



Integrated Lights Out Manager (ILOM) Administration Guide

For ILOM 1.0

Sun Microsystems, Inc.
www.sun.com

Part No. 819-1160-13
October 2006, Revision 01

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

Copyright 2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, AnswerBook2, docs.sun.com, Ultra 40, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and in other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and in other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

AMD Opteron is a trademark or registered trademark of Advanced Microdevices, Inc.

U.S. Government Rights—Commercial use. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, Californie 95054, Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. a les droits de propriété intellectuelle relatants à la technologie qui est décrit dans ce document. En particulier, et sans la limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains énumérés à <http://www.sun.com/patents> et un ou les brevets plus supplémentaires ou les applications de brevet en attente dans les Etats-Unis et dans les autres pays.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, AnswerBook2, docs.sun.com, Untra 40, et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciées de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

AMD Opteron est une marque de fabrique ou une marque déposée de Advanced Microdevices, Inc.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISÉE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET TOUTES AUTRES CONDITIONS, DÉCLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES DANS LA LIMITE DE LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE À LA QUALITÉ MARCHANDE, À L'APTITUDE À UNE UTILISATION PARTICULIÈRE OU À L'ABSENCE DE CONTREFAÇON.



Adobe PostScript

Contents

- Preface xi**

- 1. ILOM and System Management Overview 1-1**
 - 1.1 Introduction 1-1
 - 1.1.1 Common Tasks That You Can Perform With ILOM 1-2
 - 1.1.2 ILOM Default Settings 1-3
 - 1.2 About Sun N1TM System Manager 1-4

- 2. ILOM Initial Setup 2-1**
 - 2.1 Connecting to the ILOM Using a Serial Connection 2-1
 - 2.2 Connecting to the ILOM Using an Ethernet Connection 2-3
 - 2.2.1 Configure the IP Address Using BIOS Setup Utility 2-4
 - 2.2.2 Configuring the ILOM to use DHCP 2-5
 - 2.2.3 Configuring the ILOM to Use a Static IP Address 2-6
 - 2.2.3.1 Obtain the ILOM IP Address 2-6
 - 2.2.3.2 Configuring a Static IP Address Using CLI and a Serial Connection 2-7
 - 2.2.3.3 Configuring a Static IP Address Using CLI and Ethernet 2-8
 - 2.2.3.4 Configuring a Static IP Address Using the WebGUI 2-8

- 3. Using the Command Line Interface 3-1**

- 3.1 Logging In To and Out Of CLI 3-1
- 3.2 Using CLI Commands 3-3
 - 3.2.1 CLI Namespace 3-3
 - 3.2.2 Privilege Levels 3-4
 - 3.2.3 CLI Command Syntax 3-4
 - 3.2.3.1 Command Verbs 3-5
 - 3.2.3.2 Command Options 3-5
 - 3.2.3.3 Command Targets 3-6
 - 3.2.3.4 Command Properties 3-6
- 3.3 Managing Access to ILOM 3-6
 - 3.3.1 Displaying Access Settings 3-7
 - 3.3.2 Configuring Access Settings 3-7
 - 3.3.2.1 Syntax 3-7
 - 3.3.2.2 Targets, Properties, and Values 3-7
 - 3.3.2.3 Examples 3-8
- 3.4 Managing the Host 3-8
 - 3.4.1 Managing the Host State 3-9
 - 3.4.2 Managing the Host Console 3-9
 - 3.4.3 Viewing Host Sensors 3-9
- 3.5 Managing ILOM Network Settings 3-10
 - 3.5.1 Displaying Network Settings 3-10
 - 3.5.2 Configuring Network Settings 3-10
 - 3.5.2.1 Syntax 3-11
 - 3.5.2.2 Targets, Properties, and Values 3-11
- 3.6 Managing ILOM Serial Port Settings 3-12
 - 3.6.1 Displaying Serial Port Settings 3-12
 - 3.6.2 Configuring Serial Port Settings 3-12
 - 3.6.2.1 Syntax 3-12

	3.6.2.2	Targets, Properties, and Values	3-13
3.7		Managing User Accounts	3-13
	3.7.1	Adding a User Account	3-14
	3.7.2	Deleting a User Account	3-14
	3.7.3	Displaying User Accounts	3-14
	3.7.4	Configuring User Accounts	3-14
		3.7.4.1	Syntax 3-15
		3.7.4.2	Targets, Properties, and Values 3-15
3.8		Managing ILOM Alerts	3-15
	3.8.1	Displaying Alerts	3-16
	3.8.2	Configuring Alerts	3-16
		3.8.2.1	Syntax 3-16
		3.8.2.2	Targets, Properties, and Values 3-17
3.9		Managing Clock Settings	3-18
	3.9.1	Displaying Clock Settings	3-18
	3.9.2	Configuring the Clock to Use NTP Servers	3-18
		3.9.2.1	Syntax 3-18
		3.9.2.2	Targets, Properties, and Values 3-18
3.10		Displaying ILOM Information	3-19
	3.10.1	Displaying Version Information	3-19
	3.10.2	Displaying Available Targets	3-19
3.11		Updating the ILOM Firmware	3-20
4.		Using the WebGUI	4-1
	4.1	Overview of WebGUI Requirements, Users, Tasks and Features	4-1
		4.1.1	Browser and Software Requirements 4-2
		4.1.2	Users and Privileges 4-2
		4.1.3	WebGUI Tasks 4-2
		4.1.4	WebGUI Features 4-3

- 4.2 Logging In and Out of the WebGUI 4-4
- 5. System Monitoring and Maintenance Using the WebGUI 5-1**
 - 5.1 Upgrading the ILOM Firmware 5-2
 - 5.2 Resetting the ILOM 5-5
 - 5.3 Resetting the ILOM and BIOS Passwords 5-6
 - 5.4 Viewing Replaceable Component Information 5-6
 - 5.5 Viewing Temperature, Voltage, and Fan Sensor Readings 5-7
 - 5.6 Viewing Alert Destinations and Configuring Alerts 5-11
 - 5.6.1 Viewing Alert Destinations 5-11
 - 5.6.2 Configuring an Alert 5-13
 - 5.6.3 Sending a Test Alert 5-14
 - 5.7 Viewing and Clearing the System Event Log 5-15
 - 5.7.1 Interpreting the System Event Log (SEL) Time Stamps 5-17
 - 5.8 Enabling SNMP Settings and Viewing SNMP Users 5-18
 - 5.8.1 Configuring SNMP Settings 5-18
 - 5.8.2 Adding, Editing and Deleting SNMP Communities 5-20
 - 5.8.3 Adding, Modifying and Deleting SNMP Users 5-22
 - 5.9 Controlling the Server Locator Indicator 5-23
 - 5.10 Viewing ILOM Hardware, Firmware, and IPMI Versions 5-24
 - 5.11 Viewing Active Connections to the ILOM 5-25
- 6. System Configuration Using the WebGUI 6-1**
 - 6.1 Setting the ILOM Session Time-Out Period 6-1
 - 6.2 Configuring the ILOM Serial Port 6-2
 - 6.3 Setting the ILOM Clock 6-4
 - 6.3.1 Setting the ILOM Clock Manually 6-4
 - 6.3.2 Synchronizing the ILOM Clock with an NTP Server: 6-5
 - 6.3.3 Interpreting ILOM Clock Settings 6-5

- 6.4 Configuring Network Settings 6-6
- 6.5 Uploading a New SSL Certificate 6-8
- 6.6 Enabling HTTP or HTTPS Web Access 6-10

- 7. Managing Users Using the WebGUI 7-1**
 - 7.1 Managing User Accounts 7-1
 - 7.1.1 Adding User Roles and Setting Privileges 7-2
 - 7.1.2 Modifying an ILOM User Account 7-5
 - 7.1.3 Deleting a User Account 7-7
 - 7.2 Viewing and Modifying Lightweight Directory Access Protocol Settings 7-8

- 8. Using The Remote Console Application 8-1**
 - 8.1 About the Remote Console Application 8-1
 - 8.1.1 Installation Requirements 8-2
 - 8.1.2 CD and Diskette Redirection Operational Model 8-3
 - 8.2 Starting the Remote Console Application 8-4
 - 8.3 Redirecting Keyboard, Video, Mouse, or Storage Devices 8-10
 - 8.3.1 Redirecting Keyboard and Mouse Devices 8-10
 - 8.3.2 Redirecting Storage Devices 8-12
 - 8.4 Controlling Power to the Host Server 8-13

- 9. Using Intelligent Platform Management Interface (IPMI) 9-1**
 - 9.1 About IPMI 9-1
 - 9.1.1 IPMItool 9-2
 - 9.2 Supported IPMI 2.0 Commands 9-2

- 10. Lightweight Directory Access Protocol (LDAP) 10-1**
 - 10.0.1 How LDAP Servers Organize Directories 10-1
 - 10.0.2 How LDAP Clients and Servers Work 10-3
 - 10.1 Configuring LDAP 10-4

10.1.1	Configuring LDAP Server	10-4
10.1.2	Configure ILOM	10-5
10.1.2.1	Using the CLI	10-5
10.1.2.2	Using the WebGUI	10-6
11.	Using Simple Network Management Protocol (SNMP)	11-1
11.1	About SNMP	11-1
11.1.1	How SNMP Works	11-1
11.2	SNMP Management Information Base (MIB) Files	11-2
11.3	MIBs Integration	11-3
11.4	About SNMP Messages	11-3
11.5	About ILOM and SNMP	11-4
11.5.1	Integrating the MIBs	11-4
11.5.2	Adding Your Server to Your SNMP Environment	11-4
11.5.3	Configuring Receipt of SNMP Traps	11-4
11.6	Managing SNMP User Accounts	11-5
11.6.1	Adding a User Account	11-5
11.6.2	Deleting a User Account	11-5
11.6.3	Configuring User Accounts	11-5
11.6.3.1	Syntax	11-5
11.6.3.2	Targets, Properties, and Values	11-6
11.6.3.3	Examples	11-6
A.	Command Line Interface Reference	A-1
A.1	CLI Command Quick Reference	A-1
A.2	CLI Command Reference	A-5
A.2.1	Using the <code>cd</code> Command	A-6
A.2.2	Using the <code>create</code> Command	A-6
A.2.3	Using the <code>delete</code> Command	A-7

A.2.4	Using the <code>exit</code> Command	A-8
A.2.5	Using the <code>help</code> Command	A-9
A.2.6	Using the <code>load</code> Command	A-10
A.2.7	Using the <code>reset</code> Command	A-11
A.2.8	Using the <code>set</code> Command	A-12
A.2.9	Using the <code>show</code> Command	A-14
A.2.10	Using the <code>start</code> Command	A-18
A.2.11	Using the <code>stop</code> Command	A-19
A.2.12	Using the <code>version</code> Command	A-19

Glossary **Glossary-1**

Index **Index-1**

Preface

This *Integrated Lights Out Manager (ILOM) Administration Guide* provides instructions for managing Sun servers using the Integrated Lights Out Manager (ILOM).

ILOM is included on certain Sun servers. If you have one of these servers, it will include an ILOM Supplement, which contains platform-specific information, such as sensors and thresholds, and details about the hardware.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can submit your comments by going to:

<http://www.sun.com/hwdocs/feedback>

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

Integrated Lights Out Manager (ILOM) Administration Guide, part number 819-1160-13

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>

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.

Typographic Conventions

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

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

ILOM and System Management Overview

This chapter contains the following sections:

- [Section 1.1, “Introduction” on page 1-1.](#)
- [Section 1.2, “About Sun N1™ System Manager” on page 1-4.](#)

1.1 Introduction

The ILOM is a dedicated system of hardware and supporting software that allows you to manage your Sun server independently of the operating system.

ILOM includes the following components:

- **Service Processor (SP)** - This is the hardware. It consists of a dedicated processor board that communicates through the system serial port and a dedicated Ethernet port.
- **Command Line Interface (CLI)** - The command line interface is a dedicated software application that allows you to operate the ILOM using keyboard commands. You can use the command-line interface to send commands to the ILOM. You can connect a terminal or emulator directly to the system serial port, or connect over the Ethernet using a Secure Shell (SSH).

To log in to and use the CLI, see [Chapter 3](#).

- **WebGUI** - The WebGUI provides a powerful, yet easy-to-use browser interface that allows you to log in to the SP and perform system management, monitoring, and IPMI tasks.

For instructions on how to use the WebGUI, see [Chapter 4](#).

- Remote Console/Java™ Client - The Java Client supports the Remote Console functionality, which allows you to access your server's console remotely. It redirects the keyboard, mouse, and video screen, and can redirect input and output from the local machine's CD and diskette drives.

For instructions on how to use the remote console, see [Chapter 8](#).

You do not need to install additional hardware or software to begin managing your server with ILOM.

ILOM also supports industry-standard IPMI and SNMP management interfaces:

- Intelligent Platform Management Interface (IPMI) v2.0 – Using a Secure Shell (SSH), you can interact with the ILOM to do the following: establish secure remote control of your server, monitor the status of hardware components remotely, monitor system logs, receive reports from replaceable components, and redirect the server console.

For more on IPMI, see [Chapter 9](#).

- Simple Network Management Protocol (SNMP) interface – ILOM also provides an SNMP v3.0 interface (with limited support for SNMP v1 and SNMP v2c) for external data center management applications such as Sun N1 System Manager, IBM Tivoli, and Hewlett-Packard OpenView.

For more on SNMP, see [Chapter 11](#).

Which interface you use depends on your overall system management plan and the specific tasks that you wish to perform.

1.1.1 Common Tasks That You Can Perform With ILOM

[TABLE 1-1](#) shows common tasks and the management interfaces used to perform each task.

TABLE 1-1 Common Tasks

Task	IPMI	Web Interface	CLI	SNMP
Redirect the system graphical console to a remote client 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

TABLE 1-1 Common Tasks (Continued)

Task	IPMI	Web Interface	CLI	SNMP
Monitor system BIOS messages remotely.	Yes	Yes	Yes	
Monitor system operating system messages remotely.	Yes	Yes	Yes	
Interrogate system components for their IDs and/or serial numbers.	Yes		Yes	Yes
Redirect the system serial console to a remote client.	No	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

1.1.2 ILOM Default Settings

Sun has configured the ILOM card and ILOM firmware on your server to reflect the most common default settings used in the field. It is unlikely that you will need to change any of these defaults, which appear in [TABLE 1-2](#).

TABLE 1-2 ILOM Default Settings

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

1.2 About Sun N1™ System Manager

If you plan to manage your server as one resource in a comprehensive data center management solution, Sun N1 System Management provides an alternative to ILOM. This software suite provides advanced virtualization features that enable you to monitor, maintain, and provision multiple Solaris, Linux, and Microsoft Windows servers in your data center.

The Sun N1 System Manager is available to download from:

www.sun.com/software/solaris/index.jsp

You can also install it from the Sun N1 System Manager DVD shipped in your system box. This software suite is installed on a dedicated server in your data center and allows one or more remote management clients to perform the following tasks on multiple managed servers:

- Manage multiple servers – Configure, provision, deploy, manage, monitor, patch, and update from one to thousands of Sun servers.
- Monitor system information – System manufacturer, make, model, serial number, management MAC addresses, disk information, expansion slot information, and platform CPU and memory information.
- Manage power remotely – Power off, power on, power reset, and power status.
- Manage ILOMs and BIOS – Information about system ILOM firmware, version, and status. You can also perform remote upgrades to firmware on ILOMs.
- Manage system boot commands and options – Remote boot control via IPMI and remote mapping of boot devices and boot options.
- Manage remote system health checks – Information about the status of a server.
- Manage operating systems – Deploy, monitor, and patch both Solaris and Linux operating systems.
- Perform bare-metal discovery.

To learn more about this suite of powerful data center management tools, see:

http://www.sun.com/software/products/system_manager/

ILOM Initial Setup

This chapter describes how to do the ILOM initial setup.

The ILOM communicates through the system serial port and/or through a dedicated Ethernet port.

- You can run the Command Line Interface (CLI) connected directly to the serial port.
- You can run the CLI and the WebGUI through the Ethernet port.

Connecting with the Ethernet requires some configuration.

This chapter contains the following sections:

- [Section 2.1, “Connecting to the ILOM Using a Serial Connection”](#) on page 2-1.
- [Section 2.2, “Connecting to the ILOM Using an Ethernet Connection”](#) on page 2-3.

2.1 Connecting to the ILOM Using a Serial Connection

You can access the ILOM CLI at any time by connecting a terminal or a PC running terminal emulation software to the RJ-45 serial port on the ILOM board.

1. **Verify that your terminal, laptop, or terminal server is operational.**
2. **Configure that terminal device or the terminal emulation software to use the following settings:**
 - 8N1: eight data bits, no parity, one stop bit
 - 9600 baud
 - Disable hardware flow control (CTS/RTS)

3. Unpack your server and connect the system power cable to a power source.

Refer to your platform-specific documentation for instructions on installing the hardware, cabling, and powering on.

4. Connect a serial cable from the serial port on the server's back panel to a terminal device.

Refer to your -specific documentation or the supplement for the location of the serial port.

Note – The serial port requires that the serial cable connected to it use the following pin assignments. Note that these are the same as the serial cable connector for the Sun Advanced Lights Out Manager (ALOM) or Remote System Control (RSC). See [TABLE 2-1](#).

TABLE 2-1 Serial Management Port Pinouts

Pin	Signal Description
1	Request To Send (RTS)
2	Data Terminal Ready (DTR)
3	Transmit Data (TXD)
4	Ground
5	Ground
6	Receive Data (RXD)
7	Data Carrier Detect (DCD)
8	Clear To Send (CTS)

5. Press Enter on the terminal device.

This establishes the connection between the terminal device and the ILOM.

Note – If you connect a terminal or emulator to the serial port before it has been powered up or during its power up sequence, you will see bootup messages.

When the system has booted, the ILOM displays its login prompt:

```
SUNSPnnnnnnnnnnnn login:
```

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

6. Log in to the CLI:

a. Type the default user name, **root**.

b. Type the default password, **changeme**.

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

```
->
```

The ILOM is now accessing the CLI. You can now run CLI commands.

For example, to display status information about the motherboard in your server, type the following command:

```
-> show /SYS/MB
```

7. To go to the host serial console (host COM0), type the following commands:

```
cd /SP/console
```

```
start
```

Note – After you have returned to the serial console, to switch back to the CLI, enter the **Escape-** (key sequence.

[Chapter 3](#) describes how to use the CLI.

For instructions on how to use the serial console, see the platform-specific documentation.

2.2 Connecting to the ILOM Using an Ethernet Connection

To access the full range of ILOM functionality, you must connect a LAN to the Ethernet port and configure your Ethernet connection.

ILOM supports Dynamic Host Configuration Protocol (DHCP) and static IP addressing.

- To configure DHCP or a static IP address using the BIOS, see [Section 2.2.1, “Configure the IP Address Using BIOS Setup Utility”](#) on page 2-4
- To configure DHCP, see [Section 2.2.2, “Configuring the ILOM to use DHCP”](#) on page 2-5.

- To configure a static IP address, see [Section 2.2.3, “Configuring the ILOM to Use a Static IP Address”](#) on page 2-6.

2.2.1 Configure the IP Address Using BIOS Setup Utility

The BIOS Setup Utility allows you to set the ILOM IP address. It allows you to configure it manually, or use DHCP.

- 1. Unpack your server and connect the system power cable to a power source.**

Refer to your platform documentation for instructions on installing the hardware, cabling, and powering on.
- 2. If you are going to use DHCP, verify that your DHCP server is configured to accept new media access control (MAC) addresses.**
- 3. Start the BIOS Setup Utility.**
 - a. Boot the system.**
 - b. Watch the boot messages. You will see a line that says you can press F2 to enter BIOS setup.**
 - c. After you see the message, press F2.**

After some messages and screen changes, the BIOS Setup Utility appears.
- 4. Select the Advanced tab.**

The Advanced page appears.
- 5. Highlight IPMI 2.0 Configuration in the list, then select Enter.**

The IPMI 2.0 Configuration page appears.
- 6. Fill in the IPMI 2.0 Configuration page.**
 - a. Under IP Assignment, select DHCP or Static.**
 - b. If you selected Static, fill in the IP address, subnet mask and default gateway at the bottom of the page.**
- 7. Select Commit to save your changes.**

If you selected DHCP, the BIOS utility automatically updates the address fields.



Caution – You must use Commit to save the changes on this page. Using F10 will not save your changes.

2.2.2 Configuring the ILOM to use DHCP

To configure the ILOM to use a DHCP address:

1. **Verify that your DHCP server is configured to accept new media access control (MAC) addresses.**

2. **Unpack your server and connect the system power cable to a power source.**

Refer to your platform documentation for instructions on installing the hardware, cabling, and powering on.

3. **Obtain the ILOM MAC address from one of the following locations.**

MAC addresses are 12-digit hexadecimal strings in the format `xx:xx:xx:xx:xx:xx` where x represents a single hexadecimal letter (0–9, A–F, a–f). Write down that address for future reference.

- The ILOM has a serial port to which you can attach a terminal device. If you log in to the ILOM and enter the command `show /SP/network`, the ILOM displays the current Mac address.
 - The label attached to the GRASP board. You need to open the cover of the server to view this label.
 - The Customer Information Sheet shipped with your server.
 - The system BIOS setup screen. Choose Advanced - IPMI 2.0 Configuration - Set LAN Configuration - MAC address.
 - Command-line interface. Log in to the ILOM via the CLI and type the command `show /SP/network` to display the MAC address.
4. **Connect an Ethernet cable to the RJ-45 NET MGT Ethernet port.**

Refer to your platform documentation or the supplement for the location of RJ-45 NET MGT Ethernet port.
 5. **You can assign an Ethernet address directly, or you can let DHCP assign one for you.**

- a. **To assign your own Ethernet address, use the DHCP configuration software to assign an IP address to the MAC address noted above. See the DHCP server documentation for details.**

- b. **To let DHCP assign an IP address:**

Note – Different DHCP server applications running on different operating systems store these log files in different locations. Consult your DHCP system administrator to locate the correct path to the log file.

- i. **When you connect an Ethernet cable to the ILOM, the ILOM provides its MAC address and DHCP assigns the ILOM an IP address.**

ii. Log in to your DHCP server and view its DHCP log file.

iii. Identify the IP address in the log file that corresponds to the ILOM MAC address.

Typically, DHCP log file entries are individual lines with the following comma-separated fields:

ID, Date, Time, Description, IP Address, Host Name, MAC Address

Locate the MAC address of your ILOM in the MAC Address (seventh) field of the correct DHCP file entry, and record the corresponding value of the IP Address (fifth) field. This is the IP address that you must use to access the WebGUI and the remote console.

When this procedure is complete, you can access the ILOM using the IP address assigned by DHCP.

2.2.3 Configuring the ILOM to Use a Static IP Address

Usually, you will configure the ILOM to use DHCP, as described in [Section 2.2.2, “Configuring the ILOM to use DHCP” on page 2-5](#).

If you choose to configure the ILOM using a static IP address, you can do so using three different methods:

- CLI serial connection ([Section 2.2.3.2, “Configuring a Static IP Address Using CLI and a Serial Connection” on page 2-7](#))
- CLI Ethernet connection ([Section 2.2.3.3, “Configuring a Static IP Address Using CLI and Ethernet” on page 2-8](#))
- WebGUI Ethernet ([Section 2.2.3.4, “Configuring a Static IP Address Using the WebGUI” on page 2-8](#))
- BIOS Setup Utility ([Section 2.2.1, “Configure the IP Address Using BIOS Setup Utility” on page 2-4](#))

2.2.3.1 Obtain the ILOM IP Address

Before you begin, you must obtain the ILOM IP address from one of the following locations. Record the IP address for future reference.

- Command-line interface. Log in to the ILOM via the CLI and type the command `show /SP/network` to display the IP address.
- The system BIOS setup screen. Choose Advanced => IPMI 2.0 Configuration. Under LAN Configuration, look at IP Address.

Note – You can set the IP address using the BIOS Setup Utility.

If the address on the IPMI configuration page is acceptable, you do not need to change anything.

To change the IP address, type the new address in the IP address field. Type in a new subnet mask and default gateway if necessary. When you are done, click Commit.

See [Section 2.2.1, “Configure the IP Address Using BIOS Setup Utility”](#) on page 2-4 for details.

2.2.3.2 Configuring a Static IP Address Using CLI and a Serial Connection

To set a static IP address for the ILOM using the CLI and a serial line connection, do the following.

1. **Establish a serial connection to the ILOM.**

See [Section 2.1, “Connecting to the ILOM Using a Serial Connection”](#) on page 2-1 for details.

