fire X4150 server. It contains the following sections:

- "About Connection Tasks" on page 6
- "Connecting Using a Serial Connection" on page 6
- "Connecting Using Ethernet" on page 7

Note – You must install your server and configure the ELOM before communicating with the server. Information about installing the server and configuring the ELOM is available in the *Sun Fire X4150 Server Installation Guide*.

About Connection Tasks

You have two methods to connect to the ELOM in your server:

- Serial/Local
- Ethernet/Remote

Both methods require making physical cable connections to the server and logging in to the ELOM; refer to TABLE 2-1.

TABLE 2-1 Methods of Connecting to the ELOM

Connection Method	Supported Interface	Required Cable	Comments/Description
Serial, direct	CLI only	RJ-45 serial (supplied)	Connect directly to the serial management port the on server with a terminal or laptop running terminal emulation software.
Ethernet	CLI and Web browser	Ethernet LAN	You must know the ELOM's Ethernet address. **Note: This is the only method that supports web browser access.**

Note – The ELOM supports a maximum of 10 active sessions, including serial, SSH, and web browser sessions.

Connecting Using a Serial Connection

You access the ELOM CLI by connecting a terminal or a PC running terminal emulation software to the RJ-45 serial port on the server using the supplied cable.

▼ To Connect Using a Serial Connection

1. **Verify that your terminal, laptop, or terminal server is operational.**
2. **Configure the terminal device or terminal emulation software to use the following settings:**
   - 8,N,1: eight data bits, no parity, one stop bit.

- 9600 baud (default, can be set to any standard rate up to 57600).
- Disable software flow control (XON/XOFF).

3. **Connect a serial cable to the RJ-45 connection on the back of the server.**
4. **Connect the other end to the terminal or laptop.**
5. **Press Enter on the terminal device.**

   This action establishes the connection between the terminal device and the ELOM. When the server has booted, the ELOM displays its login prompt:

   `SUNSP`*`nnnnnnnnnn`* `login:`

   The first string in the prompt is the default host name. It consists of the prefix SUNSP and the ELOM's MAC address. The MAC address for each ELOM is unique.

6. **Log in to the CLI.**

   Accounts created using the web browser are available for the CLI. If this is the first login, you will need to use the preconfigured default account:

   User name: **`root`**.

   Password: **`changeme`**.

   Once you have successfully logged in, the default command prompt appears:

   `->`

   You can now run CLI commands (Chapter 7 describes how to use the CLI).

To log out of the CLI

- **Enter the following command:**

  `->` **`exit`**

Connecting Using Ethernet

Ethernet connectivity provides full access to both the ELOM command-line interface (CLI) and the web-based interface. Both connection options allow you to manage, maintain, and configure the server remotely. This section contains the following two connection procedures:

- Connecting to the CLI. See Connecting to the CLI.
- Connecting to the web-based interface. See Connecting to the Web-Based Interface.

Note – You will need the IP address of your ELOM, which you obtained during the setup and installation of your server (see the *Sun Fire X4150 Server Installation Guide).*

Connecting to the CLI

Be sure that you have connected a LAN to the NET MGT 0 port on the server, and that you have an SSH client installed on your remote system.

▼ To Connect to the CLI

1. **If necessary start your SSH client.**
2. **To log in to the ELOM, enter the following command:**

   $ **ssh** *username***@***ipaddress*

   username The user ID and *ipaddress* is the IP address of the ELOM. Accounts created using the web browser are available for the CLI. If this is the first login, you will need to use the preconfigured default account. For example,

   $ **ssh root@***ipaddress*

3. **When prompted, enter the password for the username used in Step 2.**

   The password for root is **changeme**.

   The CLI command prompt appears:

   –>

   For information about managing the server using the CLI, see Chapter 7. For information about the default account, see "About the Preconfigured Administrator Account" on page 3.

To Log Out of the CLI:

- **Enter the following command:**

  –> exit

Connecting to the Web-Based Interface

Be sure that you have connected a LAN to the NET MGT 0 port on the server.

▼ To Connect to the Web-Based Interface

1. **Type the IP address of the ELOM into your web browser.**

   The login screen appears.

2. **Type a user name and password.**

   Accounts created using the CLI are available for the web-based interface. If this is the first login, you will need to use the preconfigured default account:

   - Default user name: **`root`**
   - Default password: **`changeme`**

   For more information about the default account, see "About the Preconfigured Administrator Account" on page 3.

3. **Click Log In.**

   The web-based interface appears. Chapter 3 shows how to use the interface.

To Log Out of the web-based interface:

- **Click the Log Out button.**

  The Log Out button is located in the upper right corner of the screen.

CHAPTER 3

Monitoring the Server System Using the Web-Based Interface

This chapter provides information about how to use the web-based interface and the Sun Fire X4150 server software to monitor your server.

It includes the following sections:

- "Using the Web-Based Interface" on page 11
- "Accessing the ELOM Using a Web Browser" on page 13
- "Viewing System and Component Information" on page 16
- "Monitoring the System Sensors" on page 19
- "Viewing and Managing the Event Log" on page 24

Note – You can monitor the rudimentary state of the server using the LED fault light. A solidly lit amber LED indicates critical error. Further details about the fault light can be found in your *Service Manual*. For information about controlling the state of the fault LEDs see "To Control the State of the System Indicator LED" on page 42.

Using the Web-Based Interface

The web-based graphical user interface (GUI) allows you to use a standard web browser to monitor and manage local and remote systems.

You can redirect the server's console to a remote workstation or laptop system. This requires configuring the remote system's keyboard and mouse to act as the server's keyboard and mouse. You can configure the diskette drive or CD-ROM drive on the

remote system as if it were connected to the Sun server. You can also redirect diskette images (`.img` files) and CD-ROM images (`.iso` files) for remote access. Remote configuration issues are covered in Chapter 5.

Browser and Software Requirements

The web-based interface has been tested successfully with recently released Mozilla™ Firefox and Internet Explorer web browsers, and might be compatible with other web browsers.

The ELOM product is preinstalled on the Sun server. However, you need Java™ software on the client to perform redirection as described in Chapter 5.

Users and Privileges

After you log in to the web-based interface, you can perform basic software tasks, Intelligent Platform Management Interface (IPMI) tasks, and system monitoring.

ELOM user accounts define what you can do by roles:

- **Administrator** – Enables read/write access to all ELOM features, functions, and commands.
- **Operator, User, and Callback** – Enable limited access to ELOM features, functions, and commands. For example, users with these permissions cannot change their assigned roles or privileges.

For more information about users, including how to manage user accounts using the web-based interface, see Chapter 4.

Web-Based Interface Tasks

Some of the common tasks you can perform using the web-based interface include:

Configuring connection methods:

- Redirect the system's console to a remote client browser.
- Connect a remote diskette drive or diskette image to the system as a virtual diskette drive.
- Connect a remote CD-ROM drive or CD-ROM image to the system as a local or virtual CD-ROM drive.

Monitoring and managing system status:

- Monitor the status of system fans, temperatures, and voltages remotely.
- Monitor BIOS power-on self-test (POST) progress log entries remotely.
- View, save, and clear system event logs.
- Examine component information, including CPUs, DIMMs, voltages, and fans.
- Power on, power off, power cycle, reset the system remotely, reboot and enter the system BIOS, reboot and enter diagnostics (Pc-Check), and send NMI.

Managing and modifying system variables:

- Manage user accounts locally and remotely.
- Configure settings.
- Update BIOS firmware.

Accessing the ELOM Using a Web Browser

The ELOM boots automatically when a Sun server is cabled appropriately and plugged in to an AC power supply. This usually occurs within one minute. However, if the management Ethernet is not connected, or if the ELOM's Dynamic Host Configuration Protocol (DHCP) process fails due to the absence of a DHCP server on the management network, the ELOM might take a few minutes longer to boot.

Note – Disabling the use of the browser proxy server (if one is used) for access to the management network might speed the browser response time.

▼ To Access the ELOM Using a Web Browser

1. **To log in to the web-based interface, type the IP address of the ELOM in your web browser.**

   The login screen appears.

2. **In the login screen that appears, type the default user name and password.**

   Username: **`root`**

   Password: **`changeme`**

3. **Click Log In.**

   The web-based interface appears.

To log out of the web-based interface:

- **Click the Logout button in the upper right corner of the screen.**

Viewing the System From the Web Browser

The system is equipped with a number of sensors that measure voltages, temperatures, fan speed, and so on. The System Information tab shows the current system status and provides access to the Version, Session Time-Out, and the Components submenu tabs (see FIGURE 3-1).

FIGURE 3-1 ELOM System Information Screen

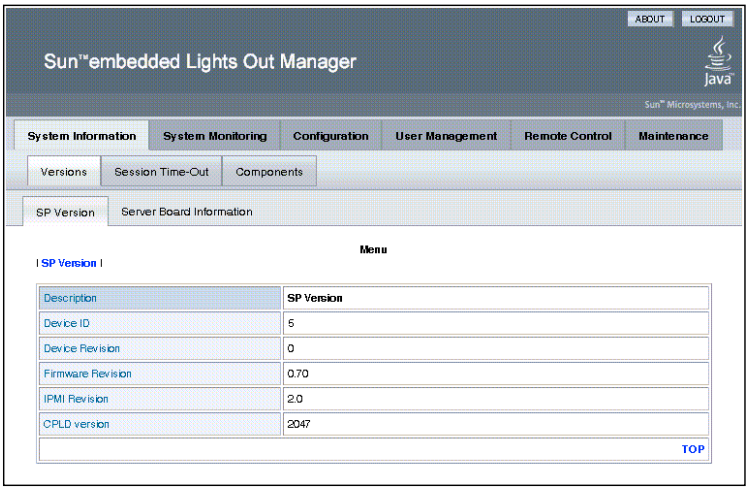


TABLE 3-1 lists the ELOM main menu and submenu tabs and points to relevant sections in this manual.

TABLE 3-1 ELOM Tab Detail Choices

Main Tab	Submenu Tab	Where to Find Details
System Information		"Viewing System and Component Information" on page 16.
	Server Board Information	"Viewing Version Information" on page 16.
	SP Version	"Viewing Version Information" on page 16.

TABLE 3-1 ELOM Tab Detail Choices *(Continued)*

Main Tab	Submenu Tab	Where to Find Details
	Session Time-Out	"Managing Session Timeout" on page 48
	Components	"Viewing Component Information" on page 17
System Monitoring		
	Sensor Reading	"Monitoring the System Sensors" on page 19
	Event Logs	"Viewing and Managing the Event Log" on page 24
	Locator Indicator Fault LED	"Managing the System Locator Indicator LED" on page 42
Configuration		
	Network	"Configuring Network Settings" on page 30
	E-mail Notification	"To Configure E-mail Notification" on page 30
	Platform Event Filter	"Configuring Platform Event Filters" on page 30
	Clock Settings	"Setting the Time" on page 49
	System Management Access	"Configuring System Management Access" on page 33
		"Recovering from a Corrupt SP" on page 46
User Management		
	User Account	"To Add a User" on page 39
	ADS Configuration	"To Configure Active Directory Service" on page 38
Remote Control		"Starting the Remote Console Application" on page 54
	Redirection	"Redirecting Keyboard, Video, Mouse, or Storage Devices" on page 56
	Remote Power Control	"Setting Power Control" on page 44
	Hotkey Setup	"To Set Parameters for the Remote Console" on page 55
Maintenance		
	Firmware Upgrade	"Updating the Firmware" on page 45
	Reset SP	"Resetting the Service Processor" on page 44

The following section describes how to monitor the server using the web browser and the Embedded Lights Out Manager software.

Viewing System and Component Information

The System Information tab provides information about system components, such as the service processor (SP), the server board, the CPU, and the memory. Details are found in the Versions and Components submenu tabs.

▼ To View System Information

- **On the main menu, click the System Information tab.**

  The System Information submenu appears, allowing you to view the Versions, Session Time-Out, and Components tabs.

Viewing Version Information

▼ To View SP Version Information

- **From the Versions submenu, select the SP Version tab.**

  The SP Version screen appears, displaying information about the server board installed in the system. It presents the information in a tabular format. For example, TABLE 3-2 shows a sample of the SP information as it is displayed in the SP Version screen:

TABLE 3-2 Sample SP Information

Description	SP Version
Device ID	5
Device Revision	0

TABLE 3-2 Sample SP Information

Description	SP Version
Firmware Revision	1.0
IPMI Revision	2.0
CPLD version	3041

Viewing Server Board Information

▼ To View Server Board Information

- **From the Versions submenu, select the Server Board Information tab.**

  The Server Board Information screen appears, displaying information such as the BIOS version and the serial number. It presents the information in a tabular format. TABLE 3-3 show a sample of the server board information as it is displayed:

TABLE 3-3 Sample Server Board Information

Description	Server Board Information
BIOS version:	1ADQWOO9
Manufacture Date:	Wed Dec 31 23:59:59 1969
Product:	Sun Fire X4150
Serial Number:	12345678901234

Viewing Component Information

▼ To View CPU Information

The CPU menu selection provides information about the processor.

- **From the System Information menu, click the Components submenu tab, then select CPU.**

  The CPU information screen appears. The CPU information is presented in a tabular format. A separate table of information is available for each of the server's CPUs, whether a CPU is installed or not. TABLE 3-4 shows a sample of the CPU information for CPU0:

TABLE 3-4 Sample CPU Information

CPU:	0
Status:	Enable
Socket:	CPU0
Manufacturer:	Intel
Model:	
Frequency:	

Viewing Memory Information

▼ To View Memory Information

- **From the System menu, select Components, and then select Memory.**

  The Memory screen appears. It displays information about total memory installed in your server; see TABLE 3-5.

TABLE 3-5 Sample Memory Information

Description	Memory Size Information
Total Memory Size:	12288 MB

The Memory screen also displays information about each DIMM installed in your system, presenting it in a tabular format that includes such information as the memory module number, the status, and module size; see TABLE 3-6 for a sample of the memory information for DIMM_A0.

TABLE 3-6 Sample Memory for DIMM_A0

Description	Memory Information
Memory Module:	1
Status:	Ok
Socket:	DIMM_A0
Module Size:	1024MB
Type:	FBDIMM
Frequency:	667MHz

Monitoring the System Sensors

Sensors placed throughout the system provide information about the state of critical server components. The sensors read temperature and voltage and report on operational status. Using the System Monitoring submenu screens you can view the these sensors and monitor the health of your server's critical components. For example, you can check the temperature of each CPU or DIMM and read the actual DC voltage of each of the system's power supply lines. The System Monitoring

submenu screens also allows you to view and manage the system log, the Locator Indicator LED, and the Fault LED. For information about the Locator Indicator LED and the Fault LED, see "Managing the System Locator Indicator LED" on page 42.

▼ To Monitor the System Sensors

- **On the main menu, click System Monitoring.**

  The System Monitoring submenu appears, allowing you to view the Sensor Reading, Event Logs, Locator Indicator, and Fault LED tabs.

Reading Sensors

▼ To Read Sensors

- **From the System Monitoring tab, click the Sensor Reading Tab.**

  The Sensor Reading tab allows you to select the Summary, Temperature, Voltage, and Chassis Status tabs.

Viewing a Sensor Summary

▼ To View a Sensor Summary

- **From the Sensor Reading tab, select the Summary tab.**

  The Summary screen appears. It provides an overview of the status of the system sensors. The screen provides the status of the Fault LED, the power, the temperature of all critical components, and each of the monitored voltage lines. For example, TABLE 3-7 shows the top portion of the summary table summarizing the status of the Fault LED and the system power.

TABLE 3-7 Top Portion of the Summary Table Showing the Fault LED and Power Status.

Fault LED Status	On
Power Status	Off

TABLE 3-8 shows a detail of the Summary table that summarizes the status of each of the system fans.

TABLE 3-8 Detail of the Summary Table Showing the Status of the System Fans.

	Fanbd1/FM1	:ok
	Fanbd1/FM0	:ok
	Fanbd1/FM3	:ok
	Fanbd1/FM2	:ok
	Fanbd1/FM5	:ok
	Fanbd1/FM4	:ok
Fan Status	Fanbd0/FM1	:ok
	Fanbd0/FM0	:ok
	Fanbd0/FM3	:ok
	Fanbd0/FM2	:ok
	Fanbd0/FM5	:ok
	Fanbd0/FM4	:ok
	Fanbd0/FM7	:ok
	Fanbd0/FM8	:ok

TABLE 3-9 shows a detail of the Summary table that summarizes the status of the temperature sensors.

TABLE 3-9 Detail of the Summary Table Showing the Status of the Temperature Sensors.

Temperature Status	CPU 0 Temp	:too high
	CPU 1 Temp	:ok
	Ambient Temp0	:ok

TABLE 3-10 shows a detail of the Summary table that summarizes the status of the DC power supply lines.

TABLE 3-10 Detail of the Summary Table Showing the Status of the Power Supply Lines.

Voltage Status	Vcc 12V	:ok
	Vtt 1.2V	:ok
	MCH 1.5V	:ok
	Vcc 3.3V	:ok
	Vcc 5V	:ok
	NIC Vtt 1.2V	:ok
	Vcc 3.3V STB	:ok
	Vcc 2.5V STB	:ok
	Vcc 1.8V	:ok

TABLE 3-11 shows a detail of the Summary table that summarized the status of the systems power supplies.

TABLE 3-11 Detail of the Summary Table Showing the Status of the Power Supplies.

Power Status	PS0 Under Volt	:ok
	PS1 Under Volt	:ok
	PS0 OC Fault	:ok
	PS1 OC Fault	:ok
	Power Supply 0	:ok
	Power Supply 1	:ok

Monitoring Fans

▼ To Monitor Fans

- **From the Sensor Reading tab, select the Fan tab.**

  The Fan screen appears, displaying the critical thresholds, the actual sensor reading, and the status for each of the systems fans. The readings are in RPM. The information is presented in tabular format. TABLE 3-12 shows sample information on the Fan screen. The sample is for the fan labeled Fanbd1/FM1.

