Integrated Lights Out Manager (ILOM) Administration Guide

For ILOM 1.1.1

Sun Microsystems, Inc.
www.sun.com

Part No. 820-0280-12
May 2007, Revision 01

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

Contents

Preface

The *Integrated Lights Out Manager (ILOM) Administration Guide for ILOM 1.1.1* provides instructions for managing Sun servers using the Integrated Lights Out Manager.

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 Blade™ 6000 products consist of a chassis containing multiple, replacable server modules. On these products, the chassis is equipped with a separate service processor that supports chassis-level functionality, such as fans and power supplies, and that provides access to the service processors on the server modules. This chassis-level service processor is called a Chassis Management Module (CMM).

- This document covers the service processor(s) in the server modules.
- Separate documents provide information about the CMM. See the documentation provided with the chassis.

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`

Shell Prompts

Shell	Prompt
C shell	*machine-name*`%`
C shell superuser	*machine-name*`#`
Bourne shell and Korn shell	`$`
Bourne shell and Korn shell superuser	`#`

Typographic Conventions

Typeface*	Meaning	Examples
`AaBbCc123`	The names of commands, files, and directories; onscreen computer output	Edit your `.login` file. Use `ls -a` to list all files. `% You have mail.`

`AaBbCc123`	What you type, when contrasted with onscreen computer output	`%` **`su`**
		`Password:`

AaBbCc123	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the *User's Guide*. These are called *class* options. You must be *superuser* to do this. To delete a file, type `rm` *filename*.

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

Documentation, Support, and Training

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

Third-Party Web Sites

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

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. 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 for ILOM 1.1.1, part number 820-0280-12

CHAPTER 1

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 10.

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 11.

- 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 14.

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 their 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

1.1.3 ILOM and Sun Blade 6000 Systems

A Sun Blade 6000 system consists of a chassis with a number of servers, called server modules, inside. Each server consists of a PC card that draws its power and cooling from the chassis.

On these systems, each server module is equipped with its own service processor. Also, the chassis is equipped with a service processor that supports chassis-level functionality, such as fans and power supplies, and that provides access to the service processors on the server modules. This chassis-level service processor is called a Chassis Management Module (CMM).

For more information on the CMM, see the corresponding documentation provided with the chassis.

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, go to:

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

CHAPTER 2

Connecting and Initial Setup

This chapter describes how to connect to the ILOM and how to do the initial setup. It contains the following sections:

- Section 2.1, "Connecting to the ILOM" on page 2-1
- Section 2.2, "Configuring the ILOM IP Address" on page 2-7

2.1 Connecting to the ILOM

The way you connect to ILOM depends on whether it is in a rack-mounted server, or whether it is in a server module installed in a chassis.

TABLE 2-1 lists the different connection methods, and their relevance to rack-mounted servers and server modules in a chassis:

TABLE 2-1 Connection Methods

Connection Method	Rack-Mounted	Server Module	Supported Interface	Comments/Description
Ethernet	Yes	Yes	CLI and WebGUI	This is the normal method of connecting to the ILOM. You must know the ILOM's Ethernet address. **Note: This is the only method that supports WebGUI access.**
Serial, direct	Yes	No	CLI only	Connect directly to serial management port on server.
Serial, through dongle cable	No	Yes	CLI only	Connect a dongle cable directly to the server module.
Serial, through chassis/CMM	No	Yes	CLI only	Log in to the CMM, navigate to server module, then execute command to start ILOM.

The following sections describe each method.

2.1.1 Connecting to the ILOM Using an Ethernet Connection

The Ethernet connectivity provides full access to the ILOM CLI and WebGUI.

- For rack mounted servers, you must connect a LAN to the Ethernet port and configure your Ethernet connection.
- For server modules in a chassis, you must connect a LAN to the NET MGT port on the chassis. When a server module is installed in a chassis, the ILOM is automatically connected to the same subnet as the CMM ILOM.

Note – Some server modules have different (non-ILOM) service processors. See the documentation provided with the server module for more details.

To connect to the Ethernet, you must know the ILOM's IP address. To discover, and or to configure the ILOM IP address, see Section 2.2.1, "Viewing the ILOM IP Address" on page 2-7 for more information.

Note – The ILOM supports a maximum of 10 active sessions, including serial, ssh, and WebGUI sessions. You can view active sessions by entering the command `show /SP/sessions` from the CLI.

Connecting to the CLI

1. **Start your ssh client.**

2. **To log in to the ILOM, type:**

   ```
   $ ssh username@ipaddress
   ```

   where *username* is the user ID, and *ipaddress* is the IP address of the ILOM. The default user is `root`.

3. **Type your password when prompted.**

   The default is `changeme`.

   The CLI command prompt appears.

Connecting to the WebGUI

For more detailed instructions, see Section 4.2, “Logging In to the WebGUI” on page 4-4.

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

   The login screen appears.

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.

3. **Click Log In.**

   The WebGUI appears.

4. **To log out of the WebGUI, click Log Out at the top right of the WebGUI.**

   The logout screen appears.

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

2.1.2 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.

- For rack-mounted systems, connect the cable directly to the RJ-45 or DB9 serial port.
- For many server modules in a chassis, you have to connect a dongle cable directly to the server module, and connect a the terminal to the DB9 connector on the dongle cable. You might also require a DB9 to RJ-45 serial adapter.

  For other server modules, you can connect directly to the serial port on the server module.

  See the server module documentation for additional details.

1. **Verify that your terminal, laptop, or terminal server is operational.**

2. **Configure the terminal device or the terminal emulation software to use the following settings:**

- 8N1: eight data bits, no parity, one stop bit
- 9600 baud (default, can be set to any standard rate up to 57600)
- Disable software flow control (XON/XOFF)

3. **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 to the server or server module.**

   For rack-mounted servers, connect a serial cable from the serial port on the server's back panel to a terminal device.

   For server modules, connect a dongle cable directly to the server module, and connect a the terminal to the DB9 connector on the dongle cable using a DB9 to RJ-45 serial adapter.

   Refer to your platform-specific documentation for additional details.

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 on or during its power on sequence, you will see bootup messages.

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

```
SUNSPnnnnnnnnnnn login:
```

The first string in the prompt is the default host name. It consists of the prefix SUNSP and the ILOM's media access control (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`.**

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

```
->
```

The ILOM is 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/PROC
```

7. **When you are done, type `exit` to quit.**

Chapter 3 describes how to use the CLI.

2.1.3 Connecting to the ILOM through the CMM

The chassis serial connector connects to the CMM ILOM, which provides a command to connect to the server module ILOM. This connection requires a terminal or a PC running terminal emulation software to the RJ-45 serial port on the chassis.

This section applies only to systems that meet the following requirements:

- The server module must be installed in a chassis equipped with a Chassis Management Module (CMM) ILOM.

  See the chassis documentation for additional details.

- The server module must be equipped with an ILOM. Some server modules have different service processors.

  See the server module documentation for additional details.

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

3. **Connect a serial cable from the serial port on the chassis to a terminal device.**

   Refer to the chassis documentation for the location of the serial port.

4. **Press Enter on the terminal device.**

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

   The CMM ILOM displays its login prompt:

   ```
   SUNCMMnnnnnnnnnn login:
   ```

   The first string in the prompt is the default host name. It consists of the prefix SUNCMM and the CMM ILOM’s MAC address. The MAC address for each service processor is unique.

5. **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 CMM ILOM displays its default command prompt:

   ```
   ->
   ```

   You are now connected to the CMM ILOM CLI.

6. **Navigate to the server module ILOM by typing this command:**

   ```
   cd /CH/BLn/SP/cli
   ```

   Where *n* is number of the server module.

7. **Enter the command `start.`**

   A prompt appears.

8. **Enter `y` to continue or `n` to cancel.**

   If you entered **`y`**, the server module ILOM prompts for its password.

Note – The CMM ILOM logs on to the server module ILOM using the user name in the `user` target under `/CH/BLn/SP/cli` (where *n* is the server module number). See the chassis documentation for additional details.

---

9. **Enter the password when prompted.**

   The default is **`changeme`**.

   The server module ILOM prompt appears.

10. **When you are done, type `exit`.**

    The server module ILOM exits and the CMM CLI prompt appears.

The following display shows an example of the login screen:

```
 -> cd /CH/BL2/SP/cli
/CH/BL2/SP/cli

-> start
Are you sure you want to start /CH/BL2/SP/cli (y/n)? y
Password:            Type the password to the server module ILOM.

Sun(TM) Integrated Lights Out Manager

Version N.N

Copyright 2006 Sun Microsystems, Inc. All rights reserved.
Use is subject to license terms.

Warning: password is set to factory default.

-> exit              Type this command to exit the server module ILOM
                     and return to the CMM ILOM.
Connection to 10.6.122.33 closed.
```

2.2 Configuring the ILOM IP Address

You can configure the ILOM IP address using one of several methods:

- Using the BIOS Setup Utility. See Section 2.2.3, "Configuring the IP Address Using the BIOS Setup Utility" on page 2-9.
- Using the CLI. See Section 2.2.4, "Configuring the ILOM Using the CLI" on page 2-10.
- Using the WebGUI. See Section 2.2.5, "Configuring the IP Address Using the WebGUI" on page 2-11.

2.2.1 Viewing the ILOM IP Address

To find the ILOM IP address:

1. **Log in to the ILOM CLI using any of the methods described in** Section 2.1, "Connecting to the ILOM" on page 2-1.

   To use the Ethernet ssh connection, you must already know the IP address.

2. **Type the command:**

- To see all the IP address-related information, type:

  `show /SP/network`

- To see only the IP address, type:

  `show /SP/network/ipaddress`

2.2.2 Using DHCP to Assign an IP Address

Most installations use DHCP to assign an IP address to the ILOM. To use DHCP, the following conditions must be present:

- A DHCP server must be connected to the same subnet as the ILOM.
- The DHCP server must be configured to accept new MAC addresses.
- The ILOM must be configured to use DHCP. This is its default setting.

  If the ILOM is not configured to use DHCP, you can configure it using any of the following sections:

  - Section 2.2.3, “Configuring the IP Address Using the BIOS Setup Utility” on page 2-9
  - Section 2.2.4, “Configuring the ILOM Using the CLI” on page 2-10
  - Section 2.2.5, “Configuring the IP Address Using the WebGUI” on page 2-11

If these conditions are present, when the ILOM is powered on or reset, DHCP automatically assigns it an IP address.

Note – Some DHCP servers allow you to specify the IP address that it will assign to the ILOM. In this case, the ILOM still must be configured for a “dynamic” IP address, even though DHCP’s choice of addresses is “static.”

Finding the ILOM’s MAC Address

The ILOM has a unique MAC address that is different from the server or server module’s MAC address. You might need this address to configure your DHCP server software.

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.

You can obtain the ILOM MAC address in one of the following ways:

- Start the ILOM CLI and enter the command **`show /SP/network`**. The ILOM displays its MAC address.

- For rack-mounted servers, there is a label attached to the GRASP board. Open the cover of the server to view this label.
- Check the Customer Information Sheet shipped with your server.
- The system BIOS setup screen. Choose Advanced - IPMI 2.0 Configuration - Set LAN Configuration - MAC address.

Using the MAC Address to Find the IP Address

Once the ILOM has been assigned an IP address by DHCP, you can use the MAC address to identify that IP address by looking in the DHCP log file.

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.

2.2.3 Configuring the IP Address Using the 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 it to a power source.**

   Refer to your platform documentation for details.

2. **If you are going to use DHCP, verify that your DHCP server is configured to accept new 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. **Highlight LAN Configuration then select Enter.**

   The LAN Configuration page appears.

7. **Fill in the IPMI 2.0 Configuration page.**

8. **Under IP Assignment, select DHCP or Static.**

- If you selected Static, fill in the IP address, subnet mask and default gateway at the bottom of the page.
- If you select DHCP, your installation must meet the conditions described in Section 2.2.2, "Using DHCP to Assign an IP Address" on page 2-8.

9. **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.

2.2.4 Configuring the ILOM Using the CLI

To configure the ILOM IP address using the CLI, do the following.

1. **Connect to the ILOM CLI using one of the methods described in Section 2.1, "Connecting to the ILOM" on page 2-1.**

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

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

```
cd /SP/network
```

4. **Configure the IP address:**

- To configure a static IP address, type:

```
set pendingipaddress=xxx.xxx.xx.xx
set pendingipnetmask=yyy.yyy.yyy.y
set pendingipgateway=zzz.zzz.zz.zzz
set pendingipdiscovery=static
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 configure a dynamic IP address, type:

```
set pendingipdiscovery=dhcp
set commitpending=true
```

If you configure the ILOM to use DHCP, your installation must meet the conditions described in Section 2.2.2, "Using DHCP to Assign an IP Address" on page 2-8.