2. **Log in to the ILOM.**

3. **Type the following command to set the working directory.**

```
cd /SP/network
```

4. **Type the following commands to specify a static Ethernet configuration.**

```
set pendingipaddress=xxx.xxx.xx.xx
```

```
set pendingipnetmask=yyy.yyy.yyy.y
```

```
set pendingipgateway=zzz.zzz.zz.zzz
```

```
set commitpending=true
```

where `xxx.xxx.xx.xx`, `yyy.yyy.yyy.y` and `zzz.zzz.zz.zzz` are the IP address, netmask, and gateway for your ILOM and network configuration. To obtain the ILOM IP address, see [Section 2.2.3.1, “Obtain the ILOM IP Address”](#) on page 2-6.

5. **Log out of the ILOM.**

2.2.3.3 Configuring a Static IP Address Using CLI and Ethernet

1. **Log in to the ILOM using Secure Shell (SSH) over the network, or by connecting a terminal to the serial port.**

To establish a Secure Shell (SSH) connection to the CLI, type the appropriate connection command in the SSH application. For example, to connect to the ILOM with an IP address of 129.144.82.20, type the following command:

```
# ssh -l root 129.144.82.20
```

Use the IP address you obtained in [Section 2.2.3.1, “Obtain the ILOM IP Address” on page 2-6](#).

2. **Type the following command to set the working directory.**

```
cd /SP/network
```

3. **Type the following commands to specify a static Ethernet configuration.**

Note – The following values are samples only. You must specify the IP address, netmask, and gateway appropriate for your ILOM and network configuration.

```
set pendingipaddress=129.144.82.26  
set pendingipnetmask=255.255.255.0  
set pendingipgateway=129.144.82.254  
set pendingipdiscovery=static  
set commitpending=true
```

2.2.3.4 Configuring a Static IP Address Using the WebGUI

To set a static IP address for the ILOM using the WebGUI, do the following.

1. **Connect to the ILOM through a web browser running on a remote system.**

Use the IP address you obtained in [Section 2.2.3.1, “Obtain the ILOM IP Address” on page 2-6](#).

2. **Log in to the WebGUI**

The default user name is **root**, and the default password is **changeme**.

3. **Choose the Configuration tab and its Network tab to display information about the current ILOM network configuration. See [FIGURE 2-1](#).**

4. **Select the Use the Following IP Address option. See [FIGURE 2-1](#).**

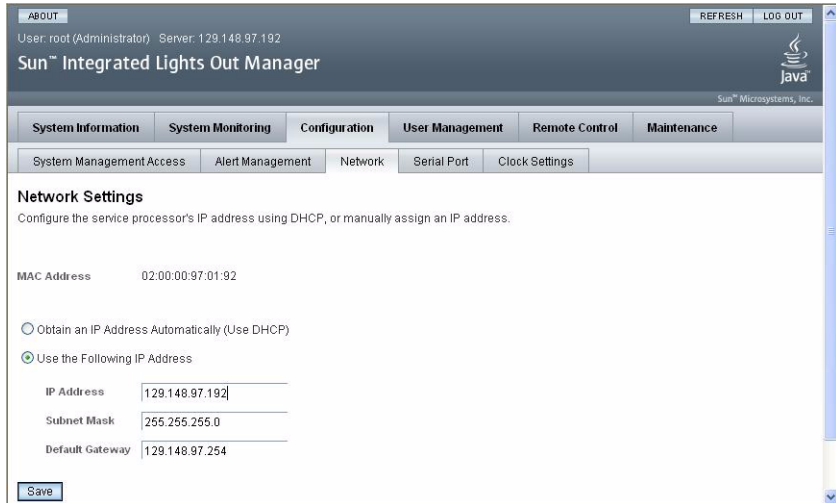


FIGURE 2-1 Integrated Lights Out Manager Network Settings Page

5. **Modify the displayed settings as required and click save.**

Using the Command Line Interface

This chapter describes how to use the ILOM's Command Line Interface (CLI). The sections include:

- [Section 3.1, “Logging In To and Out Of CLI” on page 3-1.](#)
- [Section 3.2, “Using CLI Commands” on page 3-3.](#)
- [Section 3.3, “Managing Access to ILOM” on page 3-6.](#)
- [Section 3.4, “Managing the Host” on page 3-8.](#)
- [Section 3.5, “Managing ILOM Network Settings” on page 3-10.](#)
- [Section 3.6, “Managing ILOM Serial Port Settings” on page 3-12.](#)
- [Section 3.7, “Managing User Accounts” on page 3-13.](#)
- [Section 3.8, “Managing ILOM Alerts” on page 3-15.](#)
- [Section 3.9, “Managing Clock Settings” on page 3-18.](#)
- [Section 3.10, “Displaying ILOM Information” on page 3-19.](#)
- [Section 3.11, “Updating the ILOM Firmware” on page 3-20.](#)

3.1 Logging In To and Out Of CLI

You can access the command line 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.
- **SSH** –You can connect to the CLI using an Ethernet connection. Secure shell connections (SSC) are enabled by default.

The ILOM supports a maximum of 10 active sessions, including serial, SSH, and web interface sessions. You can view active sessions by entering the command `show /SP/sessions`.

Note – Telnet connections to the ILOM are not supported.

Logging In and Out Using SSH

1. **Start your SSH client**
2. **To log in to the ILOM, type:**
`$ ssh root@SPipaddress`
3. **Type your password when prompted.**

Note – The default user name is **root**, and the default password is **changeme**.

For example:

```
$ ssh root@192.168.25.25
root@192.168.25.25's password:
Sun Integrated Lights Out Manager
Version 1.0
Copyright 2006 Sun Microsystems, Inc. All rights reserved.
Warning: password is set to factory default.
->
```

4. **To log out, type `exit`.**

Logging In and Out Using the Serial Port

1. **Configure your terminal device or the terminal emulation software running on a laptop or PC to the following settings:**
 - 8N1: eight data bits, no parity, one stop bit
 - 9600 baud
 - Disabled software flow control (CTS/RTS)
2. **Connect a serial cable from the ILOM RJ-45 Serial Mgt port to a terminal device.**
3. **Press ENTER on the terminal device to establish a connection between that terminal device and the ILOM.**

You should see the following prompt:

```
SUNSP0003BA84D777 login:
```

4. Log in to the ILOM and type the user name and password.

The default user name is **root**, and the default password is **changeme**.

Note – Once you have logged in to the ILOM as root, change the default password for increased security.

5. To log out, type **exit**.

3.2 Using CLI Commands

This section describes how to use CLI commands.

3.2.1 CLI Namespace

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 ILOM includes two namespaces: the `/SP` namespace, and the `/SYS` namespace.

- The `/SP` namespace manages the ILOM. For example, you use this space to manage users, clock settings, and other ILOM issues. [FIGURE 3-1](#) shows the `/SP` namespace.
- The `/SYS` namespace manages the host system. For example, you can change the host state, read sensor information, and access other information for managed system hardware. Your `/SYS` namespace diagram is determined by the managed hardware devices in your server.

You can view your /SYS namespace by typing the show /SYS command from the command line. FIGURE 3-1 shows the /SP namespace. The /SYS namespace is unique to each platform.

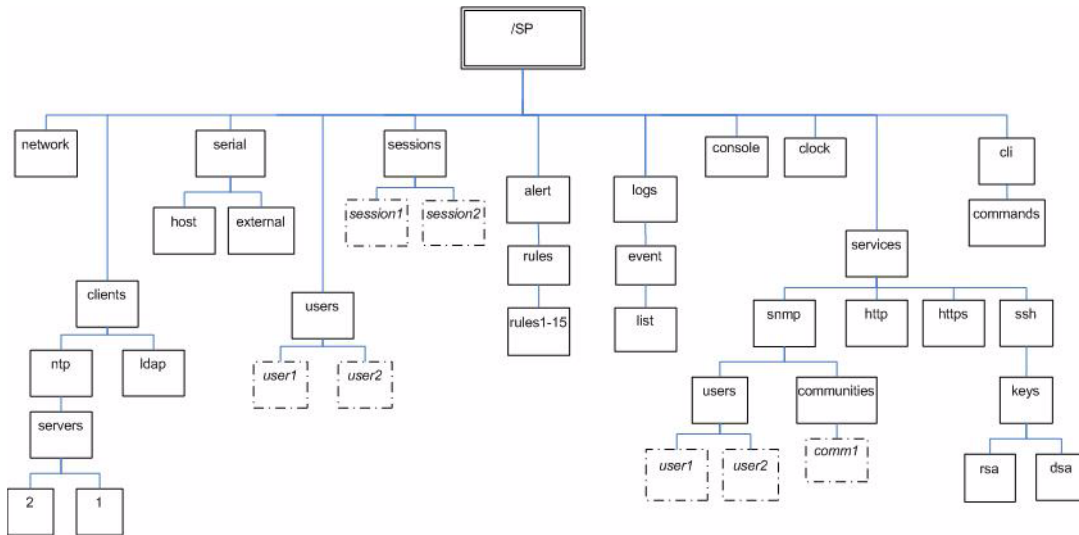


FIGURE 3-1 SP Namespace

3.2.2 Privilege Levels

The CLI provides two privilege levels: Administrator and Operator. Administrators have full access to ILOM functionality and Operators have read-only access to ILOM information.

Note – The default user, root, has administrator privileges. To create a user account with operator privileges, see [Section 3.7.1, “Adding a User Account” on page 3-14](#).

CLI commands are case-sensitive.

3.2.3 CLI Command Syntax

The syntax of a command is: <verb><options><target><properties>

The following sections describe each of these.

3.2.3.1 Command Verbs

The CLI supports the following command verbs.

TABLE 3-1 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.
load	Transfers a file from an indicated source to an indicated target.
reset	Resets the state of the target.
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 ILOM firmware running.

3.2.3.2 Command Options

The CLI supports the following options. All options are not 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 3-2 Command 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 the user wants 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 3-2 Command Options (*Continued*)

Option Long Form	Short Form	Description
-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.
-script		Skips warnings or prompts normally associated with the command.
-source		Indicates the location of a source image.

3.2.3.3 Command Targets

Every object in your namespace is a target. All targets are not supported for all commands. [Section A.2, “CLI Command Reference” on page A-5](#) lists each command, with its targets and properties.

3.2.3.4 Command Properties

Properties are the configurable attributes specific to each object. An object can have one or more properties. [Section A.2, “CLI Command Reference” on page A-5](#) lists each command, with its targets and properties.

3.3 Managing Access to ILOM

You can display or configure HTTP, HTTPS, and Secure Shell (SSH) services from the CLI. By default, HTTPS access is enabled.

ILOM is managed through the /SP namespace.

3.3.1 Displaying Access Settings

[TABLE 3-3](#) shows the commands used to display access settings.

TABLE 3-3 Commands to Display Access Settings

Type this command...	to display this setting.
<code>show /SP/services/http</code>	HTTP
<code>show /SP/services/https</code>	HTTPS
<code>show /SP/services/ssh/keys/dsa</code>	SSH key
<code>show /SP/services/ssh/keys/rsa</code>	

3.3.2 Configuring Access Settings

Use the `set` command to change properties and values for HTTP and HTTPS services.

3.3.2.1 Syntax

```
set target [propertyname=value]
```

3.3.2.2 Targets, Properties, and Values

[TABLE 3-3](#) shows the valid targets, properties, and values for HTTP, HTTPS, and SSH services.

TABLE 3-4 Valid Targets, Properties and Values for HTTP, HTTPS and SSH

Target	Property	Value	Default
/SP/services/http	port	<port number>	80
	secureredirect	enabled disabled	enabled
	servicestate	enabled disabled	disabled

TABLE 3-4 Valid Targets, Properties and Values for HTTP, HTTPS and SSH

Target	Property	Value	Default
/SP/services/https	port	<port number>	443
	servicestate	enabled disabled	enabled
/SP/services/ssh/keys/dsa	fingerprint		
	length		
	publickey		
/SP/services/ssh/keys/rsa	fingerprint		
	length		
	publickey		

3.3.2.3 Examples

To configure automatic redirection from HTTP to HTTPS, type:

```
set /SP/services/http secureredirect=true
```

To change the HTTPS port to 445 type:

```
set /SP/services/https port=445
```

3.4 Managing the Host

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

3.4.1 Managing the Host State

To send a break to the host, type:

Escape + B (press the Escape key and type upper case B).

To power on the host, type:

start /SYS

To power off the host, type:

stop /SYS

To reset the host, type:

reset /SYS

Note – Entering reset /SYS does not affect the power state of the host.

3.4.2 Managing the Host Console

Type the following command to start a session to the server console:

start /SP/console

Type the following command to terminate a server console session started by another user:

stop /SP/console

3.4.3 Viewing Host Sensors

Host systems are equipped with sensors that show 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 sensors. Use the command:

show /SYS/sensor

where *sensor* is a particular sensor. For example, the following command shows the state of sensor `/PROC/P0`:

```
-> show /SYS/PROC/P0
/SYS/PROC/P0
Targets:
Properties:
  T_CORE = 7700.000000 RPM
  V_+1V25 = 1.404000 Volts
  V_+1V5 = 45.000000 degrees C
  V_+2V5 = 7800.000000 RPM
Commands:
  cd
  show
```

For more information about sensors, including how to view them using the WebGUI, see [Section 5.5, “Viewing Temperature, Voltage, and Fan Sensor Readings”](#) on page 5-7

For details on individual sensors, see your platform supplement.

3.5 Managing ILOM Network Settings

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

3.5.1 Displaying Network Settings

Type the following command to display network settings:

```
show /SP/network
```

3.5.2 Configuring Network Settings

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

Network settings have two sets of properties: pending and active. The active settings are the settings currently in use by the ILOM. These settings are read-only. If you want to change settings, enter the updated settings as the pending settings

(pendingipaddress or pendingipgateway), then set the commitpending property to true. This prevents accidental disconnections for both port and network settings.

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

3.5.2.1 Syntax

```
set target [propertyname=value]
```

3.5.2.2 Targets, Properties, and Values

The following targets, properties, and values are valid for ILOM network settings.

TABLE 3-5 ILOM Network Targets, Properties and Values

Target	Property	Value	Default
/SP/network	commitpending	true (none)	(none)
	pendingipaddress	<ipaddress none>	none
	pendingipdiscovery	dhcp static	dhcp
	pendingipgateway	<ipaddress none>	none
	pendingipnetmask	<ipdotteddecimal>	255.255.255.255

Examples

To change the IP address for the ILOM, type:

```
-> set /SP/network ipaddress=nnn.nn.nn.nn commitpending=true
```

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

To change the network settings from DHCP to static assigned settings, type:

```
-> set /SP/network pendingipdiscovery=static pendingipaddress=
nnn.nn.nn.nn pendingipgateway=nnn.nn.nn.nn pendingipnetmask=
nnn.nn.nn.nn commitpending=true
```

3.6 Managing ILOM Serial Port Settings

You can display or configure the ILOM serial port settings from the CLI. The ILOM has two serial ports: an internal host port that interfaces directly with the host server using the `start /SP/console` command, and an external port that is exposed on back of the server.

3.6.1 Displaying Serial Port Settings

Type the following command to display settings for the external serial port:

```
show /SP/serial/external
```

Type the following command to display settings for the host serial port:

```
show /SP/serial/host
```

3.6.2 Configuring Serial Port Settings

Use the `set` command to change properties and values for serial port settings. Port settings have two sets of properties: pending and active. The active settings are the settings currently in use by the ILOM. These settings are read-only. If you want to change settings, enter the updated settings as the pending settings, then set the `commitpending` property to `true`. This prevents accidental disconnections for both port and network settings.

3.6.2.1 Syntax

```
set target [propertyname=value]
```

3.6.2.2 Targets, Properties, and Values

The following targets, properties, and values are valid for ILOM serial ports.

TABLE 3-6 Valid Targets, Properties and Values for ILOM Serial Ports

Target	Property	Value	Default
/SP/serial/external	commitpending	true (none)	(none)
	flowcontrol	none	none
	pendingspeed	<decimal>	9600
	speed	9600	9600
/SP/serial/host	commitpending	true (none)	(none)
	pendingspeed	<decimal>	(none)
	speed	9600	9600

Example

To change the speed (baud rate) for the host serial port from 9600 to 57600, type:

```
-> set /SP/serial/host pendingspeed=56000 commitpending=true
```

Note – The speed of the host serial port must match the speed setting for serial port 0, COM1, or /dev/ttyS0 on the host operating system for the ILOM to communicate properly with the host.

3.7 Managing User Accounts

This section explains how to add, modify and delete ILOM user accounts.

The ILOM supports up to 10 user accounts. Two of those, root and anonymous, are set by default and cannot be removed. Therefore, you can configure eight additional accounts.

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



Caution – The ILOM includes a user account "sunservices," which shares the ILOM root password. Normally, it is used exclusively by Sun Service personnel; however it can also be used to perform recovery procedures documented in the product notes. Incorrect use of this account can corrupt the service processor image or operations.

The roles include:

- Administrator - Enables access to all ILOM features, functions, and commands.
- Operator - Enables limited access to ILOM features, functions, and commands. In general, Operators cannot changed configuration settings.

Operators cannot:

- See or change LDAP settings
- Add or remove users
- Change network settings (view only)
- Change Network Time Protocol (NTP) settings (view only)
- Change SNMP settings (view only)
- Change HTTP settings (view only)

3.7.1 Adding a User Account

Type the following command to add a local user account:

```
create /SP/users/username password=password role=administrator|operator
```

3.7.2 Deleting a User Account

Type the following command to delete a local user account:

```
delete /SP/users/username
```

3.7.3 Displaying User Accounts

Type the following command to display information about all local user accounts:

```
show /SP/users
```

3.7.4 Configuring User Accounts

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

3.7.4.1 Syntax

```
set target [propertyname=value]
```

3.7.4.2 Targets, Properties, and Values

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

TABLE 3-7 Valid Targets, Properties and Values for Local User Accounts

Target	Property	Value	Default
/SP/users/username	permissions	administrator operator	operator
	password	<string>	

Examples

When changing the role for user1 from Administrator to Operator type:

```
-> set /SP/users/user1 role=operator
```

To change user1's password type:

```
-> set /SP/users/user1 password
```

```
Changing password for user /SP/users/user1/password...
```

```
Enter new password:*****
```

```
Enter new password again:*****
```

```
New password was successfully set for user /SP/users/user1
```

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

3.8 Managing ILOM Alerts

The system is equipped with a number of sensors that measure voltages, temperatures and other things. ILOM polls the sensors and posts an event in the event log (SEL) when they cross a threshold. Some of these readings are also used to perform actions such as adjusting fan speeds, illuminating LEDs and powering off the chassis.

The alert management view allows you to configure the system to send alerts to IP addresses.



Caution – The ILOM tags all events or actions with LocalTime=GMT (or UDT). Browser clients show these events in LocalTime. This can cause apparent discrepancies in the event log. When an event occurs on the ILOM, the event log shows it in UDT, but a client would show it local time.

An alert is an IPMI Platform Event Trap (PET) generated when a sensor crosses the specified threshold. For example, if you configure an alert for critical thresholds, the ILOM sends an IPMI trap to the specified destination when any sensor crosses the upper or lower critical (CT) threshold.

All alerts are IPMI PET traps, as defined in the Intelligent Platform Management Interface (IPMI) v2.0.

A special criteria, informational, is reserved for system events that are not related to sensors.

3.8.1 Displaying Alerts

Type the following command to display alerts:

```
show /SP/alert/rules
```

3.8.2 Configuring Alerts

Use the set command to change properties and values for alerts.

3.8.2.1 Syntax

```
set target [propertyname=value]
```

3.8.2.2 Targets, Properties, and Values

The following targets, properties, and values are valid for IPMI PET alerts.

TABLE 3-8 Valid Targets, Properties and Values for IPMI Pet Alerts

Target	Property	Value	Default
<code>/SP/alert/rules/1...15</code>	destination level	<ipaddress> disable information warning critical non-recoverable	(none) disable

The parameters are:

- rule – The number of the alert rule; a number from 1 to 15.
- ipaddress – The IP address to which the alert will be sent.
- level – The severity level of the alert (see [TABLE 3-9](#)).

TABLE 3-9 Alert Levels

Alert Levels	Name in Sensor Readings View	Description
Informational	N/A	This level traps system events that are not related to sensors, such as “The host has booted.”
warning	NC	The sensor is outside of its normal range but not critical.
critical	CT	The sensor has crossed a critical threshold.
non-recoverable	NR	The sensor has reached a threshold beyond the tolerance level of the corresponding component(s).
disable	N/A	Don’t send alerts at this level.

Examples

To configure an alert, type:

```
-> set /SP/alert/rules/1 destination=128.145.77.21 level=critical
```

To change an alert level to critical, type:

```
-> set /SP/alert/rules/1 level=critical
```

To turn off an alert, type:

```
-> set /SP/alert/rules/1 level=disable
```

3.9 Managing Clock Settings

You can display clock settings or configure your clock to synchronize with one or two Network Time Protocol (NTP) servers. If you do not configure an NTP server, the time is set by the system BIOS.

3.9.1 Displaying Clock Settings

Type the following command to display clock settings:

```
show /SP/clock
```

3.9.2 Configuring the Clock to Use NTP Servers

Use the set command to change properties and values for NTP servers.

3.9.2.1 Syntax

```
set target [propertyname=value]
```

3.9.2.2 Targets, Properties, and Values

The following targets, properties, and values are valid for NTP servers.

TABLE 3-10 Valid Targets, Properties and Values for NTP Servers

Target	Property	Value	Default
/SP/clients/ntp/server/1	address	<ipaddress>	(none)
/SP/clients/ntp/server/2	address	<ipaddress>	(none)

Example

To configure your clock to synchronize with an NTP server, type:

```
-> set /SP/clients/ntp/server/1 address=125.128.84.20
```

Then enable the NTP service by typing:

```
-> set /SP/clock/usentpserver=enabled
```

Note – Once you enable the NTP service, it can take up to five minutes for the clock to synchronize.

3.10 Displaying ILOM Information

You can display active session, current versions, and other information about the ILOM using the CLI. [TABLE 3-11](#) shows the commands and the information they display.

TABLE 3-11 Commands To Display ILOM Information

Command	Displays...
<code>version</code>	The current ILOM version
<code>show /SP/cli/commands</code>	All of the CLI commands
<code>show /SP/sessions</code>	All active sessions
<code>help targets</code>	Available valid targets

3.10.1 Displaying Version Information

Type the following command to display the current ILOM version:

3.10.2 Displaying Available Targets

Type the following command to display the available valid targets:

```
help targets
```

3.11 Updating the ILOM Firmware

You can use CLI to update the ILOM firmware. Updating the ILOM from the command line enables you to update both the ILOM firmware and the BIOS at the same time. See [Section A.2.6, “Using the load Command” on page A-10](#) for more information.



Caution – Ensure that you have reliable power before upgrading your firmware. If power to the system fails (for example, if the wall socket power fails or the system is unplugged) during the firmware update procedure, the ILOM could be left in an unbootable state.



Caution – Shut down your host operating system before proceeding. Otherwise the ILOM will shut the host down ungracefully, which could cause file system corruption.

Note – The upgrade takes about five minutes to complete. During this time, no other tasks can be performed in the ILOM.

1. If the server OS is running, perform a clean shutdown.
2. Type the following command to update the ILOM firmware:

```
load -source URL
```

Note – A network failure during the file upload will result in a time-out. This causes the ILOM to reboot with the prior version of the ILOM firmware.

Example:

```
-> load -source tftp://archive/newmainimage  
Are you sure you want to load the specified file (y/n)? y  
File upload is complete.  
Firmware image verification is complete.  
Do you want to preserve the configuration (y/n)? n  
Updating firmware in flash RAM:  
.br/>Firmware update is complete.  
ILOM will not be restarted with the new firmware.
```


Using the WebGUI

This chapter describes how to use the ILOM WebGUI.

The sections include:

- [Section 4.1, “Overview of WebGUI Requirements, Users, Tasks and Features”](#) on page 4-1.
- [Section 4.1.4, “WebGUI Features”](#) on page 4-3
- [Section 4.2, “Logging In and Out of the WebGUI”](#) on page 4-4

4.1 Overview of WebGUI Requirements, Users, Tasks and Features

The graphical user interface (GUI) enables you to monitor and manage local and remote systems. Using a standard Internet browser, you can expect to be up and running the WebGUI in less than five minutes.

One of the most powerful features of ILOM is the ability to redirect the server's graphical console to a remote workstation or laptop system. When you redirect the host console, you can configure the remote system's keyboard and mouse to act as the server's mouse and keyboard. You can also configure the diskette drive or CD-ROM drive on the remote system as a device virtually connected to the Sun server. You can also redirect diskette images (.img) and CD-ROM images (.iso) for remote access.

4.1.1 Browser and Software Requirements

The WebGUI has been tested successfully with recently released Mozilla™, Firefox, and Internet Explorer web browsers, and may be compatible with other web browsers.

The ILOM product comes preinstalled on the Sun server. However, you need Java™ software on the client to perform redirection, as described in [Chapter 8](#).