TABLE 3-12 Sample of Fan Information for Fanbd1/FM1

Description	Fanbd1/FM1
Lower critical threshold is readable:	1463
Upper critical threshold is readable:	14936
Sensor Reading:	13629
Status:	ok

Monitoring Temperatures

▼ To Monitor Temperatures

- **From the Sensor Reading tab, select the Temperature tab.**

  The Temperature screen appears, displaying the ambient chassis and CPU temperatures. The temperatures are displayed in degrees celsius. The Sensor Reading screen shows the current temperature reading. TABLE 3-13 shows sample Temperature information for CPU 0. A separate table is presented for each CPU and each ambient sensor.

TABLE 3-13 Sample Temperature Monitor Readings

Description	CPU 0 Temp
Upper noncritical threshold is readable:	93.0
Upper critical threshold is readable:	95.0
Sensor Reading:	54.0
Status:	ok

A similar panel is repeated for each monitored entity.

Monitoring Voltages

▼ To Monitor Voltage

- **From the Sensor Reading tab, click the Voltage tab.**

  The Voltage screen appears. The Voltage screen displays the critical and noncritical thresholds, the actual sensor reading, and the status for the nine monitored DC system voltage lines. The Sensor Reading value represents the actual voltage reading for that sensor. TABLE 3-14 shows a sample from the Voltage screen. The sample is for the Vcc 12V line:

TABLE 3-14 Sample of the Voltage Monitor Screen

Description	Vcc 12V
Lower noncritical threshold is readable:	11.999
Lower critical threshold is readable:	10.821
Upper noncritical threshold is readable:	12.837
Upper critical threshold is readable:	13.215
Sensor Reading:	12.081
Status:	ok

Viewing and Managing the Event Log

The Event Logs screen allows you to view and manage the system event log (SEL). The SEL is a record of event occurrences. To record events in the SEL, you must have previously determined which events require logging. See "Configuring Platform Event Filters" on page 27.

▼ To Display the Event Log

- **From the System Monitoring tab on the main menu, click the Event Logs submenu tab.**

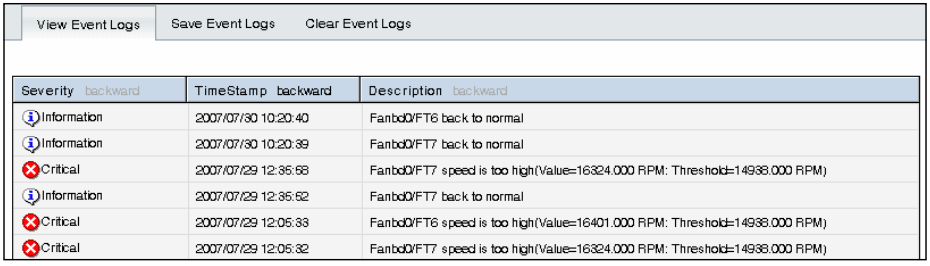
  The Event Logs screen appears. The View Event Logs, Save Event Logs, and Clear Event Logs submenus become available.

▼ To View the Event Logs

- **From the Event Logs tab, select View Event Logs.**

  The system event log appears. Each entry in the log represents an action that occurred on the system. The information is presented in a tabular format. The system lists each action, rates the action's severity, provides a time stamp, and describes the event. The severity field includes icons for both Information and Critical ratings. FIGURE 3-2 shows an excerpt from the View Event Logs screen.

FIGURE 3-2 An Excerpt of the View Event Logs Screen



▼ To Save the Event Log

You might want to save the event log for administrative or diagnostic purposes.

1. **From the Event Logs tab, click the Save Event Logs tab.**

   The Save Event Log screen appears.

2. **Click the Save Event Log button to prompt the browser to ask you where to save a copy of the event log.**

3. **Select the location, name the file (if necessary), and click save.**

▼ To Clear the Event Log

The Event Log might need to be cleared to signify a fresh procedure, or identify system performance under load.

1. **From the Event Logs tab, click Clear Event Log.**
2. **Click the Clear Event Log button to start a fresh event log.**

CHAPTER 4

Configuring, Managing and Maintaining the Server Using the Web-Based Interface

This chapter provides information about how to use a web browser and the Sun Fire X4150 server software to manage your server. The sections include:

- "Configuring the System" on page 28
- "Managing and Maintaining the System" on page 38

This chapter addresses your local system. For information about how to redirect your commands to a remote system, see Chapter 5.

Configuring the System

The Configuration submenu tabs enable you to configure the network operation and other important functions of the server. These functions are described in the following sections:

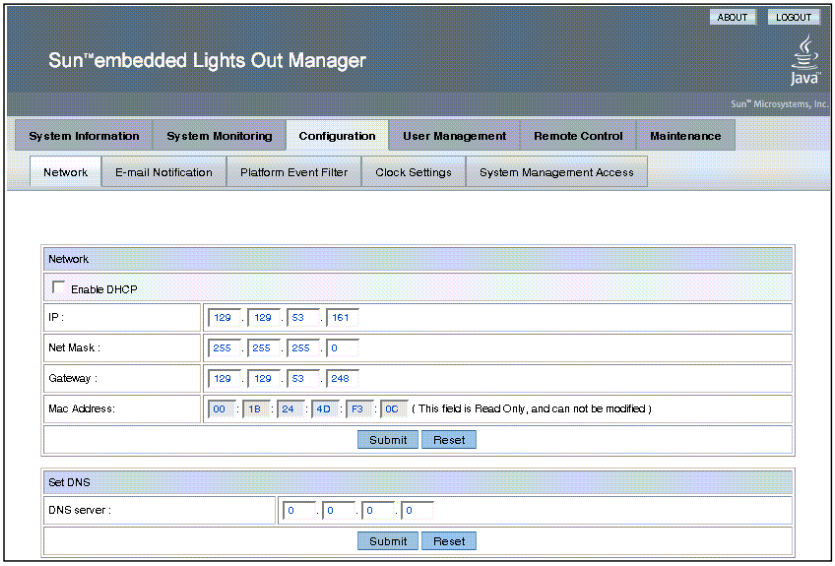
- "Configuring Network Settings" on page 30
- "Configuring E-mail Notification" on page 30
- "Configuring Platform Event Filters" on page 30
- "Configuring System Management Access" on page 33
- "Configuring SNMP" on page 34
- "Configuring Active Directory Service" on page 37

▼ To Configure the System

- **From the main menu, click the Configuration tab.**

  The Configuration tabs appear (see FIGURE 4-1). You are now able to access the Network, E-mail Notification, Platform Event Filter, Clock Settings, and System Management Access screens.

FIGURE 4-1 The Configuration Screen



Configuring Network Settings

▼ To Configure the Network Settings

- **From the Configure submenu, click the Network tab.**

  The Network configuration screen appears (see FIGURE 4-1). Use this screen to enable or disable DHCP and set DNS. If you disable DHCP, you must manually supply the IP address, the netmask, and the gateway.

Configuring E-mail Notification

The E-mail Notification screen enables you to configure the e-mail recipients for any ELOM generated events. The system allows you to designate up to 10 recipients. e-mail notification is used in conjunction with Platform Event Filters (PEF). PEFs are event traps that allow you to associate an action, or a set of actions, with the occurrence of a specific event. One such action is mail notification. The Send Mail action is enabled in the Platform Event Filter screen and configured in the E-mail Notification screen.

▼ To Configure E-mail Notification

- **From the Configuration submenu, click the E-mail Notification tab.**

  The Enable E-mail Notification screen appears. You must supply the name of the SMTP server and the sender and designate the receiver e-mail addresses.

Configuring Platform Event Filters

The Platform Event Filter option allows you to configure actions for system generated events. A system generated event is an alert that occurs when a threshold for a system sensor is reached. For example, the system uses the sensors to monitor various critical components. The components are most effective when operating within a specific range. The limits of that range are defined as thresholds. All components, such as fans, have an upper and lower critical threshold (see "To Monitor Fans" on page 23). When either critical threshold is crossed the system generates an alert. For example a fan failure would cause an alert for the lower critical threshold. You can configure an event filter to trigger off the alert and perform one or several actions. These actions include:

- Performing one of three power actions
- Performing an NMI diagnostic interrupt
- Sending alert to the SEL
- Sending mail

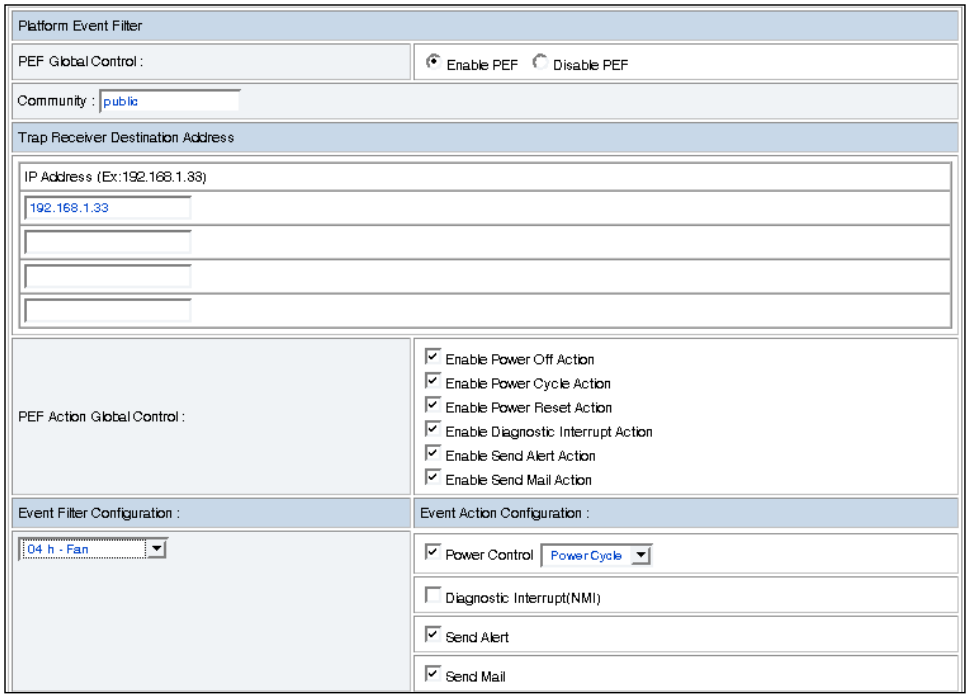
An event is configured in two parts: the event (or alert) and the response or action to be taken when that event occurs. You can configure up to six filters. You begin by determining what sort of event you want to trap.

▼ To Configure a Platform Event Filter

1. **From the Configuration submenu click Platform Event Filter tab.**

   The Platform Event Filter screen appears (see FIGURE 4-2). The PEF screen is divided into five sections:
   - Platform Event Filter
   - Trap Receiver Destination Address
   - PEF Action Global Control
   - Event Filter Configuration
   - Event Action Configuration

FIGURE 4-2 The Platform Event Filter Screen



2. **In the The Platform Event Filter section click the Enable PEF radio button.**

   To configure/create a filter, you must first enable PEF.

3. **Type the address of the trap receiver in the Trap Receiver Destination Address section.**

4. **Enable all actions that you would like to be available for your filters by selecting the appropriate check box in the PEF Action Global Control section.**

   The actions are:

   - Enable Power Off Action
   - Enable Power Cycle Action
   - Enable Power Reset Action
   - Enable Diagnostic Interrupt Action
   - Enable Send Alert Action
   - Enable Send Mail Action

5. **Select the sensor group for which you would like to filter alerts from the drop-down list in the Event Filter Configuration.**

   The options are:

   - ffh - All sensors

- 01h - Temperature
- 02h - Voltage
- 04h - Voltage
- 07h - Processor
- 0Ch - Memory

6. **Select the action for the alerts by selecting the check boxes in the Event Action Configuration section.**

   If you are selecting a power control action, select the action from the drop-down list after selecting the Power Control check box.

   In the example shown in FIGURE 4-2, the system is configured to enable all actions. A filter has been created to filter fan alerts. When an alert occurs, the system will cycle power, send an alert to the SEL, and send mail to the addresses listed in the E-mail Notification screen (see "Configuring E-mail Notification" on page 30). You can configure up to six filters.

7. **Click Submit to create the filter.**

Configuring System Management Access

The System Management Access submenus allow you to set up the SSL certificate and SNMP. The SSL configuration is used for creating certificates required in the Certificate Signing Request (CSR). The certificate is required to enable encryption for when you use HTTPS for secure web browser access. HTTPS requires a digitally signed certificate to be installed at the applicant's site. The SNMP screen allows the configuration of SNMP settings, communities, and users.

▼ To access the System Management Access Submenus

- **From the Configuration submenu click the System Management Access tab.**

  The System Management Access submenu tabs appear.

Configuring the SSL Certificate

▼ To Configure the SSL Certificate

1. **From the System Management Access submenu, click the SSL Certificate tab.**
   The SSL Certificate screen appears.
2. **Select either Certificate or CSR from the drop-down list.**
3. **Fill in the required fields in the SSL Configuration section.**
4. **Click Generate to create the certificate.**
5. **Click Upload to bring the certificate into view.**

Note – If no certificate has yet been assigned, follow the directions below to generate a new CSR.

---

6. **Follow the onscreen directions, and fill in the fields using the example as a guide.**
   The example in TABLE 4-1 represents the kind of information required.

TABLE 4-1 Example of Required SSL Information

Common Name (CN):	*localhost.localdomain*
Organization Unit (OU):	*Your Name*
Organization (O):	*Your Company Name*
Country Code (C):	*U.S.A. (drop-down list of countries)*
Locality (L):	*Your Location*
State (S):	*Your State*
E-mail Address (E):	*youradmin@localhost.localdomain*

7. **Click Generate to create a new CSR.**

Configuring SNMP

A series of screens allow you to set port, requests, and SNMP permission parameters for the system you are logged in to.

Note – The SNMP MIB file is located on the Tools and Drivers CD in the directory `/SNMP/mib/`.

▼ To Configure SNMP

1. **From the System Management submenu, click the SNMP tab.**

   The SNMP screen appears.

2. **Select SNMP settings from the drop-down list, and then click Select.**

   The SNMP Settings screen appears.

3. **Select the Set Request check box to set one or more SNMP variables.**

   This check box acts as a global override for the user and community read/write permissions. For example, if you disable Set Requests, a member of the private community accessing your Sun server or stand-alone system via the SNMP interface cannot set sysContact despite having write permission.

4. **Select the check box beside the preferred version of SNMP protocols to override the delivered system default.**

5. **Click Submit to save the configuration, or click Reset to clear your entries.**

▼ To Add an SNMP Community

1. **In the SNMP screen, select SNMP Communities from the drop-down list and click Select.**

   The SNMP Communities screen appears.

2. **Select the radio button at the head of an unoccupied row.**

3. **Click Add to create a new community.**

   The Community Setting screen appears.

4. **Type the name of the new community in the Community field.**

5. **Select a permission from the Permission drop-down list.**

6. **Click Submit to add the community.**

▼ To Delete an SNMP Community

1. **In the SNMP screen, select SNMP Communities from the drop-down list, and then click Select.**

   The SNMP Communities screen appears.

1. **Select the radio button at the head of the row for the community that you want to delete.**

2. **Click the Delete button to delete the community.**

   The system does not prompt for a confirmation.

▼ To Modify an SNMP Community

1. **In the SNMP screen, select SNMP Communities from the drop-down list, and then click Select.**

   The SNMP Communities screen appears.

2. **To change permissions for an existing community, select the radio button at the head of the row for the community you would like to modify.**

3. **Click Modify.**

   The displayed screen allows you to change file permissions for that community.

4. **Select the permission from the Permission drop-down list.**

   The permission is either read-only (ro) or read/write (rw).

5. **Click Submit to modify the community, or click Reset to clear your changes.**

▼ To Add an SNMP User

1. **In the SNMP screen, select SNMP User Settings from the drop-down list, and then click Select.**

   The SNMP User Settings screen appears.

2. **Select the radio button at the head of an unoccupied row.**

3. **Click Add to create a new user.**

   The User Setting screen appears.

4. **Fill in the open fields for the new user in the User Setting screen.**

   The Authentication Protocol options are MD5 and SHA.
   The Permission options are rw (read/write) and ro (read-only).

5. **Click Submit to create the new user.**

▼ To Delete an SNMP User

1. **In the SNMP screen, select SNMP User Settings from the drop-down list, and then click Select.**

   The SNMP User Settings screen appears.

2. **Select the radio button at the head of the row for the user that you want to delete.**

3. **Click the Delete button to delete the user.**

   The system does not prompt for a confirmation

▼ To Edit an SNMP User

1. **In the SNMP screen, select SNMP User Settings from the drop-down list, and then click Select.**

   The SNMP User Settings screen appears. This screen allows you to add, delete, and edit users.

2. **Select the radio button at the head of the row for the user setting that you would like to edit.**

3. **Click the Edit button in the same row.**

   The User Settings screen appears.

4. **Edit the necessary user settings.**

   You cannot edit the user name. To change a user name, delete and re-create the user with a different name.

5. **Click Submit to save your changes.**

Configuring Active Directory Service

The ADS Configuration screen enables you to browse and upload a certificate from Active Directory Service (ADS) for a Microsoft Windows environment. Administrators can simplify their tasks by monitoring multiple machines in one node using ADS.