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

2.2.5 Configuring the IP Address Using the WebGUI

To configure the ILOM IP address using the WebGUI, do the following.

1. **Connect to the ILOM through a web browser as described in** Section 2.1.1, "Connecting to the ILOM Using an Ethernet Connection" on page 2-2**.**

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 and configure the IP address:**

   a. **To use DHCP, select the radio button next to Obtain an IP Address Automatically (Use DHCP).**

      If you select DHCP, your installation must meet the conditions described in Section 2.2.2, "Using DHCP to Assign an IP Address" on page 2-8.

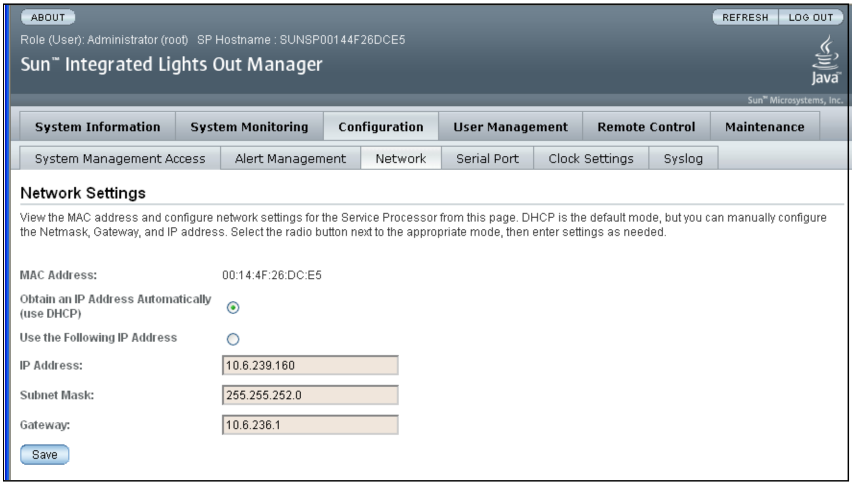
   b. **To use a static IP address:**

      i. **Select the radio button next to Use the Following IP Address**

      ii. **Enter the IP address, subnet mask, and gateway IP address in the corresponding fields.**

   See FIGURE 2-1.

FIGURE 2-1 Integrated Lights Out Manager Network Settings Page



Network Settings

View the MAC address and configure network settings for the Service Processor from this page. DHCP is the default mode, but you can manually configure the Netmask, Gateway, and IP address. Select the radio button next to the appropriate mode, then enter settings as needed.

MAC Address: 00:14:4F:26:DC:E5

Obtain an IP Address Automatically (use DHCP) ●

Use the Following IP Address ○

IP Address: 10.6.239.160

Subnet Mask: 255.255.252.0

Gateway: 10.6.236.1

5. Click Save when you are done.

CHAPTER 3

Using the Command-Line Interface

This chapter describes how to use the ILOM's command-line interface (CLI). The sections include:

- Section 3.1, "Using CLI Commands" on page 3-1
- Section 3.2, "Command Syntax" on page 3-4

To connect to the CLI, see Section 2.1, "Connecting to the ILOM" on page 2-1

3.1 Using CLI Commands

This section describes how to use CLI commands. CLI commands are case-sensitive.

3.1.1 CLI Namespace

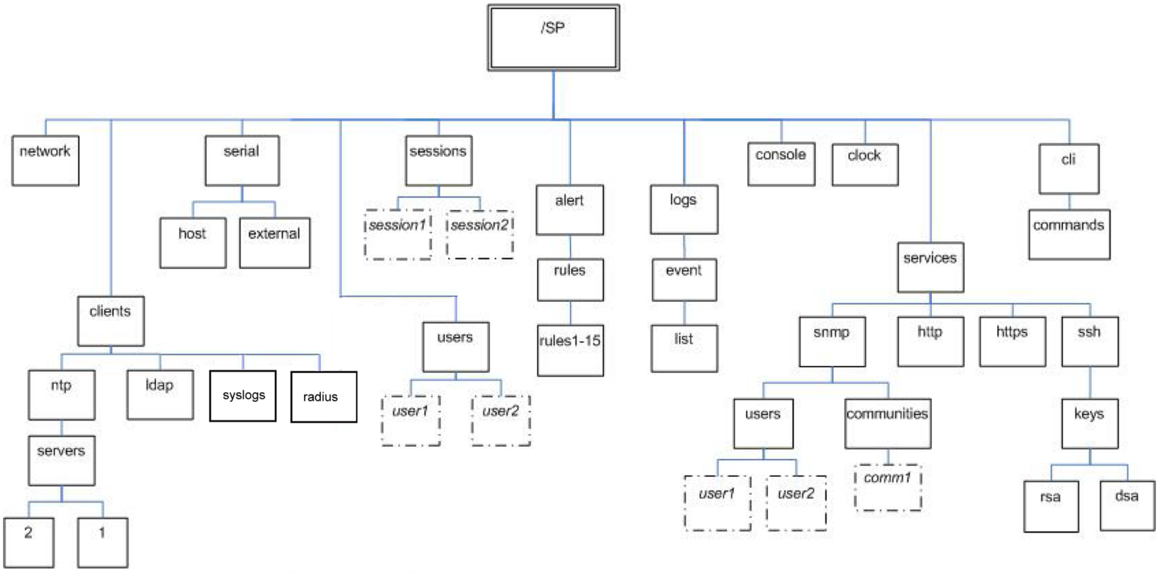
The CLI architecture is based on a hierarchical namespace, which is a predefined tree that contains every managed object in the system. This namespace defines the targets for each command verb.

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 Typical SP Namespace



3.1.2 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 Chapter 5.

3.1.3 CLI Command Syntax

The syntax of a command is: `verb options target properties`

The following sections describe each of these.

3.1.3.1 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.

3.1.3.2 Command Options

The CLI supports the options listed in TABLE 3-2. Not all options are supported for all commands. See a specific command section for the options that are valid with that command. The help option 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.
`-force`	`-f`	Causes an immediate action instead of an orderly shutdown.
`-help`	`-h`	Displays Help information.
`-level`	`-l`	Executes the command for the current target and all targets contained through the level specified.

TABLE 3-2 Command Options *(Continued)*

Option Long Form	Short Form	Description
`-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.

3.1.3.3 Command Targets

Every object in your namespace is a target. Not all targets are supported for all commands. Section A.2, "CLI Command Reference" on page A-6 lists each command, with its targets and properties.

3.1.3.4 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-6 lists each command, with its targets and properties.

3.2 Command Syntax

To execute most commands, you need to specify the location of the target, then enter the command. You can execute commands individually, or you can combine them on the same command line.

1. **To execute commands individually:**

   a. **Navigate to the namespace using the `CD` command.**

      For example:

      ```
      cd /SP/services/http
      ```

   b. **Enter the verb, target, and value.**

      For example:

      ```
      set port=80
      ```

2. **To combine commands, use the form** *verb path/target=value*.

   For example:

   set /SP/services/http port=80

   The following display shows both methods:

```
-> cd /SP/services/http          - Navigate to namespace
/SP/services/http

-> set port=80
Set 'port' to '80'               -Enter the verb, target, and value


-> set /SP/services/http port=80 - Combine path and show command
Set 'port' to '80'

->
```

CHAPTER 4

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 to 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 web 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 10.

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 that 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 changed their assigned roles or privileges.

For more information on users, including how to manage user accounts using the WebGUI, see Chapter 5.

4.1.3 WebGUI Tasks

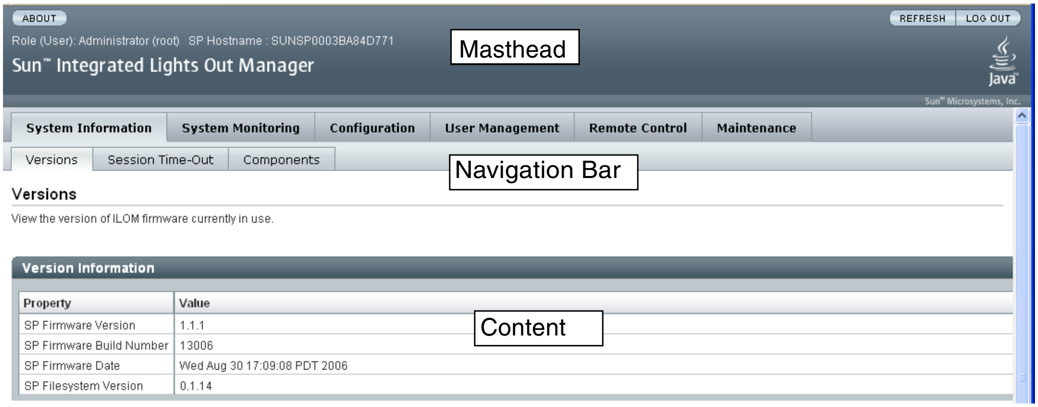
Some of the common tasks you can perform using the WebGUI include:

- 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

FIGURE 4-1 shows a WebGUI page.

FIGURE 4-1 WebGUI Sample Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Sun™ Integrated Lights Out Manager

Versions

View the version of ILOM firmware currently in use.

Version Information

Property	Value
SP Firmware Version	1.1.1
SP Firmware Build Number	13006
SP Firmware Date	Wed Aug 30 17:09:08 PDT 2006
SP Filesystem Version	0.1.14

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 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 to the WebGUI

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

Note – The ILOM boots automatically when a Sun server is cabled appropriately and plugged in to an AC supply, or when a server module is inserted into a powered chassis. This usually happens 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.