4.1.2 Users and Privileges

After you log in to the WebGUI, you can perform basic software provisioning, Intelligent Platform Management Interface (IPMI) tasks, and system monitoring.

ILOM user accounts include a role which defines what you can do. The roles are:

- Administrator - Enables access to all ILOM features, functions, and commands.
- Operator - Enables limited access to ILOM features, functions, and commands. Operators cannot change their assigned roles or privileges.

For more information on users, including how to manage user accounts using the WebGUI, see [Chapter 7](#).

4.1.3 WebGUI Tasks

Some of the common tasks you can perform using the WebGUI include:

- Redirect the system's graphical 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 virtual CD-ROM drive.
- Monitor system fans, temperatures, and voltages remotely.
- Monitor BIOS power-on self-test (POST) progress log entries remotely.
- View IPMI log entries, which the operating system can write.
- Examine component information, including CPU information, dynamic random-access memory (DRAM) configuration, host Media Access Control (MAC) addresses, system serial numbers, and other features.
- Manage user accounts remotely.
- Power on, power off, power cycle, and reset the system remotely.
- Administer user accounts.

4.1.4 WebGUI Features

A WebGUI page is shown below.

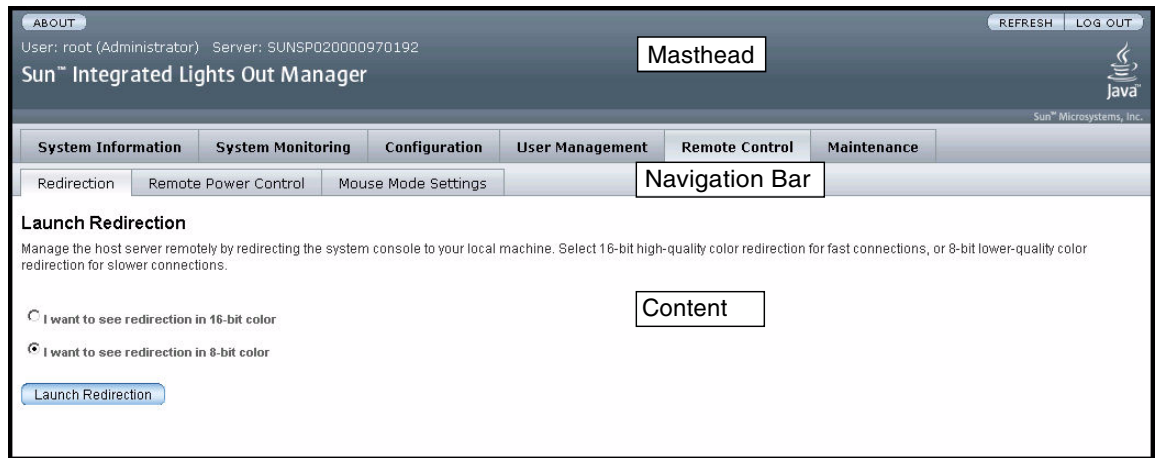


FIGURE 4-1 WebGUI Sample

Each WebGUI page has three main sections: the masthead, the navigation bar, and the content area.

The masthead provides the following buttons and fields on all pages of the WebGUI:

- Refresh button – Click to refresh the information in the content area of the page. The Refresh button does not save new data that you may have entered or selected on the page. Use the Save button that is provided in the content area for a specific WebGUI page.

Note – Do not use the Refresh button from your Internet web browser when you are using the WebGUI.

- Log Out button – Click to end the current session of the WebGUI. You are directed to the logout screen.
- About button – Click to view copyright information.
- User field – Displays the user name of the current user of the WebGUI.
- Server field – Displays the name of the ILOM.

The navigation bar provides tabs that you can click to open a specific WebGUI page. When you click a main tab, subcategories of tabs are displayed, providing you with further options to choose. Select the tabs to open the appropriate WebGUI pages.

The content area of the WebGUI page is where you find information about the specific topic or operation you chose using the tabs. The content area displays such things as logs, status indicators, task wizards, and command buttons to execute an operation.

4.2 Logging In and Out of the WebGUI

This section explains how to log in to and out of the WebGUI.

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

Disabling the use of the browser proxy server (if one is used) for access to the management network might make the WebGUI response time faster.

Note – Do not use the Refresh or Log Out buttons in your Internet web browser when using the WebGUI. Instead, only use the Refresh and Log Out buttons provided at the top right of the WebGUI window.

You need the IP address of the ILOM. The ILOM's IP address is provided in the BIOS Setup screen. You can also observe the DHCP server issue the IP address when the ILOM boots, or look up the ILOM's MAC address-to-IP address mapping in the DHCP server's logs or lease file.

1. **To log in to the WebGUI, type the IP address of the ILOM into your web browser.**

The login screen appears.

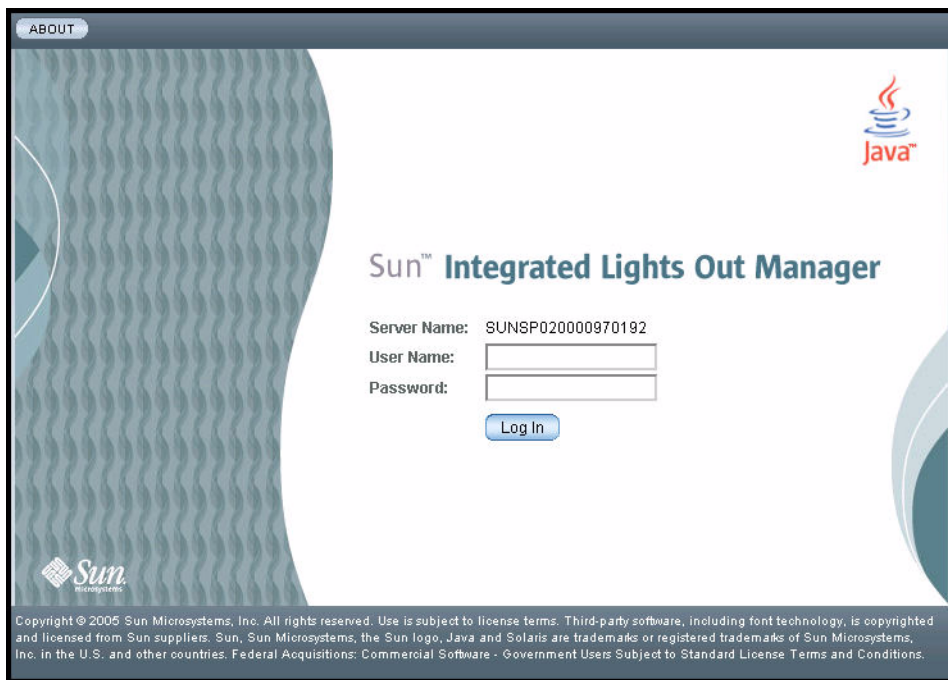


FIGURE 4-2 WebGUI Login Screen

2. Type your user name and password.

When you first try to access the WebGUI, it prompts you to type the default user name and password. The default user name and password are:

- Default user name – root
- Default password – changeme

The default user name and password are in lowercase characters.

One local user ID is predefined with the user name root with the role Administrator. You cannot delete this user ID or change its role attributes. The initial password changeme also is provided. This password is required for log in on the serial port, Secure Shell (SSH), and the WebGUI. To increase secure access to the ILOM, change the default password to a new, unique password. See [Section 5.4, “Viewing Replaceable Component Information”](#) on page 5-6.

3. Click Log In.

The WebGUI appears.

- To log out of the WebGUI, click the Log Out button at the top right of the WebGUI.

The log out screen appears.

Do not use the Log Out button in your web browser to log out from the WebGUI.

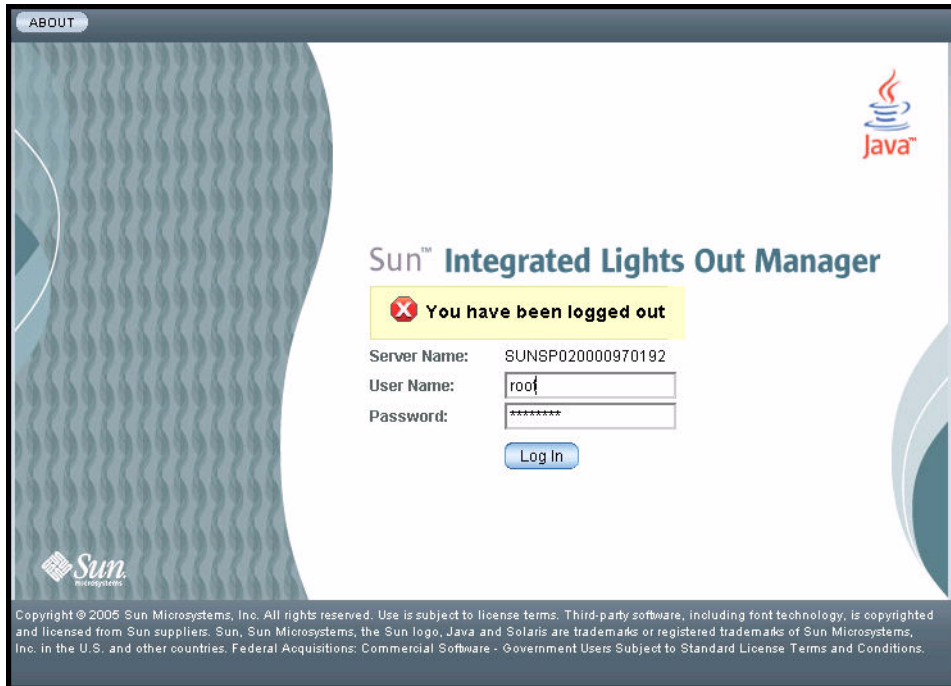


FIGURE 4-3 WebGUI Log Out Screen

System Monitoring and Maintenance Using the WebGUI

This chapter describes how to use the WebGUI to perform monitoring and maintenance.

It includes the following sections:

- [Section 5.1, “Upgrading the ILOM Firmware” on page 5-2.](#)
- [Section 5.2, “Resetting the ILOM” on page 5-5.](#)
- [Section 5.3, “Resetting the ILOM and BIOS Passwords” on page 5-6.](#)
- [Section 5.4, “Viewing Replaceable Component Information” on page 5-6.](#)
- [Section 5.5, “Viewing Temperature, Voltage, and Fan Sensor Readings” on page 5-7.](#)
- [Section 5.6, “Viewing Alert Destinations and Configuring Alerts” on page 5-11.](#)
- [Section 5.7, “Viewing and Clearing the System Event Log” on page 5-15.](#)
- [Section 5.8, “Enabling SNMP Settings and Viewing SNMP Users” on page 5-18.](#)
- [Section 5.9, “Controlling the Server Locator Indicator” on page 5-23.](#)
- [Section 5.10, “Viewing ILOM Hardware, Firmware, and IPMI Versions” on page 5-24](#)
- [Section 5.11, “Viewing Active Connections to the ILOM” on page 5-25](#)

5.1 Upgrading the ILOM Firmware

Both the ILOM and BIOS firmware are tightly coupled and are always updated together. A single firmware image contains both the ILOM and BIOS firmware.



Caution – Ensure that you have reliable power before upgrading your firmware. If power to the system fails (for example, if the wall socket power fails or the system is unplugged) during the firmware update procedure, the ILOM could be left in an unbootable state.

Do not proceed until you have reliable power.



Caution – Shut down your host operating system before proceeding. Otherwise the ILOM will shut the host down ungracefully, which could cause file system corruption.

Note – The upgrade takes about five minutes to complete. During this time, no other tasks can be performed in the ILOM.

To observe the status of the upgrade while it's happening, set the session time-out to 3 hours. See [Section 6.1, “Setting the ILOM Session Time-Out Period” on page 6-1](#) for details.

1. **Log in to the ILOM with administrator privileges.**
2. **Ensure that you can access the new flash image on the client machine that you are using to update the ILOM.**
3. **If the server OS is running, perform a clean shutdown.**
4. **From the Maintenance tab, choose Firmware Upgrade.**

The Upgrade the Firmware page appears.



Caution – Do not close the WebGUI using the Log Out button in the web browser when the ILOM is in Upgrade mode. If you must close the WebGUI, use the WebGUI's Cancel button.

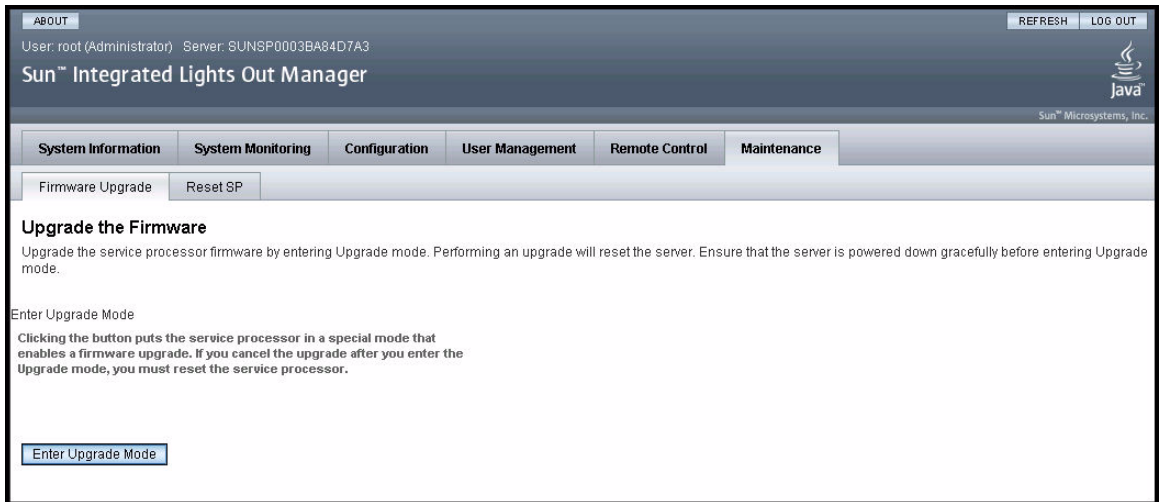


FIGURE 5-1 Upgrade Page

5. Click Enter Upgrade Mode.

A dialog box appears and asks you to confirm that you want to enter Upgrade mode.

6. Click OK to enter Upgrade mode.

The ILOM stops its normal operation and prepares for a flash upgrade.

7. Type the path to the new ILOM flash image file in the Select File to Upload field, or click the Browse button to locate and select the firmware update file (*.ima).

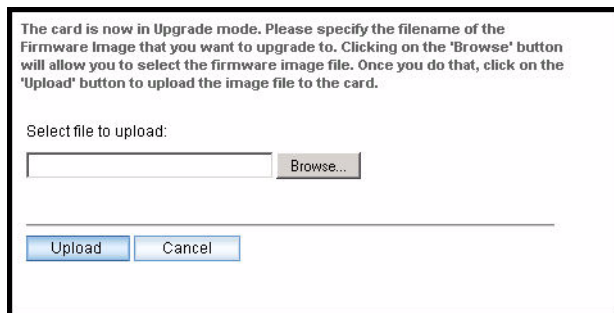


FIGURE 5-2 File Name Dialog

8. Click Upload.

The Upgrade wizard copies the selected file into the ILOM's DRAM and then verifies that the copy procedure was successful. This takes about one minute with a fast network connection.

The system displays a confirmation dialog box.

Note – A network failure during the file upload will result in a time out and the ILOM will reboot with the prior version of the ILOM firmware.

9. In the dialog box, click OK.

The Verify Firmware Image dialog appears.

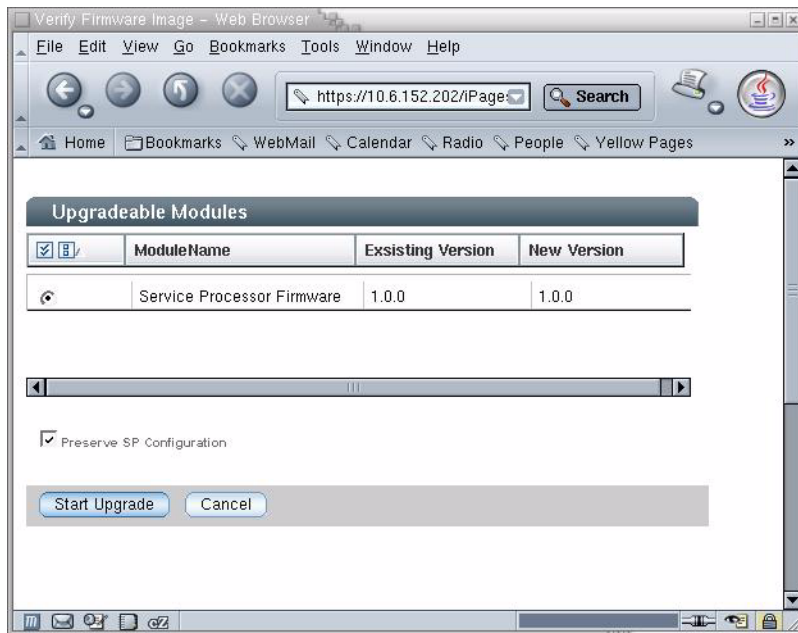


FIGURE 5-3 Verify Firmware Image Dialog

10. Select Preserve Configuration to keep your ILOM settings. Otherwise, they will be overwritten.

- Upgradeable Modules – Select Service Processor Firmware to upgrade the firmware image and BIOS.
- Preserve Configuration – Select this to retain your original configuration settings. Deselect it to overwrite them.

11. Click the Start Upgrade button, or click the Cancel button to stop the upgrade.

Note – If you choose to cancel the firmware upgrade operation, the ILOM will reboot without the updated software. You must close the Internet browser and log back in to the WebGUI before you can perform any other type of operation.

If you clicked Start Update, a progress screen indicates that the firmware image is being upgraded. Once the upgrade progress reaches 100%, the firmware upgrade is complete.

After the upgrade operation has completed successfully, the ILOM will automatically reboot. This is done so that the image upgrade can take effect.

Note – You cannot perform any other operation within your current Internet browser session.

12. Close your Internet browser and reconnect to the ILOM.

Note – If the configuration is not preserved, enter BIOS setup and save the optimal default settings.

5.2 Resetting the ILOM

1. Log in to the ILOM as Administrator or Operator to reach the WebGUI.
2. From the Maintenance tab, choose Reset SP.

The Reset Service Processor page appears.

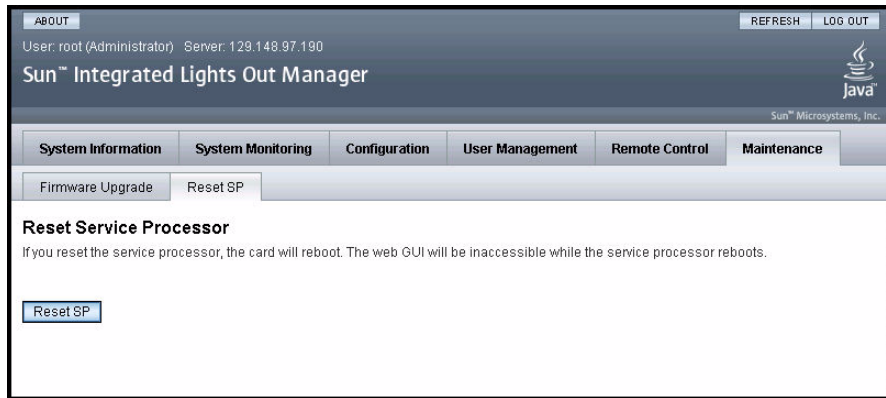


FIGURE 5-4 Reset Service Processor Page

3. Click the **Reset SP** button to reset the ILOM.

The ILOM reboots. The WebGUI is unavailable while the ILOM reboots.

5.3 Resetting the ILOM and BIOS Passwords

This procedure causes the ILOM to reset the administration password and to clear the BIOS password.

- The administration (root) password becomes changeme.
- The BIOS password is cleared, so that when you attempt to access the BIOS, it does not prompt for a password.

This procedure requires changing a hardware jumper in your server enclosure. See your service manual for details.

5.4 Viewing Replaceable Component Information

This section explains how to view detailed information about the Sun server replaceable components, sometimes referred to as field-replaceable units (FRUs) and customer-replaceable units (CRUs).

Depending on the component you select, information about the manufacturer, component name, serial number, and part number might be displayed.

1. Log in to the ILOM as Administrator or Operator to reach the WebGUI.
2. From the System Information tab, select Components.

The Replaceable Component Information page appears.

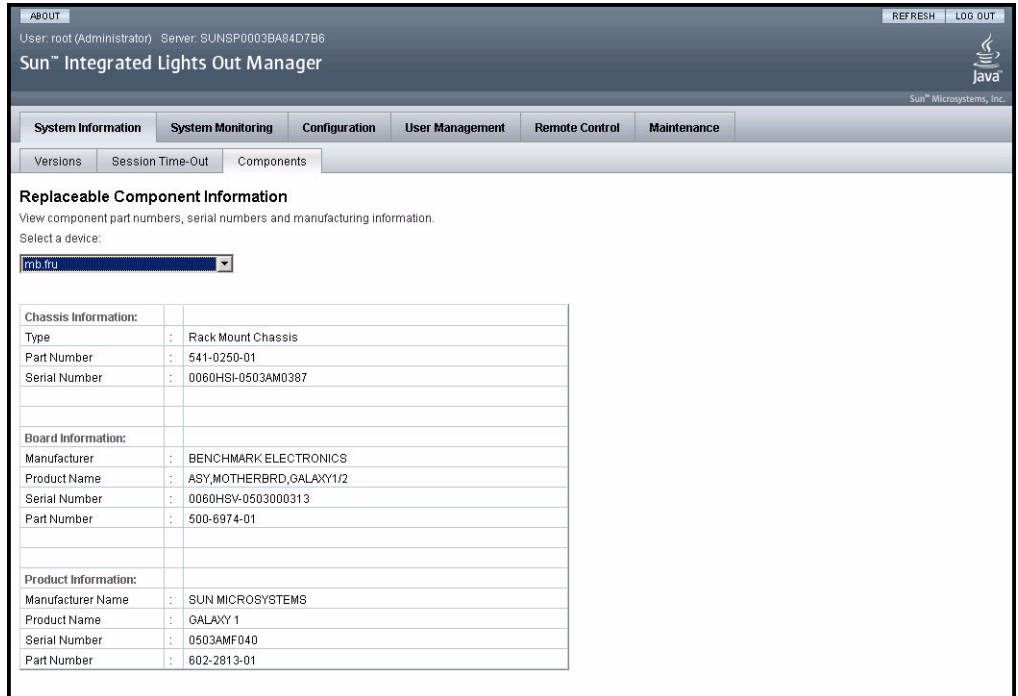


FIGURE 5-5 Sample Replaceable Component Page

3. Select a component from the drop-down list.

Information about the selected component appears.

5.5 Viewing Temperature, Voltage, and Fan Sensor Readings

This section explains how to view the temperature, voltage, and fan sensor readings. For details on individual sensors, see your platform supplement.

The system is equipped with a number of sensors that measure voltages, temperatures, and other settings. ILOM polls the sensors and posts an event in the sensor event log (SEL) when they cross a threshold. Some of these readings are also used to perform actions, such as adjusting fan speeds, illuminating LEDs and powering off the chassis.

If an event crosses a threshold defined in the Alert Destinations view, it generates an alert, which is sent to the destination configured in [Section 5.6, “Viewing Alert Destinations and Configuring Alerts”](#) on page 5-11.

The thresholds appear in the Sensor Readings view shown in [FIGURE 5-6](#).



Caution – The ILOM tags all events or actions with LocalTime=GMT (or UDT). Browser clients show these events in LocalTime. This can cause apparent discrepancies in the event log. When an event occurs on the ILOM, the event log shows it in UDT, but a client would show it local time.

1. **Log in to the ILOM as Administrator or Operator to reach the WebGUI.**
2. **From the System Monitoring tab, choose Sensor Readings.**

Note – The sensor displays in this section are examples. The sensor names, ranges and functions might be different on your system. For details, see your platform supplement.

The Sensor Readings page appears.