▼ To Configure Active Directory Service

1. **From the User Management submenu, click the ADS Configuration tab.**
   The ADS Configuration screen appears.
2. **Enter the Primary, Secondary DNS and the Root Domain addresses.**
3. **If one is available, upload your certificate.**
4. **Click Submit, or click Reset to clear your changes.**

Managing and Maintaining the System

The User Management, System Monitoring, Remote Control, Maintenance, and System Information submenus enable you to manage and maintain server-related functions. These functions are described in the following sections:

- "Managing Users and Accounts" on page 38
- "Managing the System Locator Indicator LED" on page 42
- "Setting Power Control" on page 44
- "Resetting the Service Processor" on page 44
- "Updating the Firmware" on page 45
- "Recovering from a Corrupt SP" on page 46
- "Managing Session Timeout" on page 48
- "Setting the Time" on page 49

Managing Users and Accounts

The User Management tab provides access to the User Account screen, which lists current users by privilege and status, and enables the administrator to add, delete, modify and enable/disable user accounts.

The ELOM supports up-to 10 user accounts. One of the user accounts is root, which is set by default and cannot be removed. Therefore, you can configure 9 additional accounts. Each user account consists of a user name, a password, and a permission.

Note – User permissions extend to both the web-based interface and the serial connection methods.

The permissions that a user can be assigned include:

- **Administrator** – Enables read and write access to all ELOM software features, functions, and commands.
- **Operator** – Enables limited access to SP software features, functions, and commands. Operators cannot change their assigned roles.
- **User** – Enables a user to access the system without being able to add, modify, or delete accounts.
- **Callback** – Enables access to commands that set up the callback feature.

Note – If the SP password has been changed and then lost, a BIOS option exists to reset the password back to the default `changeme`. See "Resetting the Service Processor" on page 44. This method is *not* supported if you use a virtual CD-ROM.

▼ To Add a User

1. **From the User Management submenu, click the User Account tab.**

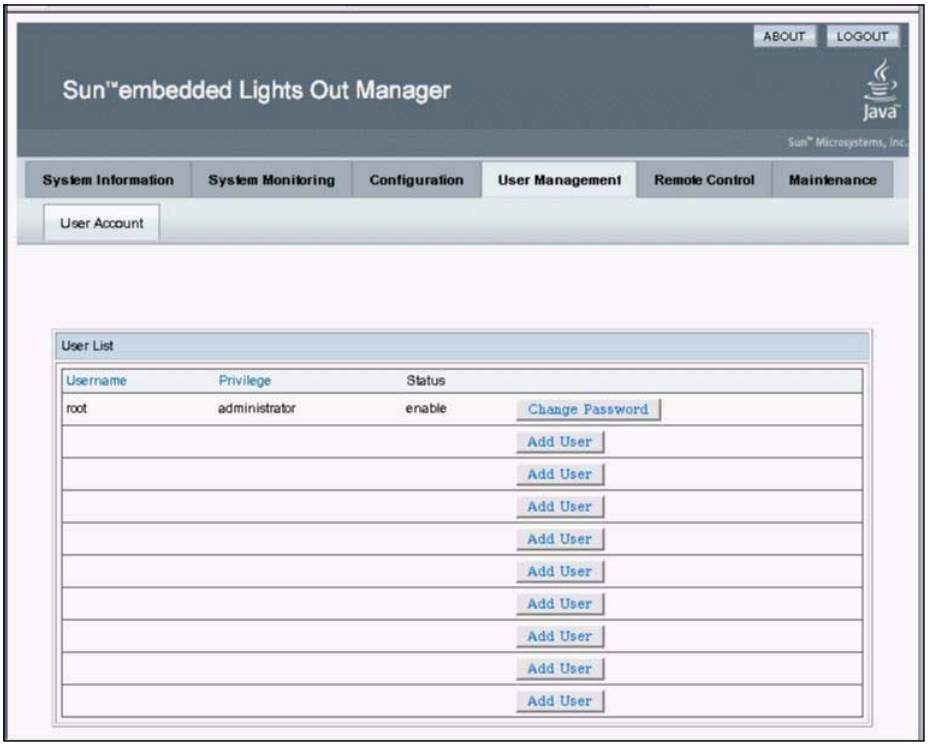
   The User List screen appears.

2. **Click any button labeled Add User.**

   The Manage User Account screen appears (see FIGURE 4-3).

   If all 10 user account slots are configured, you must delete an existing user account before you can add a new user account. See "To Delete a User Account" on page 41.

FIGURE 4-3 The User Management Screen



3. **Complete the following information.**

   a. **Type a user name in the User Name field.**

      The user name must be at least 4 characters and no more than 20 characters. User names are case-sensitive and must start with an alphabetical character. You can use alphabetical characters, numerals, hyphens, and underscores. Do not include spaces in user names.

   b. **Type a password in the Password field.**

      The password must be at least 8 characters and no more than 16 characters. The password is case-sensitive. Use alphabetical, numeric, and special characters for better security. You can use any character except a colon. Do not include spaces in passwords.

   c. **Retype the password in the Confirm Password field to ensure that the password is correct.**

   d. **Select either Administrator, Operator, User, or Callback for the user permission.**

e. **When you finish entering the new user's information, click Add.**

The User Accounts screen appears. The new user account and associated information is displayed on the User Accounts screen.

▼ To Change a User Password or Privilege

1. **From the User Management submenu, click the User Account tab.**

   The User List screen appears.

2. **Click either the Change Password or Change Permission button for the user.**

3. **Change the password or privilege as needed.**

4. **After you have modified the user information, click Submit for your changes to take effect, or click Reset to return to the previous settings.**

   A confirmation screen verifies that the user account was modified successfully.

▼ To Delete a User Account

1. **From the User Management submenu, click the User Account tab.**

   The User List screen appears.

2. **Click the Delete button for the user that you would like to delete.**

   You do *not* receive a confirmation prompt.

▼ To Disable or Enable a User

Disabling a user makes the user account inactive. This might be preferable to deleting the account.

1. **From the User Management submenu, click the User Account tab.**

   The User List screen appears.

2. **Click the Disable or Enable button for the appropriate user.**

   You do *not* receive a confirmation prompt.

Managing the System Locator Indicator LED

The System Locator Indicator LED is located on the front and rear panel of the server. You can activate the Locator Indicator LED in the ELOM. By activating the Locator Indicator LED for a particular server, you can identify that server from the many other servers installed in a rack. You can manage the state of the System Locator Indicator LED from the ELOM Maintenance screens.

▼ To Control the State of the System Indicator LED

1. **From the main menu, click the System Monitoring tab.**

   The System Monitoring submenu tabs appear.

2. **Click the Locator Indicator tab.**

   The System Indicator LED screen appears.

3. **Select the appropriate radio button to either turn the LED on or turn it off.**

4. **Click Submit to change the state of the LED, or click Reset to cancel.**

Managing the Front Panel and On-Board Fault LEDs

Your server is equipped with six fault LEDS. Four of the LEDs are on the front panel, and two are located inside the server on the motherboard. Three of the front panel LEDs are located on the right front side of the server front panel, the Top Open (Check Fan Status) LED, the Power Supply (PS) LED, and the Overtemperature Warning LED. These LEDs alert you to problems specific to a particular subsystem. Use these LEDs in conjunction with the ELOM to troubleshoot down to the component level.

The Fault LED (Service Required LED) is located on the left side of the server front panel. This LED alerts you to an internal problem on the motherboard. Use the Fault LED in conjunction with the two internal on-board fault LEDs, the CPU LED and the DIMM LED to troubleshoot issues related to a specific CPU or DIMM.

You can monitor and manage the state of the Fault LEDs from the ELOM Maintenance screens. For more information about using the fault LEDs to troubleshoot server problems, see the *Sun Fire X4150 Server Service Manual.*

▼ To View the State of the Fault LEDs

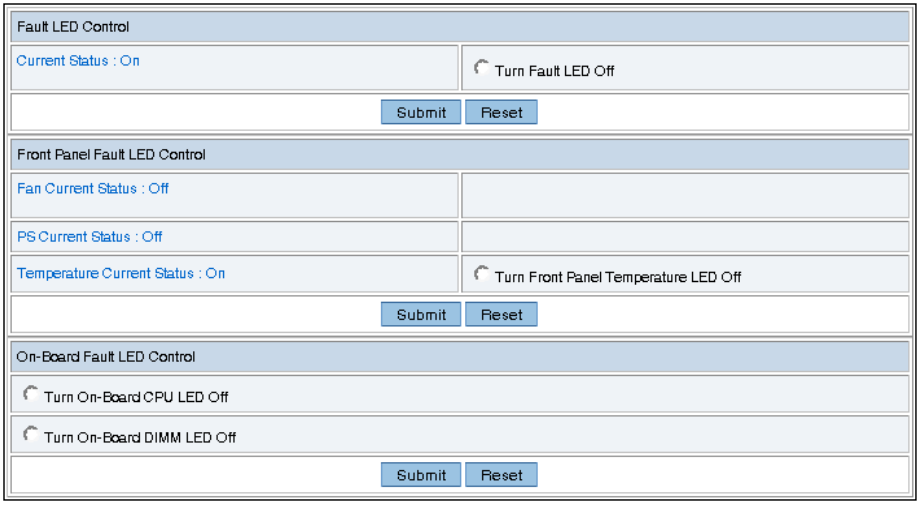
1. **In the main menu, click the System Monitoring tab.**

   The System Monitoring submenu tabs appear.

2. **Click the Fault LED submenu tab.**

   The Fault LED Control screen appears (see FIGURE 4-4).

FIGURE 4-4 The Fault LED Screen



The Fault LED screen is divided into three sections, the Fault LED Control section, the Front Panel Fault LED Control, and the On-Board Fault LED Control. These sections allow you to monitor and change the status of each LED. If the current status of an LED is On, then you will have the option to turn it Off. Otherwise, the LED status is shown as Off. For example in FIGURE 4-4, the front panel Fault LED, the Overtemperature Warning LED and the internal on-board CPU LED and DIMM LED are On.

▼ To Turn the Fault LEDs Off

1. **Select the appropriate radio button for the fault LED that you would like to turn off.**

2. **Click the appropriate Submit button for the particular section to turn the LED off.**

Setting Power Control

You can control power to the server you are logged in to by using the Remote Power Control submenu screen to set the power control action.

▼ To Set Power Control

1. **From the Remote Control tab of the Embedded Lights Out Manager software screen, choose Remote Power Control.**

   The Power Control screen appears showing a drop-down list of various power-off and restart options: Force Power Off, Reset, Graceful Shutdown, Boot Option: BIOS Setup, Boot Option: PC Check, and NMI.

2. **Select power option you want and click Save.**

   For example, select Boot Option: BIOS Setup to reboot the system and enter the BIOS.

3. **When you have made your changes, click Submit to save the changes, or click Reset to clear the changes.**

Resetting the Service Processor

The baseboard management controller holds the original default settings of the service processor. In the event of system lock-up or panic you can reset the SP to its original state.

▼ To Reset the Service Processor

1. **From the main menu click the Maintenance tab.**

   The Maintenance submenus appear.

2. **Click the Reset SP submenu tab.**

   The Reset SP screen appears.

Note – Resetting the SP is a hard reset. Because you are logged in to the web-based interface when the SP is reset, the interface will become inactive.

---

3. **Click Reset SP button.**

   The following message appears:

   Please wait for SP reset then reconnect.

Updating the Firmware

There are multiple ways to update the SP firmware.

- Use the Tools and Drivers CD.

1. Power on the system and boot the system using the Tools and Drivers CD.
2. Five menu options appear. To update the firmware, select one of the following two options:
   - Flash System BIOS/Service Processor Firmware—Clear BIOS CMOS and load default settings (recommended).
   - Flash the System BIOS/Service Processor Firmware—Preserve BIOS CMOS settings (advanced use only).

Note – Use the second option only if you have customized BIOS settings and would like to retain these settings. This option might require user intervention during the reboot.

- Use `TftpUpdate` through the CLI. See "To Update the Firmware" on page 86.
- Use `CPLDUpdate` through the CLI. See to "To Update the Firmware" on page 86.
- Use a web browser to update firmware. See the next section, "Updating the Firmware Using a Web Browser" on page 45.

Updating the Firmware Using a Web Browser

This section explains how to update firmware to a remote server. There are two options for updating firmware.

1. Clear CMOS (default)
2. Preserve CMOS

If the system BIOS has not been customized, select option #1: Clear CMOS. If the system BIOS has been customized, select option #2: Preserve CMOS.

Note – Selecting option #2 might require user interaction during the reboot.

▼ To Update the Firmware Using a Web Browser

Note – The system *must* be powered off for you to perform an update. If the server is powered on, the SP warns the user to power off before continuing. The option to update firmware will not be available if the server is powered on. For information about how to power-off the server, see "Setting Power Control" on page 44.

1. **From the main menu, select the Maintenance tab.**

   The Maintenance submenu tabs appear.

2. **Click the Firmware Update tab.**

   The Firmware Update screen appears.

3. **Select the firmware file or CPLD file to update.**

   These files are located on the Tools and Drivers CD in the `Remote_Firmware` directory.

4. **Choose whether to preserve the system BIOS CMOS and load optimized defaults.**

5. **Firmware will perform a check and ask the user to confirm the update by displaying current and proposed firmware revisions.**

6. **When the update is finished, after approximately five minutes, the SP resets and you are logged out.**

Recovering from a Corrupt SP

Should the SP (service processor) software become corrupted, you can reinstall the default image from the CD. You need a bootable USB flash device and a jumper cap.

Note – The server has a a jumper cap installed on the motherboard for this purpose. It is next to the AST 2000 chip.

▼ To Recover From a Corrupt SP

1. **Copy all SP files from the Tools and Drivers CD to a USB flash device.**

   The SP files are located in the `BMCrecovery` directory, on the Tools and Drivers CD. They consist of:

   - SOCFLASH.EXE
   - DOS4GW
   - BMC Binary *(SP Binary file)*

2. **Remove AC power from system to be flashed.**

Note – Do not attempt to flash the system while it is still powered on. An unrecoverable error might occur.

---

3. **Remove the server's top cover.**
4. **Using a jumper cap, short the pins at jumper JP20 on the server motherboard.**

   JP20 is located toward the rear of the board. See the *Sun Fire X4150 Server Service Manual* for the precise location.

5. **Insert the bootable flash drive into the USB port.**
6. **Connect AC power and power on the system.**

   a. **A message appears stating that the BMC was not found.**

      The system takes up to three minutes to boot.

   b. **Press F2 to enter system BIOS and verify that the Flash device is in the boot order.**

7. **Once the flash device is booted, run the following command:**

   `socflash.exe` *SP binary backup file*

   For example:

   `socflash.exe s92v092.bin backup.bin`

8. **After a successful flash, remove the AC power and jumper, and leave the system powered off for up to 30 seconds.**
9. **Power on the system.**
10. **Confirm that the SP is listed in the BIOS settings under Server/AST2000 LAN Configuration.**

Managing Session Timeout

The session timeout is an inactivity timer. If an open session enters a state of inactivity that exceeds the preset timer, the system closes (logs out) the session. This function prevents unauthorized access to the system by providing an automated logout function. The session timeout is *enabled* by default.

▼ To Set the Session Timeout

1. **From the main menu, click the System Information tab.**
   The Versions, Session Time-Out, and Components submenu tabs appear.
2. **Select the Session Time-Out tab.**
   The Session Time-Out screen appears.
3. **Click the Enable Timeout radio button.**
4. **Select a session time from the Session Time drop-down list.**
   The options are 15 minutes (default), 30 minutes, 1-hour, and 2 hours.
5. **Click the Submit button to set the session timeout.**

▼ To Disable the Session Timeout

1. **From the main menu, click the System Information tab.**
   The Versions, Session Time-Out, and Components submenu tabs appear.
2. **Select the Session Time-Out tab.**
   The Session Time-Out screen appears.
3. **Click the Disable Time-Out radio button.**
4. **Click the Submit button to disable the session timeout.**

Setting the Time

▼ To Set the Time

1. **From the Configuration submenu, click the Set Time tab.**

   The Set Time screen appears. Use the radio buttons to either manually input the date and time, or to use an NTP server. For the latter, you will have to input the IP address of the server.

CHAPTER 5

Using the Remote Console Application

This chapter describes how to use the remote console application. It includes the following sections:

- "Accessing the Remote Console" on page 51
- "Starting the Remote Console Application" on page 54
- "Redirecting Keyboard, Video, Mouse, or Storage Devices" on page 56
- "Installing an Operating System on a Remote Server" on page 58
- "Other Remote Options" on page 59

Accessing the Remote Console

The remote console application, which you access via a web browser, enables you to control your server's operating system remotely using the screen, mouse, and keyboard, and to redirect local CD and diskette drives as if they were connected directly to the server.

Requirements

A compatible web browser and a minimum of JRE™ 1.6.0 are required to operate the remote console application. See TABLE 5-1.

Note – You do not need to install any OS-specific drivers or helper applications on client systems to run the remote console application.

TABLE 5-1 Client Installation Requirements

Client OS	Java Runtime Environment Including Java Web Start	Web Browsers
Microsoft Windows XP Pro	JRE 1.6 (Java 6.0 or later)	Internet Explorer 6.0 and later Mozilla 1.7.5 or later Mozilla Firefox 1.0
Red Hat Linux 4.0 or later Desktop and Workstation Editions	JRE 1.6 (Java 6.0 or later)	Mozilla 1.7.5 or later Mozilla Firefox 1.0
Solaris 9	JRE 1.6 (Java 6.0 or later)	Mozilla 1.7.5
Solaris 10	JRE 1.6 (Java 6.0 or later)	Mozilla 1.7.5
SUSE Linux 9.2	JRE 1.6 (Java 6.0 or later)	Mozilla 1.7.5

Note – You can download the JRE 1.6 at `http://java.sun.com`.

Note – To start the remote console successfully, pop-ups must be allowed on the browser. With some browsers you can do this by pressing and holding the Control key when launching the remote console session.