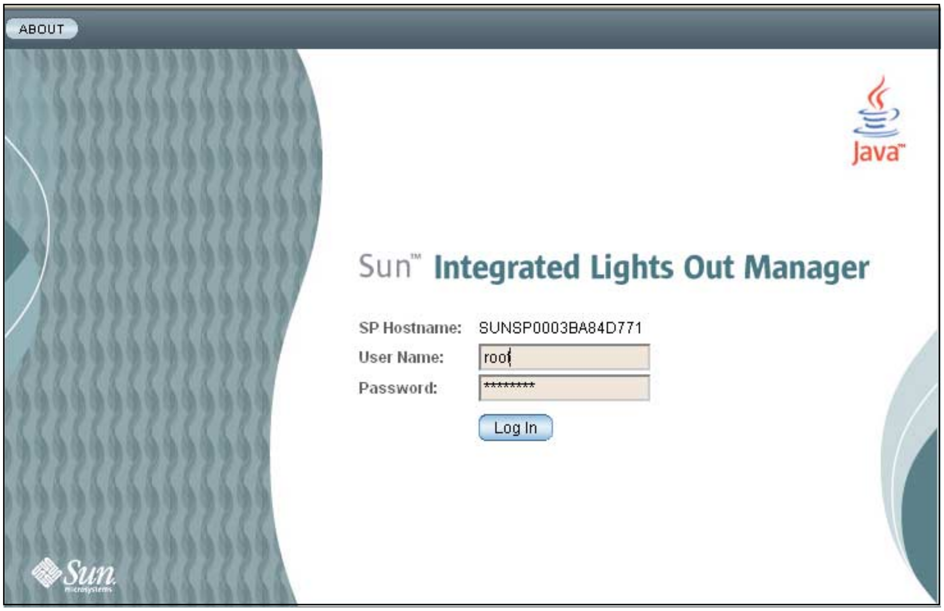
Note – Do not use the Refresh or Log Out buttons in your Internet web browser when using the WebGUI. Instead, use only the Refresh and Log Out buttons provided at the top right of the WebGUI window.

You need the IP address of the ILOM. For information on viewing and setting the IP address, see Section 2.2, “Configuring the ILOM IP Address” on page 2-7.

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



SP Hostname: SUNSP0003BA84D771

User Name: root

Password: ********

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.

   The user `root` is preconfigured, with the role administrator. You cannot delete this user ID or change its role attributes. The initial password `changeme` is also provided. This password is required to 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 Chapter 5 for details.

3. **Click Log In.**

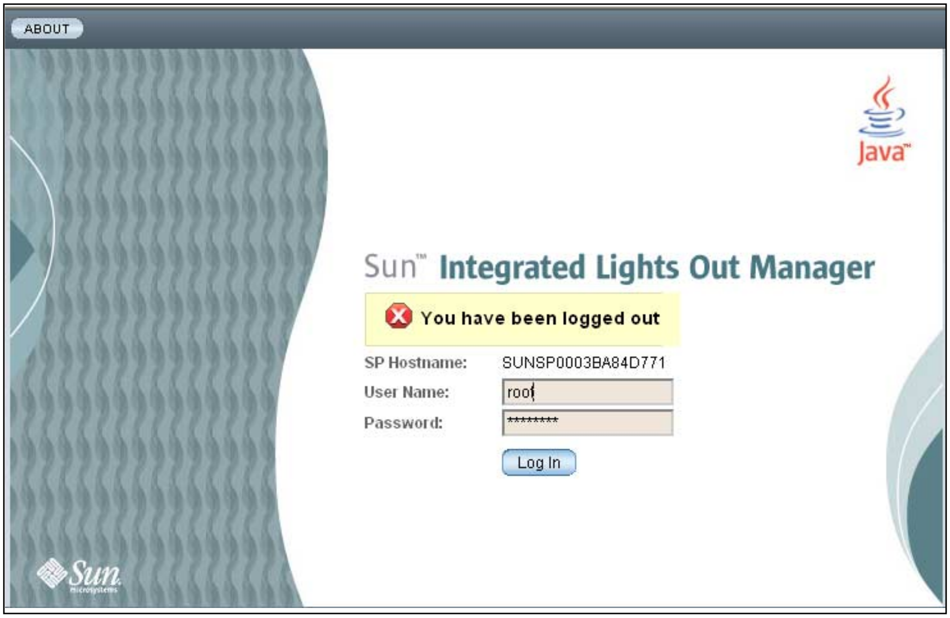
   The WebGUI appears.

4. **To log out of the WebGUI, click Log Out at the top right of the WebGUI.**

   You are logged out and the Login screen appears.

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

FIGURE 4-3 WebGUI Log Out Screen



You have been logged out

SP Hostname: SUNSP0003BA84D771

User Name: root

Password: *********

CHAPTER 5

Managing User Accounts

This chapter describes how to manage user accounts using the CLI and the WebGUI. It includes the following sections:

- Section 5.1, "User Accounts Overview" on page 5-1
- Section 5.2, "Managing User Accounts Using the CLI" on page 5-2
- Section 5.3, "Managing User Accounts Using the WebGUI" on page 5-4

5.1 User Accounts Overview

The ILOM supports up to nine user accounts. The root account is 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 called sunservice, 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 change configuration settings.

  Operators cannot:

  - See or change LDAP settings
  - See or change RADIUS 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)

5.2 Managing User Accounts Using the CLI

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

5.2.1 Adding a User Account

Type the following command to add a local user account:

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

Only accounts with administrator privileges are allowed to add, modify, or delete user accounts. However, operators can modify their own password.

5.2.2 Deleting a User Account

Type the following command to delete a local user account:

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

5.2.3 Displaying User Accounts

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

```
show /SP/users
```

5.2.4 Configuring User Accounts

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

5.2.4.1 Syntax

`set target` *[propertyname=value]*

5.2.4.2 Targets, Properties, and Values

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

TABLE 5-1 Valid Targets, Properties, and Values for Local User Accounts

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

Examples

When changing the role for user1 from administrator to operator type:

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

To change the password for user1, 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.

5.3 Managing User Accounts Using the WebGUI

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

5.3.1 Adding User Roles and Setting Privileges

1. **Log in to the ILOM as administrator.**

   Only accounts with administrator privileges are allowed to add, modify, or delete user accounts. However, operators can modify their own password.

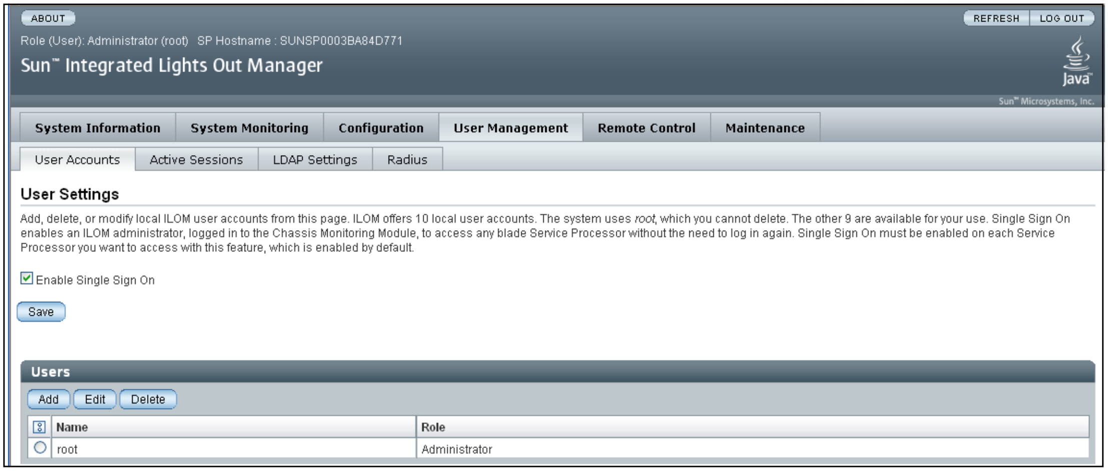
   If a new user is given administrator privileges, those privileges are also automatically granted for the command-line interface (CLI) and Intelligent Platform Management Interface (IPMI) to the ILOM.

2. **Select User Management => User Accounts.**

   The User Accounts page appears.

Note – The ILOM supports a maximum of nine user accounts. If all nine user account slots are configured, you must delete an existing user account before you can add a new user account. See Section 5.3.3, "Deleting User Accounts" on page 5-9.

FIGURE 5-1 User Accounts Page



User Settings

Add, delete, or modify local ILOM user accounts from this page. ILOM offers 10 local user accounts. The system uses *root*, which you cannot delete. The other 9 are available for your use. Single Sign On enables an ILOM administrator, logged in to the Chassis Monitoring Module, to access any blade Service Processor without the need to log in again. Single Sign On must be enabled on each Service Processor you want to access with this feature, which is enabled by default.

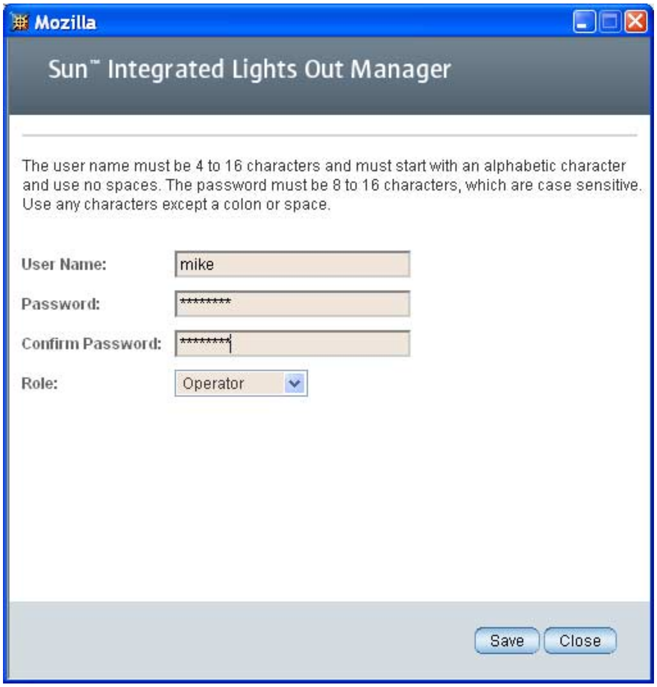
☑ Enable Single Sign On

	Name	Role
○	root	Administrator

3. **Click Add.**

   The Add User dialog box appears.

FIGURE 5-2 Add User Dialog Box



The user name must be 4 to 16 characters and must start with an alphabetic character and use no spaces. The password must be 8 to 16 characters, which are case sensitive. Use any characters except a colon or space.

User Name: mike

Password: *********

Confirm Password: *********

Role: Operator

4. **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.**

   d. **Select Administrator or Operator from the Role drop-down menu.**

   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.

5.3.2 Modifying User Accounts

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

Note – Normally, only accounts with administrator privileges are allowed to add, modify, or delete user accounts. However, operators can modify their own password.