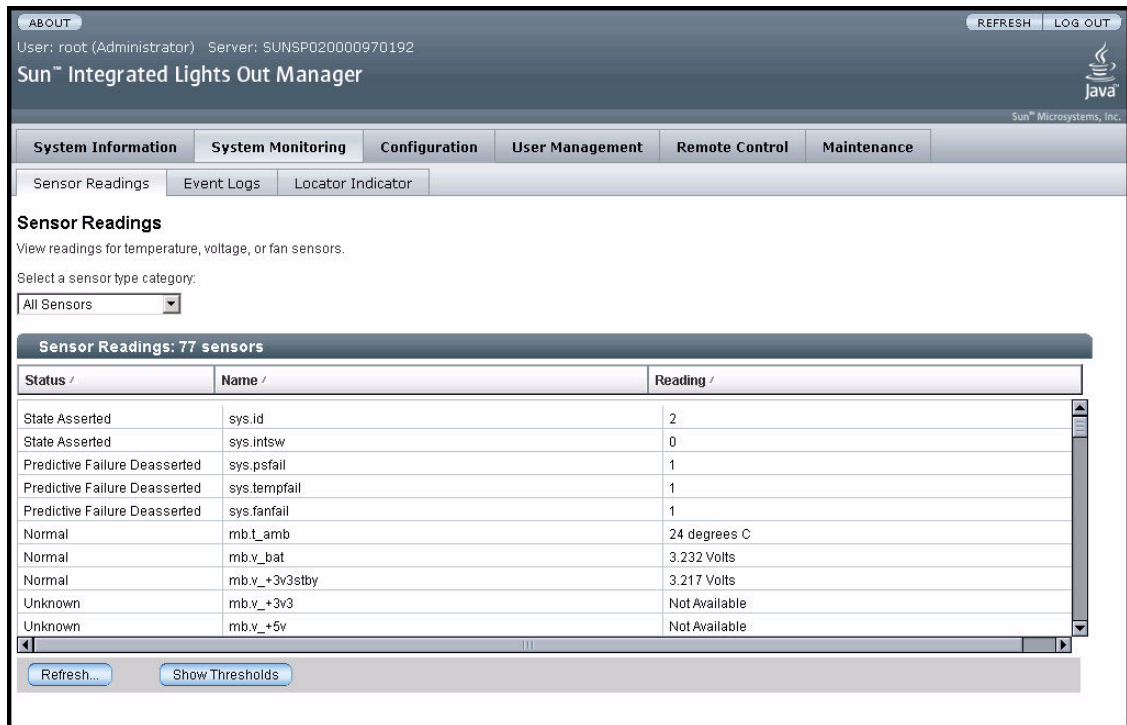


FIGURE 5-6 Sample Sensor Readings Page

3. **Select the type of sensor readings that you want to view from the drop-down list.**
The selections are All Sensors, Temperature Sensors, Voltage Sensors, or Fan Sensors. The WebGUI displays the readings. For details, see your platform supplement.
4. **To sort the data by the values in any column, click the triangle symbol next to the column heading.**
For example, clicking the symbol next to Status sorts the entries by Status. Clicking it again reverses the sort order.



5. **Click the Refresh button to update the sensor readings to their current status.**
6. **Click the Show Thresholds button to display the settings that trigger alerts.**
The WebGUI updates the Sensor Readings table.

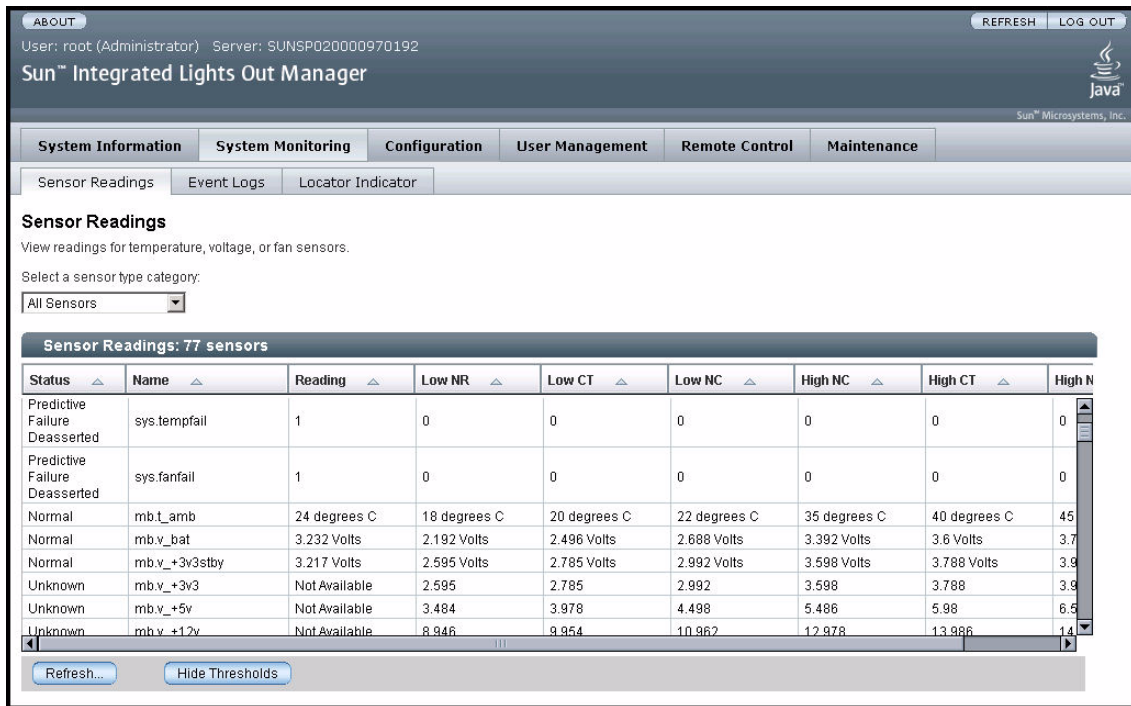


FIGURE 5-7 Sample Updated Sensor Readings With Thresholds

Note – The sensors shown in [FIGURE 5-7](#) are examples only. The actual sensor names, ranges, and functions might be different on your platform. For details, see your platform supplement.

In this example, if the system temperature reaches 35° C, the ILOM will send an alert.

Sensor thresholds include the following:

- Low/High NR – Low or high non-recoverable
- Low/High CT – Low or high critical
- Low/High NC – Low or high non-critical

7. Click the Hide Thresholds button hide the thresholds.

The WebGUI redispays the sensor readings without the thresholds.

5.6 Viewing Alert Destinations and Configuring Alerts

This section explains how to view alert destinations and configure alert settings for the ILOM.

The alert management view allows you to map alert levels to destinations (IP addresses). For example, you can configure it so that all critical alerts are sent to one destination and all non-recoverable alerts are sent to another.

An alert is generated when a sensor crosses the specified threshold. For example, if you configure an alert for critical thresholds, the ILOM sends an IPMI trap to the specified destination when any sensor crosses the upper or lower critical (CT) threshold.

All alerts are IPMI PET traps, as defined in the Intelligent Platform Management Interface (IPMI) v2.0. A special criteria, informational, is reserved for system events that are not related to sensors.

Each line in the alert management view is called a “rule”. Each rule identifies an alert level and sends all alerts at that level to the specified IP address.

Note – Because there are four alert levels and 15 alert rules, you can configure the system to send the same level of alert to multiple destinations.

5.6.1 Viewing Alert Destinations

Users with operator privileges can view the alert settings. Changing them requires administrator privileges.

1. **Log in to the ILOM as Administrator or Operator to reach the WebGUI**

2. From the Configuration tab, choose Alert Management.

The Alert Destinations page appears, displaying a list of alerts.

Alert Destinations

Select a radio button to configure an alert. You can configure up to 15 alerts. Only IPMI Platform Event Traps (PETs) are supported.

Alert Table: 15 entries

Alert #	Alert Level	Destination IP Address
<input checked="" type="radio"/> 1	Disable All	Not Configured
<input type="radio"/> 2	Disable All	Not Configured
<input type="radio"/> 3	Disable All	Not Configured
<input type="radio"/> 4	Disable All	Not Configured
<input type="radio"/> 5	Disable All	Not Configured
<input type="radio"/> 6	Disable All	Not Configured
<input type="radio"/> 7	Disable All	Not Configured
<input type="radio"/> 8	Disable All	Not Configured
<input type="radio"/> 9	Disable All	Not Configured
<input type="radio"/> 10	Disable All	Not Configured
<input type="radio"/> 11	Disable All	Not Configured
<input type="radio"/> 12	Disable All	Not Configured

Edit Send Test Alert

FIGURE 5-8 Alert Destination Page

The alert table includes four columns:

- Radio buttons – Use to select an alert.
- Alert # – The number of the alert rule. A number from 1 to 15.
- Alert Level – Displays the severity level of the alert. Possible levels include:

TABLE 5-1 Alert Levels

Alert Levels	Name in Sensor Readings View	Description
Informational	N/A	This level traps system events that are not related to sensors, such as “The host has booted.”
Warning	NC	The sensor is outside of its normal range but not critical.
Critical	CT	The sensor has crossed a critical threshold.
Non-Recoverable	NR	The sensor has reached a threshold beyond the tolerance level of the corresponding component(s).
Disable All	N/A	Don’t send alerts at this level.

- Destination IP Address – The IP address to which the alert will be sent.

5.6.2 Configuring an Alert

Configuring an alert requires administrator privileges.

To configure an alert:

1. **Select a radio button to select an alert in the table.**
2. **Click the Edit button.**

The Alert dialog box appears.

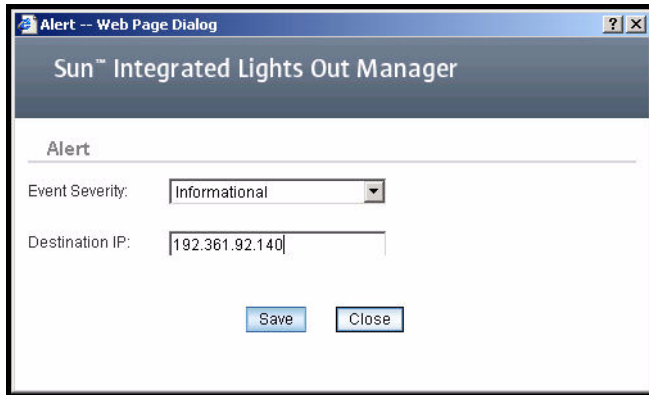


FIGURE 5-9 Alert Dialog Box

3. **Select an event severity from the drop-down list.**
4. **Type the destination IP address for the alert.**
5. **Click the Save button.**

The modified alert appears in the Alert Destinations table.

5.6.3 Sending a Test Alert

This procedure causes the ILOM to send a test alert. It requires administrator privilege.

To send a test alert:

1. **Select a radio button to select an alert in the table.**
2. **Click the Send Test Alert button.**

A confirmation dialog box indicates that the alert was sent to the specified IP address.

3. **Click OK to exit the dialog.**
4. **On the destination machine, verify that the alert was sent successfully.**

5.7 Viewing and Clearing the System Event Log

This section explains how to view and clear the system event log (SEL).

The IPMI system event log provides status information about the Sun server's hardware and software to the ILOM software, which displays the events in the WebGUI. Events are notifications that occur in response to some actions.



Caution – The ILOM tags all events or actions with LocalTime=GMT (or UDT). Browser clients show these events in LocalTime. This can cause apparent discrepancies in the event log. When an event occurs on the ILOM, the event log shows it in UDT, but a client would show it local time.

To view and clear the system event logs:

1. Log in to the ILOM as Administrator or Operator to reach the WebGUI.
2. Select System Monitoring => Event Logs.

The System Event Logs page appears.

The screenshot shows the Sun Integrated Lights Out Manager (ILOM) WebGUI interface. The user is logged in as 'root (Administrator)' on server 'SUNSP020000970192'. The main navigation menu includes System Information, System Monitoring, Configuration, User Management, Remote Control, and Maintenance. Under System Monitoring, there are sub-tabs for Sensor Readings, Event Logs, and Locator Indicator. The 'Event Logs' sub-tab is active, showing the 'System Event Logs' section. Below this, there is a dropdown menu for 'Sensor-Specific Events'. A summary bar indicates 'Event Log: 4 event entries'. The main content is a table with the following data:

Event ID /	Time Stamp /	Sensor Name /	Sensor Type /	Description /
4	12/31/1969 16:01:01	ps1.vinok	Power Supply	State Asserted - Asserted
3	12/31/1969 16:01:01	ps0.prsnt	Entity Presence	Device Removed / Device Absent - Asserted
2	12/31/1969 16:00:57	ps1.prsnt	Entity Presence	Device Inserted / Device Present - Asserted
1	12/31/1969 16:00:56	ps1.pwrok	Power Supply	State Deasserted - Asserted

FIGURE 5-10 System Event Log Page

3. Select an event log category that you want to view from the drop-down list.

You can select from the following types of events:

- Sensor-specific events – Events generated by sensors.
- BIOS-generated events – Error messages generated in the BIOS.
- System management software events – Events that occur within the ILOM software.

After you have selected a category of event, the Event Log table displays the specified events.

The fields in the Event Log table are described below.

Field	Description
Event ID	The number of the event, in sequence from number 1.
Time Stamp	The day and time the event occurred. If the Network Time Protocol (NTP) server is enabled to set the ILOM time, the ILOM clock will use Universal Coordinated Time (UTC)
Sensor Name	The name of a component for which an event was recorded. The sensor name abbreviations correspond to the following components: <ul style="list-style-type: none">• sys – System or chassis• p – Processor• io – I/O board• ps – Power supply• fp – Front panel• ft – Fan tray• mb – Motherboard If there are multiple components, the name is followed by a number. For example p0 represents processor 0.
Sensor Type	The type of sensor for the specified event.
Description	A description of the event.

4. To clear the event log, click the Clear Event Log button.

A confirmation dialog box appears.

5. Click OK to clear all entries in the log.

5.7.1 Interpreting the System Event Log (SEL) Time Stamps

The SEL time stamps are related to the ILOM clock settings. If the clock settings change, the change is reflected in the time stamps.

When the ILOM reboots, the ILOM clock is set to Thu Jan 1 00:00:00 UTC 1970. The ILOM reboots as a result of the following:

- A complete system unplug/replug power cycle
- An IPMI command; for example, mc reset cold
- A command-line interface (CLI) command; for example, reset /SP
- WebGUI operation; for example, selecting Reset SP from the Maintenance tab
- An ILOM firmware upgrade

Note – Log event timestamps might appear different between host and client systems because of time zone adjustment.

The timestamps on events reported in the server's system event log and IPMI logs are always based on GMT/UTC. However, when you view system information from a client system using the GUI or IPMITool, the timestamps displayed are adjusted based on the time zone of the client system. Therefore, the same event can appear to have two different timestamps when viewed directly from the host and from a client system in a different time zone.

After an ILOM reboot, the ILOM clock is changed by the following:

- When the host is booted – The host's BIOS unconditionally sets the ILOM time to that indicated by the host's RTC. The host's RTC is set by the following operations:
 - When the host's CMOS is cleared as a result of changing the host's RTC battery or inserting the CMOS-clear jumper on the motherboard. The host's RTC starts at Jan 1 00:01:00 2002.
 - When the host's operating system sets the host's RTC. The BIOS does not consider time zones. Solaris and Linux software respect time zones and will set the system clock to UTC. Therefore, after the OS adjusts the RTC, the time set by the BIOS will be UTC. Microsoft Windows software does not respect time zones and sets the system clock to local time. Therefore, after the OS adjusts the RTC, the time set by the BIOS will be local time.
- When the users sets the RTC using the host BIOS Setup screen.

- Continuously by NTP if NTP is enabled on the ILOM – NTP jumping is enabled to recover quickly from an erroneous update from the BIOS or user. NTP servers provide UTC time. Therefore, if NTP is enabled on the ILOM, the ILOM clock will be in UTC.
- Through the CLI, WebGUI and IPMI.

To set the ILOM clock, see [Section 6.3, “Setting the ILOM Clock” on page 6-4](#).

5.8 Enabling SNMP Settings and Viewing SNMP Users

This section explains how to enable monitoring and management of the Sun server using the Simple Network Management Protocol (SNMP). The Sun server supports SNMP versions 1, 2c, and 3. SNMP v3, which is the preferred version to use for secure operations, is enabled by default. The ILOM has a preinstalled SNMP agent that enables you to manage the server using the ILOM. You can use any management application that supports SNMP to manage the Sun server.

SNMP is used to access and manipulate Management Information Base (MIB) files on the target agent. For more information about SNMP and the classes of MIB files that the Sun server supports, see [Section 11.1, “About SNMP” on page 11-1](#).

5.8.1 Configuring SNMP Settings

- 1. Log in to the ILOM as Administrator to reach the WebGUI.**

Only accounts with administrator privileges are enabled to modify SNMP settings.

- 2. From the Configuration tab, select System Management Access, and then select SNMP.**

The SNMP Settings page appears.

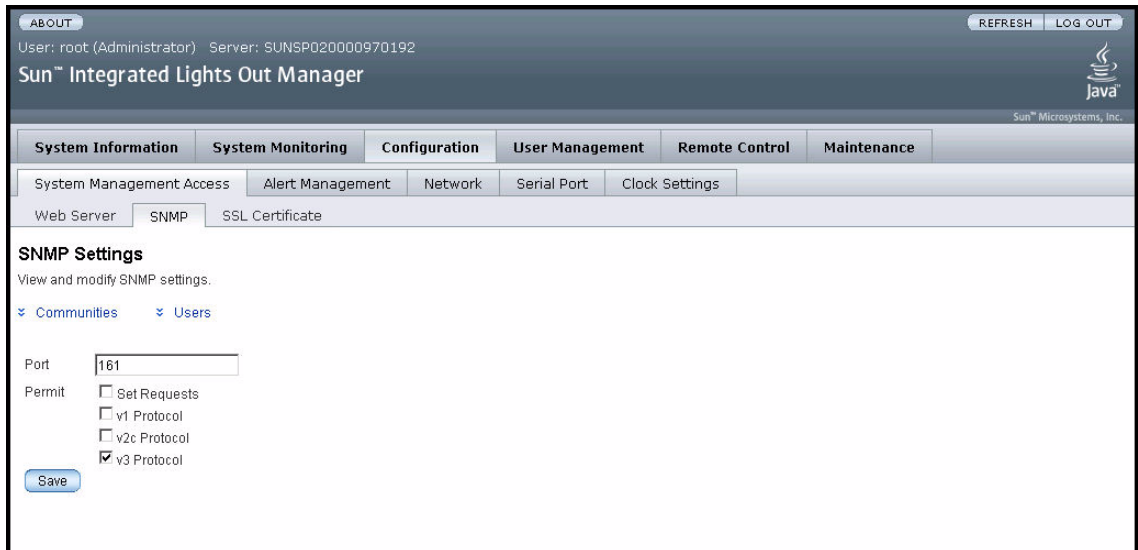


FIGURE 5-11 SNMP Settings

- 3. Type the port number in the Port field.**
- 4. Enable or disable Set Requests by clicking the Set Requests checkbox.**
If sets are disabled, all SNMP objects are read only.
- 5. If disabled, everything defaults to read**
- 6. If you want to permit SNMP set requests, select the Set Requests check box.**
- 7. Select a check box to enable SNMP v1, v2c, or v3.**
SNMP v3 is enabled by default. You can independently enable or disable v1, v2c, and v3 protocol versions.
- 8. Click the Save button for your settings to take effect.**
- 9. At the bottom of the page, you can also add, edit, or delete SNMP communities, as well as SNMP users. See [FIGURE 5-12](#).**

SNMP Communities

	Community Name	Permission
<input type="radio"/>	asdfasdfasdf	ro
<input type="radio"/>	paris	ro
<input type="radio"/>	private	rw
<input type="radio"/>	public	ro

[↩ Back to top](#)

SNMP Users

	User Name	Authentication Protocol	Permission	Privacy Protocol
<input type="radio"/>	alice	MD5	ro	DES
<input type="radio"/>	dougt	MD5	ro	none
<input type="radio"/>	dougt2	MD5	rw	DES
<input type="radio"/>	michelle	SHA	ro	none
<input type="radio"/>	surfboards	SHA	ro	none
<input type="radio"/>	testuser	MD5	rw	none

[↩ Back to top](#)

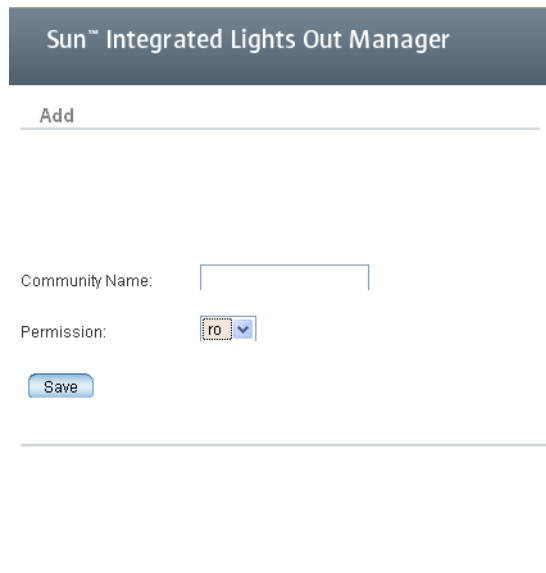
FIGURE 5-12 SNMP Communities and Users

5.8.2 Adding, Editing and Deleting SNMP Communities

To add an SNMP community:

1. Click the **Communities** link, or scroll down to the **Communities** list.
2. Click the **Add** button under the **SNMP Communities** list.

The Add dialog box appears.



The screenshot shows a web-based dialog box titled "Sun™ Integrated Lights Out Manager" with a subtitle "Add". Below the subtitle is a horizontal line. The main content area contains a "Community Name:" label followed by a text input field. Below that is a "Permission:" label followed by a dropdown menu showing "ro" with a downward arrow. At the bottom left of the form is a "Save" button. A horizontal line is at the bottom of the dialog box.

FIGURE 5-13 Add Community Dialog Box

3. Type the name in Community Name field.

The name can contain up to 35 characters. It must start with an alphabetic character and cannot contain a space.

4. Select either read-only (ro) or read-write (rw) permissions.

5. Click the Save button.

To edit an SNMP community:

1. Click the Communities link, or scroll down to the Communities list.

2. Select the radio button of the SNMP community to edit.

3. Click the Edit button under the SNMP Communities list.

The Edit dialog box appears.

4. Select either read-only (ro) or read-write (rw) permissions.

5. Click the Save button.

To delete an SNMP community

1. Click the Communities link, or scroll down to the Communities list.

2. **Select the radio button of the SNMP community to be deleted.**
3. **Click the Delete button under the SNMP Communities list.**
A confirmation dialog box appears.
4. **Click OK to delete the SNMP community.**

5.8.3 Adding, Modifying and Deleting SNMP Users

To add an SNMP User:

1. **Click the Users link or scroll down to the Users list.**

1. **Click the Add button under the SNMP Users list.**

The Add dialog box appears.

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

The name can include up to 35 characters. It must start with an alphabetic character and cannot contain a space.

3. **Select either Message Digest 5 (MD5) or Secure Hash Algorithm (SHA).**

4. **Type in an authentication password.**

The authentication password must contain 8 to 16 characters, with no colon or space characters. It is case sensitive.

5. **Type it again in the Confirm Password field.**

6. **Select either read-only (ro) or read-write (rw) permissions.**

7. **Select either DES or none for a privacy protocol.**

8. **Type in a privacy password.**

The privacy password must contain 8 to 16 characters, with no colon or space characters. It is case sensitive.

9. **Type it again in the Confirm Password field.**

10. **Click the Save button.**

To edit an SNMP User:

1. **Click the Users link or scroll down to the Users list.**

2. **Select the radio button of the SNMP user to be edited.**

3. **Click the Edit button under the SNMP Users list.**

The Edit dialog box appears.

4. **Select either Message Digest 5 (MD5) or Secure Hash Algorithm (SHA).**
5. **Type in an authentication password.**

The authentication password must contain 8 to 16 characters, with no colon or space characters. It is case sensitive.
6. **Type it again in the Confirm Password field.**
7. **Select either read-only (ro) or read-write (rw) permissions.**
8. **Select either DES or none for a privacy protocol.**
9. **Type in a privacy password.**

The privacy password must contain 8 to 16 characters, with no colon or space characters. It is case sensitive.
10. **Type it again in the Confirm Password field.**
11. **Click the Save button.**

To delete an SNMP user

 1. **Click the Users link, or scroll down to the Users list.**
 2. **Select the radio button of the SNMP user to be deleted.**
 3. **Click the Delete button under the SNMP Users list.**

A confirmation dialog box appears.
 4. **Click OK to delete the SNMP user.**

5.9 Controlling the Server Locator Indicator

This section explains how to turn the Locator indicator on the Sun server on and off.

Note – Your platform might have a Server Locator Indicator. Check your platform supplement.

The Server Locator Indicator is a pair of small lights that you turn on to help you identify a specific server among many in a data center. One light is positioned on the front of the server in the upper left corner, and the other is on the back of the server in the upper center section.

1. **Log in to the ILOM as Administrator or Operator to reach the WebGUI.**

2. From the System Monitoring tab, select Locator Indicator.

The Locator Indicator page appears.