CD and Diskette Redirection Operational Model

When you redirect the local client CD drive or diskette drive to a remote host server, the following rules apply:

- In all cases, the CD drive and diskette drive appear to be plugged in to the host.
- If you do not redirect them, the host acts as if there is no medium unless there is a CD in the host CD drive. If there is a CD in the host CD drive, the host accesses it normally.

The information in TABLE 5-2 describes different case scenarios in which the remote console application and CD drive and diskette drive redirection operate.

TABLE 5-2 Remote Console Operation With DVD Drive and Diskette Drive

Case	Status	DVD Seen by Host	Diskette Seen by Host
1	Remote console application not started or remote console started but DVD/diskette redirection not started.	DVD device present. No medium indication is sent to the host from the ELOM when the hosts asks.	Diskette device present. No medium indication is sent to the host from the ELOM when the host asks.
2	Remote console application started with no medium present in the drive.	DVD device present. Whenever the host asks, which may be automatic or when you access the device on the host, the remote client sends a status message. In this case since there is no medium, the status is no medium.	Diskette device present. Whenever the host asks (for example, you double-click a drive), the remote client sends a status message. In this case since there is no medium, the status is no medium.
3	Remote console application started with no medium, then medium is inserted.	DVD device present. Whenever the hosts asks (automatic or manual), the remote client sends a status message as medium present and also indicates the medium change.	Diskette device present. Whenever the host asks (manual), the remote client sends a status message as medium present and also indicates the medium change.
4	Remote console application started with medium inserted.	Same as 3.	Same as 3.
5	Remote console application started with medium present, then medium is removed.	Next command from the host gets a status message indicating medium not present.	Next command from the host gets a status message indicating medium not present.
6	Remote console application started with image redirection.	Same as 3.	Same as 3.
7	Remote console application started with image, but redirection is stopped (which is the only way to stop ISO redirection).	Driver knows DVD redirection stopped so it sends a medium absent status on the next host query.	Driver knows DVD redirection stopped so it sends a medium absent status on the next diskette query.
8	Network failure.	The software has a keep alive mechanism. The software detects keep alive failure since there is no communication and closes the socket, assuming the client is unresponsive. Driver sends a no medium status to the host.	The software has a keep alive mechanism. The software detects and unresponsive client, closes the socket, and indicates to the driver that the remote connection went away. Driver sends a no medium status to the host.
9	Client crashes.	Same as 8.	Same as 8.

Starting the Remote Console Application

Use this procedure to start the remote console application from a web browser. You might be presented with a series of questions. In each case, select Run.

Note – Each new ELOM system is delivered with DHCP set as the default. If an IP address is not found within 5 seconds, the system retries three times to find a DHCP server. It it is still unsuccessful, the SP will default to the IP address 192.168.xxx.xxx where xxx.xxx is based upon the last two fields of the SP MAC address, to allow instant web access.

▼ To Start the Remote Console Application

1. **Open your web browser.**
2. **In the address bar, enter the IP address of the SP.**

   The login screen appears.
3. **Type an administrator user name and password.**

   Or use the default preconfigured account:

   ```
   Username: root
   Password: changeme
   ```
4. **Click Login.**

   The main menu screen appears.
5. **Click the Remote Control tab, and select Redirection.**

   The screen displays a Launch Redirection button.
6. **Click Launch Redirection.**

   A screen identifies your current host name, IP address, and user name. The Launch button opens the remote console.
7. **Click Launch.**

Note – For systems using Firefox and Mozilla web browsers, the required version of JRE must be at least version 1.6 or later.

The web browser downloads the embedded remote control application automatically, and the Remote Console screen appears.

If the remote console does not appear, it might be blocked by web browser security controls. Reduce security configuration to allow the remote console to appear.

Note – To start the remote console successfully, pop-ups must be allowed on the browser. With some browsers you can do this by pressing and holding the Control key when launching the remote console session.

Changing the format of the screen is described in the following section, "To Set Parameters for the Remote Console" on page 55.

Setting Parameters for the Remote Console

This section explains how to define the quality of video, the size of the screen, and set hot keys for the remote console application.

▼ To Set Parameters for the Remote Console

1. **From the Remote Control submenu, select Hotkey Setup.**

   The User Profile screen appears. The User Profile screen allows you to set up separate video, KVM, and hot key settings for each user. The subsequent window displays a version of the screen output. This requires a Java Webstart application to be launched.

   a. **The first time this application is launched you must respond to accept various security questions before the application is installed and operates correctly.**

   b. **Right-click to display the remote console as a full screen.**

      By default, the remote console will synchronize both mouse cursors, and display only one mouse cursor within the remote console screen.

      When the mouse cursor leaves the screen, the local cursor takes over and the other mouse cursor remains in the remote console screen.

      You can enable user modes in the setup of the web-based interface or in the remote console screen.

2. **When the login is successful, the remote console screen appears.**

   The remote console application starts with the video and keyboard enabled by default. In most cases, you need only enable the mouse redirection. You can now use the remote console application to start your server's operating system.

Note – For detailed instructions on how to enable and disable I/O and storage devices (CD-ROM and diskette drives), see "Redirecting Keyboard, Video, Mouse, or Storage Devices" on page 56.

Redirecting Keyboard, Video, Mouse, or Storage Devices

The remote console application supports the redirection of the following types of devices:

- Video quality display – the server's video output is automatically displayed on the local console screen.
- Hot key – enable a single key to mimic a series of keystrokes.
- Keyboard and mouse devices – Standard keyboards, mouse, and other pointing devices.
  - Keyboard redirection is enabled by default.
  - Mouse redirection must be enabled manually.
- Storage devices – CD/DVD drives, Flash, DVD-ROM or diskette disk drives, hard drives, or NFS.

▼ To Redirect Keyboard and Mouse Devices

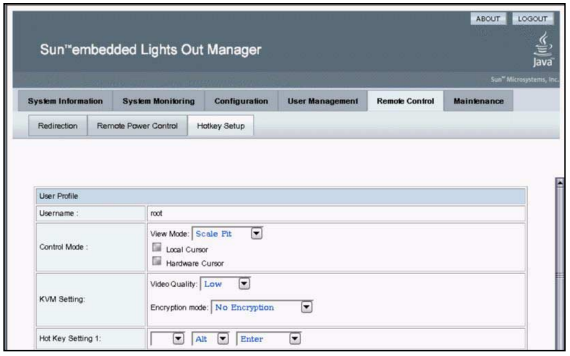
Use the following procedure to redirect your local workstation or laptop keyboard and mouse to a remote Sun Fire X4150 server.

1. **Start the remote console application as described in** "Starting the Remote Console Application" on page 54**.**
2. **From the Remote Control submenu, select the Hotkey Setup tab.**

   The Control Mode section of the Hotkey Setup screen enables mouse redirection.
3. **Select Hardware Cursor to enable a variety of cursor movements.**

Note – For the mouse to work correctly, you might have to change the mouse mode. Click the double mouse cursor on the navigation bar to toggle between local and remote mouse cursor movement. Keyboard redirection is selected by default.

FIGURE 5-1 Keyboard, Video, and Mouse Selections



You can click Submit to enable your options after each choice to observe the consequences, or continue directly to Step 4.

4. **When you have completed your selections, click Submit to enable your options.**

▼ To Redirect Storage Devices

Use the following procedure to enable a storage device attached to your local workstation or laptop to serve as a storage device for a server. You can use this option to install software from a local CD/DVD drive to multiple remote servers.

You can also redirect a CD image file or a diskette image file stored on your hard drive.

1. **Start the remote console application as described in** "Starting the Remote Console Application" on page 54**.**

   The Remote Console screen appears.

2. **Select Storage from the drop-down list, and click Mount Device.**

   This enables the corresponding local storage device to connect to the remote server as though it were a storage device attached directly to that remote server.

3. **Select a source device from the drop-down list.**

- To store a selection to a real CD-ROM device, select from the Drive Name drop-down list.
- To store a CD image file or a diskette image file to your hard drive, select ISO file from the Source Device drop-down list.

Note – You cannot select two CD-ROM devices or two diskette devices. For example, you cannot select CD-ROM and CD-ROM image. Use the web browser to navigate to the corresponding file, then click Submit.

Installing an Operating System on a Remote Server

This method includes using a CD or DVD drive or image of the operating system on a remote networked system to install the operating system, for example, onto the Sun Fire X4150 server.

Requirements for Remote KMVS Over IP installation include:

- Remote system connected to the network
- CD/DVD drive connected to the remote system
- Media for installing the operating system of your choice
- SP of the server set up as instructed in the *Sun Fire X4150 Server Installation Guide*.

▼ To Install an OS on a Remote Server Using a Virtual CD-ROM

Note – Disable the timeout function when installing remotely from the virtual CD-ROM.

---

1. **On your laptop or local terminal, open a web browser, and enter the IP address of the Sun Fire X4150 server service processor for the target system.**

   This is the Sun Fire X4150 server on which you want to install the operating system.

2. **Type the user name and password in the login screen.**

3. **From the Remote Control submenu, click the Redirection tab.**
4. **Click the Launch Redirection button to open a remote console screen.**
5. **Insert the operating system CD/DVD to be installed on the Sun Fire X4150 server into your laptop or local CD/DVD drive.**
6. **In the remote console screen, choose Storage –>Mount devices.**

   The Device Configuration screens appears.
7. **Under Storage 1, in the drop-down list, select the local CD/DVD that you will be using for the installation.**
8. **Click Submit.**
9. **Reboot the server.**

   The system will add the virtual CD-ROM to the boot order, and boot from it.

Other Remote Options

Command-line options that are available to address many of these tasks include IPMI tools (Chapter 6), CLI (Chapter 7), and SSH (Secure Shell).

CHAPTER 6

Using IPMI

This chapter describes the Intelligent Platform Management Interface (IPMI) functionality and lists the supported IPMI commands. It includes the following sections:

- "About IPMI" on page 61.
- "Supported IPMI 2.0 Commands" on page 63.

About IPMI

The Intelligent Platform Management Interface (IPMI) is an open-standard hardware management interface specification that defines a specific way for embedded management subsystems to communicate. IPMI information is exchanged through the service processor (SP), an IPMI-compliant hardware component. Using low-level hardware intelligence instead of the operating system has two main benefits: First, this configuration allows for out-of-band server management, and second, the operating system is not burdened with transporting system status data.

You can manage your server with the IPMI v.1.5/2.0 on your server or stand-alone server, which runs a daemon to do the following:

- Support low pin count (LPC) host interface in two modes:
  - KCS Mode (3 channels)
  - BT Mode (1 channel with 32 bytes of FIFO)
- Support dedicated NIC or shared lights out management (LOM)
- Support Serial-On-LAN (SOL)
- Customize FRU/Sensor Data Record data (firmware independent)
- Provide KVM over IP (remote access to the server)
- Enable the user interface (UI) for hot key definitions (for example Ctrl-Alt-Del)

- Provide full screen display switch
- Set dynamic video scaling (4x4 Video Scalar)

Your Sun Fire X4150 server is IPMI v2.0 compliant. You can access IPMI functionality through the command line with the IPMItool utility either in-band or out-of-band. Additionally, you can generate an IPMI-specific trap from the web interface or manage the server's IPMI functions from any external management solution that is IPMI v1.81 or v2.0 compliant. For more information about the IPMI v2.0 specification, go to:

http://www.intel.com/design/servers/ipmi/spec.htm#spec2

IPMItool

IPMItool is a simple command-line interface that is useful for managing IPMI-enabled devices. You can use this utility to perform IPMI functions with a kernel device driver or over a LAN interface. IPMItool enables you to manage system field-replaceable units (FRUs), monitor system health, and monitor and manage system environmentals, independent of the operating system.

Download this tool from http://ipmitool.sourceforge.net/, or locate IPMItool and its related documentation on your server Tools and Drivers CD.

When IPMItool is installed, it includes a man page. To view it, enter:

```
man ipmitool
```

If your client machine has a default installation of Solaris 10, you can find a preinstalled version of IPMItool in the following directory:`/usr/sfw/bin`. The binary file is called `ipmitool`.

Sensors

Your server includes a number of IPMI-compliant sensors. Some sensors measure voltages, and temperature ranges, and others are capable of monitoring switches, such as the chassis interlocks, which detect whether the chassis cover is open or shut. For a complete list of sensors, see your platform supplement. To obtain sensor information on specific sensors, enter the following command:

ipmitool -H *ipaddressof the SP* -U *username* -P *password* [sensor | sdr]

The sensors can activate system fault lights, and register events in the system event log (SEL). To see the system event log from the IPMItool, at the prompt, enter the following command:

ipmitool -H *ipaddress of the SP* **-U root -P** *password* **sel list**

Depending on where IPMItool is installed from, the `-P` option might be missing. In such a case, do not type the `-P` in the previous command, and enter the password when prompted.

Supported IPMI 2.0 Commands

TABLE 6-2 lists the supported IPMI 2.0 commands.

For details on individual commands, see the IPMI Intelligent Platform Management Interface Design Specification, v2.0. A copy is available at:

`http://www.intel.com/design/servers/ipmi/spec.htm`

TABLE 6-1 Supported IPMI 2.0 Commands

Commands	Description
raw	Send a RAW IPMI request and print response
i2c	Send an I2C Master Write-Read command and print response
lan	Configure LAN channels
chassis	Get chassis status and set power state
power	Shortcut to chassis power commands
event	Send predefined events to MC
mc	Management Controller status and global enables
sdr	Print Sensor Data Repository entries and readings
sensor	Print detailed sensor information
fru	Print built-in FRU and scan SDR for FRU locators
sel	Print system event log (SEL)
pef	Configure platform event filtering (PEF)
sol	Configure and connect IPMIv2.0 Serial-over-LAN
tsol	Configure and connect with Tyan IPMIv1.5 Serial-over-LAN
isol	Configure IPMIv1.5 Serial-over-LAN
user	Configure Management Controller users
channel	Configure Management Controller channels
session	Print session information

TABLE 6-1 Supported IPMI 2.0 Commands *(Continued)*

Commands	Description
sunoem	OEM commands for Sun servers
kontronoem	OEM commands for Kontron devices
picmg	Run a PICMG/ACTA extended `cmd`
fwum	Update IPMC using Kontron OEM Firmware Update Manager
exec	Run list of commands from file
set	Set runtime variable for `shell` and `exec`

TABLE 6-2 Supported IPMI 2.0 Commands

Supported IPMI 2.0 Commands
General Commands
Get Device ID
Cold Reset
Get Self Test Results
Set/Get ACPI Power State
Reset/Set/Get Watchdog Timer
Set/Get BMC Global Enables
Clear/Get Message Flags
Enable Message Channel Receive
Get/Send Message
Read Event Message Buffer
Get Channel Authentication Capabilities
Get Session Challenge
Activate/Close Session
Set Session Privilege Level
Get Session Info
Set/Get Channel Access
Get Channel Info
Set/Get User Access
Set/Get User Name

TABLE 6-2 Supported IPMI 2.0 Commands *(Continued)*

Supported IPMI 2.0 Commands *(Continued)*
Set User Password
Master Write-Read
Set/Get System Boot Options
Set/Get Event Receiver IPMI
System Interface Support
KCS
BT
Serial Over LAN
RCMP
• Multiple Payloads
• Enhanced Authentication
• Encryption
PEF and Alerting Commands
Get PEF Capabilities
Arm PEF Postpone Timer
Set/Get PEF Configuration Parameters
Set/Get Last Processed Event ID
Alert Immediate
PET Acknowledge
Sensor Device Commands
Get Sensor Reading Factors
Set/Get Sensor Hysteresis
Set/Get Sensor Threshold
Set/Get Sensor Event Enable
Get Sensor Reading
FRU Device Commands
Get FRU Inventory Area Info

TABLE 6-2 Supported IPMI 2.0 Commands *(Continued)*

Supported IPMI 2.0 Commands *(Continued)*
Read/Write FRU Data SDR Device
Get SDR Repository Info
Get SDR Repository Allocation
Reserve SDR Repository
Get/Add SDR
Clear SDR Repository
Get SDR Repository Time
Run Initialization Agent
SEL Device Commands
Get SEL Info
Get SEL Allocation Info
Reserve SEL
Get/Add SEL Entry
Clear SEL
Set/Get SEL Time
LAN Device Commands
Get LAN Configuration Parameters
Serial/Modem Device Commands
Set/Get Serial Modem Configuration
Set Serial Modem MUX
Get TAP Response Codes
Serial/Modem Connection Active
Callback
Set/Get User Callback Options
Event Commands
Get Event Count

TABLE 6-2 Supported IPMI 2.0 Commands *(Continued)*

Supported IPMI 2.0 Commands *(Continued)*
Set/Get Event Destination
Set/Get Event Reception State
Send ICMB Event Message

CHAPTER 7

Using the Command-Line Interface

This chapter describes how to use the Embedded Lights Out Manager command-line interface (CLI). The sections include:

- "Logging In to the CLI" on page 69.
- "Command Syntax" on page 70.
- "Managing the Host" on page 72.
- "Managing ELOM Network Settings" on page 74.
- "Managing Local User Accounts With the CLI" on page 75.
- "Managing Alerts" on page 78.
- "Displaying Version Information" on page 85.
- "Updating the Firmware" on page 86.

Logging In to the CLI

You can access the command-line interface through the serial port or over the Ethernet.

- Serial port – The serial port provides access to the CLI and to the system console. IPMI terminal mode and PPP mode are not available on the serial port. For information about logging in to the CLI using the serial port, see "Connecting Using a Serial Connection" on page 6.
- SSH –You can connect to the CLI using an Ethernet connection. Secure Shell connections (SSC) are enabled by default. For information about logging in to the CLI using an Ethernet connection, see "Connecting Using Ethernet" on page 7.

The Sun Fire X4150 server ELOM supports a maximum of 10 active sessions, including serial, SSH, and web interface sessions. Telnet connections to the ELOM are not supported.