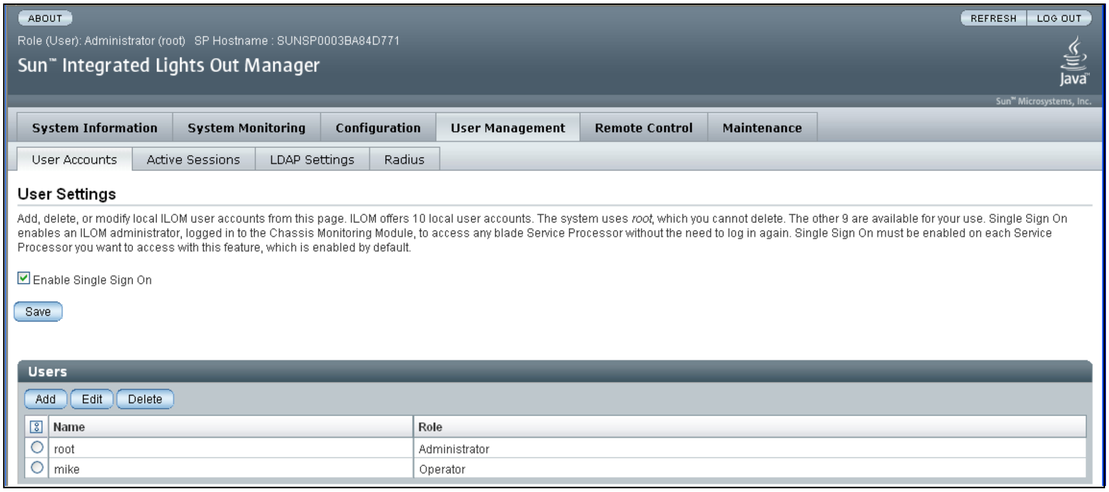
If a new user is given administrator privileges, those privileges are also automatically granted to the user for the command-line interface (CLI) and Intelligent Platform Management Interface (IPMI) to the ILOM.

1. **Log in to the ILOM as administrator.**

2. **Select User Management => User Accounts.**

   The User Accounts page appears.

FIGURE 5-3 User Accounts Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Sun™ Integrated Lights Out Manager

User Settings

Add, delete, or modify local ILOM user accounts from this page. ILOM offers 10 local user accounts. The system uses *root*, which you cannot delete. The other 9 are available for your use. Single Sign On enables an ILOM administrator, logged in to the Chassis Monitoring Module, to access any blade Service Processor without the need to log in again. Single Sign On must be enabled on each Service Processor you want to access with this feature, which is enabled by default.

☑ Enable Single Sign On

Users

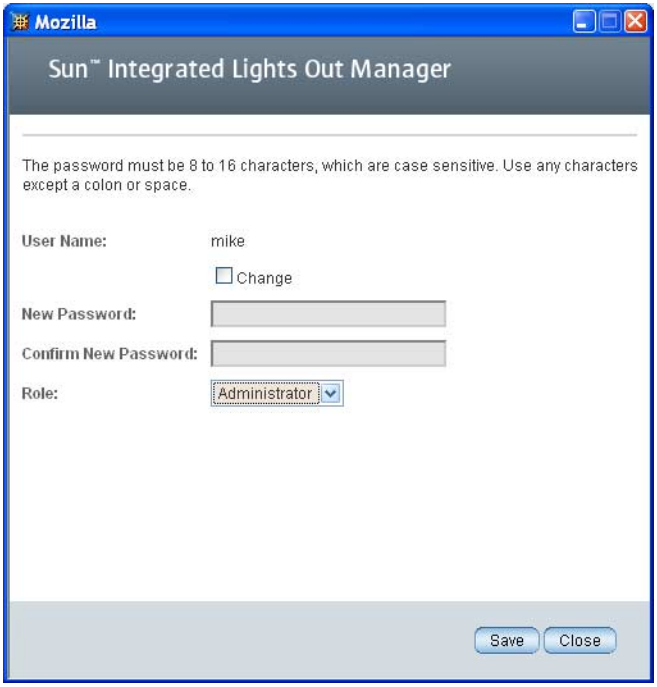
	Name	Role
○	root	Administrator
○	mike	Operator

3. **Select a radio button to select a user account to modify.**

4. **Click Edit.**

   The Edit User dialog box appears.

FIGURE 5-4 Edit User Dialog Box



The password must be 8 to 16 characters, which are case sensitive. Use any characters except a colon or space.

User Name: mike

□ Change

New Password:

Confirm New Password:

Role: Administrator

5. **Modify the password if needed.**

   a. **Select the Change 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. **Select a role from the Role drop-down menu.**

7. **After you have modified the account information, click Save for your changes to take effect, or click Close to return to the previous settings.**

   The User Accounts page is redisplayed.

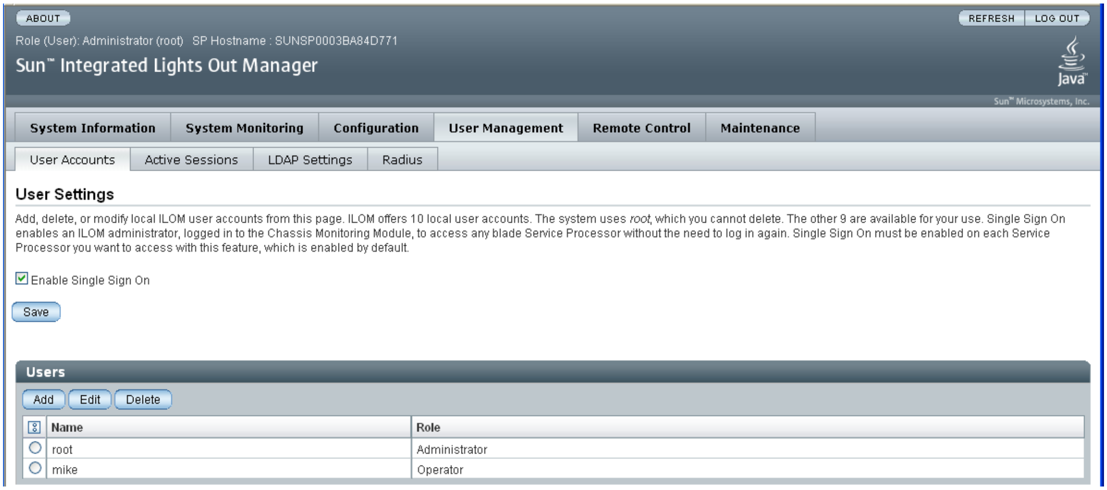
5.3.3 Deleting User Accounts

This section describes how to delete a user account.

1. **Log in to the ILOM as administrator.**
2. **Select User Management => User Accounts.**

   The User Accounts page appears.

FIGURE 5-5 User Accounts Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

User Settings

Add, delete, or modify local ILOM user accounts from this page. ILOM offers 10 local user accounts. The system uses *root*, which you cannot delete. The other 9 are available for your use. Single Sign On enables an ILOM administrator, logged in to the Chassis Monitoring Module, to access any blade Service Processor without the need to log in again. Single Sign On must be enabled on each Service Processor you want to access with this feature, which is enabled by default.

☑ Enable Single Sign On

	Name	Role
○	root	Administrator
○	mike	Operator

3. **Select the radio button next to the user account you want to delete.**

   You cannot delete the root account.

4. **Click Delete.**

   The user accounts page appears with the user deleted.

CHAPTER 6

Managing the ILOM Using the CLI

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

6.1 Configuring the Serial Port

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 the back of the server.

6.1.1 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
```

6.1.2 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.

6.1.2.1 Syntax

`set target` *[propertyname=value]*

6.1.2.2 Targets, Properties, and Values

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

TABLE 6-1 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=57600 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.

6.2 Configuring ILOM Network Settings

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

6.2.1 Displaying Network Settings

Type the following command to display network settings:

```
show /SP/network
```

6.2.2 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.

6.2.2.1 Syntax

`set target` *[propertyname=value]*

6.2.2.2 Targets, Properties, and Values

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

TABLE 6-2 ILOM Network Targets, Properties, and Values

Target	Property	Value	Default
`/SP/network`	ipaddress ipdiscovery ipgateway ipnetmask	These read only values are updated by the system	
	macaddress	MAC address of ILOM	
	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 disconnects 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
```

6.3 Setting the ILOM Clock

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.

6.3.1 Displaying Clock Settings

Type the following command to display clock settings:

```
show /SP/clock
```

6.3.2 Configuring the Clock to Use NTP Servers

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

6.3.2.1 Syntax

`set target` *[propertyname=value]*

6.3.2.2 Targets, Properties, and Values

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

TABLE 6-3 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.

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 is in UTC.
- **Through the CLI, WebGUI, and IPMI**

6.4 Resetting the ILOM

To reset the ILOM using the CLI, type **`reset /SP`**.

6.5 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.

6.6 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 filesystem corruption.

Note – The upgrade takes about five minutes. 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 results 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:
.
Firmware update is complete.
ILOM will not be restarted with the new firmware.
```

6.7 Enabling HTTP or HTTPS Web Access

The ILOM allows you to enable HTTP or HTTPS, and it allows you to automatically redirect HTTP access to HTTPS. It also allows you to set the HTTP and HTTPS ports.

The properties are located in `/SP/services/http` and `/SP/services/https`.

Use the `set` command to change properties and values as follows:

TABLE 6-4 Values for HTTP and HTTPS Settings

Desired State	Target	Values
Enable HTTP only	HTTP	securedirect=enabled
	HTTP	servicestate=disabled
	HTTPS	servicestate=disabled
Enable HTTP and HTTPS	HTTP	securedirect=disabled
	HTTP	servicestate=enabled
	HTTPS	servicestate=enabled
Enable HTTPS only	HTTP	securedirect=disabled
	HTTP	servicestate=disabled
	HTTPS	servicestate=enabled
Automatically redirect HTTP to HTTPS	HTTP	securedirect=enabled
	HTTP	servicestate=disabled
	HTTPS	servicestate=enabled

6.7.0.1 Targets, Properties, and Values

The following table shows the properties and values for HTTP and HTTPS.

TABLE 6-5 Valid Targets, Properties, and Values for HTTP and HTTPS

Target	Property	Value	Default
`/SP/services/http`	securedirect	enabled | disabled	enabled
	servicestate	enabled | disabled	disabled
	port	<portnum>	80
`/SP/services/https`	servicestate	enabled | disabled	enabled
	port	<portnum>	443

6.8 Viewing ssh Settings

Use the `show` command to view ssh settings. These are read-only values that you can display but not write.

TABLE 6-6 shows the valid targets and properties for ssh values.

TABLE 6-6 Valid Targets and Properties for ssh

Target	Property
`/SP/services/ssh/keys/dsa`	fingerprint length publickey
`/SP/services/ssh/keys/rsa`	fingerprint length publickey

Use the `show` command to enter `dsa` or `rsa` values.

Example:

```
 -> show /SP/services/ssh/keys/dsa

 /SP/services/ssh/keys/dsa
    Targets:

    Properties:
        fingerprint =
f7:49:85:b0:e3:65:c0:d0:96:48:06:f5:8c:b7:9c:6b
        length = 1024
        publickey =
AAAAB3NzaC1kc3MAAACBAKh+LPnkehPiIou96JraqiZ7qjJ4KTc4DdNJ3ZkBZ94X
Krz2B5BNROCL7h4Gb7uAaMZEgtpPqefKy5awEvkA8jNyL5P=