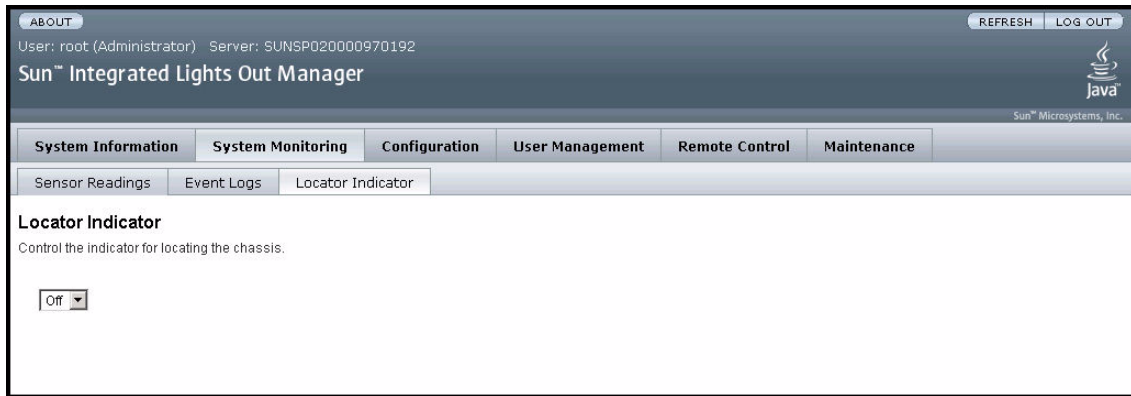


FIGURE 5-14 Locator Indicator Page

3. To turn the Locator indicator on and off, use the drop-down list.

The Locator indicator is either illuminated or turned off, according to your selection.

5.10 Viewing ILOM Hardware, Firmware, and IPMI Versions

This section explains how to view the ILOM hardware and firmware revisions, as well as the Intelligent Platform Management Interface (IPMI) version.

1. Log in to the ILOM as Administrator or Operator to reach the WebGUI.
2. From the System Information tab, select Versions.

The Version Information page appears (see [FIGURE 5-15](#)). This page displays the ILOM hardware and software revisions, and the IPMI version.

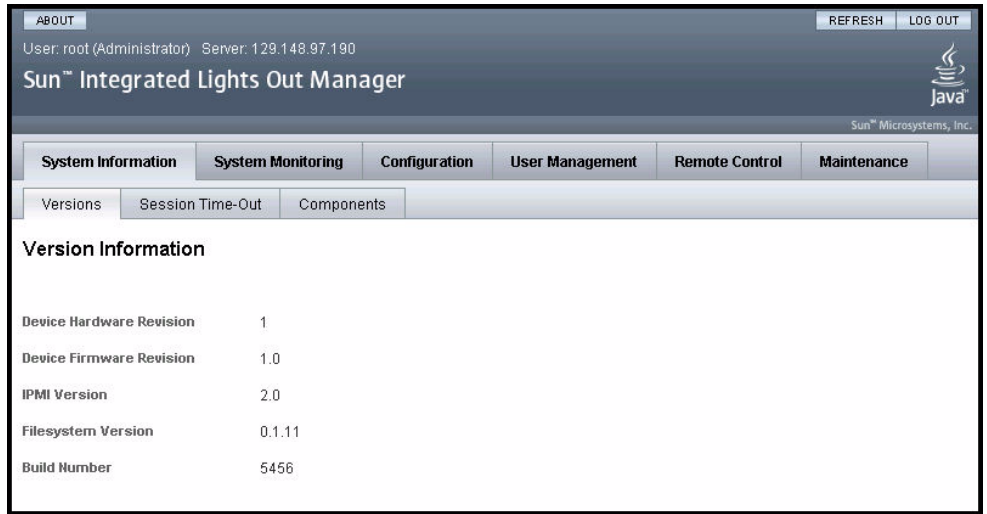


FIGURE 5-15 Version Information Page

5.11 Viewing Active Connections to the ILOM

This section explains how to view all active connections to the ILOM.


1. **Log in to the ILOM as Administrator or Operator to reach the WebGUI.**
2. **From the User Management tab, select Active Sessions.**

The Active Sessions page appears. You can find the user name, the date and time that the user initiated the session, and the type of session(web or command shell).

ABOUT REFRESH LOG OUT

User: root (Administrator) Server: SUNSP020000970192

Sun™ Integrated Lights Out Manager

Sun™ Microsystems, Inc. 

System Information System Monitoring Configuration **User Management** Remote Control Maintenance

User Accounts Active Sessions LDAP Settings

Active Sessions

View the users currently logged in to the service processor.

Active Sessions		
User Name /	Start Time /	Type /
root	Thu Jan 1 01:01:37 1970	web

FIGURE 5-16 Active Sessions Page

System Configuration Using the WebGUI

This chapter describes how to do system configuration using the WebGUI.

It includes the following sections:

- [Section 6.1, “Setting the ILOM Session Time-Out Period” on page 6-1.](#)
- [Section 6.2, “Configuring the ILOM Serial Port” on page 6-2.](#)
- [Section 6.3, “Setting the ILOM Clock” on page 6-4.](#)
- [Section 6.4, “Configuring Network Settings” on page 6-6.](#)
- [Section 6.5, “Uploading a New SSL Certificate” on page 6-8.](#)
- [Section 6.6, “Enabling HTTP or HTTPS Web Access” on page 6-10.](#)

6.1 Setting the ILOM Session Time-Out Period

This section explains how to set the time-out period for your ILOM session. Once you set the time-out period, if your session is inactive for that amount of time, you will be automatically logged out of the session.

- 1. Log in to the ILOM as Administrator or Operator to reach the WebGUI.**
- 2. From the System Information tab, select Session Time-Out.**

The Session Time-out page appears.

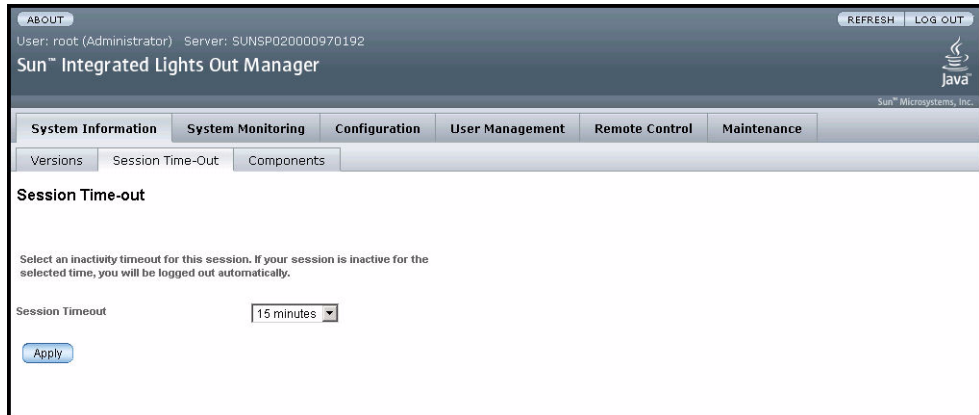


FIGURE 6-1 Session Time-Out Page

3. From the drop-down list, select the amount of time for the session time-out period.
4. Click the Apply button.
A confirmation dialog box appears.
5. Click OK in the dialog box.

The session time-out period is set to the selected amount of time. If you exceed the amount of time set for your session, you are automatically logged out of the WebGUI.

6.2 Configuring the ILOM Serial Port

This section explains how to configure the ILOM serial port. Use this procedure only when you need to change the serial port default settings, which are 9600 baud and no flow control.

The serial port provides access to the WebGUI, the command-line interface (CLI), and to the system console stream using serial port redirection.

- The internal serial port is the connection between the host server and the ILOM that allows an ILOM user to access the host serial console. The ILOM internal serial port speed must match the speed of the serial console port on the host server, often referred to as serial port 0, COM1, or `/dev/ttyS0`.

- The external serial port is the RJ-45 serial port on the ILOM. Typically the internal and external serial port connections should run at the same speed to avoid flow control issues when connecting to the host console from the ILOM external serial port.

1. **Log in to the ILOM as Administrator to reach the WebGUI.**
2. **From the Configuration tab, select Serial Port.**

The Serial Port Settings page appears.

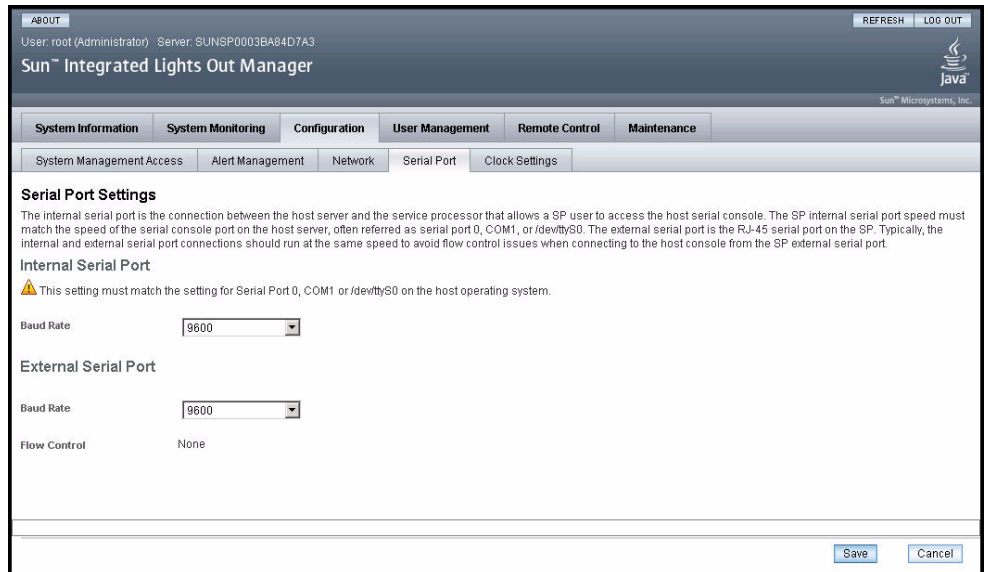


FIGURE 6-2 Serial Port Settings Page

3. **Select the baud rate for the internal serial port using the Internal Serial Port drop-down list.**

This setting must match the setting for serial port 0, COM1 or /dev/ttyS0 on the host operating system.

The baud rate value must match the speed that was specified for the BIOS serial redirection feature (default is 9600 baud) and the speed used for the boot loader and operating system configuration.

4. **Select the baud rate for the external serial port using the External Serial Port drop-down list.**

This setting must match the baud rate on the RJ-45 serial port on the Sun server.

5. **Click the Save button for your changes to take effect, or click the Cancel button to return to the previous settings.**

6.3 Setting the ILOM Clock

This section explains how to set the ILOM clock manually or to synchronize the ILOM date and time with a Network Time Protocol (NTP) server.

The ILOM clock is described in [Section 5.7.1, “Interpreting the System Event Log \(SEL\) Time Stamps”](#) on page 5-17.

Before you begin, obtain IP addresses of the NTP servers you want to use.

6.3.1 Setting the ILOM Clock Manually

1. Log in to the ILOM as Administrator to reach the WebGUI.
2. From the Configuration tab, select Clock Settings.

The Clock Settings page appears.

The screenshot shows the Sun Integrated Lights Out Manager (ILOM) web interface. At the top, there is a header with "ABOUT" on the left, "REFRESH" and "LOG OUT" on the right, and the user information "User: root (Administrator) Server: 129.148.97.190". The main title is "Sun™ Integrated Lights Out Manager" with the Java logo and "Sun™ Microsystems, Inc." below it. A navigation bar contains tabs for "System Information", "System Monitoring", "Configuration", "User Management", "Remote Control", and "Maintenance". Under the "Configuration" tab, there are sub-tabs for "System Management Access", "Alert Management", "Network", "Serial Port", and "Clock Settings". The "Clock Settings" sub-tab is active, showing the "Clock Settings" section. Below the title, there is a paragraph: "To set the service processor clock manually, type the date in the format mm/dd/yyyy, then select the hour and minute. To synchronize the service processor clock with an NTP server, select the Enable check box, then type the IP addresses of the NTP servers to use." The form includes a "Date" field with the value "9/14/1970", a "Time" field with "15" and "36" in dropdown menus, a "Synchronize Time Using NTP:" section with an unchecked "Enable" checkbox, and two text input fields for "Primary Time Server:" and "Secondary Time Server:", both containing the value "none". A "Save" button is located at the bottom left of the form.

FIGURE 6-3 Clock Settings Page

3. **Type a date in the Date text box.**
Type the date in the format mm/dd/yyyy.
4. **Set the hour and minute using the drop-down lists.**
5. **Click the Save button for your changes to take effect.**

6.3.2 Synchronizing the ILOM Clock with an NTP Server:

1. **Log in to the ILOM as Administrator to reach the WebGUI.**
2. **From the Configuration tab, select Clock Settings.**
The Clock Settings page appears. See [FIGURE 6-3](#).
3. **Click the Enable check box next to Synchronize Time Using NTP.**
4. **Type the IP addresses of the NTP servers you want to use.**
5. **Click the Save button for your changes to take effect.**

6.3.3 Interpreting ILOM Clock Settings

When the ILOM reboots, the ILOM clock is set to Thu Jan 1 00:00:00 UTC 1970. The ILOM reboots as a result of the following:

- A complete system unplug/replug power cycle
- An IPMI command; for example, mc reset cold
- A command-line interface (CLI) command; for example, reset /SP
- WebGUI operation; for example, from the Maintenance tab, select Reset SP
- An ILOM firmware upgrade

Note – Log event timestamps might appear different between host and client systems because of time zone adjustment.

The timestamps on events reported in the server's system event log and IPMI logs are always based on GMT/UTC. However, when you view system information from a client system using the GUI or IPMITool, the timestamps displayed are adjusted based on the time zone of the client system. Therefore, the same event can appear to have two different timestamps when viewed directly from the host and from a client system in a different time zone.

After an ILOM reboot, the ILOM clock is changed by the following:

- When the host is booted – The host’s BIOS unconditionally sets the ILOM time to that indicated by the host’s RTC. The host’s RTC is set by the following operations:
 - When the host’s CMOS is cleared as a result of changing the host’s RTC battery or inserting the CMOS-clear jumper on the motherboard. The host’s RTC starts at Jan 1 00:01:00 2002.
 - When the host’s operating system sets the host’s RTC. The BIOS does not consider time zones. Solaris and Linux software respect time zones and will set the system clock to UTC. Therefore, after the OS adjusts the RTC, the time set by the BIOS will be UTC. Microsoft Windows software does not respect time zones and sets the system clock to local time. Therefore, after the OS adjusts the RTC, the time set by the BIOS will be local time.
 - When the user sets the RTC using the host BIOS Setup screen.
- Continuously through NTP if NTP is enabled on the ILOM - NTP jumping is enabled to recover quickly from an erroneous update from the BIOS or user. NTP servers provide UTC time. Therefore, if NTP is enabled on the ILOM, the ILOM clock will be in UTC.
- Through the CLI, WebGUI, and IPMI

6.4 Configuring Network Settings

This section explains how to configure the network parameters for the ILOM.

The ILOM automatically configures its IP settings using the Dynamic Host Configuration Protocol (DHCP). If your network does not support this protocol, you need to set the parameters manually.

- 1. Log in to the ILOM as Administrator to reach the WebGUI.**
- 2. From the Configuration tab, select Network.**

The Network Settings page appears.

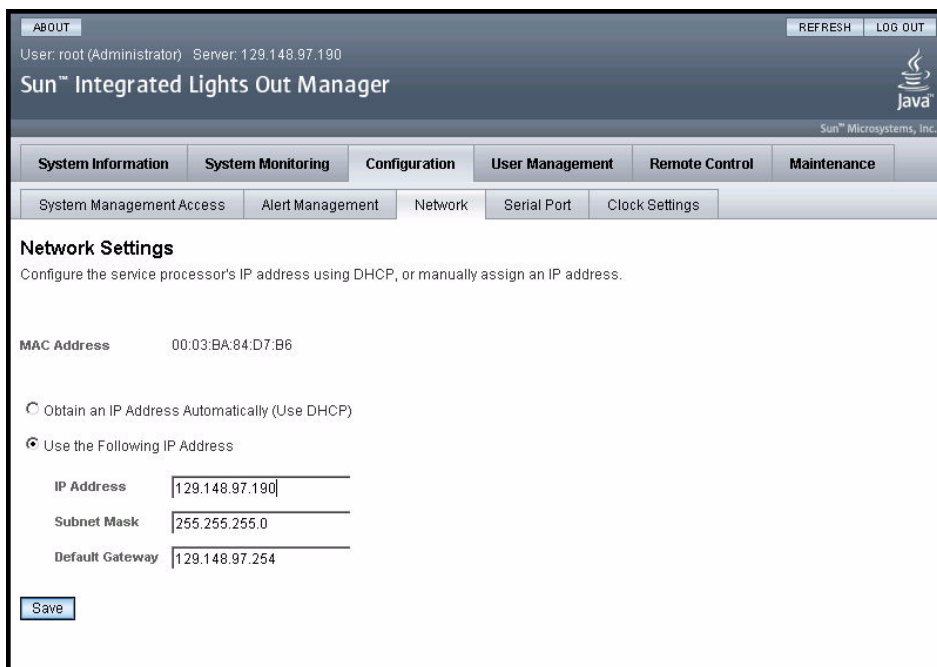


FIGURE 6-4 Network Settings Page

3. Complete the information in the Network Settings page.

Use the descriptions in [TABLE 6-1](#) when completing the information.

TABLE 6-1 Network Settings Page Fields

Item	Description
MAC Address	The ILOM's media access control (MAC) address is set at the factory. The MAC address is a hardware address that is unique to each networked device. The ILOM's MAC address is provided on a label on the ILOM, on the Customer Information Sheet included on the ship kit, and in the BIOS Setup screen.
Configuration Method	Select one of the following radio buttons to configure the ILOM's IP address either dynamically or statically. <ul style="list-style-type: none"> Obtain an IP Address Automatically (Use DHCP) – Enables a DHCP server to configure the ILOM's IP address dynamically. Use the Following IP Address – Enables you to configure the ILOM's IP address with a static IP. The IP Address, Subnet Mask, and Default Gateway fields will become editable when you select this option.

TABLE 6-1 Network Settings Page Fields

Item	Description
IP Address	Type the ILOM's IP address. The IP address is a unique name that identifies the system on a TCP/IP network.
Subnet Mask	Type the subnet mask of the network on which the ILOM resides.
Default Gateway	Type the ILOM's gateway access address.

4. Click the Save button for your settings to take effect.

Settings are considered pending until you click the Save button. Changing the IP address will end your ILOM session.

You are prompted to close your Internet browser.

5. Log back in to the ILOM using the new IP address.

Note – If you changed the network settings, you must log back in with a new browser session.

6.5 Uploading a New SSL Certificate

This section explains how to upload a Secure Sockets Layer (SSL) certificate and SSL private key to use when accessing the ILOM.

To establish a secure HTTPS connection to the ILOM, you must upload an SSL certificate and a private key into the ILOM. These two together help provide a secure connection to the correct server when using HTTPS. Ensure that the uploaded SSL certificate and private key match. If they do not match, secure access may not work properly.

1. Log in to the ILOM as Administrator to reach the WebGUI.

2. From the Configuration tab, select System Management Access, then select SSL Certificate.

The SSL Certificate Upload page appears.

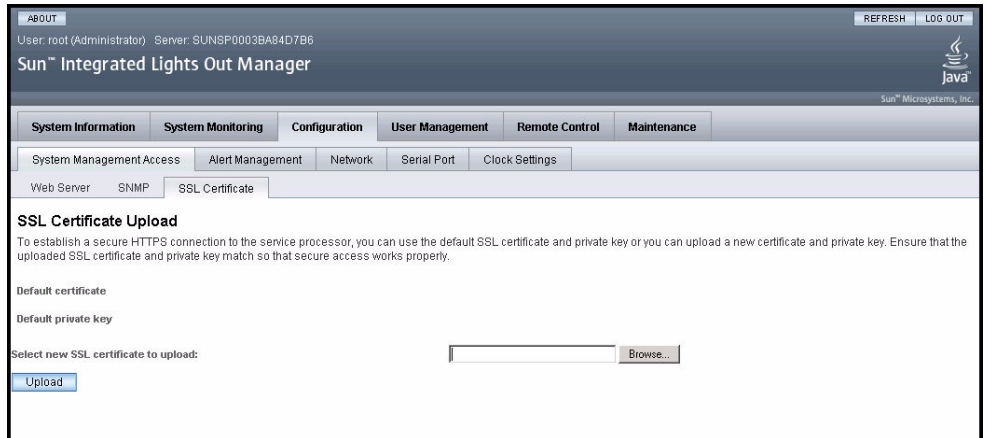


FIGURE 6-5 SSL Certificate Upload Page

3. **Type the file name of the new SSL certificate or click the Browse button to search for a new SSL certificate.**

The file name has a `.pem` file extension. The ILOM does not support pass-phrase encrypted certificates.

4. **Click the Upload button to upload the selected SSL certificate.**

The SSL Certificate Upload Status dialog appears.

5. **Once you have uploaded the certificate and private key, click the OK button to reset the ILOM immediately, or click the Cancel button to reset the ILOM later.**

The ILOM must be reset for the new certificate to take effect. If you click OK, you must close your Internet browser and reconnect to the ILOM. HTTPS is enabled by default.

You can now access the ILOM securely using the following format in your IP Address field from your Internet browser:

```
https://<ILOM IP address>
```

For example, if the ILOM's IP address is 192.168.0.30, type the following:

```
https://192.168.0.30
```

Note – Ensure that you include the "s" after **http**.

6.6 Enabling HTTP or HTTPS Web Access

This section explains how to view and modify web server settings. Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) enable you to retrieve hypertext messages from client to server and server to client. Both protocols are based on the Transmission Control Protocol/Internet Protocol (TCP/IP). HTTPS is an extension of HTTP that uses Secure Sockets Layer (SSL) to enable secure transmissions over a TCP/IP network. HTTPS is enabled by default.

1. **Log in to the ILOM as Administrator to reach the WebGUI.**
2. **From the Configuration tab, select System Management Access, then select Web Server.**

The Web Server Settings page appears.

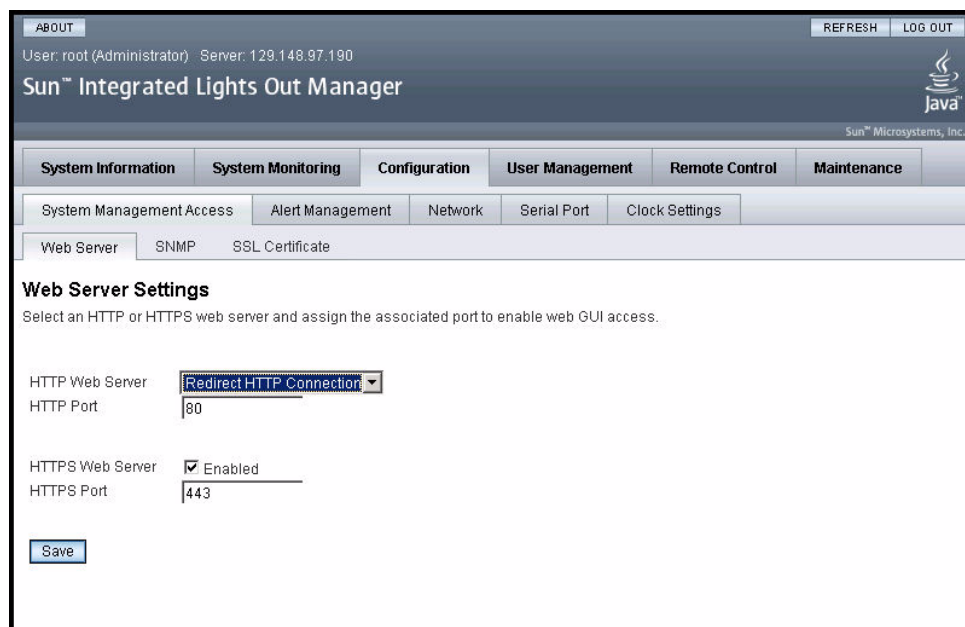


FIGURE 6-6 Web Server Settings Page

3. **Select the HTTP or HTTPS web server.**
 - To select an HTTP web server – Select Enabled from the drop-down list. You can also select:
 - Redirect HTTP Connection to HTTPS. HTTP connections are automatically redirected to HTTPS.

- Disabled - Turn HTTP off.
 - To select an HTTPS web server – Select the HTTPS Web Server Enabled check box. The HTTPS web server is enabled by default.
- 4. Assign an HTTP or HTTPS port number.**
 - 5. Click the Save button for your settings to take effect.**

Managing Users Using the WebGUI

This chapter describes how to do manage users using the WebGUI. It includes the following sections:

- [Section 7.1, “Managing User Accounts” on page 7-1.](#)
- [Section 7.2, “Viewing and Modifying Lightweight Directory Access Protocol Settings” on page 7-8.](#)

Note – You can also add users with the Command Line Interface (CLI), as described in [Section 3.7, “Managing User Accounts” on page 3-13.](#)

7.1 Managing User Accounts

This section explains how to add, modify and delete ILOM user accounts.

The ILOM supports up to 10 user accounts, Two of those, root and anonymous, are set by default and cannot be removed. Therefore, you can configure eight additional accounts.