Note – If you have changed the serial redirection output in the system BIOS from SP to SYSTEM, the system output is displayed on the serial connection. To view the SP output on the serial connection, change the system BIOS back to the default BMC.

Command Syntax

The CLI architecture is based on a hierarchical namespace, which is a predefined tree that contains every managed object in the system. This namespace defines the targets for each command verb.

The Embedded Lights Out Manager (ELOM) software includes the `/SP` and /SYS namespaces.

The `/SP` namespace manages the ELOM. The children of this namespace are /user, /network, /clock, /AgentInfo, /TftpUpdate, and /CPLDUpdate, which allow you to use this space to manage users, clock settings, and other issues.

The /SYS namespace monitors the ELOM. The children of this namespace include /BoardInfo, /ProductInfo, /ChassisInfo, /CtrlInfo, /CPU, /MemModule, /Fan, /Temperature, and /Voltage

The CLI provides two privilege levels: Administrator and User. Administrators have full access to ELOM functionality, and users have read-only access to information.

Note – The default user, root, has administrator privileges. For information about how to create a user account with user privileges, see "Adding a User Account Using the CLI" on page 76.

CLI commands are case-sensitive.

Syntax

The syntax of a command is *verb options target properties.*

Command Verbs

TABLE 7-1 describes the CLI command verbs.

TABLE 7-1 CLI Command Verbs

Command	Description
`cd`	Navigates the object namespace.
`create`	Sets up an object in the namespace.
`delete`	Removes an object from the namespace.
`exit`	Terminates a session to the CLI.
`help`	Displays Help information about commands and targets.
`losd`	
`reset`	Resets the target's state.
`set`	Sets target properties to the specified value.
`show`	Displays information about targets and properties.
`start`	Starts the target.
`stop`	Stops the target.
`version`	Displays the version of ELOM firmware that is running.

Options

The CLI supports the following options. Not all options are supported for all commands. See a specific command section for the options that are valid with that command. The `-help` and `-examine` options can be used with any command.

TABLE 7-2 CLI Options

Option Long Form	Short Form	Description
`-default`		Causes the verb to perform only its default functions.
`-destination`		Specifies the destination for data.
`-display`	`-d`	Shows the data you want to display.
`-examine`	`-x`	Examines the command but does not execute it.
`-force`	`-f`	Causes an immediate action instead of an orderly shutdown.
`-help`	`-h`	Displays Help information.

TABLE 7-2 CLI Options *(Continued)*

Option Long Form	Short Form	Description
`-keep`	`-k`	Establishes a holding time for command job ID and status.
`-level`	`-l`	Executes the command for the current target and all targets contained through the level specified.
`-output`	`-o`	Specifies the content and form of command output.
`-resetstate`		Indicates to what target-specific state to reset the target.
`-script`		Skips warnings or prompts normally associated with the command.
`-source`		Indicates the location of a source image.

Targets

Every object in your namespace is a target. Not all targets are supported for all commands. Each command section lists the valid targets for that command.

Properties

Properties are the configurable attributes specific to each object. An object can have one or more properties. Each command section lists the valid properties for each target.

Managing the Host

You can use the ELOM to change the host's state and to access the host console.

Managing the Host State

- To power on the host, enter one of the following commands:

  `set /SYS/CtrlInfo PowerCtrl=on`

  -or-

  `start SYS`

- To power off the host gracefully, enter the following command:

  set /SYS/CtrlInfo PowerCtrl=graceful_off

- To power off the host, enter one of the following commands:

  set /SYS/CtrlInfo PowerCtrl=off

  -or-

  stop SYS

- To reset the host, enter one of the following commands:

  set /SYS/CtrlInfo PowerCtrl=reset

  -or-

  reset SYS

- To reboot and enter the BIOS automatically, enter the following command:

  set /SYS/CtrlInfo PowerCtrl=BIOSSetup

- To reboot and enter Pc-Check diagnostic automatically, enter the following command:

  set /SYS/CtrlInfo PowerCtrl=PCCheck_enable

Managing the Host Console

To start a session to the server console, enter this command:

start /SP/AgentInfo/Console

To revert to CLI once the console has been started, press Esc-Shift-9 keys.

To terminate a server console session started by another user, enter this command:

stop /SP/AgentInfo/Console

Viewing Host Sensors

Host systems are equipped with sensors that monitor the state of critical components. For example, they record things like temperatures, voltages, and fan speeds. The `show` command can be used to show the state of the critical components. Use the command:

show /SYS/CPU/*component*

component The particular critical component.

For example, the following command shows the state of CPU 0:

show /SYS/CPU/CPU0

For more information about sensors, including how to view them using a web browser, see "Monitoring the System Sensors" on page 19.

Managing ELOM Network Settings

You can display or configure the ELOM network settings from the CLI.

▼ To Display Network Settings

Enter the following command to display or set network settings:

show /SP/network *(This will display all network settings.)*

▼ To Configure Network Settings

Use the `set` command to change properties and values for network settings.

Note – Ensure that the same IP address is always assigned to an ELOM by either assigning a static IP address to your ELOM after initial setup, or configuring your DHCP server to always assign the same IP address to an ELOM. This enables the ELOM to be easily located on the network.

Targets, Properties, and Values

These targets, properties, and values are valid for ELOM network settings.

TABLE 7-3

Target	Property	Value	Default
/SP/network	IpAddress	*ipaddress* | *none*	192.168. *last 2 digits of MAC address*
			enabled (only if DHCP not found)
	IPSource	*static/dhcp*	dhcp
	Gateway	*ipaddress* | *none*	None
			255.255.255.0
	Netmask	*ipdotteddecimal*	

Examples

To change the IP address for the ELOM, Enter:

Note – Changing the IP address will disconnect your active session if you are connected to the ELOM via a network.

Syntax

```
set /SP/network IPAddress=n.n.n.n
set /SP/network Gateway=n.n.n.n
set /SP/network DNS=n.n.n.n
set /SP/network IPSource=[static|dhcp]
```

Managing Local User Accounts With the CLI

This section describes how to add, modify, and delete user accounts using the CLI.

The ELOM supports up to 10 user accounts. One of those, root, is set by default and cannot be removed. Therefore, you can configure 9 additional accounts.

Each user account consists of a user name, a password, and a permission.

The permisisons include:

- **Administrator** – Enables read and write access to all ELOM software features, functions, and commands.
- **Operator** – Enables limited access to SP software features, functions, and commands. Operators cannot change their assigned roles.
- **User** – Enables a user to access the system without being able to add, modify, or delete accounts.
- **Callback** – Enables access to commands that set up the callback feature.

The syntax is:

set *username* **Permission=[administrator|operator|user]**

Adding a User Account Using the CLI

▼ To Add a User Account Using the CLI

- **Enter the following command:**

  create /SP/users/*username*

  You are prompted for a password.

  The username must be 4-20 characters long, and passwords must be a minimum of eight characters long.

To Delete a User Account Using the CLI

- **Enter the following command:**

  delete /SP/users/*username*

▼ To Display User Accounts Using the CLI

- **Enter the following command:**

  show /SP/users

Configuring User Accounts

Use the `set` command to change passwords and permissions for configured user accounts.

Note – You must have administrator privileges to change user properties.

Syntax

`set target` *[propertyname=value]*

Targets, Properties, and Values

These targets, properties, and values are valid for local user accounts.

TABLE 7-4

Target	Property	Value	Default
`/SP/users/`*username*	permissions password	administrator | operator *string*	operator

Examples

When changing the permissions for user1 from administrator to operator Enter:

`set /SP/users/user1 Permission=operator`

To change user1's password Enter:

`set /SP/users/user1 password=`*password*

Managing Alerts

The system is equipped with sensors that read several system critical parameters, such as voltages and temperatures. The system monitors these sensors and creates an alert when a sensor reading crosses an upper or lower critical threshold level (for more information, see "Configuring Platform Event Filters" on page 30).

You can manage these alerts, by using the CLI to create filters that trap alerts based on the sensor type. You can then have the filters perform various preconfigured actions in response to the alert. Configuring alerts with the CLI is a two step process. First, configure a destination IP address in the PET. Second, configure a platform event filter (PEF) to enable and perform various alert-triggered actions.

You manage alerts from the /SP/AgentInfo namespace, using the `show` and `set` commands. The `show` command allows you to display current alert property and value settings. The `set` command allows you to configure alert property and value settings.

Displaying Alerts

Use the `show` command to display PET and PEF targets, properties, and values.

▼ To Display Alerts

- **To display targets, properties, and target commands for PET, enter the following command:**

  `show /SP/AgentInfo/PET`.

- **To display targets, properties, and target commands for PEF, enter the following command:**

  `show /SP/AgentInfo/PEF`

  Before configuring alerts, you might want to display a target's current settings. This allows you to examine the current status of alerts. Use the `cd` command and the `show` command, respectively, to navigate to targets and display property values. For example:

  –> **`cd /SP/AgentInfo/PET`**

  /SP/AgentInfo/PET –> **`show`**

The output of the `show` command appears:

```
/SP/AgentInfo/PET
   Targets:
       Destination1
       Destination2
       Destination3
       Destination4

   Properties:
       CommunityString = public

   Target Commands:
       show
       cd
       set
```

Displaying PET Target Properties

▼ To Display PET Target Properties

- **To display properties, enter the following commands:**

  /SP/AgentInfo/PET –> **`cd Destination1`**

  /SP/AgentInfo/PET –> **`show`**

  The result of executing the show command for the target, Destination1 appears:

```
/SP/AgentInfo/PET/Destination1
    Targets:

    Properties:
        IPAddress = 10.5.157.112
        MACAddress = 00:00:00:00:00:00
        Status = enable

    Target Commands:
        show
        set
```

  You can now examine the values for the properties, IPAddress, MACAddress, and Status.

Configuring Alerts

The first step to configuring alerts is to configure the PET IP address. After you configure the IP address, you need to configure the individual PEF filter tables. Filter tables are where you designate the specific alert-triggered actions

Use the `set` command to configure alerts in PET and PEF:

Syntax

`set` *target propertyname=value*

Targets, Properties, and Values

This target, property, and value is valid when using the set command to set the IPMI PET IP address:

Target	Property	Value	Default
/SP/AgentInfo/PET/[Destination1...Destination4]	IPAdress	*ipaddress*	(None)

Configuring the PET IP Address

▼ To Configure the PET IP Address

- **To set the IP address for Destination1, enter the following commands:**

  –> **`cd /SP/AgentInfo/PET/Destination1`**

  /SP/AgentInfo/PET/Destination1 –> **`set IPAddress=`***xxx.xxx.xxx.xxx*

  Repeat the above `set` command to configure the IP address for additional destination targets.

Configuring the PEF Global Controls

PEF Global Controls allow you to enable PEF actions globally. These settings override settings in the PEF filter table. These targets and properties are valid for configuring the gobal PEF controls:.

Target	Property*
/SP/AgentInfo/PEF/PEFGlobalCtrl	= enable | disable (default)
/SP/AgentInfo/PEF/PEFActionGlobalCtrlPowerOff	= enable | disable (default)
/SP/AgentInfo/PEF/PEFActionGlobalCtrlPowerCycle	= enable | disable (default)
/SP/AgentInfo/PEF/PEFActionGlobalCtrlPowerReset	= enable | disable (default)
/SP/AgentInfo/PEF/PEFActionGlobalCtrlAlert	= enable | disable (default)
/SP/AgentInfo/PEF/PEFActionGlobalCtrlMail	= enable | disable (default)
/SP/AgentInfo/PEF/PEFActionGlobalCtrlInterrupt	= enable | disable (default)

▼ To Configure the PEF Global Controls

1. **To configure the PEF global controls, you must first enable global control by entering the following commands:**

   –> **`cd /SP/AgentInfo/PEF`**

   /SP/AgentInfo/PEF –> **`set PEFGlobalCtrl=enable`**

   After enabling global control, you can enable global control for specific actions.

2. **To enable global PEF control for a specific action, enter the following commands for each PEFActionGlobalCtrl that you want to enable:**

Note – This example shows how to enable the power reset PEF global action:

–> **`cd /SP/AgentInfo/PEF`**

/SP/AgentInfo/PEF –> **`set PEFActionGlobalCtrlPowerReset=enable`**

Configuring the Event Filter Tables

The event filter table is where you designate the specific altert-triggered actions. You can configure up to six event filter tables. These targets, properties, and values are valid for setting the PEF:

Target	Property
/SP/AgentInfo/PEF/EventFilterTable[*1-6*]/status	enable | disable
/SP/AgentInfo/PEF/EventFilterTable[*1-6*]/sensortype	All, Memory, Processor, Temperature, Voltage, Fan
/SP/AgentInfo/PEF/EventFilterTable[*1-6*]/powercrtl	enable | disable
/SP/AgentInfo/PEF/EventFilterTable[*1-6*]/diagnosticinterrupt	enable | disable
/SP/AgentInfo/PEF/EventFilterTable[*1-6*]/sendalert	enable | disable
/SP/AgentInfo/PEF/EventFilterTable[*1-6*]/sendmail	enable | disable

▼ To Configure the Event Filter Tables

1. **To configure a PEF EventFilterTable target, enter the following commands:**

   –> **cd /SP/AgentInfo/PEF**

   /SP/AgentInfo/PEF –> **show**

   The result of executing the show command appears:

```
/SP/AgentInfo/PEF
    Targets:
        EventFilterTable1
        EventFilterTable2
        EventFilterTable3
        EventFilterTable4
        EventFilterTable5
        EventFilterTable6

    Properties:
        PEFGlobalCtrl = enable
        PEFActionGlobalCtrlPowerOff = enable
        PEFActionGlobalCtrlPowerCycle = enable
        PEFActionGlobalCtrlPowerReset = enable
        PEFActionGlobalCtrlAlert = enable
        PEFActionGlobalCtrlMail = enable
        PEFActionGlobalCtrlInterrupt = enable

    Target Commands:
        show
        cd
        set
```

   By examining the output of the `show` command, you can view the current global control configuration. If necessary use the `cd` and `show` commands to navigate to and examine the individual event filter table targets. You will need to decide which table you are going to configure.

2. **When you have decided which EventFilterTable to configure, enable the table by entering the following commands:**

Note – This example uses EventFilterTable1.

   /SP/AgentInfo/PEF –> **cd EventFilterTable1**

   /SP/AgentInfo/PEF/EventFilterTable1–> **set status=enable**

3. **Display EventFilterTable1 by entering the following command:**

   /SP/AgentInfo/PEF/EventFilterTable1–> **show**

   The result of executing the show command appears:

```
/SP/AgentInfo/PEF/EventFilterTable1
    Targets:

    Properties:
        Status = enable
        SensorType = All
        PowerCtrl = disable
        DiagnosticInterrupt = disable
        SendAlert = disable
        SendMail = disable

    Target Commands:
        show
        set
```

   Next, set the sensor type. There are six values for the sensor type: All, Memory, Processor, Temperature, Voltage, and Fan.

4. **Use the** `set` **command to configure the sensor type.**

   set *sensortype***=***value*

   For example, to set the temperature sensor, enter:

   /SP/AgentInfo/PEF/EventFilterTable1–> **set sensortype=Temperature**

5. **Enable the properties or triggered actions for the sensor.**

6. **Use the** `set` **command to enable (or disable) actions. For example, to set the sendalert and sendmail actions, enter:**

   /SP/AgentInfo/PEF/EventFilterTable1–> **set sendalert=enable**

   /SP/AgentInfo/PEF/EventFilterTable1–> **set sendmail=enable**

7. **When you are finished, use the** `show` **command to verify the PEF configuration:**

   /SP/AgentInfo/PEF/EventFilterTable1–> **`show`**

   The output from the command appears:

```
/SP/AgentInfo/PEF/EventFilterTable1
    Targets:

    Properties:
        Status = enable
        SensorType = temperature
        PowerCtrl = disable
        DiagnosticInterrupt = disable
        SendAlert = enable
        SendMail = enable

    Target Commands:
        show
        set
```

   In the example above, EventFilterTable1 is enabled to activate the SendAlert and SendMail actions, based on temperature related alerts.

Displaying Version Information

You can display active session, current versions, and other information about the SP using the CLI.

To Display the Current SP Version Information

- **To display the current SP version, enter the following command:**

  `version`

Updating the Firmware

You can use CLI to update the SP firmware. Updating the ELOM from the command line enables you to update both the SP firmware and the BIOS at the same time. If you are using the CLI to update the firmware, a TFTPServer is required.

▼ To Update the Firmware

Caution – Power interruptions during the update process could leave the SP in a unbootable or nonrecoverable state. Before upgrading your firmware, ensure that you have reliable power and protect against accidental power interruptions.

Note – The upgrade takes about 5 minutes to complete, depending on network traffic. During this time, no other tasks can be performed in the Embedded Lights Out Manager software.

1. **Copy the combined image from the Tools and Driver CD to your TFTP server.**

   The image is located in the `/remoteflash` directory.

2. **If the server OS is running, perform a clean shutdown.**

3. **Log in to the CLI and change to the `TftpUpdate` directory:**

   `/SP ->`**`cd TftpUpdate`**

Note – A network failure during the file upload will result in a timeout. This causes the SP to reboot with the prior version of the firmware.

4. **Enter the following command to set the IP address of the TFTP server:**

   `/SP/TftpUpdate ->` **`set ServerIP=`***`n.n.n.n`*

   n.n.n.n The server IP address.

5. **Enter the following command to set the file name of the combined `bmc.bios` image:**

   `/SP/TftpUpdate ->`**`set Filename=x4150-10_3A01`**

   a. **To update the firmware, enter one of the following commands:**

- To erase BIOS settings and load optimized defaults (recommended):

  ```
  /SP/TftpUpdate ->set BIOSCMOS=[SaveCMOS|PreservCMOS]
  ```

- To save the BIOS settings:

  ```
  /SP/TftpUpdate ->set SaveFlag=yes
  ```

6. **Start the TFTP download:**

   ```
   /SP/TftpUpdate -> set Update=action
   ```

   After you enter this command, the system displays the current firmware version and the upgrade version and prompts for confirmation.