    Commands:
        cd
        show

->
```

6.9 Displaying ILOM Information

You can display active sessions, current versions, and other information about the ILOM using the CLI. TABLE 6-7 shows the commands and the information they display.

TABLE 6-7 Commands to Display ILOM Information

Command	Information Displayed
`version`	The current ILOM version
`show /SP/cli/commands`	All the CLI commands
`show /SP/sessions`	All active sessions
`help targets`	Available valid targets

6.9.1 Displaying Version Information

Type the following command to display the current ILOM version:

`version`

For example:

```
-> version
SP firmware 1.1.1
SP firmware build number: r14021
SP firmware date: Fri Oct 13 21:18:44 PDT 2006
SP filesystem version: 0.1.14

->
```

6.9.2 Displaying Available Targets

Type the following command to display the available valid targets:

`help targets`

CHAPTER 7

Managing the ILOM Using the WebGUI

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

It includes the following sections:

7.1 Configuring the Serial Port

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

The serial port provides access to the WebGUI, the command-line interface (CLI), and 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.

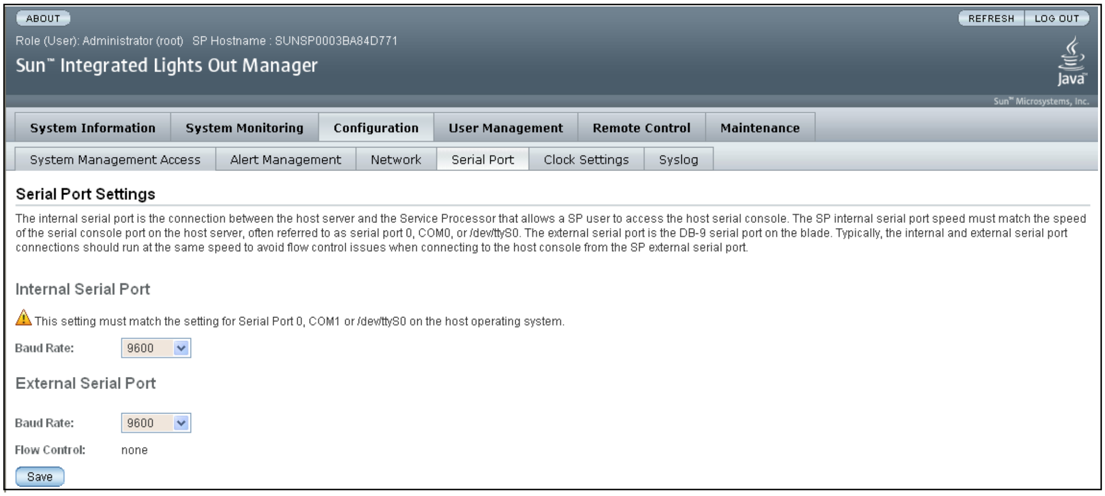
Note – Normally, the console matches the ILOM's default settings (9600 baud, 8N1 [eight data bits, no parity, one stop bit], no flow control).

- 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.**
2. **Select Configuration => Serial Port.**

   The Serial Port Settings page appears.

FIGURE 7-1 Serial Port Settings Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Sun™ Integrated Lights Out Manager

Serial Port Settings

The internal serial port is the connection between the host server and the Service Processor that allows a SP user to access the host serial console. The SP internal serial port speed must match the speed of the serial console port on the host server, often referred to as serial port 0, COM0, or /dev/ttyS0. The external serial port is the DB-9 serial port on the blade. 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 SP external serial port.

Internal Serial Port

⚠ This setting must match the setting for Serial Port 0, COM1 or /dev/ttyS0 on the host operating system.

Baud Rate: 9600

External Serial Port

Baud Rate: 9600

Flow Control: none

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

   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.

   To connect to the system console using the ILOM, the ILOM must be set to its default settings (9600 baud, 8N1 [eight data bits, no parity, one stop bit], no flow control).

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

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

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

7.2 Configuring ILOM Network Settings

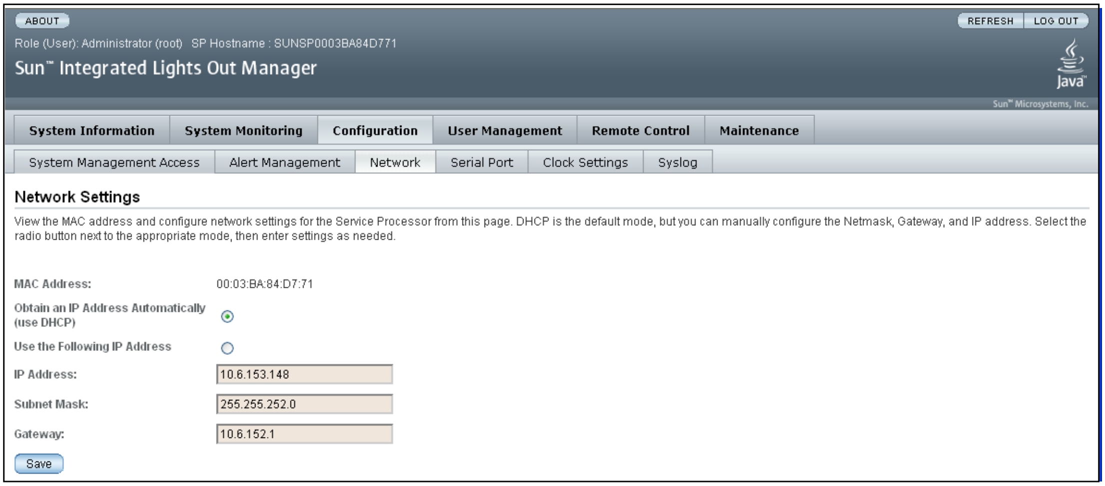
This section describes how to configure the network parameters for the ILOM.

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.**
2. **Select Configuration => Network.**

   The Network Settings page appears.

FIGURE 7-2 Network Settings Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Sun™ Integrated Lights Out Manager

Network Settings

View the MAC address and configure network settings for the Service Processor from this page. DHCP is the default mode, but you can manually configure the Netmask, Gateway, and IP address. Select the radio button next to the appropriate mode, then enter settings as needed.

MAC Address: 00:03:BA:84:D7:71

Obtain an IP Address Automatically (use DHCP) ●

Use the Following IP Address ○

IP Address: 10.6.153.148

Subnet Mask: 255.255.252.0

Gateway: 10.6.152.1

3. **Complete the information in the Network Settings page.**

   Use the descriptions in TABLE 7-1 when completing the information.

TABLE 7-1 Network Settings Page Fields

Item	Description
MAC Address	The ILOM's 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. • **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.
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 Save for your settings to take effect.**

Note – Changing the IP address ends your ILOM session.
Settings are considered pending until you click Save.

You are prompted to close your web 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.

7.3 Setting the ILOM Clock

This section describes 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 7.3.3, "Interpreting ILOM Clock Settings" on page 7-7.

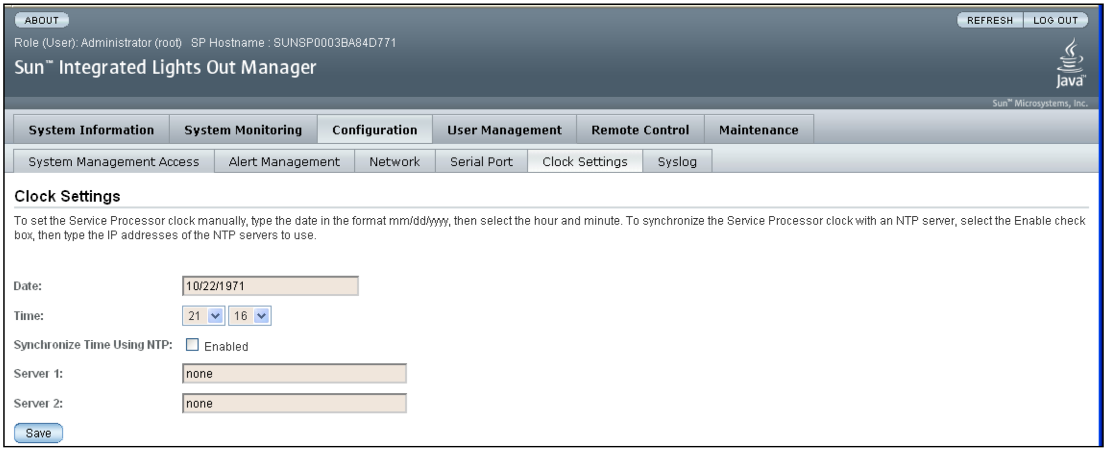
Before you begin, obtain IP addresses of the NTP servers you want to use.

7.3.1 Setting the ILOM Clock Manually

1. **Log in to the ILOM as administrator.**
2. **Select Configuration => Clock Settings.**

   The Clock Settings page appears.

FIGURE 7-3 Clock Settings Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Clock Settings

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.

Date: 10/22/1971

Time: 21 16

Synchronize Time Using NTP: □ Enabled

Server 1: none

Server 2: none

3. **Type a date in the Date field.**

   The date format is *mm/dd/yyyy*.

4. **Set the hour and minute using the drop-down menus.**

5. **Click Save for your changes to take effect.**

7.3.2 Synchronizing the ILOM Clock with an NTP Server

1. **Log in to the ILOM as administrator.**

2. **Select Configuration => Clock Settings.**

   The Clock Settings page appears. See FIGURE 7-3.

3. **Select 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 Save for your changes to take effect.**

7.3.3 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 power cycle (unplugging and replugging the AC power cord).

- 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:

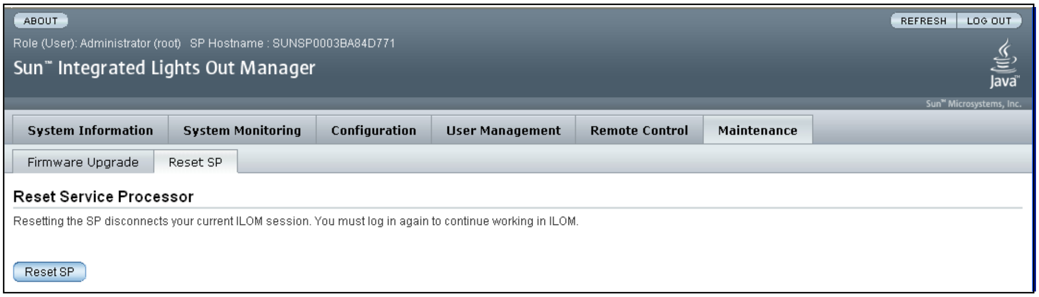
- **When the host is booted** – The host's BIOS unconditionally sets the ILOM time to that indicated by the host's RTC. The host's RTC is set by the following operations:
  - When the host's CMOS is cleared as a result of changing the host's RTC battery or inserting the CMOS-clear jumper on the motherboard. 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.**

7.4 Resetting the ILOM

1. **Log in to the ILOM as administrator or operator.**
2. **Select Maintenance => Reset SP.**

   The Reset Service Processor page appears.

FIGURE 7-4 Reset Service Processor Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Reset Service Processor

Resetting the SP disconnects your current ILOM session. You must log in again to continue working in ILOM.

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

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

7.5 Resetting the ILOM and BIOS Passwords

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

7.6 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.

Occasionally, you might need to downgrade your firmware. Downgrading is done exactly the same as upgrading, only you choose an older (downgraded) image in Step 7.

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.

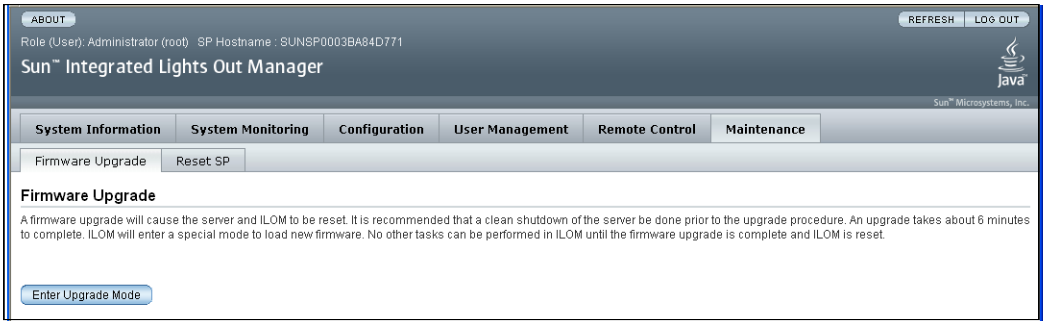
To observe the status of the upgrade while it's happening, set the session timeout to 3 hours. See Section 7.9, "Setting the ILOM Session Timeout Period" on page 7-16 for details.

1. **Log in to the ILOM as administrator.**
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. **Select Maintenance => 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 7-5 Firmware Upgrade Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Firmware Upgrade