Each account has an associated user name, password, and role. The roles include Administrator, which provides access to all ILOM functionality and commands, and Operator, which provides limited access to the ILOM functionality and commands. Operator and Administrator roles can be assigned separately for network and serial use.



Caution – The ILOM includes a user account "sunservices," which shares the ILOM root password. Normally, it is used exclusively by Sun Service personnel; however it can also be used to perform recovery procedures documented in the product notes. Incorrect use of this account can corrupt the service processor image or operations.

7.1.1 Adding User Roles and Setting Privileges

Each user account consists of a user name, a password, and assigned network and serial roles.

The roles include:

- Administrator – Enables access to all ILOM features, functions, and commands.
- Operator – Enables limited access to ILOM features, functions, and commands. Operators cannot change their assigned roles.

The GUI includes a Network Privilege and a Serial Privilege selection.

- Network Privilege assigns the user to a role.
- Serial Privilege is unused.

1. Log in to the ILOM as Administrator to reach the WebGUI.

Only accounts with Administrator privileges are allowed to add, modify, or delete user accounts.

If a new user is given Administrator privileges, those privileges are also automatically granted for the command-line interface (CLI) and Intelligent Platform Management Interface (IPMI) to the ILOM.

2. From the User Management tab, select User Accounts.

The User Accounts page appears.

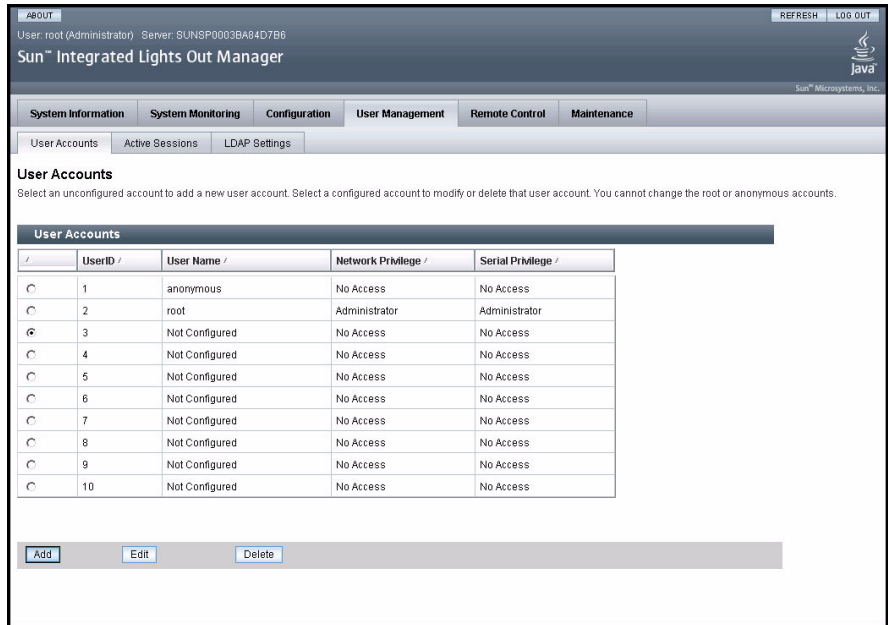


FIGURE 7-1 User Accounts Page

3. Select a radio button next to a user account identified as Not Configured.

If all 10 user account slots are configured, you must delete an existing user account before you can add a new user account. See [Section 7.1.3, “Deleting a User Account” on page 7-7](#).

4. Click the Add button.

The Add User dialog box appears.

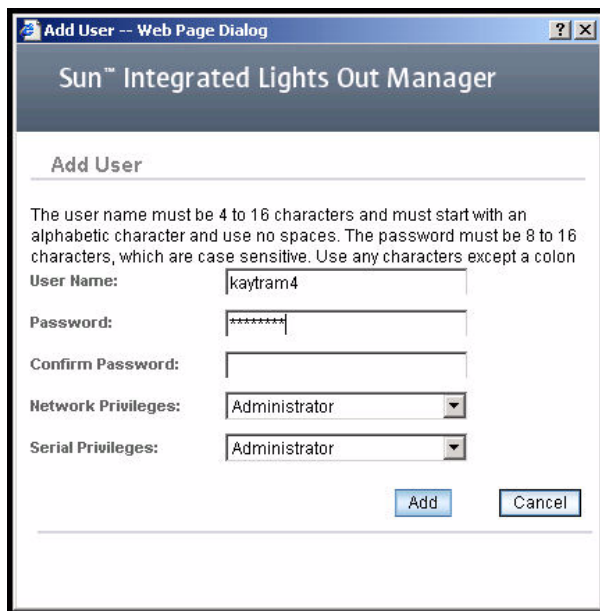


FIGURE 7-2 Add User Dialog Box

5. 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 16 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 confirm the password.

d. Assign network and serial privileges by selecting either Administrator or Operator in each field.

e. When you are done entering the new user's information, click Add.

The User Accounts page is redisplayed. The new user account and associated information is listed on the User Accounts page.

7.1.2 Modifying an ILOM User Account

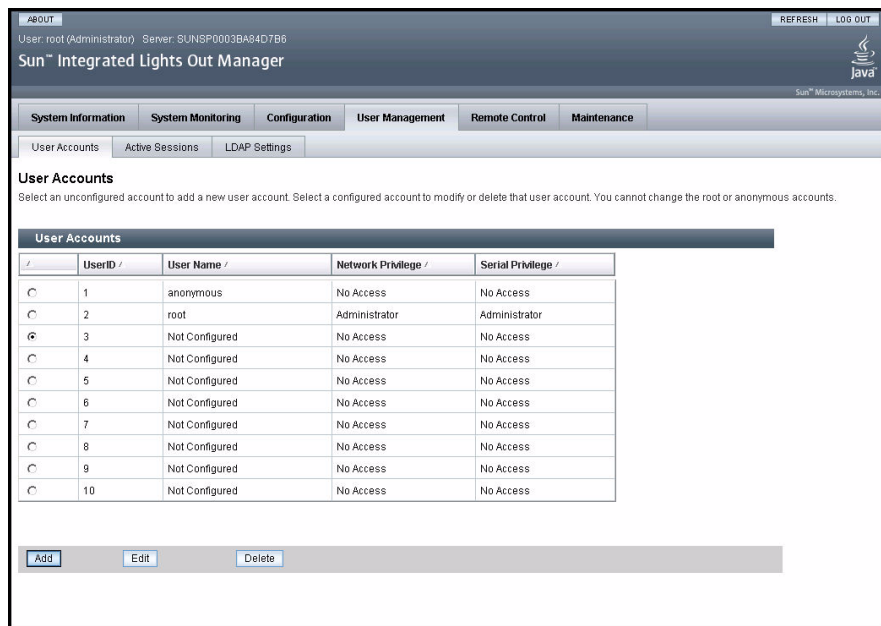
This section explains how to modify an ILOM user account. Modifying a user account can change the user's password, and their network and serial privileges.

Note – Only accounts with Administrator privileges are enabled to add, modify, or delete user accounts.

If a new user is given Administrator privileges, those privileges are also automatically granted to the user for the command-line interface (CLI) and Intelligent Platform Management Interface (IPMI) to the ILOM

1. Log in to the ILOM as Administrator to reach the WebGUI.
2. From the User Management tab, select User Accounts.

The User Accounts page appears.



The screenshot shows the Sun Integrated Lights Out Manager (ILOM) web interface. The top navigation bar includes tabs for System Information, System Monitoring, Configuration, User Management, Remote Control, and Maintenance. Under the User Management tab, there are sub-tabs for User Accounts, Active Sessions, and LDAP Settings. The main content area is titled "User Accounts" and contains a table of user accounts. Below the table are buttons for "Add", "Edit", and "Delete".

	UserID /	User Name /	Network Privilege /	Serial Privilege /
<input type="radio"/>	1	anonymous	No Access	No Access
<input type="radio"/>	2	root	Administrator	Administrator
<input checked="" type="radio"/>	3	Not Configured	No Access	No Access
<input type="radio"/>	4	Not Configured	No Access	No Access
<input type="radio"/>	5	Not Configured	No Access	No Access
<input type="radio"/>	6	Not Configured	No Access	No Access
<input type="radio"/>	7	Not Configured	No Access	No Access
<input type="radio"/>	8	Not Configured	No Access	No Access
<input type="radio"/>	9	Not Configured	No Access	No Access
<input type="radio"/>	10	Not Configured	No Access	No Access

FIGURE 7-3 User Accounts Page

3. Select a radio button to select a user account to modify.
4. Click the Edit button.

The Edit User dialog box appears.

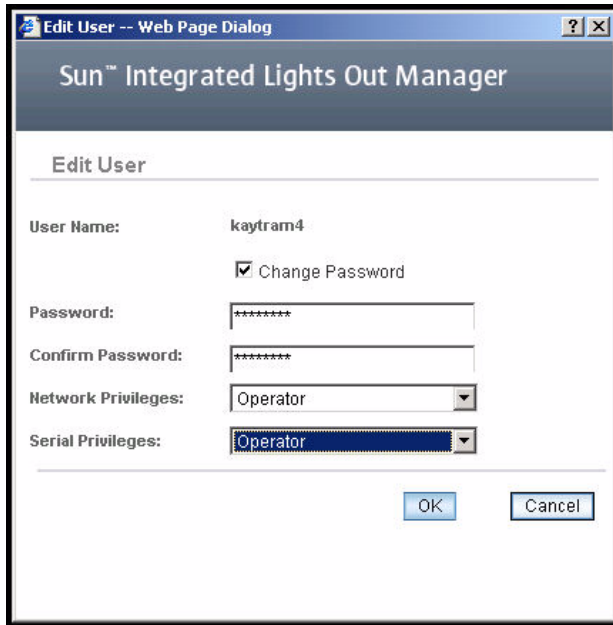


FIGURE 7-4 Edit User Dialog Box

5. **Modify the password if needed.**
 - a. **Select the Change Password check box if you want to change the user password. If you do not want to change the password, deselect the check box.**
 - b. **Type a new 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 confirm the password.**
6. **Modify network and serial privileges as needed.**

In the Network and Serial fields, select either Administrator or Operator.
7. **After you have modified the account information, click the OK button for your changes to take effect, or click the Cancel button to return to the previous settings.**

A confirmation dialog box verifies that the user account was modified successfully. The User Accounts page then is redisplayed.

7.1.3 Deleting a User Account

This section explains how to delete an ILOM user account.

1. Log in to the ILOM as Administrator to reach the WebGUI.
2. From the User Management tab, select User Accounts.

The User Accounts page appears.

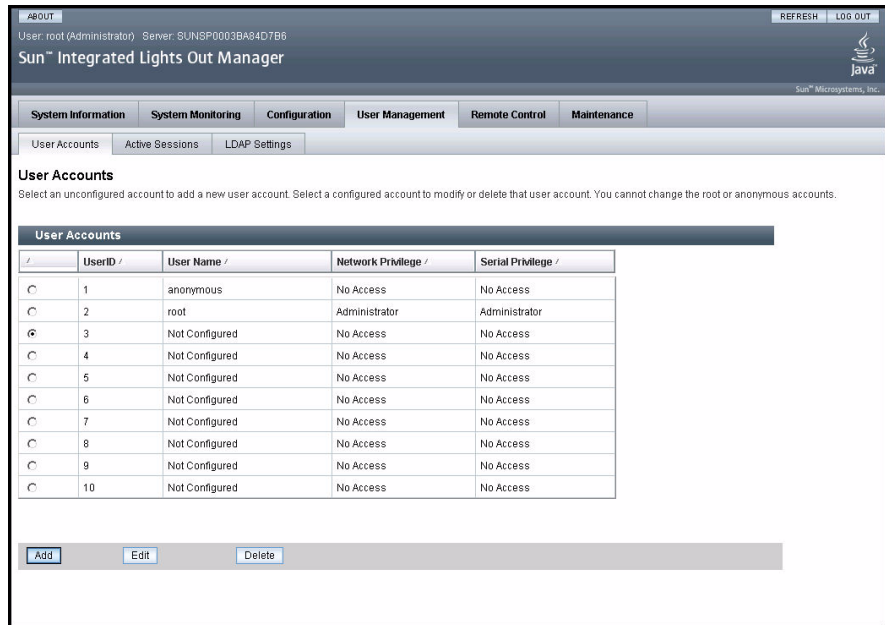


FIGURE 7-5 User Accounts Page

3. Select the radio button next to the user account you want to delete.
4. Click the Delete button.

The confirmation dialog box appears.



FIGURE 7-6 Delete User Confirmation Dialog Box

5. **Click the OK button to confirm the deletion, or click the Cancel button to stop the deletion.**

If you click the OK button, the user account reverts to an unassigned user account.

7.2 Viewing and Modifying Lightweight Directory Access Protocol Settings

This section explains how to view and modify the Lightweight Directory Access Protocol (LDAP) settings. You must properly configure your LDAP server before you can use LDAP authentication on the ILOM.

The Sun server supports LDAP authentication for users. LDAP is a general-purpose directory service. A directory service is a distributed database application designed to manage the entries in a directory, and to make those entries available to users and other applications. For more information, see [Chapter 10](#).

1. **Log in to the ILOM as Administrator to reach the WebGUI.**
2. **From the User Management tab, select LDAP Settings.**

The LDAP Settings page appears.

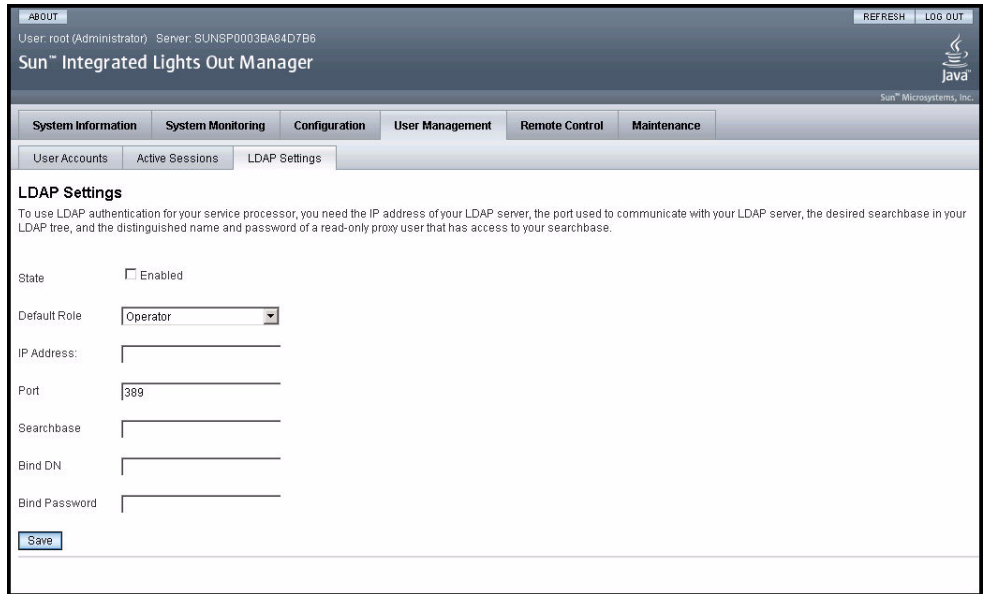


FIGURE 7-7 LDAP Settings Page

3. Complete the information in the LDAP Settings page.

Use the descriptions in the following table when completing the information.

TABLE 7-1 LDAP Settings Page Fields

Check Box or Field	Description
State	Select the Enabled check box to authenticate LDAP and local users. Deselect the check box to authenticate only local users.
Default Role	Select either Administrator or Operator.
IP Address	Type the IP address of the LDAP server.
Port	Type the port number used to communicate with the LDAP server.
Searchbase	Type the branch of your LDAP server to search for users. For example, ou=people, ou=sales, dc=sun, dc=com
Bind DN	Type the Distinguished Name (DN) of a read-only proxy user on the LDAP server. The ILOM must have read-only access to your LDAP server to search for and to authenticate users.
Bind Password	Type the password of a read-only user.

4. Click the Save button for your changes to take effect.

Using The Remote Console Application

This chapter describes how to use the remote console application.

It includes the following sections:

- [Section 8.1, “About the Remote Console Application” on page 8-1.](#)
- [Section 8.2, “Starting the Remote Console Application” on page 8-4.](#)
- [Section 8.3, “Redirecting Keyboard, Video, Mouse, or Storage Devices” on page 8-10.](#)
- [Section 8.4, “Controlling Power to the Host Server” on page 8-13.](#)

8.1 About the Remote Console Application

The remote console application, which is started using the WebGUI, allows you to control your server’s operating system remotely, using the screen, mouse and keyboard, and to redirect local CD and diskette (floppy) drives as if they were connected directly to the server.

- The screen, mouse and keyboard functionality allows you to use the operating system and other GUI-based programs, instead of restricting you to the command-line-based utilities provided by terminals and emulators.
- The ability to redirect CD and diskette drives allows you to download and upload software to and from the server as if you were accessing its own CD and diskette drives.

8.1.1 Installation Requirements

You do not need to install software on the host system (server). The ILOM ships with the remote console application installed.

A compatible web browser and JRE 1.5 are required to operate the remote console application. See [TABLE 8-1](#).

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

TABLE 8-1 Client Installation Requirements

Client OS	Java Runtime Environment Including Java Web Start	Browser(s)
Microsoft Windows XP Pro	JRE 1.5 (Java 5.0)	Internet Explorer 6.0 and later Mozilla 1.7.5 or later Mozilla Firefox 1.0
Red Hat Linux 3.0 and 4.0 Desktop and Workstation Editions	JRE 1.5 (Java 5.0)	Mozilla 1.7.5 or later Mozilla Firefox 1.0
Solaris 9	JRE 1.5 (Java 5.0)	Mozilla 1.7.5
Solaris 10	JRE 1.5 (Java 5.0)	Mozilla 1.7.5
SUSE Linux 9.2	JRE 1.5 (Java 5.0)	Mozilla 1.7.5

Note – To download the Java 1.5 runtime environment, go to <http://java.com>.

The remote console application uses the following TCP ports:

TABLE 8-2 Remote Console Ports and Interfaces

Port	Interface	Application
443	TCP	HTTPS
5120	TCP	Remote CD
5121	TCP	Remote keyboard and mouse
5123	TCP	Remote Diskette
6577	TCP	CURI (API) - TCP and SSL

TABLE 8-2 Remote Console Ports and Interfaces (Continued)

Port	Interface	Application
TCP	7578	Video Data
UDP	161	SNMP V3 Access
UDP	3072	Trap Out (outgoing only)

Note – If the ILOM is configured to use HTTP, it uses TCP port 80.

8.1.2 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 don't redirect them, the host will act 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.

Information in [TABLE 8-3](#) describes different case scenarios in which the remote console application and CD drive and diskette drive redirection operate.

TABLE 8-3 Remote Console Operation With DVD Drive and Diskette Drive

Case	Status	DVD As Seen by Host	Diskette As 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 ILOM whenever the hosts asks.	Diskette device present. No medium indication is sent to the host from the ILOM whenever 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 on 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.

TABLE 8-3 Remote Console Operation With DVD Drive and Diskette Drive *(Continued)*

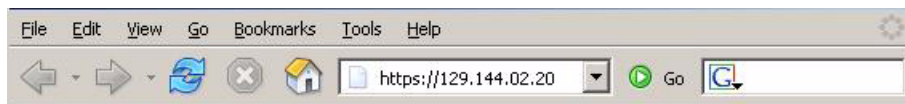
Case	Status	DVD As Seen by Host	Diskette As Seen by Host
4	Remote console application started with medium inserted	Same as 3.	Same as 3.
5	Remote console application started with medium present, then medium is removed	Next command from the host will get a status message indicating medium not present.	Next command from the host will get 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 keepalive mechanism. The software will detect keep-alive failure since there is no communication and will close the socket, assuming the client is unresponsive. Driver will send a no medium status to the host.	The software has a keepalive mechanism. The software will detect unresponsive client and close the socket, as well as indicate to the driver that the remote connection went away. Driver will send a no medium status to the host.
9	Client crashes.	Same as 8.	Same as 8.

8.2 Starting the Remote Console Application

Use this procedure to start the remote console application from the WebGUI.

1. **Type the IP address of the ILOM into the browser locator box and press ENTER.**

The ILOM login page appears, as shown in [FIGURE 8-2](#).

**FIGURE 8-1** URL Sample

2. Type the user name and password.

The default user name is root and the default password is changeme.

During this procedure, you might see security warnings. When you are prompted, select Accept, Allow, or whatever else will tell your security software to enable the connection.



FIGURE 8-2 ILOM Page

The ILOM screen displays the System Information => Versions Information page.

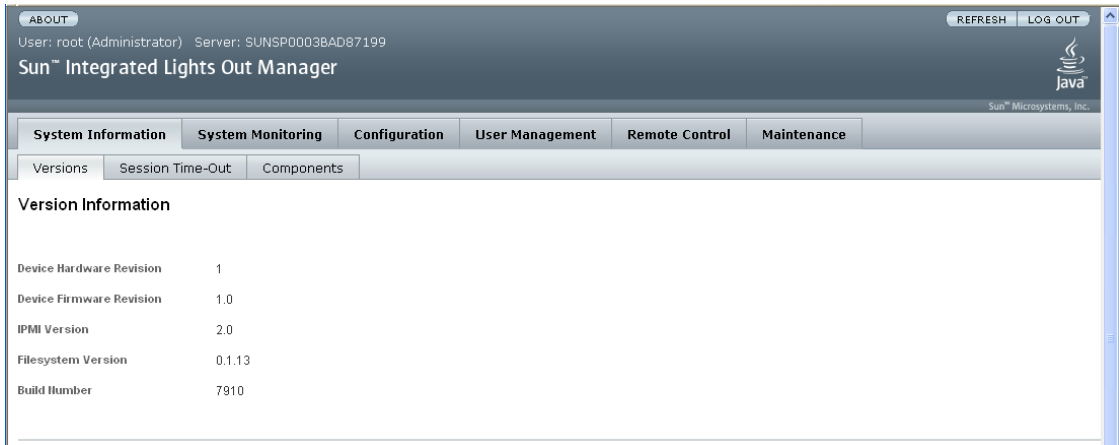


FIGURE 8-3 Version Information

3. Select the Remote Control tab.

The Remote Control options appear.

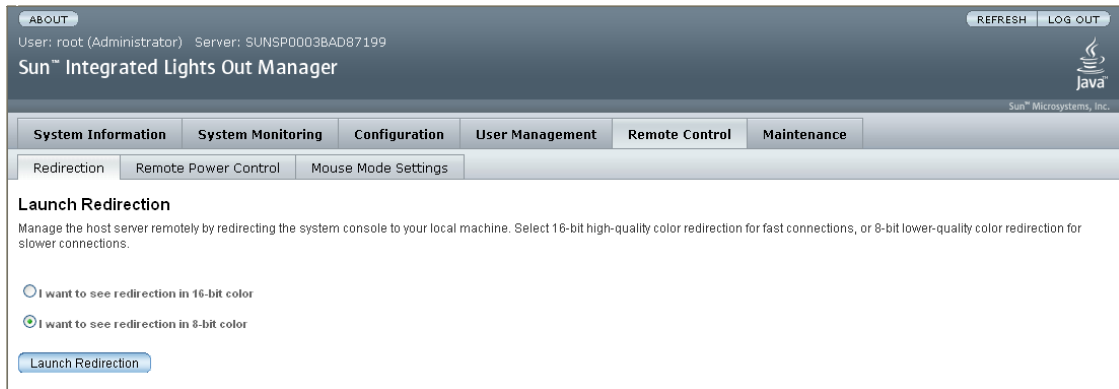


FIGURE 8-4 Launch Redirection Page

4. If necessary, set the mouse mode.

If you are not changing the mouse mode, skip to [Step 5](#).

- Absolute mouse mode – Select this setting for best performance when you are using a Solaris or Microsoft Windows operating system.
- Relative mouse mode – Select this setting for best performance when you are using a Linux operating system. Linux currently does not support Absolute mode.



Caution – Do not change the mouse mode unless it is necessary, as it causes the ILOM to reset itself.

a. Select Remote Control => Mouse Mode Settings.

The Mouse Mode Settings page appears.