7. **Select Yes to continue, or No to exit.**

CHAPTER 8

Using Simple Network Management Protocol

This chapter describes how to use Simple Network Management Protocol (SNMP). It includes the following sections:

- "About SNMP" on page 89.
- "SNMP MIB Files" on page 90.
- "MIBs Integration" on page 90.
- "SNMP Messages" on page 91.
- "Configuring SNMP on the ELOM" on page 92.
- "Managing SNMP User Accounts" on page 92.

About SNMP

The Sun server supports the Simple Network Management Protocol (SNMP) interface, versions 1, 2c, and 3. SNMP is an open technology that enables the management of networks and devices, or nodes, connected to the network. SNMP messages are sent over IP using the User Datagram Protocol (UDP). Any management application that supports SNMP can manage your server.

How SNMP Works

Utilizing SNMP requires two components, a network management station and a managed node (in this case, the ELOM). Network management stations host management applications, which monitor and control managed nodes.

Managed nodes are any number of devices, including servers, routers, and hubs, that host SNMP management agents responsible for carrying out the requests from management stations. The management station monitors nodes by polling management agents for the appropriate information using queries. Managed nodes can also provide unsolicited status information to a management station in the form of a trap. SNMP is the protocol used to communicate management information between the management stations and agents.

The SNMP agent is preinstalled and runs on the ELOM, so all SNMP management of the server should occur through the ELOM. To utilize this feature, your operating system must have an SNMP client application. See your operating system vendor for more information. The SNMP agent on your ELOM provides inventory management and sensor and system state monitoring capabilities.

SNMP MIB Files

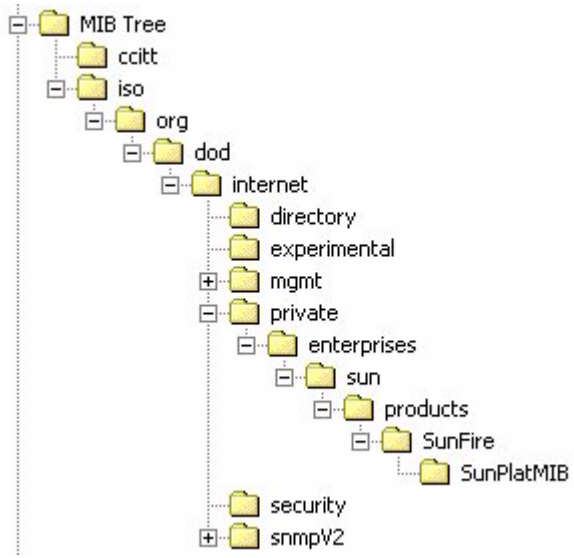
The base component of an SNMP solution is the management information base (MIB). MIB is a text file that describes a managed node's available information and where it is stored. When a management station requests information from a managed node, the agent receives the request and retrieves the appropriate information from the MIBs. The Sun server supports the following MIB files. Download and install the MIB files from the Tools and Drivers CD. The files are located in the `/SNMP/mib` directory.

- The system group and SNMP group from RFC1213 MIB
- SNMP-FRAMEWORK-MIB
- SNMP-USER-BASED-MIB
- SNMP-MPD-MIB
- SUN-PLATFORM-MIB
- ENTITY-MIB

MIBs Integration

Use the MIBs to integrate the management and monitoring of the server into SNMP management consoles. The MIB branch is a private enterprise MIB, located at MIB object iso(1).org (3). dod (6) .internet (1) .private (4) .enterprises (1) .sun (42) .products (2). See FIGURE 8-1. The standard SNMP port, 161, is used by the SNMP agent on the ELOM.

FIGURE 8-1 Sun Server MIB Tree



SNMP Messages

SNMP is a protocol, not an operating system, so you need some type of application to use SNMP messages. Your SNMP management software might provide this functionality, or you can use an open-source tool like net-SNMP, which is available at

http://net-snmp.sourceforge.net/

Both management stations and agents use SNMP messages to communicate. Management stations can send and receive information. Agents can respond to requests and send unsolicited messages in the form of a trap. There are five functions that management stations and agent, use:

- Get
- GetNext
- GetResponse
- Set
- Trap

By default, port 161 is used for SNMP messages, and port 162 is used to listen for SNMP traps.

Configuring SNMP on the ELOM

The ELOM has a preinstalled SNMP agent that supports trap delivery to an SNMP management application.

To use this feature, you must integrate the platform-specific MIBs into your SNMP environment, tell your management station about your server, then configure the specific traps.

Adding Your Server to Your SNMP Environment

Add your Sun server as a managed node using your SNMP management application. See your SNMP management application documentation for further details.

Configuring Receipt of SNMP Traps

Configure a trap in your ELOM. See "Managing Alerts" on page 78, or "Configuring E-mail Notification" on page 30.

Managing SNMP User Accounts

You can add, delete, or configure SNMP user accounts from the CLI. By default, SNMP v3 is enabled, and SNMP v1 and v2c are disabled.

Adding a User Account

To add an SNMP v3 read-only user account, enter the following command:

`create /SP/AgentInfo/SNMP/user/`*`username`* **`authenticationpassword=`** *`password`*

To add an SNMP v1/v2c user account, enter the following command:

`create /SP/AgentInfo/SNMP/communities/`*`communityname`*

Deleting a User Account

To delete an SNMP v3 user account, enter the following command:

delete /SP/AgentInfo/SNMP/user/*username*

To delete an SNMP v1/v2c user account, enter the following command :

delete /SP/AgentInfo/SNMP/communities/*communityname*

Configuring User Accounts

To configure SNMP user accounts, use the `set` command

Syntax

set target *[propertyname=value]*

Targets, Properties, and Values

These targets, properties, and values are valid for SNMP user accounts.

TABLE 8-1 SNMP Targets, Properties, and Values

Target	Property	Value	Default
/**SP/AgentInfo/SNMP**/communities/*communityname*	Permission	ro | rw	ro
/**SP/AgentInfo/SNMP**/users/*username*	AuthProtocol	MD5 | SHA	MD5
	AuthPassword	*string*	(Null string)
	Permission	ro | rw	ro
	PrivacyProtocol	None | DES	None*
	PrivacyPassword	*string*	(Null string)

* If the PrivacyProtocol property has a value other than none, then PrivacyPassword must be set.

Examples

```
-> set /SP/AgentInfo/SNMP/users/al privacyprotocol=DES
```

Tip – To reduce the length of commands, navigate to the target first using the `cd` command.

```
-> cd /SP/AgentInfo/SNMP/users/albert

-> set PrivacyProtocol=DES

-> set PrivacyPassword=password AuthProtocol=SHA AuthPassword=
password
```

Note – You can change SNMP user permissions without resetting the privacy and authentication properties.

To show an SNMP user's properties, Enter this command:

```
-> show
```

The result appears as follows:

```
/SP/AgentInfo/SNMP/users/sicilian
     Targets:
Properties:
          Permission = ro
          AuthProtocol = MD5
          AuthPassword = (Cannot show property)
          PrivacyProtocol = none
          PrivacyPassword = (Cannot show property)

     Target Commands:
          show
          set

/SP/AgentInfo/SNMP/users/sicilian ->
```

APPENDIX **A**

Command-Line Interface Reference

This chapter contains the most common Embedded Lights Out Manager commands used to administer your Sun server from the command-line interface (CLI). This chapter contains the following sections:

- "CLI Command Quick Reference" on page 95.
- "CLI Command Reference" on page 99.

CLI Command Quick Reference

The following tables provide a quick reference to the most common ELOM CLI commands.

TABLE A-1 Command Syntax and Usage

Content	Typeface	Description
Your input	**`Fixed-width bold`**	Text that you type into the computer. Type it in exactly as shown.
Onscreen output	`Fixed-width regular`	Text that the computer displays.
Variable	*Italic*	Replace these with a name or value you choose.
Square brackets, [ ]		Text in square brackets is optional.
Vertical bars, |		Text separated by a vertical bar represents the only available values. Select one.

TABLE A-2 General Commands

Description	Command
Log out of the CLI.	`exit`
Display the version of the ELOM firmware running on the SP.	`version`
Display information about commands and targets.	`help`
Display information about a specific command.	`help show`

TABLE A-3 User Commands

Description	Command
Add a local user.	**`create /SP/users/`***user1*
Set or change password.	**`set /SP/users/`***username* **`Password=`***password*
Set or change permission.	**`set /SP/users/`***username* **`Permission= [operator|administrator|user|callback]`**
Delete a local user named user1.	**`delete /SP/users/user1`**
Change the permission level of a local user named user1.	**`set /SP/users/user1 Permission=operator`**

TABLE A-4 Network and Serial Port Setting Commands

Description	Command
Display network configuration information.	**`show /SP/network`**
Change network properties for the ELOM. Changing certain network properties, like the IP address, will disconnect your active session.	**`set /SP/network`** **`IPAddress`**=*xxx.xxx.xxx.xxx* **`NetMask=`***xxx.xxx.xxx.xxx* **`Gateway=`***xxx.xxx.xxx.xxx*
Set DHCP or change to static settings.	**`set /SP/network IPSource= [dhcp|static]`**

TABLE A-5 Alert Commands

Description	Command
Display information about PET alerts Destination1.	**show /SP/AgentInfo/PET/Destination1**
Change alert configuration.	**set /SP/AgentInfo/PET/Destination[n] IPAddress=** *ipaddress*

TABLE A-6 SNMP Commands

Description	Command
Display information about SNMP settings. By default, the SNMP port is 161, and v3 is enabled.	**show /SP/AgentInfo/SNMP port=**snmpportnumber **set=** enabled|disabled **version1**=enabled|disabled **version2c=**enabled|disabled **version3**=enabled|disabled
Display SNMP users.	**show /SP/AgentInfo/SNMP/user**
Add an SNMP user.	**create /SP/AgentInfo/SNMP/user/***snmpusername* **AuthPassword=***password* **AuthProtocol=**MD5|SHA **Permission=**rw|ro **PrivacyPassword=***password* **PrivacyProtocol=**none|DES
Delete an SNMP user.	**delete /SP/AgentInfo/SNMP/user/***snmpusername*
Display information about SNMP public (read-only) communities.	**show /SP/AgentInfo/SNMP/communities/public**

TABLE A-7 System Start, Stop, and Reset Commands

Description	Command
Start the host system.	**set /SYS/CtrlInfo PowerCtrl=on**
Stop the host system	**set /SYS/CtrlInfo PowerCtrl=off**
Stop the host system gracefully.	**set /SYS/CtrlInfo PowerCtrl=gracefuloff**

TABLE A-7 System Start, Stop, and Reset Commands *(Continued)*

Description	Command
Reset the host system.	**set /SYS/CtrlInfo PowerCtrl=reset**
Start a session to connect to the host console.	**start /SP/AgentInfo/Console**
Stop the session connected to the host console.	**stop /SP/AgentInfo/Console**

CLI Command Reference

This section provides reference information about the CLI commands.

cd

Use the `cd` command to navigate the namespace. When you use `cd` to change to a target location, that location then becomes the default target for all other commands.

Using the - `default` option with no target returns you to the top of the namespace. Typing just `cd` displays your current location in the namespace. Typing `help targets` displays a list of all targets in the entire namespace.

Syntax

`cd` *target*

Options

`[-h|help]`

Targets and Properties

Any location in the namespace.

Examples

To create a user named sally, use `cd` to change to `/SP/User`, then execute the `create` command with `/SP/User` as the default target.

```
SP-> cd /SP/User

SP-> create sally
```

create

Use the `create` command to set up an object in the namespace. Unless you specify properties with the `create` command, they are empty.

Syntax

`create [`*`options`***`] target [`***`propertyname=value`***`]`**

Options

`[-h|help]`

Targets, Properties, and Values

TABLE A-8 Create command Targets, Properties, Values, and Defaults

Valid Targets	Properties	Values	Default
`/SP/User/`*`username`*	password	*string*	(None)
	permission	administrator | operator | user | callback	operator
`/SP/SNMP/communities/` *communityname*	Permissions	ro | rw	ro
`/SP/SNMP/communities/user/` *username*	AuthProtocol	MD5	MD5
	AuthPassword	*string*	(Null string)
	Permissions	ro | rw	ro
	PrivacyProtocol	none | DES	DES
	PrivacyPassword	*string*	(Null string)

Example

```
-> create /SP/User/susan role=administrator
```

delete

Use the `delete` command to remove an object from the namespace. You are not prompted to confirm a `delete` command.

Eliminate this prompt by using the `-script` option.

Syntax

`delete [`*options***`]`** *target*

Options

`[-h|help]`

Targets

TABLE A-9 `delete` Command Targets

Valid Targets
`/SP/User/`*username*
`/SP/SNMP/communities/`*communityname*
`/SP/SNMP/communities/user/`*username*

Examples

```
-> delete /SP/User/susan
-> delete /SP/SNMP/communities/johnny
```

exit

Use the `exit` command to terminate a session to the CLI.

Syntax

`exit [`*options***`]`**

Options

[-h|help]

help

Use the `help` command to display Help information about commands and targets. Using the `-output terse` option displays usage information only. The **-**`output verbose` option displays usage, description, and additional information including examples of command usage. If you do not use the `-output` option, usage information and a brief description of the command are displayed.

Specifying `command` *targets* displays a complete list of valid targets for that command from the fixed targets in `/SP`. Fixed targets are targets that cannot be created by a user.

Specifying `command` *targets* `legal` displays copyright information and product use rights.

Syntax

help [*options***] command [***targets* **]**

Options

[-h|help]

Commands

cd, create, delete, exit, help, load, reset, set, show, start, stop, version

Examples

-> **help load**

Use the `load` command to transfer a file from a server and update a target.

Usage: **load -source** *URL* **[***target***]**

`-source`: specific the location to get a file

```
-> help reset
```

Use the `reset` command to reset a target.

Usage: `reset` **[-***script***]** **[***target***]**

Available options for this command:

`-script` : do not prompt for yes/no confirmation, and act as if yes was specified.

set

Use the `set` command to change the value of a property associated with a target.

Syntax

set [target] property=value [*propertyname***=***value***]**

Options

[-h help]

Targets, Properties, and Values

TABLE A-10 `set` Command Targets, Properties, and Values

Valid Targets	Properties	Values	Default
/SP/User/*username*	password	*string*	(None)
	permission	administrator | operator	operator
/SP/clock	Date	MM/DD/CCYY	/SP/clock
	Time	hh/mm/ss	
	NTPstatus	enabled | disabled	
	NTPserver	i*paddress*	
/SP/AgentInfo/SNMP	port	*decimal*	161
	snmpset	enabled | disabled	disabled
	version1	enabled | disabled	disabled
	version2	enabled | disabled	disabled
	version3	enabled | disabled	enabled

TABLE A-10 `set` Command Targets, Properties, and Values *(Continued)*

Valid Targets	Properties	Values	Default
/SP/AgentInfo/SNMP community/*communityname*	Permission	ro | rw	ro
/SP/AgentInfo/SNMP/user */username*	AuthProtocol	MD5 | SHA	MD5
	AuthPassword	*string*	(Null string)
	Permission	ro | rw	ro
	PrivacyProtocol	none | DES	DES
	PrivacyPassword	*string*	(null string)
/SP/network	IIPaddress	*IP address* | *none*	(None)
	DNS	*IP address* | *none*	(None)
	IPSource	*dhcp* | *static*	dhcp
	Gateway	*IP address* | *none*	(None)
	Netmask	*IP dotted decimal*	xxx.xxx.xxx.xxx

Examples

```
-> set /SP/users/susan permission=administrator
```

show

Use the `show` command to display information about targets and properties.

The show command is used to display information about managed elements. It can be used to view information about single managed elements, a tree of managed elements, or managed elements matching a property value filter.

The **-**`level` option controls the depth of the `show` command, and it applies to all modes of the **-**`display` option. Specifying **-**`level 1` displays the level of the namespace where the object exists. Values greater than 1 return information for the target's current level in the namespace and the *specified value* levels below. If the argument is `-level all`, it applies to the current level in the namespace and everything below.

Syntax

show [options] target[*propertyname***]**

Options

[-h|help]

Targets and Properties

Examples

->**show /SP/network** (This is the only valid command as it displays all parameters)

```
 /SP/network

Targets:
    Target Commands:
        show
        set
```

start

Use the `start` command to turn on the target or to initiate a connection to the host console.

Syntax

start [options] target

Options

[-h|help]

Targets

TABLE A-11 `start` Command Target

Valid Target	Description
/SP/AgentInfo/Console	Starts an interactive session to the console stream.

Examples

```
-> start /SP/AgentInfo/Console
```

stop

Use the `stop` command to shut down the target or to terminate another user's connection to the host console. You will be prompted to confirm a `stop` command. Eliminate this prompt by using the `-script` option.

Syntax

```
stop [options] target
```

Options

```
[-h|help] [-s|script]
```

Targets

TABLE A-12 `stop` Command Target

Valid Target	Description
`/SP/AgentInfo/Console`	Terminate another user's connection to the host console.

Examples

```
-> stop /SP/AgentInfo/Console
```

reset

Use the `reset` command to reset the target's state. This command can be used with and without options.

Syntax

reset [*target***]**

Options

[-h|help]

Example

-> **reset /system3**

version

Use the `version` command to display ELOM version information.

Syntax

version

Options

[-x|examine] [-h|help]

Example

-> **version**

```
version SP firmware version: 1.0.0
SP firmware build number: 4415
SP firmware date: Mon Mar 28 10:39:46 EST 2005
SP filesystem version: 0.1.9
```

Glossary

The following terms are used within the Sun server documentation.