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 6 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.

5. **Click Enter Upgrade Mode.**

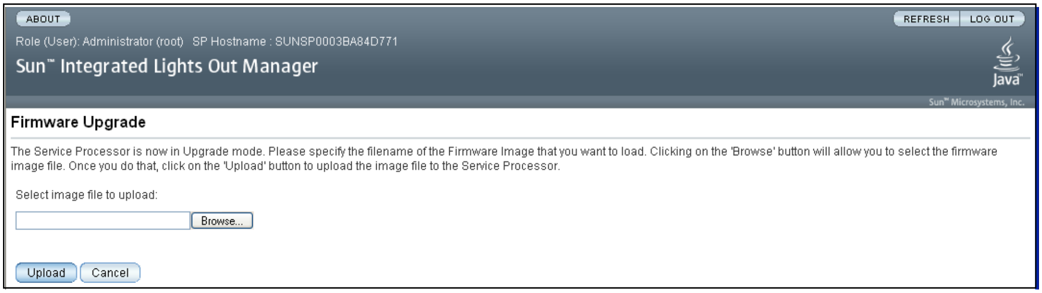
   A dialog box appears. It asks you to confirm that you want to enter Upgrade mode.

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 Image File to Upload field, or click Browse to locate and select the firmware update file (`*.ima`).**

FIGURE 7-6 Image File Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Sun™ Integrated Lights Out Manager

Firmware Upgrade

The Service Processor is now in Upgrade mode. Please specify the filename of the Firmware Image that you want to load. Clicking on the 'Browse' button will allow you to select the firmware image file. Once you do that, click on the 'Upload' button to upload the image file to the Service Processor.

Select image file to upload:

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.

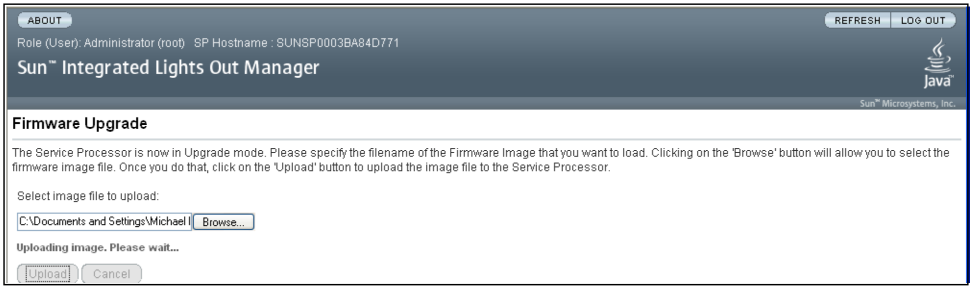
Note – A network failure during the file upload will result in a time out and the ILOM will reboot with the prior version of the ILOM firmware.

---

9. **Click OK.**

   The Verify Firmware Image page appears.

FIGURE 7-7 Verify Firmware Image Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Sun™ Integrated Lights Out Manager

Firmware Upgrade

The Service Processor is now in Upgrade mode. Please specify the filename of the Firmware Image that you want to load. Clicking on the 'Browse' button will allow you to select the firmware image file. Once you do that, click on the 'Upload' button to upload the image file to the Service Processor.

Select image file to upload:

C:\Documents and Settings\Michael I

Uploading image. Please wait...

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

- Upgradable 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 Start Upgrade, or click Cancel 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 web 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.

A screen prompt might ask you to repeat the upgrade. *This is not due to any problem*. If this happens, repeat the procedure, starting at Step 1.

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

---

12. **Close your web browser and reconnect to the ILOM.**

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

7.7 Enabling HTTP or HTTPS Web Access

This section describes how to view and modify web server settings.

ILOM provides the option to control access to the web interface. There are four choices:

- HTTP only
- HTTPS only
- HTTP and HTTPS
- HTTPS and HTTP automatically redirected to HTTPS

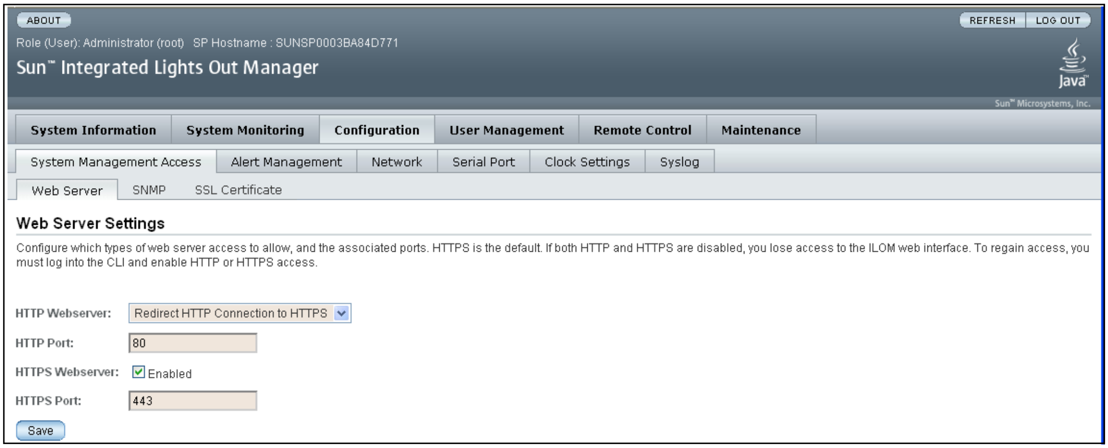
HTTPS is enabled by default.

1. **Log in to the ILOM as administrator.**

2. **Select Configuration => System Management Access =>Web Server.**

   The Web Server Settings page appears.

FIGURE 7-8 Web Server Settings Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Web Server Settings

Configure which types of web server access to allow, and the associated ports. HTTPS is the default. If both HTTP and HTTPS are disabled, you lose access to the ILOM web interface. To regain access, you must log into the CLI and enable HTTP or HTTPS access.

HTTP Webserver: Redirect HTTP Connection to HTTPS

HTTP Port: 80

HTTPS Webserver: ☑ Enabled

HTTPS Port: 443

3. **Select the HTTP or HTTPS web server.**

- **To enable HTTP** – 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 enable HTTPS** – Select the HTTPS Web Server Enabled check box.

  The HTTPS web server is enabled by default.

Note – If you disable HTTP or select Redirect HTTP Connection to HTTPs, and then disable HTTPS, you will be unable to access the WebGUI. To restore access, use the CLI /SP/services/http or https commands, as described in Section 6.7, "Enabling HTTP or HTTPS Web Access" on page 6-8.

---

4. **Assign an HTTP or HTTPS port number.**

5. **Click Save to save your settings.**

7.8 Uploading a New SSL Certificate

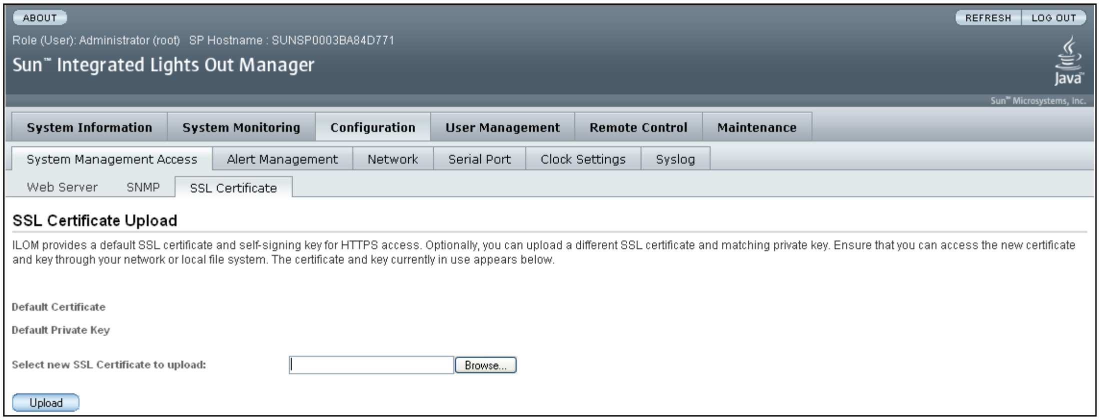
This section describes how to upload a Secure Sockets Layer (SSL) certificate and SSL private key to use when accessing the ILOM.

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.**
2. **Select Configuration => System Management Access => SSL Certificate.**

   The SSL Certificate Upload page appears.

FIGURE 7-9 SSL Certificate Upload Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Sun™ Integrated Lights Out Manager

SSL Certificate Upload

ILOM provides a default SSL certificate and self-signing key for HTTPS access. Optionally, you can upload a different SSL certificate and matching private key. Ensure that you can access the new certificate and key through your network or local file system. The certificate and key currently in use appears below.

Default Certificate

Default Private Key

Select new SSL Certificate to upload:

3. **Type the file name of the new SSL certificate, or click Browse 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 Upload to upload the selected SSL certificate.**

   The SSL Certificate Upload Status dialog appears.

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

7.9 Setting the ILOM Session Timeout Period

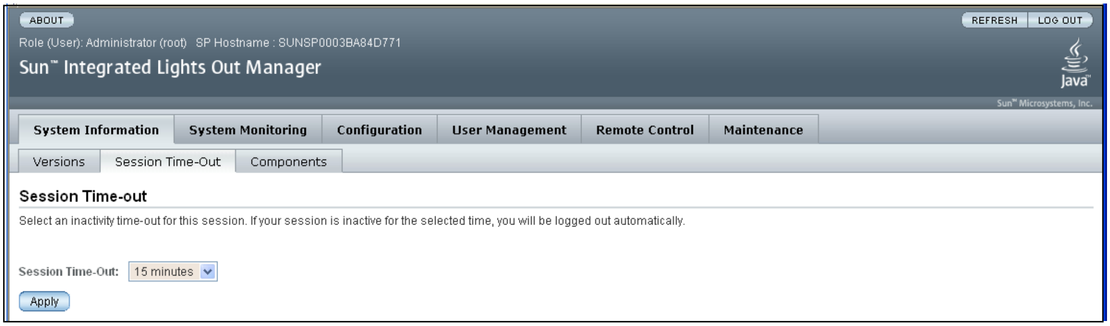
This section describes how to set the timeout period for your ILOM session. Once you set the timeout period, if your session is inactive for that amount of time, you will be automatically logged out of the session.

1. **Log in to the ILOM as administrator or operator.**

2. **Select System Information => Session Time-Out.**

   The Session Time-out page appears.

FIGURE 7-10 Session Time-Out Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Session Time-out

Select an inactivity time-out for this session. If your session is inactive for the selected time, you will be logged out automatically.

Session Time-Out: 15 minutes

3. **From the Session Time-Out drop-down list, select the amount of time for the session time-out period.**

4. **Click Apply.**

   A confirmation dialog box appears.

5. **Click OK.**

   The session timeout 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.

7.10 Viewing Active Connections to the ILOM

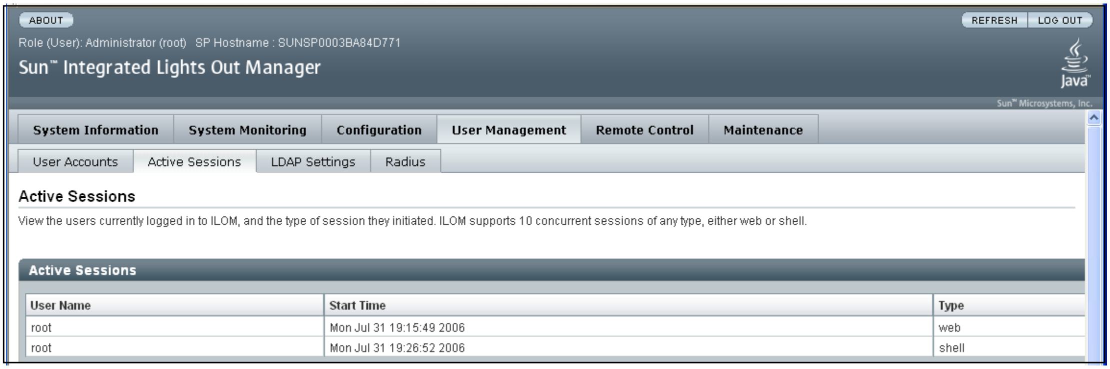
This section describes how to view all active connections to the ILOM.

1. **Log in to the ILOM as administrator or operator.**

2. **Select User Management => Active Sessions.**

   The Active Sessions page appears. The information on this page includes the user name, the date and time that the user initiated the session, and the type of session (web or command shell).

FIGURE 7-11 Active Sessions Page



Active Sessions

View the users currently logged in to ILOM, and the type of session they initiated. ILOM supports 10 concurrent sessions of any type, either web or shell.

Active Sessions

User Name	Start Time	Type
root	Mon Jul 31 19:15:49 2006	web
root	Mon Jul 31 19:26:52 2006	shell

CHAPTER 8

Managing the Host Using the CLI

This chapter describes how to use the ILOM's command-line interface (CLI) to manage the host. The sections include:

8.1 Controlling Power to the Host Server

- 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.

- To send a break to the host, type:

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

8.2 Starting and Stopping the Host Console

- Type the `start` command to start a session to the server console:

  ```
  start /SP/console
  ```

- Type the `stop` command to terminate a server console session started by another user:

  ```
  stop /SP/console
  ```

Note – Before connecting to the console, the ILOM must be set to its default settings (9600 baud, 8N1 [eight data bits, no parity, one stop bit], no flow control).

If the host is booting, you will see its bootup messages.

8.3 Viewing System Components, Indicators, and Sensors

On the CLI, components, indicators (LEDs), and sensors are located in /SYS.

Note – When displayed on the WebGUI, the components, indicators, and sensors are divided into separate screens. They are described in:
Section 9.2, "Viewing Replaceable Component Information" on page 9-2
Section 9.3, "Viewing Sensors" on page 9-5
Section 9.4, "Viewing Indicator LEDs and Controlling the Locate LED" on page 9-8.

The following display shows the contents of a typical /SYS.

Note – The displays in this section are examples. For exact sensor information, see your platform supplement.

```
-> show /SYS

 /SYS
    Targets:
        INTSW
        BIOS
        SP
        REAR_SVC
        TOP_SVC
        TEMP_FAULT
        POWER
        LOCATE
        SERVICE
        V_+12V
        V_+1V2
        V_+3V3
        V_+3V3STBY
        V_+5V
        FP
        BP
        FT0
        FT1
        FT2
        FT3
        PROC
        IO
        PS0
        PS1
        PS2
        HD
Properties
       (additional information appears here)

->
```

- **To display information about a particular sensor, indicator or component, use the `show` command.**

  In this example, `/SYS/SASBP` represents the disk backplane. It has the following targets:

```
-> show /SYS/SASBP

 /SYS/SASBP
    Targets:
        ID0
        ID1
        T_AMB
        HDD0
        HDD1
        HDD2
        HDD3

    Properties:
        type = Disk Backplane

    Commands:
        cd
        show

->
```

The following display shows a device (HDD0) and a temperature sensor (T_AMB).

```
-> show /SYS/HD/HDD0

 /SYS/HD/HDD0
    Targets:
        STATE
        FAIL
        OK2RM

    Properties:
        type = Hard Disk FRU
        product_name = (none)
        product_manufacturer = HITACHI
        product_version = V44OA94A
        product_part_number = HDS7225SBSUN250G
        product_serial_number = VDK41DT4EG9GNK

    Commands:
        cd
        show

-> show /SYS/HD/T_AMB

 /SYS/HD/T_AMB
    Targets:

    Properties:
        type = Temperature
        class = Threshold Sensor
        value = 25.000 degree C
        upper_nonrecov_threshold = 43.00 degree C
        upper_critical_threshold = 38.00 degree C
        upper_noncritical_threshold = 33.00 degree C
        lower_nonrecov_threshold = 0.00 degree C
        lower_critical_threshold = 0.00 degree C
        lower_noncritical_threshold = 0.00 degree C

    Commands:
        cd
        show

->
```

8.4 Setting the Locate LED

The locate LED is a white LED that you can light to help you find your server in a crowded equipment room. It has two states, fast blink and Off.

- To turn off the LED, type:

```
set /SYS/LOCATE value=Off
```

- To turn on the LED, type:

```
set /SYS/LOCATE value=Fast_Blink
```

8.5 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 in 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.

The mapping between alert levels and sensors is:

TABLE 8-1 Mapping Between Alerts and Sensors

Alert	Sensor
Warning	Upper non-critical, lower non-critical
Critical	Upper critical, lower critical
Non recoverable	Upper non-recoverable, lower non-recoverable
Informational	System events not related to sensors

8.5.1 Displaying Alerts

- Type the following command to display alerts:

  `show /SP/alert/rules`

- Type the following to display information about a single alert:

  `show /SP/alert/rules/`*N*

  where *N* is 1 to 15.

8.5.2 Configuring Alerts

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

8.5.2.1 Syntax

`set target` *[propertyname=value]*

8.5.2.2 Targets, Properties, and Values

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

TABLE 8-2 Valid Targets, Properties, and Values for IPMI Pet Alerts

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

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 8-3).

TABLE 8-3 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
```

8.5.3 Sending Test Alerts

The CLI allows you to send test alerts. It sends one alert for every rule that is configured.

1. **Navigate to** `/SP/alert/rules`
2. **Type the command `set testalert=true`.**

   This sends a test alert for every rule that is not disabled.

8.6 Viewing and Clearing Event Logs

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

Caution – The system event log accumulates various events, including administration changes to the ILOM, software events, and warnings and alerts. It also accumulates events from the IPMI log.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. **Navigate to** `/SP/logs/event`**.**
2. **From the CLI, type `show list.`**

   The event log scrolls onto your screen.

```
-> cd /SP/logs/event
/SP/logs/event

-> show list

  /SP/logs/event/list
    Targets:

    Properties:

    Commands:
        show

ID     Date/Time                 Class     Type      Severity
-----  ------------------------  --------  --------  --------
1522   Sun Jul 30 01:11:36 2006  Audit     Log       minor
       root : Close Session : object = /session/type : value = www : success
1521   Sun Jul 30 01:05:34 2006  Audit     Log       minor
       root : Close Session : session ID = 1307912184 : success
```

3. **To scroll down, press any key except q.**
4. **To stop displaying the log, press q.**
5. **To clear the event log, type `set clear=true`.**

   The CLI asks you to confirm.

6. **Type `y`.**

   The CLI clears the event log.

   For example:

```
-> set clear=true
Are you sure you want to clear /SP/logs/event (y/n)? y
Set 'clear' to 'true'

->
```

Note – The SEL accumulates many types of events, including copies of entries that IPMI posts to the IPMI log. Clearing the SEL clears all entries, including the copies of the IPMI log entries. However, clearing the SEL does NOT clear the actual IPMI log. You must use IPMI commands to view and clear the IPMI log.

8.7 Sending Logs to Other Machines

You can send logs to other machines. After an address is configured, new messages are sent to the destination machine(s) in syslog format.

1. **Navigate to** `/SP/clients/syslog`**.**

2. **Enter the IP address of the receiving machine:**

```
-> cd syslog
/SP/clients/syslog

-> show

 /SP/clients/syslog
    Targets:

    Properties:
        destination_ip1 = (none)
        destination_ip2 = (none)

    Commands:
        cd
        set
        show

-> set destination_ip1 = nn.nn.nn.nn
```

CHAPTER 9

Managing the Host Using the WebGUI

This chapter describes how to view the state of the host, and how to manage it using the WebGUI.

It contains the following sections:

- Section 9.1, "Controlling Power to the Host Server" on page 9-1
- Section 9.2, "Viewing Replaceable Component Information" on page 9-2
- Section 9.3, "Viewing Sensors" on page 9-5
- Section 9.4, "Viewing Indicator LEDs and Controlling the Locate LED" on page 9-8
- Section 9.5, "Managing Alerts" on page 9-10
- Section 9.6, "Viewing and Clearing the System Event Log" on page 9-13
- Section 9.7, "Viewing ILOM Hardware, Firmware, and IPMI Versions" on page 9-17

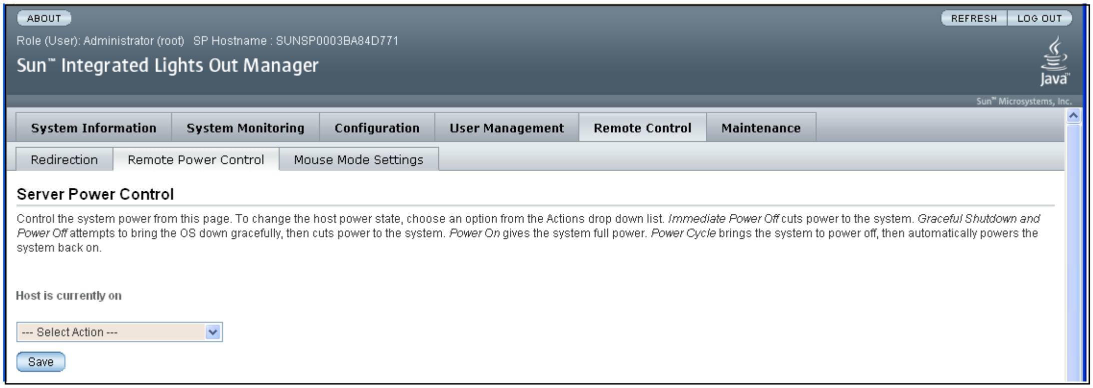
9.1 Controlling Power to the Host Server

1. **Log in to the WebGUI as described in** Section 4.2, "Logging In to the WebGUI" on page 4-4**.**

2. **Select Remote Control => Remote Power Control.**

   The Server Power Control page appears.