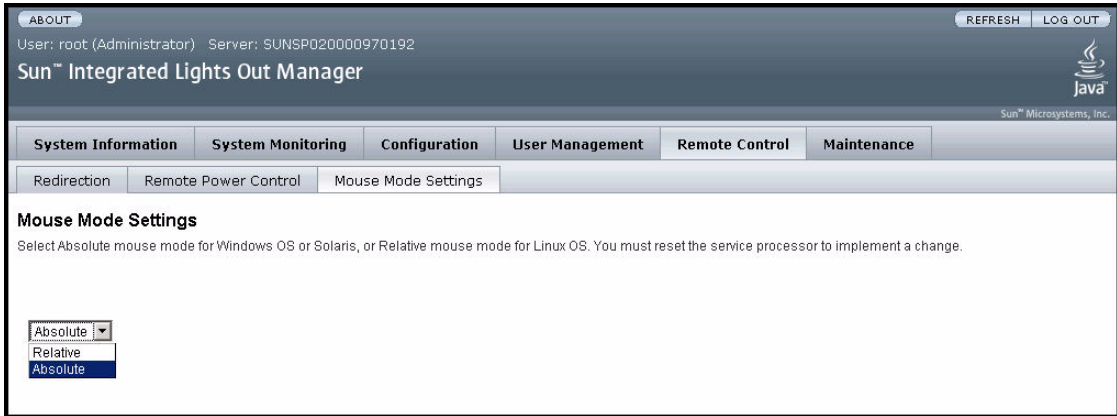


FIGURE 8-5 Mouse Mode Settings

b. Check to see if the mouse mode is set correctly, and if it is, proceed to [Step 5](#).

c. If the mouse mode is set incorrectly, select either Absolute or Relative mouse mode from the drop-down list.

A confirmation dialog box appears.

d. Click the OK button in the dialog box.

The ILOM is reset. This process takes about two or three minutes, during which time the ILOM is unavailable.

Note – Do not reboot the host while the ILOM is resetting itself, or the host might become confused about the mouse mode. For best results, change the mouse mode to the desired state prior to booting the host.

e. After the ILOM resets itself, repeat [Step 1](#) through [Step 3](#), then proceed to [Step 5](#).

The new mouse mode is now in effect. The mouse mode setting is stored on the ILOM. Therefore, subsequent connections to the WebGUI will use the new mode.

Note – If you use Relative mouse mode, you might have difficulty getting a redirected mouse out of the remote console window. To regain control of the cursor, type ALT+m

5. Select 8-bit or 16-bit color.

Note – For faster performance, select 8-bit color.

6. Click Launch Redirection.

The Redirection page appears.

During this procedure, you might see security warnings. When you are prompted, select Accept, Allow, Yes, or whatever else will tell your security software to enable the connection.

The JavaRConsole message appears.



FIGURE 8-6 Java Web Start

7. When you see the login dialog box, type the username and password.

The defaults username is root and the default password is changeme.

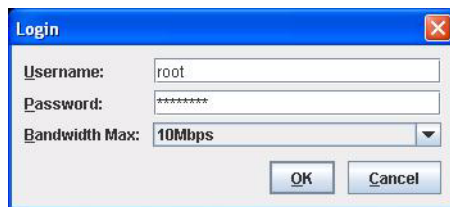


FIGURE 8-7 Remote Console Login Dialog Box

8. Select a bandwidth (optional).

Choose bandwidth that matches your actual bandwidth.

Note – Setting the bandwidth higher than what is actually available can degrade performance. Sometimes you can improve performance by setting the bandwidth lower.

9. Click the OK button to launch the remote console application.

When the login is successful, the Remote Console screen appears.

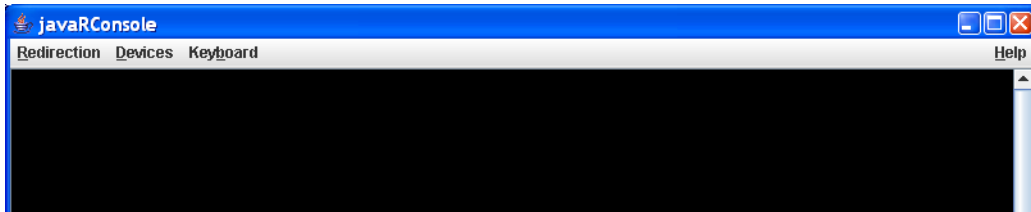


FIGURE 8-8 Remote Console Screen

The remote console application starts with the video and keyboard enabled.

10. Choose Devices => Mouse to enable mouse redirection (Optional).



FIGURE 8-9 Mouse and Keyboard Redirection Selected

You should now be able to use the remote console application to start your server's operating system.

Video and keyboard are enabled by default. In most cases, all you need to do is enable the mouse redirection.

For detailed instructions on how to enable and disable I/O and storage devices (CD-ROM and Diskette drives), see [Section 8.3, "Redirecting Keyboard, Video, Mouse, or Storage Devices"](#) on page 8-10.

8.3 Redirecting Keyboard, Video, Mouse, or Storage Devices

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

- Video display – the server’s video output is automatically displayed on the remote console window.
- 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 or diskette drives

8.3.1 Redirecting Keyboard and Mouse Devices

Use the following procedure to redirect a server keyboard and mouse device to your local workstation or laptop.

Note – For the mouse to work correctly, you might have to change the mouse mode as well. This is described in [Step 4](#) of the procedure [Section 8.2, “Starting the Remote Console Application”](#) on page 8-4.

1. **Start the remote console application as described in [Section 8.2, “Starting the Remote Console Application”](#) on page 8-4.**

The Remote Console screen appears.

2. **Choose Devices => Mouse to enable mouse redirection.**
3. **If keyboard redirection is disabled, select Devices => Keyboard to enable it.**

Note – Keyboard redirection is selected by default.

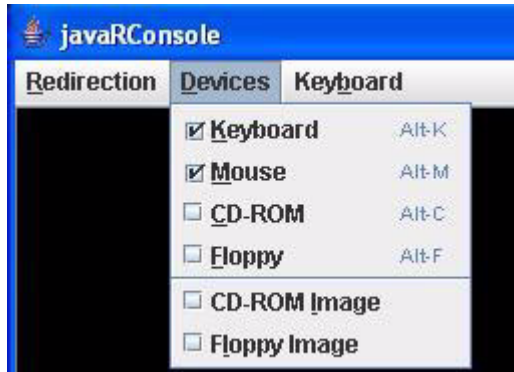


FIGURE 8-10 Keyboard and Mouse Selected

4. Use the Keyboard menu to control keyboard attributes and to send special characters that might not be available on the keyboard in remote console mode.



FIGURE 8-11 Keyboard Options

- Selecting Auto-Keybreak Mode causes the SP to send a key release event automatically. Use this mode when network latency causes the host to act as if keys are being held down.
- To simulate a Ctrl+Alt key sequence:
 - a. Choose Left Alt Key (or Right Alt Key).
 - b. Hold down the Ctrl key.
 - c. Release the Ctrl key.
 - d. Deselect Left Alt Key (or Right Alt Key).
- To send F10 (used in BIOS), click F10.
- To send a break, click Control Alt Delete.

8.3.2 Redirecting 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.

Note – You can also use this procedure to redirect a CD image file or a diskette image file stored on your hard drive.

1. **Start the remote console application as described in Section 8.2, “Starting the Remote Console Application” on page 8-4.**

The Remote Console screen appears.

2. **Choose Devices => CD-ROM or Devices => Floppy.**

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.

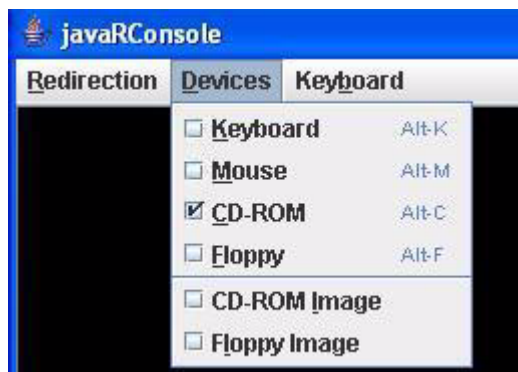


FIGURE 8-12 CD-ROM Selected

3. **To start a CD image file or a diskette image file from your hard drive, select CD-ROM Image or Floppy Image.**

A browser appears.

Note – You cannot select two CD-ROM devices or two diskette devices. For example, you cannot select CD-ROM and CD-ROM image.

4. **Use the browser to navigate to the corresponding image file, then click the OK button.**
5. **To disconnect a device from the server, deselect the corresponding menu item.**

8.4 Controlling Power to the Host Server

This section explains how to control the power to a Sun server.

1. Log in to the WebGUI as described in [Section 4.2, “Logging In and Out of the WebGUI”](#) on page 4-4.
2. Select Remote Control => Remote Power Control.

The Server Power Control page appears.



FIGURE 8-13 Server Power Control Page

3. To change the power status of the server, select an action from the drop-down list.
 - Reset – Select to reboot the server immediately.
 - Immediate Power Off – Select to power off the server.
 - Graceful Shutdown and Power Off – Select to gracefully shut down the system operating system before the system is powered off.
 - Power On – Select to power on the server.
 - Power Cycle – Select to power off the server, wait, and then power on the server again.
4. Click the OK button in the confirmation dialog to implement your selection.

Using Intelligent Platform Management Interface (IPMI)

This chapter describes introduces the ILOM's Intelligent Platform Management Interface (IPMI) functionality and lists the supported IPMI commands.

This chapter includes the following sections:

- Section 9.1, “About IPMI” on page 9-1.
- Section 9.2, “Supported IPMI 2.0 Commands” on page 9-2.

9.1 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 baseboard management controllers (BMCs), which are located on IPMI-compliant hardware components. 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.

Your ILOM 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 v1.5 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>.

Note – Your server includes a number of IPMI-compliant sensors that measure things such as voltages, temperature ranges and security latches that detect when the enclosure is opened. For a complete list of sensors, see your platform supplement.



Caution – Do not use any interface other than the ILOM CLI or WebGUI to alter the state or configuration of any sensor or LED. Doing so could void your warranty.

9.1.1 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.

You can download IPMItool from <http://ipmitool.sourceforge.net/>, or locate IPMItool and its related documentation on your server Resource CD.

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

```
man ipmitool
```

9.2 Supported IPMI 2.0 Commands

[TABLE 9-1](#) lists the supported IPMI 2.0 commands.

Note – When a hard drive is unconfigured in the host OS, the command `ipmitool ... sdr elist` shows it as “Drive Present, Hot Spare.” This means it is inserted but safe to remove.

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

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

TABLE 9-1 Supported IPMI 2.0 Commands

Supported IPMI 2.0 Commands
<i>General Commands</i>
Get Device ID
Cold Reset
Warm 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 Command
Set/Get User Access Command
Set/Get User Name
Set User Password Command
Master Write-Read
Set/Get Chassis Capabilities
Get Chassis Status
Chassis Control
Chassis Identify
Set Power Restore Policy
Get System Restart Cause

TABLE 9-1 Supported IPMI 2.0 Commands (*Continued*)

Supported IPMI 2.0 Commands (<i>Continued</i>)
Set/Get System Boot Options
Set/Get Event Receiver IPMI
System Interface Support
KCS
BT
RCMP
<ul style="list-style-type: none">• Multiple Payloads• Enhanced Authentication• Encryption
<i><u>PEF and Alerting Commands</u></i>
Get PEF Capabilities
Arm PEF Postpone Timer
Set/Get PEF Configuration Parameters
Set/Get Last Processed Event ID
Alert Immediate
PET Acknowledge
<i><u>Sensor Device Commands</u></i>
Get Sensor Reading Factors
Set/Get Sensor Hysteresis
Set/Get Sensor Threshold
Set/Get Sensor Event Enable
Get Sensor Reading
Set Sensor Type
<i><u>FRU Device Commands</u></i>
Get FRU Inventory Area Info
Read/Write FRU Data SDR Device Commands
Get SDR Repository Info

TABLE 9-1 Supported IPMI 2.0 Commands (*Continued*)

Supported IPMI 2.0 Commands (<i>Continued</i>)
Get SDR Repository Allocation
Reserve SDR Repository
Get/Add SDR
Partial Add SDR
Clear SDR Repository
Get SDR Repository Time
Enter/Exit SDR Repository Update
Run Initialization Agent
<u><i>SEL Device Commands</i></u>
Get SEL Info
Get SEL Allocation Info
Reserve SEL
Get/Add SEL Entry
Clear SEL
Set/Get SEL Time
<u><i>LAN Device Commands</i></u>
Get LAN Configuration Parameters
Suspend BMC ARPs
<u><i>Serial/Modem Device Commands</i></u>
Set/Get Serial Modem Configuration
Set Serial Modem MUX
Get TAP Response Codes
Serial/Modem Connection Active
Callback
Set/Get User Callback Options
<u><i>Event Commands</i></u>

TABLE 9-1 Supported IPMI 2.0 Commands (*Continued*)

Supported IPMI 2.0 Commands (<i>Continued</i>)
Get Event Count
Set/Get Event Destination
Set/Get Event Reception State
Send ICMB Event Message

Lightweight Directory Access Protocol (LDAP)

The ILOM supports LDAP authentication for users, based on the OpenLDAP software. LDAP is a general-purpose directory service. A directory service is a centralized database for distributed applications designed to manage the entries in a directory. Thus, multiple applications can share a single user database. For more detailed information on LDAP, see <http://www.openldap.org/>.

LDAP is based on a client-server model. LDAP provides the directory, and the clients use the directory service to access entries. The data stored in a directory can be distributed among several LDAP servers.

10.0.1 How LDAP Servers Organize Directories

Data in LDAP is organized hierarchically, starting at a root and branching down into individual entries. Entries at the top level of the hierarchy represent larger organizations, and under the larger organizations are entries for smaller organizations. At the bottom of the hierarchy are entries for individual people or resources.

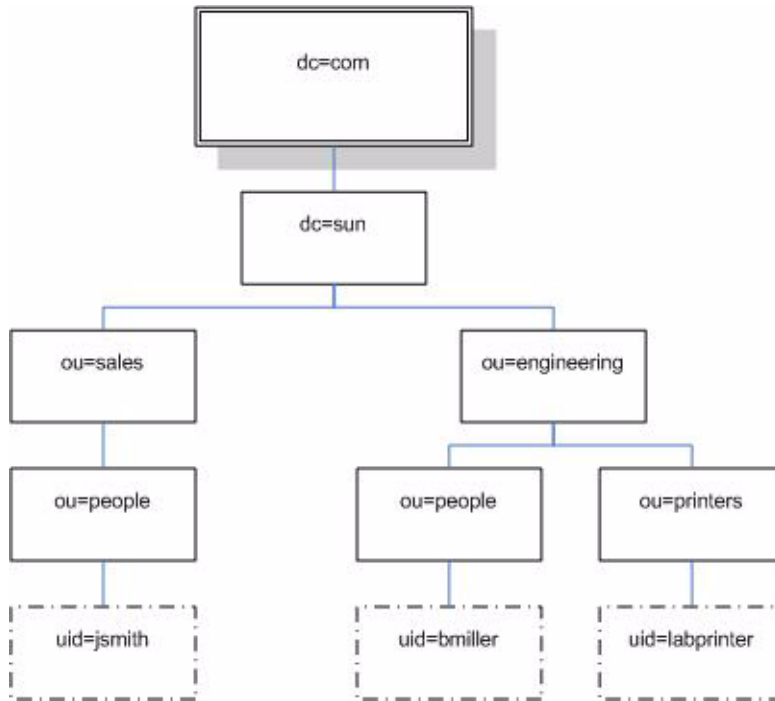


FIGURE 10-1 LDAP Directory Structure

Each entry is uniquely identified by a distinguished name (dn). A distinguished name consists of a name that uniquely identifies the entry at that hierarchical level and a path that traces the entry back to the root of the tree.

For example, the distinguished name for jsmith is:

```
dn: uid=jsmith, ou=people, dc=sun.com
```

Here, `uid` represents the user ID of the entry, `ou` represents the organizational unit in which the entry belongs, and `dc` represents the larger organization in which the entry belongs. The following diagram shows how distinguished names are used to identify entries uniquely in the directory hierarchy.

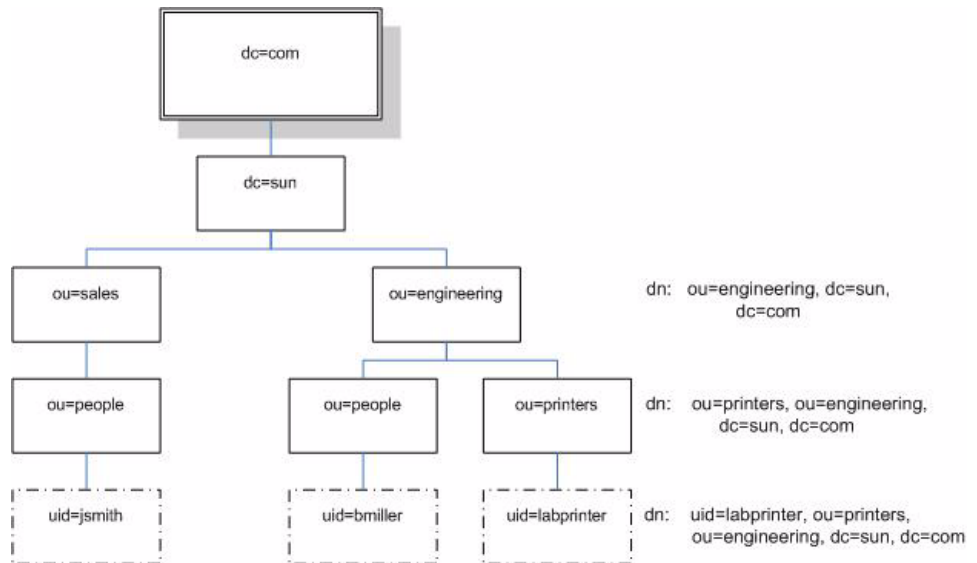


FIGURE 10-2 LDAP Distinguished Names

10.0.2 How LDAP Clients and Servers Work

In the LDAP client-server model, LDAP servers make information about people, organizations, and resources accessible to LDAP clients. Clients make changes to the LDAP database using a client utility, usually bundled with the LDAP server. When a change is made to the LDAP database, all client applications see the change immediately so there is no need to update each distributed application. An LDAP client can perform these operations, among others:

- Search for and retrieve entries from the directory
- Add new entries to the directory
- Update entries in the directory
- Delete entries from the directory
- Rename entries in the directory

For example, to update an entry in the directory, an LDAP client submits the distinguished name of the entry with updated attribute information to the LDAP server. The LDAP server uses the distinguished name to find the entry and performs a modify operation to update the entry in the directory. The updated information is immediately available to all the distributed applications using that LDAP server.

To perform any of these LDAP operations, an LDAP client needs to establish a connection with an LDAP server. LDAP specifies the use of TCP/IP port number 389, although servers may run on other ports.

Your Sun server can be a client of an LDAP server. In order to use LDAP authentication, you need to create a user on your LDAP server that your Sun server can authenticate, or bind to, so the client has permission to search the proper directory on the LDAP server.

10.1 Configuring LDAP

To use LDAP, you must configure your LDAP server, according to your LDAP server's documentation, and your ILOM, using either the CLI or the WebGUI.

This procedure requires detailed knowledge of your LDAP server configuration. Gather basic network information about your LDAP server, including its IP address, before you begin.

Note – This task is similar to configuring LDAP as a name service for Linux or Solaris.

10.1.1 Configuring LDAP Server

1. **Ensure that all users authenticating to the ILOM have passwords stored in crypt or MD5 crypt.**

The ILOM only supports LDAP authentication for passwords in these two formats.

2. **Add object classes `posixAccount` and `shadowAccount`, and populate the required property values for this schema (RFC 2307).**

TABLE 10-1 LDAP Property Values

Required Property	Description
uid	User name for logging in to your ILOM
uidNumber	Any unique number
gidNumber	Any unique number

TABLE 10-1 LDAP Property Values (*Continued*)

Required Property	Description
userPassword	Password
homeDirectory	Any value (this property is ignored by the ILOM)
loginShell	Any value (this property is ignored by the ILOM)

3. Provide the ILOM access to user accounts on your LDAP server.

Either enable your LDAP server to accept anonymous binds, or create a proxy user on your LDAP server that has read-only access to all user accounts that will authenticate through the ILOM.

See your LDAP server documentation for further details.

10.1.2 Configure ILOM

Once the LDAP server is configured, you must configure the ILOM, using either the CLI or the WebGUI.

10.1.2.1 Using the CLI

1. Enter the proxy user name and password. From the command line, type:

```
set /SP/clients/ldap binddn=cn=proxyuser, ou=sales, dc=sun, dc=com bindpw=  
password
```

2. Enter the IP address of the LDAP server. From the command line, type:

```
set /SP/clients/ldap ipaddress=ldapipaddress
```

3. Assign the port used to communicate with the LDAP server; the default port is 389. From the command line, type:

```
set /SP/clients/ldap port=ldapport
```

Enter the distinguished name of the branch of your LDAP tree that contains users and groups. From the command line, type:

```
set /SP/clients/ldap searchbase="ou=people, ou=sales, dc=sun, dc=com"
```

This is the location in your LDAP tree that you want to search for user authentication.

4. Set the state of the LDAP service to enabled. From the command line, type:

```
set /SP/clients/ldap state=enabled
```

5. To verify that LDAP authentication works, log in to the ILOM using an LDAP user name and password.

Note – The ILOM searches local users before LDAP users. If an LDAP user name exists as a local user, the ILOM uses the local account for authentication.

10.1.2.2 Using the WebGUI

1. Log in to the ILOM as Administrator or Operator to reach the WebGUI.
2. Select User Management => LDAP Settings.

The LDAP Settings page appears.

ABOUT User: root (Administrator) Server: SUNSP0003BA84D7B6 REFRESH LOG OUT

Sun™ Integrated Lights Out Manager

System Information System Monitoring Configuration User Management Remote Control Maintenance

User Accounts Active Sessions LDAP Settings

LDAP Settings

To use LDAP authentication for your service processor, you need the IP address of your LDAP server, the port used to communicate with your LDAP server, the desired searchbase in your LDAP tree, and the distinguished name and password of a read-only proxy user that has access to your searchbase.

State Enabled

Default Role Operator

IP Address:

Port 389

Searchbase

Bind DN

Bind Password

Save

FIGURE 10-3 LDAP Settings Page

3. Enter the following values:

- State – Select the Enabled check box to authenticate LDAP users
- Role – The default role of LDAP users. Select either Operator or Administrator.
- IP Address – The IP address of the LDAP server
- Port – The port number on the LDAP server.
- Searchbase – Type the branch of your LDAP server to search for users.
- Bind DN – Type the Distinguished Name (DN) of a read-only proxy user on the LDAP server. ILOM must have read-only access to your LDAP server to search for and to authenticate users.

- Bind Password – Type the password of the read-only user.
4. **To verify that LDAP authentication works, log in to the ILOM using an LDAP user name and password.**

Note – The ILOM searches local users before LDAP users. If an LDAP user name exists as a local user, the ILOM uses the local account for authentication.

Using Simple Network Management Protocol (SNMP)

This chapter describes how to use SNMP. It includes the following sections:

- [Section 11.1, “About SNMP” on page 11-1.](#)
- [Section 11.2, “SNMP Management Information Base \(MIB\) Files” on page 11-2.](#)
- [Section 11.3, “MIBs Integration” on page 11-3.](#)
- [Section 11.4, “About SNMP Messages” on page 11-3.](#)
- [Section 11.5, “About ILOM and SNMP” on page 11-4.](#)
- [Section 11.6, “Managing SNMP User Accounts” on page 11-5.](#)

11.1 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.

11.1.1 How SNMP Works

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

Managed nodes are any number of devices, including servers, routers, and hubs, which 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 ILOM, so all SNMP management of the server should occur through the ILOM. 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 ILOM provides the following capabilities: inventory management, and sensor and system state monitoring.

11.2 SNMP Management Information Base (MIB) Files

The base component of an SNMP solution is the Management Information Base (MIB). A 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 SNMP classes of Management Information Base (MIB) files. Download and install the product-specific MIB files from your Resource CD or Tools and Drivers CD for your platform.

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

11.3 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). [FIGURE 11-1](#). The standard SNMP port (161) is used by the SNMP agent on the ILOM.

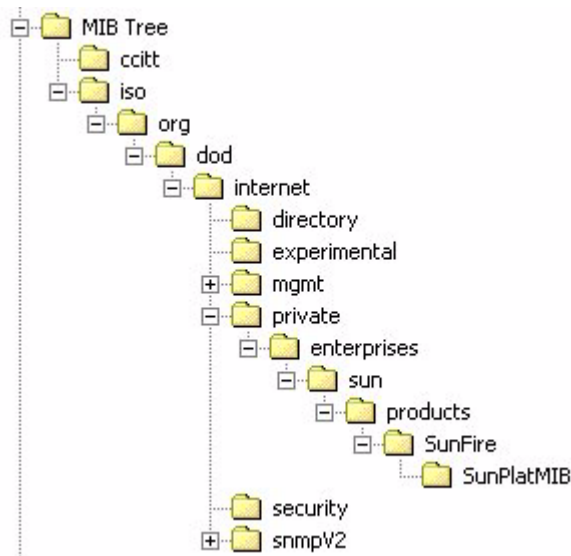


FIGURE 11-1 Sun server MIB Tree

11.4 About 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 may 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.