A

access control list (ACL) A software authorization mechanism that enables you to control which users have access to a server. Users can define ACL rules that are specific to a particular file or directory, granting or denying access to one or more users or groups.

address In networking, a unique code that identifies a node in the network. Names such as “host1.sun.com” are translated to dotted-quad addresses like “168.124.3.4” by the domain name service (DNS).

address resolution A means for mapping Internet addresses into physical media access control (MAC) addresses or domain addresses.

Address Resolution Protocol (ARP) A protocol used to associate an Internet Protocol (IP) address with a network hardware address (MAC address).

Administrator The person with full access (root) privileges to the managed host system.

Advanced Configuration and Power Interface (ACPI) An open-industry specification that provides power management capabilities to a system that enables the operating system to determine when peripheral devices are idle and to utilize ACPI-defined mechanisms for putting the devices into low power modes. The ACPI specification also describes a large number of power states for CPUs, devices, and systems as a whole. One feature of the ACPI enables the OS to modify the voltage and frequency of a

CPU in response to system load, thus enabling the system's main power-consuming element (the CPU) to vary its power consumption based on system load.

Advanced Programmable Interrupt Controller (APIC) A device that manages interrupt requests for multiple central processing units (CPUs). The APIC decides which request has the highest priority and sends an interrupt to the processor for that request.

Advanced Technology Attachment (ATA) A specification that describes the physical, transport, electrical, and command protocols used to attach storage devices to host systems.

Advanced Technology Attachment Packet Interface (ATAPI) An extension to the Advanced Technology Attachment (ATA) standard for connecting removable media storage devices in host systems, including CD/DVD drives, tape drives, and high-capacity diskette drives. Also called "ATA-2" or "ATA/ATAPI."

agent A software process, usually corresponding to a particular local managed host, that carries out manager requests and makes local system and application information available to remote users.

alert A message or log generated by the collection and analysis of error events. An alert indicates that there is a need to perform some hardware or software corrective action.

Alert Standard Format (ASF) A preboot or out-of-band platform management specification that enables a device, such as an intelligent Ethernet controller, to autonomously scan ASF-compliant sensors on the motherboard for voltage, temperature, or other excursions and to send Remote Management and Control Protocol (RMCP) alerts according to the platform event trap (PET) specification. ASF was intended primarily for out-of-band management functions for client desktops. ASF is defined by the Distributed Management Task Force (DMTF).

authentication The process that verifies the identity of a user in a communication session, or a device or other entity in a computer system, before that user, device, or other entity can access system resources. Session authentication can work in two directions. A server authenticates a client to make access control decisions. The client can authenticate the server as well. With Secure Sockets Layer (SSL), the client always authenticates the server.

authorization The process of granting specific access privileges to a user. Authorization is based on authentication and access control.

AutoYaST An installation program for SUSE Linux that automates the process of configuring one or more servers.

B

bandwidth A measure of the volume of information that can be transmitted over a communication link. Often used to describe the number of bits per second a network can deliver.

baud rate The rate at which information is transmitted between devices, for example, between a terminal and a server.

bind In the Lightweight Directory Access Protocol (LDAP), refers to the authentication process that LDAP requires when users access the LDAP directory. Authentication occurs when the LDAP client binds to the LDAP server.

BIOS (Basic Input/Output System) System software that controls the loading of the operating system and testing of hardware at system power-on. BIOS is stored in read-only memory (ROM).

bits per second (bps) The unit of measurement for data transmission speed.

boot loader A program contained in read-only memory (ROM) that automatically runs at system power-on to control the first stage of system initialization and hardware tests. The boot loader then transfers control to a more complex program that loads the operating system.

C

cache A copy of original data that is stored locally, often with instructions or the most frequently accessed information. Cached data does not have to be retrieved from a remote server again when requested. A cache increases effective memory transfer rates and processor speed.

certificate Public key data assigned by a trusted Certificate Authority (CA) to provide verification of an entity's identity. This is a digitally signed document. Both clients and servers can have certificates. Also called a "public key certificate."

Certificate Authority (CA) A trusted organization that issues public key certificates and provides identification to the owner of the certificate. A public key Certificate Authority issues certificates that state a relationship between an entity named in the certificate and a public key that belongs to that entity, which is also present in the certificate.

client In the client-server model, a system or software on a network that remotely accesses resources of a server on a network.

command-line interface (CLI) A text-based interface that enables users to type executable instructions at a command prompt.

Common Information Model (CIM) An open systems information model published by the Distributed Management Task Force (DMTF) that enables a common application to manage disparate resources, such as printers, disk drives, or CPUs.

console A terminal or dedicated window on a screen where system messages are displayed. The console window enables you to configure, monitor, maintain, and troubleshoot many server software components.

Coordinated Universal Time (UTC) The international standard for time. UTC was formerly called Greenwich Meridian Time (GMT). UTC is used by Network Time Protocol (NTP) servers to synchronize systems and devices on a network.

core file A file created by the Solaris or Linux operating system when a program malfunctions and terminates. The core file holds a snapshot of memory, taken at the time the fault occurred. Also called a "crash dump file."

critical event A system event that seriously impairs service and requires immediate attention.

custom JumpStart™ A type of installation in which the Solaris software is automatically installed on a system that is based on a user-defined profile.

customer-replaceable unit (CRU) A system component that the user can replace without special training or tools.

D

Data Encryption Standard (DES) A common algorithm for encrypting and decrypting data.

Desktop Management Interface (DMI) A specification that sets standards for accessing technical support information about computer hardware and software. DMI is hardware and operating system (OS) independent, and can manage workstations, servers, or other computing systems. DMI is defined by the Distributed Management Task Force (DMTF).

digital signature A certification of the source of digital data. A digital signature is a number derived from a public key cryptographic process. If the data is modified after the signature was created, the signature becomes invalid. For this reason, a digital signature can ensure data integrity and detection of data modification.

Digital Signature Algorithm (DSA) A cryptographic algorithm specified by the Digital Signature Standard (DSS). DSA is a standard algorithm used to create digital signatures.

direct memory access (DMA) The transfer of data directly into memory without supervision of the processor.

directory server In the Lightweight Directory Access Protocol (LDAP), a server that stores and provides information about people and resources within an organization from a logically centralized location.

disk array A storage subsystem containing an arrangement of multiple disk drives, designed to provide performance, high availability, serviceability, and other benefits.

disk partition A logical section of a physical hard disk drive reserved for a specific file system and function.

Distinguished Name (DN) In the Lightweight Directory Access Protocol (LDAP), a unique text string that identifies an entry's name and location within the directory. A DN can be a fully qualified domain name (FQDN) that includes the complete path from the root of the tree.

Distributed Management Task Force (DMTF) A consortium of over 200 companies that authors and promotes standards for the purpose of furthering the ability to remotely manage computer systems. Specifications from the DTMF include the Desktop Management Interface (DMI), the Common Information Model (CIM), and the Alert Standard Format (ASF).

domain A grouping of hosts that is identified by a name. The hosts usually belong to the same Internet Protocol (IP) network address. The domain also refers to the last part of a fully qualified domain name (FQDN) that identifies the company or organization that owns the domain. For example, "sun.com" identifies Sun Microsystems as the owner of the domain in the FQDN "docs.sun.com."

domain name The unique name assigned to a system or group of systems on the Internet. The host names of all the systems in the group have the same domain name suffix, such as "sun.com." Domain names are interpreted from right to left. For example, "sun.com" is both the domain name of Sun Microsystems, and a subdomain of the top-level ".com" domain.

domain name server (DNS) The server that typically manages host names in a domain. DNS servers translate host names, such as "www.example.com," into Internet Protocol (IP) addresses, such as "030.120.000.168."

domain name service (DNS) The data query service that searches domains until a specified host name is found.

Domain Name System (DNS) A distributed name resolution system that enables computers to locate other computers on a network or the Internet by domain name. The system associates standard Internet Protocol (IP) addresses, such as "00.120.000.168," with host names, such as "www.sun.com." Machines typically get this information from a DNS server.

dual inline memory module (DIMM) A circuit board that holds double the amount of surface-mount memory chips that a single inline memory module (SIMM) holds. A DIMM has signal and power pins on both sides of the board, whereas a SIMM has pins on only one side of the board. A DIMM has a 168-pin connector and supports 64-bit data transfer.

Dynamic Host Configuration Protocol (DHCP) A protocol that enables a DHCP server to assign Internet Protocol (IP) addresses dynamically to systems on a Transmission Control Protocol/Internet Protocol (TCP/IP) network.

dynamic random access memory (DRAM) A type of random access memory (RAM) that stores information in integrated circuits that contain capacitors. Because capacitors lose their charge over time, DRAM must be periodically recharged.

E

electrically erasable programmable read-only memory (EEPROM) A type of nonvolatile programmable read-only memory (PROM) that can be erased by being exposed to an electrical charge.

electrostatic discharge (ESD) The sudden dissipation of static electrical charge. ESD can easily destroy semiconductor components.

Embedded Lights Out Manager (ELOM) A dedicated system of hardware and supporting software that enables you to manage your Sun server using several interfaces, independent of the operating system, and under various power conditions.

enhanced parallel port (EPP) A hardware and software standard that enables systems to transmit data at twice the speed of standard parallel ports.

erasable programmable read-only memory (EPROM) A nonvolatile programmable read-only memory (PROM) that can be written to as well as read from.

Ethernet An industry-standard type of local area network (LAN) that enables real-time communication between systems connected directly through cables. Ethernet uses a Carrier Sense Multiple Access/Collision Detection (CSMA/CD) algorithm as its access method, wherein all nodes listen for, and any node can begin transmitting, data. If multiple nodes attempt to transmit at the same time (a collision), the transmitting nodes wait for a random amount of time before attempting to transmit again.

event A change in the state of a managed object. The event-handling subsystem can provide a notification to which a software system must respond when it occurs, but which the software did not solicit or control.

externally initiated reset (XIR) A signal that sends a "soft" reset to the processor in a domain. XIR does not reboot the domain. An XIR is generally used to escape from a hung system to reach the console prompt. You then can generate a core dump file, which can be useful in diagnosing the cause of the hung system.

F

failover The automatic transfer of a computer service from one system, or more often a subsystem, to another to provide redundant capability.

Fast Ethernet Ethernet technology that transfers data up to 100 Mbit/sec. Fast Ethernet is backward compatible with 10 Mbit/sec. Ethernet installations.

fdisk partition A logical partition of a physical disk drive that is dedicated to a particular operating system on an x86-based system.

Fibre Channel (FC) A connector that provides high bandwidth, increased distance, and additional connectivity from hosts to peripherals.

Fibre Channel-Arbitrated Loop (FCAL) A 100 Mbit/sec. loop topology used with Fibre Channel that enables connection of multiple devices such as disk drives and controllers. An arbitrated loop connects two or more ports, but enables only two ports to communicate at a given time.

field-replaceable unit (FRU) A system component that is replaceable at the customer site.

file system A consistent method by which information is organized and stored on physical media. Different operating systems typically have different file systems. File systems are often a tree-structured network of files and directories, with a root directory at the top and parent and child directories below the root.

File Transfer Protocol (FTP) A basic Internet protocol based on Transmission Control Protocol/Internet Protocol (TCP/IP) that enables the retrieving and storing of files between systems on the Internet without regard to the operating systems or architectures of the systems involved in the file transfer.

firewall A network configuration, usually both hardware and software, that protects networked computers within an organization from outside access. A firewall can monitor or prohibit connections to and from specified services or hosts.

firmware Software that is typically used to help with the initial booting stage of a system and with system management. Firmware is embedded in read-only memory (ROM) or programmable ROM (PROM).

flash PROM Programmable read-only memory (PROM) that can be reprogrammed while installed within the system, from software on a disc, by a voltage pulse, or flash of light.

fully qualified domain name (FQDN) The complete and unique Internet name of a system, such as "www.sun.com." The FQDN includes a host server name (www) and its top-level (.com) and second-level (.sun) domain names. A FQDN can be mapped to a system's Internet Protocol (IP) address.

G

gateway A computer or program that interconnects two networks and then passes data packets between the networks. A gateway has more than one network interface.

Gigabit Ethernet Ethernet technology that transfers data up to 1000 Mbit/sec.

Grand Unified Bootloader (GRUB) A boot loader that can install two or more operating systems (OS) onto a single system and that can manage which OS to boot at power-on.

graphical user interface (GUI) An interface that uses graphics, along with keyboard and mouse, to provide easy-to-use access to an application.

H

heatsink A structure, attached to or part of a semiconductor device, that can dissipate heat to the surrounding environment.

host A system, such as a back-end server, with an assigned Internet Protocol (IP) address and host name. The host is accessed by other remote systems on the network.

host ID Part of the 32-bit Internet Protocol (IP) address used to identify a host on a network.

host name The name of a particular machine within a domain. Host names always map to a specific Internet Protocol (IP) address.

hot plug Describes a component that is safe to remove or add while the system is running. Typically, the system must be rebooted before the hot-pluggable component is configured into the system.

hot swap Describes a component that you can install or remove by simply pulling the component out and putting a new component into a running system. The system either automatically recognizes the component change and configures it, or requires user interaction to configure the system. However, in neither case is a reboot required. All hot-swappable components are hot-pluggable components, but not all hot-pluggable components are hot-swappable components.

Hypertext Transfer Protocol (HTTP) The Internet protocol that retrieves hypertext objects from remote hosts. HTTP messages consist of requests from client to server and responses from server to client. HTTP is based on Transmission Control Protocol/Internet Protocol (TCP/IP).

Hypertext Transfer Protocol Secure (HTTPS) An extension of HTTP that uses Secure Sockets Layer (SSL) to enable secure transmissions over a Transmission Control Protocol/Internet Protocol (TCP/IP) network.

I

in-band system management Server management capability that is enabled only when the operating system is initialized and the server is functioning properly.

install server A server that provides the Solaris software DVD or CD images from which other systems on a network can install the Solaris software.

Intelligent Platform Management Interface (IPMI) A hardware-level interface specification that was designed primarily for out-of-band management of server systems over a number of different physical interconnects. The IPMI specification describes extensive abstractions regarding sensors, enabling a management application running on the operating system (OS) or in a remote system to comprehend the environmental makeup of the system and to register with the system's IPMI subsystem to receive events. IPMI is compatible with management software from heterogeneous vendors. IPMI functionality includes FRU inventory reporting, system monitoring, logging, system recovery (including local and remote system resets and power on and off capabilities), and alerting.

Internet Control Message Protocol (ICMP) An extension to the Internet Protocol (IP) that provides for routing, reliability, flow control, and sequencing of data. ICMP specifies error and control messages used with the IP.

Internet Protocol (IP) The basic network layer protocol of the Internet. IP enables the unreliable delivery of individual packets from one host to another. IP does not guarantee that the packet will be delivered, or how long it will take, or if multiple packets will be delivered in the order they were sent. Protocols layered on top of IP add connection reliability.

Internet Protocol (IP) address In Transmission Control Protocol/Internet Protocol (TCP/IP), a unique 32-bit number that identifies each host or other hardware system on a network. The IP address is a set of numbers separated by dots, such as "192.168.255.256," that specifies that actual location of a machine on an intranet or the Internet.

interrupt request (IRQ) A signal that a device requires attention from the processor.

IPMItool A utility used to manage IPMI-enabled devices. IPMItool can manage IPMI functions of either the local system or a remote system. Functions include managing field-replaceable unit (FRU) information, local area network (LAN) configurations, sensor readings, and remote system power control.

J

Java Web Start application A web application starter. With Java Web Start, you start applications by clicking the web link. If the application is not present on your system, Java Web Start downloads it and caches it onto your system. Once an application is downloaded to its cache, it can be started from a desktop icon or web browser link. The most current version of the application is always presented.

JumpStart installation A type of installation in which the Solaris software is automatically installed on a system by using the factory-installed JumpStart software.

K

kernel The core of the operating system (OS) that manages the hardware and provides fundamental services, such as filing and resource allocation, that the hardware does not provide.

Keyboard Controller Style (KCS) interface A type of interface implemented in legacy personal computer (PC) keyboard controllers. Data is transferred across the KCS interface using a per-byte handshake.

keyboard, video, mouse, storage (KVMS) A series of interfaces that enables a system to respond to keyboard, video, mouse, and storage events.

L

lights out management (LOM) Technology that provides the capability for out-of-band communication with the server even if the operating system is not running. This enables the system administrator to switch the server on and off; view system temperatures, fan speeds, and so forth; and restart the system from a remote location.

Lightweight Directory Access Protocol (LDAP) A directory service protocol used for the storage, retrieval, and distribution of information, including user profiles, distribution lists, and configuration data. LDAP runs over Transmission Control Protocol/Internet Protocol (TCP/IP) and across multiple platforms.

Lightweight Directory Access Protocol (LDAP) server A software server that maintains an LDAP directory and service queries to the directory. The Sun Directory Services and the Netscape Directory Services are implementations of an LDAP server.

Linux Loader (LILO) A boot loader for Linux.

local area network (LAN) A group of systems in close proximity that can communicate via connecting hardware and software. Ethernet is the most widely used LAN technology.

local host The processor or system on which a software application is running.

M

major event A system event that occurred that impairs service, but not seriously.

management information base (MIB) A tree-like, hierarchical system for classifying information about resources in a network. The MIB defines the variables that the master Simple Network Management Protocol (SNMP) agent can access. The MIB provides access to the server's network configuration, status, and statistics. Using SNMP, you can view this information from a network management station (NMS). By industry agreement, individual developers are assigned portions of the tree structure to which they may attach descriptions that are specific to their own devices.

man pages Online UNIX documentation.

media access control (MAC) address Worldwide unique, 48-bit, hardware address number that is programmed into each local area network interface card (NIC) at the time of manufacture.

Message Digest 5 (MD5) A secure hashing function that converts an arbitrarily long data string into a short digest of data that is unique and of fixed size.

minor event A system event that occurred that does not currently impair service, but which needs correction before it becomes more severe.

N

namespace In the tree structure of a Lightweight Directory Access Protocol (LDAP) directory, a set of unique names from which an object name is derived and understood. For example, files are named within the file namespace, and printers are named within the printer namespace.

network file system (NFS) A protocol that enables disparate hardware configurations to function together transparently.

Network Information Service (NIS) A system of programs and data files that UNIX systems use to collect, collate, and share specific information about machines, users, file systems, and network parameters throughout a network of computer systems.

network interface card (NIC) An internal circuit board or card that connects a workstation or server to a networked device.

network management station (NMS) A powerful workstation with one or more network management applications installed. The NMS is used to remotely manage a network.

network mask A number used by software to separate the local subnet address from the rest of a given Internet Protocol (IP) address.

Network Time Protocol (NTP) An Internet standard for Transmission Control Protocol/Internet Protocol (TCP/IP) networks. NTP synchronizes the clock times of networked devices with NTP servers to the millisecond using Coordinated Universal Time (UTC).

node An addressable point or device on a network. A node can connect a computing system, a terminal, or various peripheral devices to the network.

nonmaskable interrupt (NMI) A system interrupt that is not invalidated by another interrupt.

nonvolatile memory A type of memory that ensures that data is not lost when system power is off.

nonvolatile random access memory (NVRAM) A type of random access memory (RAM) that retains information when system power is off.

O

object identifier (OID) A number that identifies an object's position in a global object registration tree. Each node of the tree is assigned a number, so that an OID is a sequence of numbers. In Internet usage the OID numbers are delimited by dots, for example, "0.128.45.12." In the Lightweight Directory Access Protocol (LDAP), OIDs are used to uniquely identify schema elements, including object classes and attribute types.

OpenBoot™ PROM A layer of software that takes control of an initialized system after the power-on self-test (POST) successfully tests components. OpenBoot PROM builds data structures in memory and boots the operating system.

OpenIPMI An operating system-independent, event-driven library for simplifying access to the Intelligent Platform Management Interface (IPMI).

operator A user with limited privileges to the managed host system.

out-of-band (OOB) system management Server management capability that is enabled when the operating system network drivers or the server is not functioning properly.

P

parity A method used by a computer for checking that data received matches data sent. Also refers to information stored with data on a disk that enables the controller to rebuild data after a drive failure.

partition A physical section on a hard disk drive.

Peripheral Component Interconnect (PCI) A local bus standard used to connect peripherals to 32-bit or 64-bit systems.

Peripheral Interface Controller (PIC) An integrated circuit that controls peripherals in an interrupt request (IRQ)–driven system, taking away that load from the central processing unit (CPU).

permissions A set of privileges granted or denied to a user or group that specify read, write, or execution access to a file or directory. For access control, permissions state whether access to the directory information is granted or denied, and the level of access that is granted or denied.

physical address An actual hardware address that matches a memory location. Programs that refer to virtual addresses are subsequently mapped to physical addresses.

Platform Event Filter (PEF) A mechanism that configures the service processor to take selected actions when it receives event messages, for example, powering off or resetting the system or triggering an alert.

Platform Event Trap (PET) A configured alert triggered by a hardware or firmware (BIOS) event. A PET is an Intelligent Platform Management Interface (IPMI)–specific, Simple Network Management Protocol (SNMP) trap, which operates independently of the operating system.

port The location (socket) to which Transmission Control Protocol/Internet Protocol (TCP/IP) connections are made. Web servers traditionally use port 80, the File Transfer Protocol (FTP) uses port 21, and Telnet uses port 23. A port enables a client program to specify a particular server program in a computer on a network. When a server program is started initially, it binds to its designated port number. Any client that wants to use that server must send a request to bind to the designated port number.

port number A number that specifies an individual Transmission Control Protocol/Internet Protocol (TCP/IP) application on a host machine, providing a destination for transmitted data.

power cycling The process of turning the power to a system off then on again.

power-on self-test (POST) A program that takes uninitialized system hardware and probes and tests its components at system startup. POST configures useful components into a coherent, initialized system and hands it over to the OpenBoot PROM. POST passes to OpenBoot PROM a list of only those components that have been successfully tested.

PowerPC An embedded processor.

Preboot Execution Environment (PXE) An industry-standard client-server interface that enables a server to boot an operating system (OS) over a Transmission Control Protocol/Internet Protocol (TCP/IP) network using Dynamic Host Configuration Protocol (DHCP). The PXE specification describes how the network adapter card and BIOS work together to provide basic networking capabilities for the primary bootstrap program, enabling it to perform a secondary bootstrap over the network, such as a TFTP load of an OS image. Thus, the primary bootstrap program, if coded to PXE standards, does not need knowledge of the system's networking hardware.

Privacy Enhanced Mail (PEM) A standard for Internet electronic mail that encrypts data to ensure privacy and data integrity.

programmable read-only memory (PROM) A memory chip on which data can be programmed only once and which retains the program forever. PROMs retain data even when power is off.

protocol A set of rules that describes how systems or devices on a network exchange information.

proxy A mechanism whereby one system acts on behalf of another system in responding to protocol requests.

public key encryption A cryptographic method that uses a two-part key (code) that is made up of public and private components. To encrypt messages, the published public keys of the recipients are used. To decrypt messages, the recipients use their unpublished private keys, which are known only to them. Knowing the public key does not enable users to deduce the corresponding private key.

R

rack unit (U) A measure of vertical rack space equal to 1.75 inches (4.45 cm).

random access memory (RAM) Volatile, semiconductor-based memory in which any byte of memory can be accessed without touching the preceding bytes.

read-only file A file that a user cannot modify or delete.

read-only memory (ROM) A nonvolatile memory chip on which data has been prerecorded. Once written onto a ROM chip, data cannot be removed and can only be read.

real-time clock (RTC) A battery-backed component that maintains the time and date for a system, even when the system is powered off.

reboot An operating system–level operation that performs a system shutdown followed by a system boot. Power is a prerequisite.

Red Hat Package Manager (RPM) A collection of tools developed by Red Hat, Inc. for Red Hat Linux that can automate the install, uninstall, update, verify, and query software processes on a computer. RPM is now commonly used by many Linux vendors.

redirection The channeling of input or output to a file or device rather than to the standard input or output of a system. The result of redirection sends input or output that a system would normally display to the display of another system.

redundant array of independent disks (RAID) A way of storing the same data at different places, thus redundantly, on multiple hard disks. RAID enables a set of disk drives to appear as a single logical disk drive to an application such as a database or file system. Different RAID levels provide different capacity, performance, high availability, and cost characteristics.

Remote Management and Control Protocol (RMCP) A networking protocol that enables an administrator to respond to an alert remotely by powering the system on or off, or forcing a reboot.

remote procedure call (RPC) A method of network programming that enables a client system to call functions on a remote server. The client starts a procedure at the server, and the result is transmitted back to the client.

remote system A system other than the one on which the user is working.

reset A hardware-level operation that performs a system power-off, followed by a system power-on.

root In UNIX operating systems, the name of the superuser (root). The root user has permissions to access any file and carry out other operations not permitted to ordinary users. Roughly equivalent to the Administrator user name on Windows Server operating systems.

root directory The base directory from which all other directories stem, either directly or indirectly.

router A system that assigns a path over which to send network packets or other Internet traffic. Although both hosts and gateways do routing, the term "router" commonly refers to a device that connects two networks.

RSA algorithm A cryptographic algorithm developed by RSA Data Security, Inc. It can be used for both encryption and digital signatures.

S

schema Definitions that describe what type of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the directory might be unable to display the proper results.

Secure Shell (SSH) A UNIX shell program and network protocol that enables secure and encrypted login and execution of commands on a remote system over an insecure network.

Secure Sockets Layer (SSL) A protocol that enables client-to-server communication on a network to be encrypted for privacy. SSL uses a key exchange method to establish an environment in which all data exchanged is encrypted with a cipher and hashed to protect it from eavesdropping and alteration. SSL creates a secure connection between a web server and a web client. Hypertext Transfer Protocol Secure (HTTPS) uses SSL.

sensor data record (SDR) To facilitate dynamic discovery of features, the Intelligent Platform Management Interface (IPMI) includes this set of records that include software information such as how many sensors are present, what type they are, their events, threshold information, and so forth. The sensor data records enable software to interpret and present sensor data without any prior knowledge about the platform.

Serial Attached SCSI (SAS) A point-to-point serial peripheral interface that links controllers directly to disk drives. SAS devices include two data ports that enable failover redundancy, which guarantees data communication through a separate path.

serial console A terminal or a tip line connected to the serial port on the service processor. A serial console is used to configure the system to perform other administrative tasks.

server certificate A certificate used with Hypertext Transfer Protocol Secure (HTTPS) to authenticate web applications. The certificate can be self-signed or issued by a Certificate Authority (CA).

Server Message Block (SMB) protocol A network protocol that enables files and printers to be shared across a network. The SMB protocol provides a method for client applications to read and write to files on, and to request services from, server programs in the network. The SMB protocol enables you to mount file systems between Windows and UNIX systems. The SMB protocol was designed by IBM and subsequently modified by Microsoft Corp. Microsoft renamed the protocol the "Common Internet File System (CIFS)."

service processor (SP) A device used to manage server environmental, configuration, and service functions, and receive event data from other parts of the system. It receives data through sensor interfaces and interprets this data by using the sensor data record (SDR) to which it provides an interface. The SP provides another interface to the system event log (SEL). Typical function of the SP is to measure processor temperature, power supply values, and cooling fan status. The SP can take autonomous action to preserve system integrity.

session timeout A specified duration after which a server can invalidate a user session.

Simple Mail Transfer Protocol (SMTP) A Transmission Control Protocol/Internet Protocol (TCP/IP) used for sending and receiving e-mail.

Simple Network Management Protocol (SNMP) A simple protocol used to exchange data about network activity. With SNMP, data travels between a managed device and a network management station (NMS). A managed device can be any device that runs SNMP, such as hosts, routers, web servers, or other servers on the network.

Small Computer System Interface (SCSI) An ANSI standard for control of peripheral devices by one or more host computers. SCSI defines a standard I/O bus-level interface and a set of high-level I/O commands.

Spanning Tree Protocol (STP) A networking protocol based on an intelligent algorithm that enables bridges to map a redundant topology and eliminates packet looping in local area networks (LANs).

subnet A working scheme that divides a single logical network into smaller physical networks to simplify routing. The subnet is the portion of an Internet Protocol (IP) address that identifies a block of host IDs.

subnet mask A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long and selects the network portion of the Internet address and one or more bits of the local portion. Also called an "address mask."

superuser A special user who has privileges to perform all administrative functions on a UNIX system. Also called "root."

system event log (SEL) A log that provides nonvolatile storage for system events that are logged autonomously by the service processor, or directly with event messages sent from the host.

T

Telnet The virtual terminal program that enables the user of one host to log in to a remote host. A Telnet user of one host who is logged in to a remote host can interact as a normal terminal user of the remote host.

threshold Minimum and maximum values within a range that sensors use when monitoring temperature, voltage, current, and fan speed.

timeout A specified time after which the server should stop trying to finish a service routine that appears to be hung.

transmission control block (TCB) Part of the Transmission Control Protocol/Internet Protocol (TCP/IP) that records and maintains information about the state of a connection.

Transmission Control Protocol/Internet Protocol (TCP/IP) An Internet protocol that provides for the reliable delivery of data streams from one host to another. TCP/IP transfers data between different types of networked systems, such as systems running Solaris, Microsoft Windows, or Linux software. TCP guarantees delivery of data and that packets will be delivered in the same sequence in which they were sent.

trap Event notification made by Simple Network Management Protocol (SNMP) agents by their own initiative when certain conditions are detected. SNMP formally defines seven types of traps and permits subtypes to be defined.

Trivial File Transport Protocol (TFTP) A simple transport protocol that transfers files to diskless systems. TFTP uses User Datagram Protocol (UDP).

U

uninterruptible power supply (UPS) An auxiliary or backup power supply that provides electrical service over extended system power outages. A UPS for a LAN or computer system provides continuous power in the event of a power failure.

Universal Serial Bus (USB) An external bus standard that supports data transfer rates of 450 Mbit/sec. (USB 2.0). A USB port connects devices, such as mouse devices, keyboards, modems, and printers to the computer system.

unshielded twisted pair/shielded twisted pair (UTP/STP) A type of Ethernet cable.

user account A record of essential user information that is stored on the system. Each user who accesses a system has a user account.

User Datagram Protocol (UDP) A connectionless, transport layer protocol that adds some reliability and multiplexing to the Internet Protocol (IP). UDP enables one application program to deliver, via IP, datagrams to another application program on another machine. The Simple Network Management Protocol (SNMP) is usually implemented over UDP.

user identification (userID) A unique string identifying a user to a system.

user identification number (UID number) The number assigned to each user accessing a UNIX system. The system uses UID numbers to identify, by number, the owners of files and directories.

user name A combination of letters, and possibly numbers, that identifies a user to the system.

V

voltage regulator module (VRM) An electronic device that regulates a system's microprocessor voltage requirements to maintain the correct voltage.

volume One or more disk drives that can be grouped into a unit for data storage.

volume manager Software that organizes data blocks on physical disk drives into logical volumes, which makes the disk data independent of the physical path name of the disk drives. Volume manager software provides data reliability through disk striping, concatenation, mirroring, and dynamic growth of metadevices or volumes.

W

W3C Refers to the World Wide Web Consortium. W3C is an international organization that governs Internet standards.

web server Software that provides services to access the Internet or an intranet. A web server hosts web sites, provides support for HTTP/HTTPS and other protocols, and executes server-side programs.

wide area network (WAN) A network consisting of many systems that provides file transfer services. A WAN can cover a large physical area, sometimes worldwide.

X

X.509 certificate The most common certificate standard. X.509 certificates are documents containing a public key and associated identity information, digitally signed by a Certificate Authority (CA).

X Window System A common UNIX window system that enables a workstation or terminal to control multiple sessions simultaneously.

Index

A

Active Directory Service (ADS), 37
adding a user, 39
administrator password, changing, 3
alerts, 30
  configuring with a web browser, 31
  configuring with the CLI, 80

B

baseboard management controller (BMC), 44

C

CD/DVD, 57
Certificate Signing Request (CSR), 33
check fan status LED, 42
CLI
  alerts
    configuring, 80
  command syntax, 95
  commands
    alert, 97
    cd, 99
    character case, 70
    command verbs overview, 71
    create, 100
    delete, 101
    exit, 101
    help, 102
    miscellaneous, 96
    network and serial port, 96
    options, 71
    set, 103
    show, 104
    start, 105
    stop, 106
    user, 96
    version, 107
  managing
    network settings, 74
    user accounts, 75
  namespaces, 70
clock, setting with CLI, 103
configuring
  alerts with the CLI, 80
  connection methods, 12
  network settings with the CLI, 74
  platform event filters, 30
  SNMP, 34 to 37
  SSL, 33
  SSL certificate, 34
  system management access, 33
  terminal device, 6
  user accounts with the CLI, 77
configuring the system, 28 to 38
connecting to the ELOM, 5
CPU LED, 42
cursor settings, 55

D

default SP settings, 3
DIMM LED, 42

E

ELOM serial connection, 6

e-mail, creating event triggers, 30
Embedded Lights Out Manager
  definition, 2
  namespaces, 70
  redirecting keyboard and mouse, 56
event log, 24
events, 30

F

fault LED, 42
firmware, updating, 45, 86

H

hardware cursor, 55
hardware, redirecting
  keyboard and mouse, 56
  storage devices, 57
host, managing, 72

I

ID LED Control, 42
IPMI, 12
  IPMItool, 62
  overview, 61
  sensors, 62

J

Java RTE, for remote console, 52

L

LED
  check fan status LED, 42
  CPU, 42
  DIMM, 42
  fault LED, 42
  over temperature, 42
  power supply, 42
  top open, 42
LED control, 42
local cursor, 55
logging events, 24
logging using a web browser, 13

M

MAC address, server module level, 7
management information base (MIB)
  description of, 90
managing alerts, CLI, 78
managing network settings, 74
mouse settings, 55

N

namespace, SP, 71
network, default, 104

O

over temperature LED, 42

P

password
  default, 3
  parameters, 40
  set using CLI, 103
platform event filter (PEF), 30
power supply LED, 42
preconfigured ELOM Administrator account, 4

R

redirecting local storage, 51
remote client, redirecting hardware to, 52
remote console
  benefits, 51
  difficulty, 55
  redirecting
    keyboard and mouse, 56
    storage devices, 57
  requirements for, 51
remote console, Java RTE, 52
remote cursor, 55
remote storage devices, 52, 57
remotely updating firmware, 45
resetting BMC, 44

S

security certificate, 33
sensors, IPMI, 62
server module ELOM, connecting with serial connector, 6
service required LED, see fault LED, 42
setting password, CLI, 103
SNMP, 89 to 94

communities, 36
host state, managing, 72
MIB and, 90
overview, 89
settings, 35
user accounts, 92, 93
SP
default settings, 3
firmware update, 45
logging in with a web browser, 13
managing network settings, 74
namespace, 71
resetting, 44
tasks and management interfaces, 2
SP namespace, 70
SSL configuration, 33
starting the remote console application, 54
storage media
redirection, 52
remote, 57
system panic, 44

T

thresholds, 23, 24
top open LED, 42

U

updating firmware using the CLI, 86
user accounts
CLI, 75
overview, 12
users, SNMP, 33

V

voltage thresholds, 24

W

web browser login, 13
web-based interface
configuring alert, 31
WebGUI
remote console benefits, 51
setting ADS, 37
storage device redirection, 57