11.5 About ILOM and SNMP

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

To use this feature, you must 1) integrate the platform-specific MIBs into your SNMP environment, 2) tell your management station about your server, then 3) configure the specific traps.

The Sun server MIB tree appears in [FIGURE 11-1](#).

11.5.1 Integrating the MIBs

Use a third party SNMP management application to load the SUN-PLATFORM-MIB.

11.5.2 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.

11.5.3 Configuring Receipt of SNMP Traps

To configure a trap in your ILOM, see [Section 3.8, “Managing ILOM Alerts” on page 3-15](#), or [Section 5.6, “Viewing Alert Destinations and Configuring Alerts” on page 5-11](#).

11.6 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.

To do this on the WebGUI, see [Section 5.8.1, “Configuring SNMP Settings” on page 5-18](#).

11.6.1 Adding a User Account

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

```
create /SP/services/snmp/users/username authenticationpassword=  
password
```

To add an SNMP v1/v2c user account, type this command:

```
create /SP/services/snmp/communities/communityname
```

11.6.2 Deleting a User Account

To delete an SNMP v3 user account, type this command :

```
delete /SP/services/snmp/users/username
```

To delete an SNMP v1/v2c user account, type this command:

```
delete /SP/services/snmp/communities/communityname
```

11.6.3 Configuring User Accounts

To configure SNMP user accounts, use the set command.

11.6.3.1 Syntax

```
set target [propertyname=value]
```

11.6.3.2 Targets, Properties, and Values

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

TABLE 11-1 SNMP User Account Targets, Properties and Values

Target	Property	Value	Default
/SP/services/snmp/communities/ <i>communityname</i>	permissions	ro rw	ro
/SP/services/snmp/users/ <i>username</i>	authenticationprotocol	MD5 SHA	MD5
	authenticationpassword	<string>	(null string)
	permissions	ro rw	ro
	privacyprotocol	none DES	none*
	privacypassword	<string>	(null string)
/SP/services/snmp	engineid = none	string	(null string)
	port = 161	integer	161
	sets = enabled	enabled disabled	disabled
	v1 = disabled	enabled disabled	disabled
	v2c = disabled	enabled disabled	disabled
	v3 = disabled	enabled disabled	enabled

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

11.6.3.3 Examples

When changing the parameters of SNMP users, you must set values for all of the properties, even if you are not changing all of the values. For example, to change user al's privacyprotocol to DES you must type:

```
-> set /SP/services/snmp/users/al privacyprotocol=DES  
privacypassword=password authenticationprotocol=SHA  
authenticationpassword=password
```

Your changes would be invalid if you only typed:

```
-> set /SP/services/snmp/users/al privacyprotocol=DES
```

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

Command Line Interface Reference

This chapter contains the following sections:

- [Section A.1, “CLI Command Quick Reference” on page A-1.](#)
- [Section A.2, “CLI Command Reference” on page A-5.](#)

A.1 CLI Command Quick Reference

This chapter contains the most common ILOM commands used to administer your Sun server from the command-line interface (CLI).

TABLE A-1 Command Syntax and Usage

Content	Typeface	Description
Your input	Fixed-width bold	Text that you type into the computer. Type it exactly as shown.
Onscreen output	Fixed-width regular	Text that the computer displays
Variable	<i>Italic</i>	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
Show all valid targets.	<code>help targets</code>
Log out of the CLI.	<code>exit</code>
Display the version of the ILOM firmware running on the ILOM.	<code>version</code>
Display clock information.	<code>show /SP/clock</code>
Display all of the CLI commands.	<code>show /SP/cli/commands</code>
Display the active ILOM sessions.	<code>show /SP/sessions</code>
Display information about commands and targets.	<code>help</code>
Display information about a specific command.	<code>help create</code>
Update the ILOM and BIOS firmware.	<code>load -source tftp://newSPimage</code>
Display a list of the ILOM event logs.	<code>show /SP/logs/event/list</code>

TABLE A-3 User Commands

Description	Command
Add a local user.	<code>create /SP/users/user1 password=password role=administrator operator</code>
Delete a local user.	<code>delete /SP/users/user1</code>
Change a local user's properties.	<code>set /SP/users/user1 role=operator</code>
Display information about all local users.	<code>show -display [targets properties all] -level [value all] /SP/users</code>
Display information about LDAP settings.	<code>show /SP/clients/ldap</code>
Change LDAP settings.	<code>set /SP/clients/ldap binddn=proxyuser bindpw=proxyuserpassword defaultrole=administrator operator ipaddress=ipaddress</code>

TABLE A-4 Network and Serial Port Setting Commands

Description	Command
Display network configuration information.	show /SP/network
Change network properties for the ILOM. Changing certain network properties, like the IP address, will disconnect your active session.	set /SP/network pendingipaddress=<i>ipaddress</i> pendingipdiscovery=<i>dchp static</i> pendingipgateway=<i>ipgateway</i> pendingipnetmask=<i>ipnetmask</i> commitpending=true
Display information about the external serial port.	show /SP/serial/external
Change the external serial port configuration.	set /SP/serial/external pendingspeed=<i>integer</i> commitpending=true
Display information about the serial connection to the host.	show /SP/serial/host
Change the host serial port configuration. Note: This speed setting must match the speed setting for serial port 0, COM1 or /dev/ttyS0 on the host operating system.	set /SP/serial/host pendingspeed=<i>integer</i> commitpending=true

TABLE A-5 Alert Commands

Description	Command
Display information about PET alerts. You can configure up to 15 alerts.	show /SP/alert/rules/1...15
Change alert configuration.	set /SP/alert/rules/1...15 destination=<i>ipaddress</i> level=<i>down critical major minor</i>

TABLE A-6 System Management Access Commands

Description	Command
Display information about HTTP settings.	show /SP/services/http
Change HTTP settings, such as enabling automatic redirection to HTTPS.	set /SP/services/http port=portnumber secureredirect enabled disabled servicestate=enabled disabled
Display information about HTTPS access.	show /SP/services/https
Change HTTPS settings.	set /SP/services/https port=portnumber servicestate=enabled disabled
Display SSH DSA key settings.	show /SP/services/ssh/keys/dsa
Display SSH RSA key settings.	show /SP/services/ssh/keys/rsa

TABLE A-7 SNMP Commands

Description	Command
Display information about SNMP settings. By default, the SNMP port is 161 and v3 is enabled.	show /SP/services/snmp engineid=snmpengineid port=snmpportnumber sets=enabled disabled v1=enabled disabled v2c=enabled disabled v3=enabled disabled
Display SNMP users.	show /SP/services/snmp/users
Add an SNMP user.	create /SP/services/snmp/users/snmpusername authenticationpassword=password authenticationprotocol=MD5 SHA permissions=rw ro privacypassword=password privacyprotocol=none DES
Delete an SNMP user.	delete /SP/services/snmp/users/snmpusername
Display information about SNMP public (read-only) communities.	show /SP/services/snmp/communities/public
Add this device to an SNMP public community.	create /SP/services/snmp/communities/public/comm1
Delete this device from an SNMP public community.	delete /SP/services/snmp/communities/public/comm1

TABLE A-7 SNMP Commands (Continued)

Description	Command
Display information about SNMP private (read-write) communities.	show /SP/services/snmp/communities/private
Add this device to an SNMP private community.	create /SP/services/snmp/communities/private/comm2
Delete this device from an SNMP private community.	delete /SP/services/snmp/communities/private/comm2

TABLE A-8 Host System Commands

Description	Command
Start the host system.	start /SYS
Stop the host system.	stop /SYS
Reset the host system.	reset /SYS
Start a session to connect to the host console.	start /SP/console
Stop the session connected to the host console.	stop /SP/console

TABLE A-9 Clock Settings

Description	Command
Set the ILOM clock to synchronize with a primary NTP server.	set /SP/clients/ntp/server/1 address=ntpIPAddress
Set the ILOM clock to synchronize with a secondary NTP server.	set /SP/clients/ntp/server/2 address=ntpIPAddress2

A.2 CLI Command Reference

This section provides reference information about the CLI commands.

A.2.1 Using the `cd` Command

Use the `cd` command to navigate the namespace. When you `cd` 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

`[-d|default] [-e|examine] [-h|help]`

Targets and Properties

Any location in the namespace.

Examples

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

```
-> cd /SP/users
```

```
-> create sally
```

To find your location, type `cd`.

```
-> cd /SP/users
```

A.2.2 Using the `create` Command

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

```
[-d|default] [-e|examine] [-h|help]
```

Targets, Properties, and Values

TABLE A-10 Targets, Properties and Values for `create` Command

Valid Targets	Properties	Values	Default
<i>/SP/users/username</i>	password	<string>	(none)
	role	administrator /operator	operator
<i>/SP/services/snmp/community/ communityname</i>	permissions	ro rw	ro
<i>/SP/services/snmp/user/ username</i>	authenticationprotocol	MD5	MD5
	authenticationpassword	<string>	(null string)
	permissions	ro rw	ro
	privacyprotocol	none DES	DES
	privacypassword	<string>	(null string)

Example

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

A.2.3 Using the delete Command

Use the `delete` command to remove an object from the namespace. You will be prompted to confirm a `delete` command. Eliminate this prompt by using the `-script` option.

Syntax

```
delete [options] [-script] target
```

Options

[-x|examine] [-f|force] [-h|help] [-script]

Targets

TABLE A-11 Targets for delete Command

Valid Targets
<i>/SP/users/username</i>
<i>/SP/services/snmp/community/communityname</i>
<i>/SP/services/snmp/user/username</i>

Examples

-> **delete /SP/users/susan**

-> **delete -script /SP/alert/rules/tojohn**

A.2.4 Using the exit Command

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

Syntax

exit [*options*]

Options

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

A.2.5 Using the help Command

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` and `/SYS`. 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

```
[-x|examine] [-h|help] [-output terse|verbose]
```

Commands

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

Examples

```
-> help load
```

The `load` command is used to transfer a file from a server to a target.

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

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

```
-> help -output verbose reset
```

The `reset` command is used 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.

Examples:

```
-> reset /SYS
```

```
Are you sure you want to reset /SYS (y/n)? y
```

```
Performing hard reset on /SYS
```

```
-> reset
```

```
/SP Are you sure you want to reset /SP (y/n)? n
```

```
Command aborted. ->
```

A.2.6 Using the load Command

Use the load command to transfer an image file from a source, indicated by a Uniform Resource Indicator (URI), to update the ILOM firmware. The URI can specify a protocol and credentials used for the transfer. Only the TFTP protocol is supported, so the URL must begin with tftp:// . If credentials are required and not specified, the command prompts you for a password.

Note – Use this command to update your ILOM firmware and BIOS.

Syntax

```
load -source URL
```

Options

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

Example

```
-> load -source tftp://archive/newmainimage
```

Note – A firmware upgrade will cause the server and ILOM to be reset. It is recommended that a clean shutdown of the server be done prior to the upgrade procedure. An upgrade takes about five minutes to complete. ILOM will enter a special mode to load new firmware. No other tasks can be performed in ILOM until the firmware upgrade is complete and ILOM is reset.

```
-> load -source tftp://archive/newmainimage
Are you sure you want to load the specified file (y/n)? y
File upload is complete.
Firmware image verification is complete.
Do you want to preserve the configuration (y/n)? n
Updating firmware in flash RAM:
.
Firmware update is complete.
ILOM will not be restarted with the new firmware.
```

A.2.7 Using the reset Command

Use the `reset` command to reset the state of the target. You will be prompted to confirm a reset operation. Eliminate this prompt by using the `-script` option.

Note – The `reset` command does not affect the power state of hardware devices.

Syntax

```
reset [options] target
```

Options

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

Targets

TABLE A-12 Targets for `reset` Command

Valid Targets
<code>/SP</code>
<code>/SYS</code>

Examples

```
-> reset /SP
```

```
-> reset /SYS
```

A.2.8 Using the `set` Command

Use the `set` command to specify the properties of the target.

Syntax

```
set [options] [-default] target [propertyname=value]
```

Options

```
[-x examine] [-h help]
```

Targets, Properties, and Values

TABLE A-13 Targets, Properties and Values for `set` Command

Valid Targets	Properties	Values	Default
<code>/SP/users/username</code>	password	<string>	(none)
	role	administrator operator	operator
<code>/SP/alert/rules/rulename</code> <i>rulename</i> = 1 through 15	level	down critical major minor	critical
	destination	<ipaddress>	(none)
<code>/SP/clock</code>	usentpserver	enabled disabled	/SP/clock

TABLE A-13 Targets, Properties and Values for set Command (Continued)

Valid Targets	Properties	Values	Default
/SP/services/http	servicestate	enabled disabled	/SP/services/http
/SP/services/https	servicestate	enabled disabled	/SP/services/https
/SP/services/snmp	engineid	<hexadecimal>	IP address
	port	<decimal>	161
	sets	enabled disabled	disabled
	traps	enabled disabled	disabled
	v1	enabled disabled	disabled
	v2c	enabled disabled	disabled
	v3	enabled disabled	enabled
/SP/services/snmp/ community/communityname	permissions	ro rw	ro
/SP/services/snmp/user /username	authenticationprotocol	MD5	MD5
	authenticationpassword	<string>	(null string)
	permissions	ro rw	ro
	privacyprotocol	none DES	DES
	privacypassword	<string>	(null string)
/SP/clients/ldap	binddn	<username>	(none)
	bindpw	<string>	(none)
	defaultrole	administrator operator	operator
	ipaddress	<ipaddress> none	none
	port	<decimal>	389
	searchbase	<string>	(none)
	state	enable disabled	disabled
/SP/clients/servers/[1 2]	address	<IP address> <hostname> none	(none)
/SP/network	commitpending	true	(none)
	pendingipaddress	<IP address> none	(none)
	pendingdiscovery	dhcp static	dhcp
	pendingipgateway	<IP address> none	(none)
	pendingipnetmask	<IP dotted decimal>	255.255.255.255
/SP/serial/external	commitpending	true	(none)
	flowcontrol	none	none
	pendingspeed	<decimal from list>	9600
/SP/serial/host	commitpending	true	(none)
	pendingspeed	<decimal from list>	9600

Examples

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

```
-> set /SP/clients/ldap state=enabled binddn=proxyuser bindpw=ez24get
```

A.2.9 Using the show Command

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

Using the `-display` option determines the type of information shown. If you specify `-display targets`, then all targets in the namespace below the current target are shown. If you specify `-display properties`, all property names and values for the target are shown. With this option you can specify certain property names, and only those values are shown. If you specify `-display all`, all targets in the namespace below the current target are shown, and the properties of the specified target are shown. If you do not specify a `-display` option, the show command acts as if `-display all` was specified.

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] [-display targets|properties|all] [-level value|all] target [propertyname]
```

Options

```
[-d|-display] [-e|examine] [-l|level]
```

Targets and Properties

TABLE A-14 Targets for show Command

Valid Targets	Properties
/SYS	
/SP	
/SP/alert	
/SP/alert/rules/alertrulename	type level destination
/SP/clients/ldap	binddn bindpw defaultrole ipaddress port searchbase state
/SP/clients/ntp	
/SP/clients/ntp/server	
/SP/clients/ntp/server/[1 2]	
/SP/clock	datetime usentpserver
/SP/logs	
/SP/logs/event	clear
/SP/logs/event/lis	
/SP/network	commitpending ipaddress ipdiscovery ipgateway ipnetmask linkstatus macaddress pendingipaddress pendingdiscovery pendingipgateway pendingipnetmask

TABLE A-14 Targets for show Command (Continued)

Valid Targets	Properties
/SP/serial	
/SP/serial/external	commitpending flowcontrol pendingspeed speed
/SP/serial/host	commitpending pendingspeed speed
/SP/services	
/SP/services/http	port secureredirect servicestate
/SP/services/https	port servicestate
/SP/services/snmp	ngineid port sets traps v1 v2c v3
/SP/services/snmp/communities/	
/SP/services/snmp/communities/private	permissions
/SP/services/snmp/communities/public	permissions
/SP/services/snmp/users	
/SP/services/ssh	
/SP/services/ssh/keys	
/SP/services/ssh/keys/dsa	fingerprint length publickey
/SP/services/ssh/keys/rsa	fingerprint length publickey
/SP/sessions	

TABLE A-14 Targets for show Command (Continued)

Valid Targets	Properties
/SP/sessions/sessionid	starttime source type user
/SP/users	
/SP/users/username	role

Examples

```
-> show -display properties /SP/users/susan
```

```
/SP/users/susan
```

```
Properties:
```

```
role = Administrator
```

```
-> show /SP/clients -level 2
```

```
/SP/clients
```

```
Targets:
```

```
ldap  
ntp
```

```
Properties:
```

```
Commands:
```

```
cd  
show
```

```
/SP/clients/ldap
```

```
Targets:
```

```
Properties:
```

```
binddn = cn=Manager,dc=sun,dc=com  
bindpw = secret  
defaultrole = Operator  
ipaddress = 129.144.97.180  
port = 389  
searchbase = ou=people,dc=sun,dc=com  
state = disabled
```

<pre> Commands: cd show /SP/clients/ntp Targets: server Properties: Commands: cd show </pre>
--

A.2.10 Using the start Command

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

Syntax

```
start [options] target
```

Options

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

Targets

TABLE A-15 Targets for `start` Command

Valid Targets	Description
/SYS	Starts (powers on) the system.
/SP/console	Starts an interactive session to the console stream.

Examples

```
-> start /SP/console
```

```
-> start /SYS
```

A.2.11 Using the stop Command

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] [-script] target
```

Options

```
[-x|examine] [-f|force] [-h|help]
```

Targets

TABLE A-16 Targets for `stop` Command

Valid Targets	Description
<code>/SYS</code>	Perform an orderly shutdown, followed by a power off of the specified hardware. Use the <code>-force</code> option to skip the orderly shutdown and force an immediate power off.
<code>/SP/console</code>	Terminate another user's connection to the host console.

Examples

```
-> stop /SP/console
```

```
-> stop -force /SYS
```

A.2.12 Using the version Command

Use the `version` command to display ILOM 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, such as "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 enable 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.
- baseboard management controller (BMC)** A device used to manage chassis 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 BMC provides another interface to the system event log (SEL). Typical functions of the BMC are to measure processor temperature, power supply values, and cooling fan status. The BMC can take autonomous action to preserve system integrity.
- 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), this 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 which 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 exposing it to an electrical charge.

electrostatic discharge (ESD)	The sudden dissipation of static electrical charge. ESD can easily destroy semiconductor components.
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 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 in order to reach the console prompt. A user 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 100M bits per second. Fast Ethernet is backward compatible with 10M-bit per second 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 (FC-AL)	A 100-Mbyte per second 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 allows 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 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 for 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	A programmable read-only memory (PROM) that can be reprogrammed while installed within the system, from software on a disk, 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 1000M bits per second.

**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 backend 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-plug component is configured into the system.

hot swap Describes a component that can be installed or removed 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, but not all hot-pluggable components are hot swappable.

**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.

Integrated Lights Out Manager (ILOM)

An integrated hardware, firmware, and software solution for in-chassis or in-blade system management.

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. This enables 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 Field Replacable Unit (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, 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 the 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 launcher. With Java Web Start, applications are launched by clicking on 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 launched from a desktop icon or 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 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 in to 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 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.
- OpenBootTM 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 are 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 Filtering (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 multiple 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.
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.

S

Secure Shell (SSH) A UNIX shell program and network protocol that enables secure and encrypted log in 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 . They include software information, such as how many sensors are present, what type they are, their events, threshold information, and so on. 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 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 chassis 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 functions of the SP are to measure processor temperature, power supply values, and cooling fan status. The SP can take autonomous action to preserve system integrity.

session time-out 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 email.

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 controlling 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 allows 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.

time-out 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 450M bits per second (USB 2.0). A USB port connects devices, such as mouse pointers, 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 in order 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

alerts

- configuring, 5-11
- ILOM, 3-16

B

baud rate, setting, 6-3

BIOS password, resetting, 5-6

break

- sending, 3-9, 8-11

C

case, 3-4

CLI

- access settings, 3-6
- alerts, 3-16
- command
 - syntax, A-1
- commands
 - access settings, A-4
 - alert, A-3
 - cd, A-6
 - character case, 3-4
 - clock settings, A-5
 - command verbs overview, 3-5
 - create, A-6
 - delete, A-7
 - displaying, 3-19
 - exit, A-8
 - help, A-9
 - host, A-5
 - load, A-10

miscellaneous, A-2

network and serial port, A-3

options, 3-5

reset, A-11

set, 3-18, A-12

show, A-14

SNMP, A-4

start, A-18

stop, A-19

user, A-2

version, A-19

namespaces, 3-3

overview

privilege levels, 3-4

SSH log in, 3-2

SSH log out, 3-2

clock, 5-17, A-2

settings, 3-18, A-5

Command Line Interface

see CLI

configuring alerts, 5-11

configuring DHCP, 2-5

customer replaceable units (CRUs), 5-6

D

default root password, 3-2

DHCP

configuring, 2-5

ILOM, 2-3

E

event log

- clearing, 5-15, 5-16
- interpreting time stamps, 5-17
- viewing, 5-15

F

- fan sensors, 5-7
- field replacable units (FRUs), 5-6
- firmware
 - upgrading, 5-2
 - viewing revisions, 5-24
- FRUs, 5-6

H

- hardware
 - power and WebGUI, 8-13
 - redirecting
 - keyboard and mouse, 8-10
 - storage devices, 8-12
 - replaceable components, 5-6
 - viewing revisions, 5-24
- host serial console, 6-2
- host, managing, 3-8
- HTTP settings, 3-6
- HTTPS
 - enabling, 6-10
 - settings, 3-6

I

- ILOM
 - alerts and CLI, 3-16
 - and LDAP, 10-1 to 10-5, ?? to 10-6
 - CLI
 - SSH log in, 3-2
 - SSH log out, 3-2
 - static IP, Ethernet, 2-8
 - static IP, serial, 2-7
 - clock, 6-4
 - configuring alerts, 5-11
 - configuring DHCP, 2-5
 - configuring static IP address, 2-6
 - default settings, 1-3
 - Ethernet connection, 2-3
 - managing network settings, 3-10
 - managing serial port settings, 3-12
 - managing user accounts, 3-13
 - namespaces, 3-3
 - password authentication, 10-4

- power and WebGUI, 8-13
- redirecting keyboard and mouse, 8-10
- resetting password, 5-6
- serial connection, 2-1
- serial port, configuring, 6-2
- tasks and management interfaces, 1-2
- time-out, 6-1
- upgrading firmware, 5-2
- user accounts, 7-2
- WebGUI, configuring static IP, 2-8

- internal serial port, 6-2

- IP address

- static, 2-6

- IPMI, 3-17, 4-2

- alerts and traps, 3-16

- IPMITool, 9-2

- overview, 1-2, 9-1

- sensors, 9-2

J

- Java Client, remote console, 1-2

L

- LDAP

- authentication, 10-4

- log in

- CLI and SSH, 3-2

- WebGUI, 4-4

- log out

- CLI and SSH, 3-2

- WebGUI, 4-4

M

- MAC address, 1-4, 2-2, 2-5

- Management Information Base (MIB)

- description of, 11-2

N

- N1, 1-4

- NTP, configuring, 3-18

P

- password, root, 3-2

- PET alerts, 3-17

R

- remote client, redirecting hardware to, 8-3
- remote console
 - overview, 1-2, 8-1
 - redirecting
 - keyboard and mouse, 8-10
 - storage devices, 8-12
 - sending a break to host, 8-11
 - starting, 8-4
- replaceable components, 5-6
- root password, 3-2

S

- sending a break to host, 3-9, 8-11
- sensors
 - fan sensors, temperature, 5-7
 - voltage, 5-7
- server locator, 5-23
- service processor, 1-1
- SNMP, 11-1 to 11-6
 - and MIB, 11-2
 - enabling settings and users, 5-18
 - host state, how to manage, 3-8
 - management software, 11-3
 - overview, 1-2, 11-1
 - Port, Standard (161), 11-3
 - user accounts
 - adding, 11-5
 - configuring, 11-5
 - deleting, 11-5
 - properties, 11-6
 - v1, v2c, v3, 11-6
- SP
 - overview, 1-1
 - software, *see* ILOM
- SSH
 - CLI log in, 3-2
 - CLI log out, 3-2
 - settings, 3-6
- static IP address, 2-6
- system management using N1, 1-4

T

- temperature sensors, 5-7
- time stamp, 5-17

U

- user accounts, ILOM, 7-2
- user privilege levels, 3-4
- users, enabling with SNMP, 5-18

V

- viewing
 - event log, 5-15
 - replaceable components, 5-6
- voltage sensors, 5-7

W

- WebGUI
 - configuring serial port, 6-2
 - controlling power, 8-13
 - log in, 4-4
 - log out, 4-4
 - overview, 1-1
 - remote console, 8-1
 - setting clock, 6-4
 - static IP, configuring, 2-8
 - time-out, 6-1