FIGURE 9-1 Server Power Control Page



Server Power Control

Control the system power from this page. To change the host power state, choose an option from the Actions drop down list. *Immediate Power Off* cuts power to the system. *Graceful Shutdown and Power Off* attempts to bring the OS down gracefully, then cuts power to the system. *Power On* gives the system full power. *Power Cycle* brings the system to power off, then automatically powers the system back on.

Host is currently on

--- Select Action ---

Save

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 OK in the confirmation dialog to implement your selection.**

9.2 Viewing Replaceable Component Information

This section describes 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.

Hot-Swappable and Hot-Pluggable Components

Some components are hot-swappable, meaning that you can remove them from the system without warning or preparation.

Other components are hot-pluggable, meaning that they can be removed while the system is running, but the system must be prepared first.

Some hot-pluggable components can be prepared for removal using the Components Management page. Those components display a radio button in the left-hand column of the Component Management page (FIGURE 9-2).

Still other components require the system to be shut down before they can be removed.

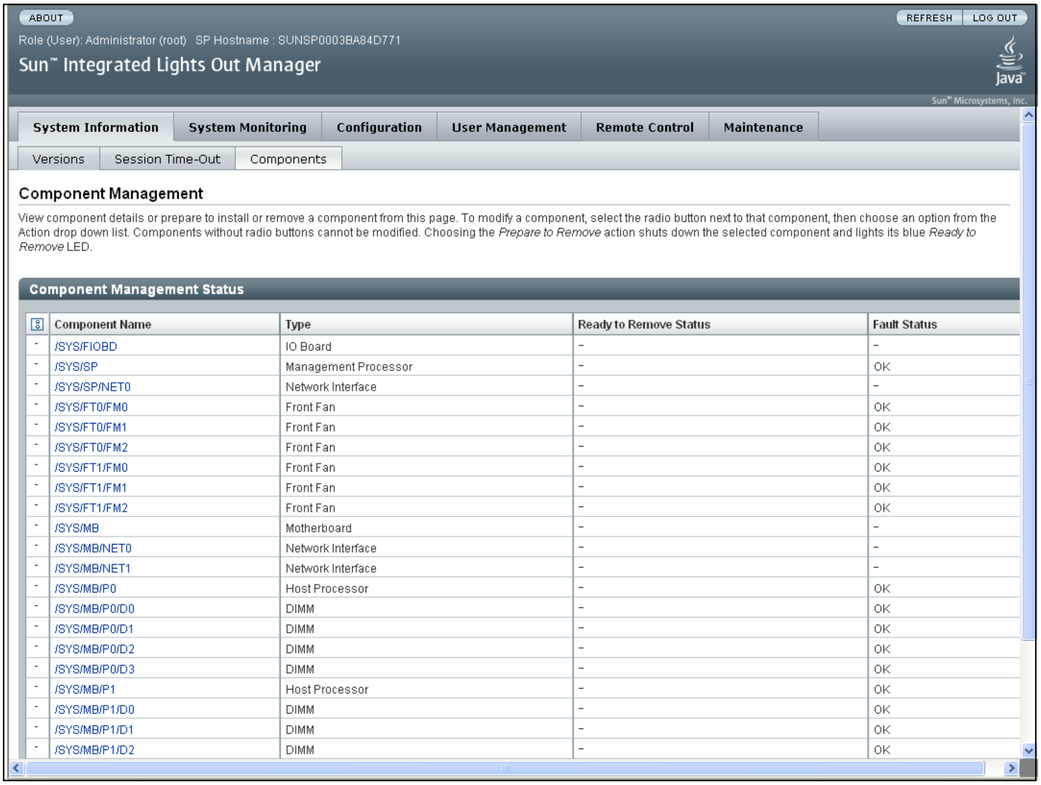
Note – The data shown in FIGURE 9-2 and FIGURE 9-3 are examples only. The actual data you see might be different on your platform. For details, see your platform supplement.

---

1. **Log in to the ILOM as administrator or operator.**
2. **Select System Information => Components.**

   The Component Management page appears.

FIGURE 9-2 Sample Repleacable Component Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Component Management

View component details or prepare to install or remove a component from this page. To modify a component, select the radio button next to that component, then choose an option from the Action drop down list. Components without radio buttons cannot be modified. Choosing the *Prepare to Remove* action shuts down the selected component and lights its blue *Ready to Remove* LED.

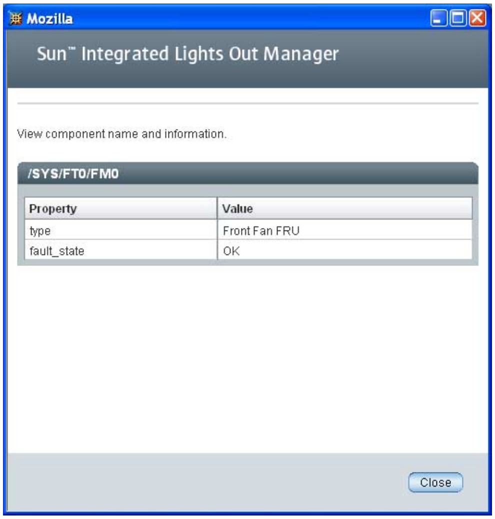
Component Management Status

	Component Name	Type	Ready to Remove Status	Fault Status
-	/SYS/FIOBD	IO Board	-	-
-	/SYS/SP	Management Processor	-	OK
-	/SYS/SP/NET0	Network Interface	-	-
-	/SYS/FT0/FM0	Front Fan	-	OK
-	/SYS/FT0/FM1	Front Fan	-	OK
-	/SYS/FT0/FM2	Front Fan	-	OK
-	/SYS/FT1/FM0	Front Fan	-	OK
-	/SYS/FT1/FM1	Front Fan	-	OK
-	/SYS/FT1/FM2	Front Fan	-	OK
-	/SYS/MB	Motherboard	-	-
-	/SYS/MB/NET0	Network Interface	-	-
-	/SYS/MB/NET1	Network Interface	-	-
-	/SYS/MB/P0	Host Processor	-	OK
-	/SYS/MB/P0/D0	DIMM	-	OK
-	/SYS/MB/P0/D1	DIMM	-	OK
-	/SYS/MB/P0/D2	DIMM	-	OK
-	/SYS/MB/P0/D3	DIMM	-	OK
-	/SYS/MB/P1	Host Processor	-	OK
-	/SYS/MB/P1/D0	DIMM	-	OK
-	/SYS/MB/P1/D1	DIMM	-	OK
-	/SYS/MB/P1/D2	DIMM	-	OK

3. **Click a component for detailed information about it.**

   Detailed information about the selected component appears.

FIGURE 9-3 Sample Component Details View



View component name and information.

/SYS/FT0/FM0

Property	Value
type	Front Fan FRU
fault_state	OK

4. **To prepare a hot-pluggable component for removal, click the corresponding radio button.**

Note – Most components are either hot-swappable (can be removed without preparation), or you must shut down the system to remove them. For these components, there is no radio button.

The system prepares the component for removal, then displays its status in the Ready to Remove Status column.

For a detailed list of components, see your platform supplement.

9.3 Viewing Sensors

This section describes how to view the temperature, voltage, and fan sensor readings.

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.

For details on individual sensors, see your platform supplement.

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 9.5, "Managing Alerts" on page 9-10.

The thresholds appear in the Sensor Readings view shown in FIGURE 9-4.

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 as local time.

---

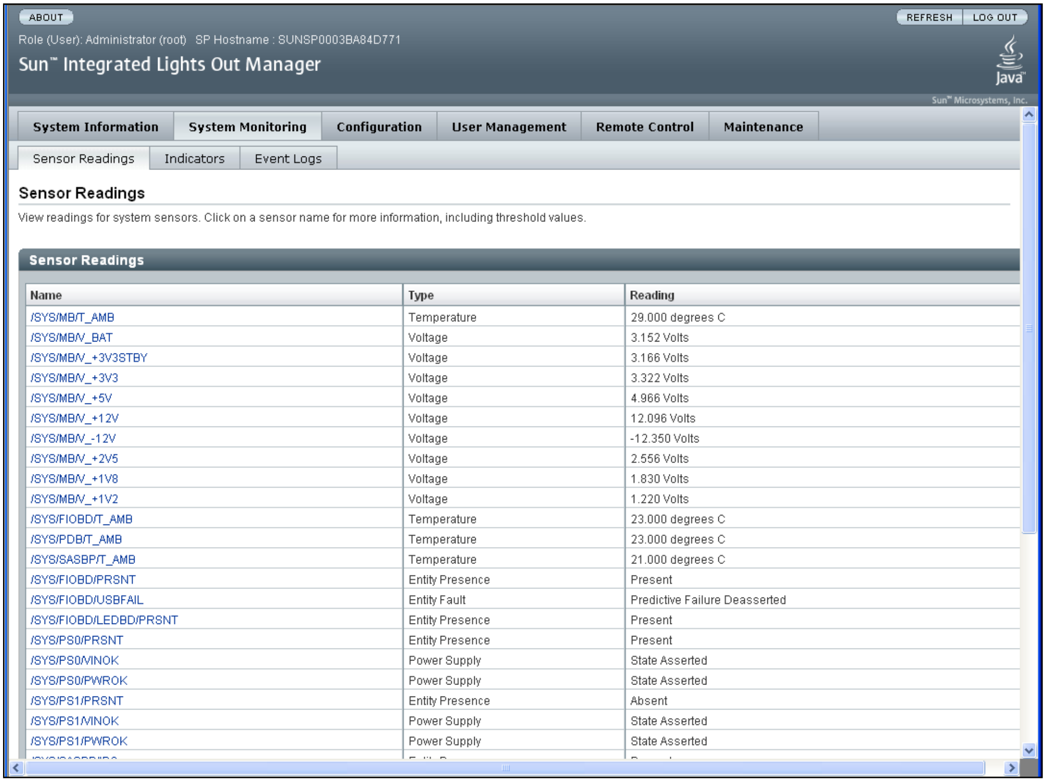
1. **Log in to the ILOM as administrator or operator.**
2. **Select System Monitoring => Sensor Readings.**

   The Sensor Readings page appears.

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.

Note – If the server is powered off, many components will appear as "no reading." To power it on, see Section 9.1, "Controlling Power to the Host Server" on page 9-1.

FIGURE 9-4 Sample Sensor Readings Page



Sensor Readings

View readings for system sensors. Click on a sensor name for more information, including threshold values.

Sensor Readings

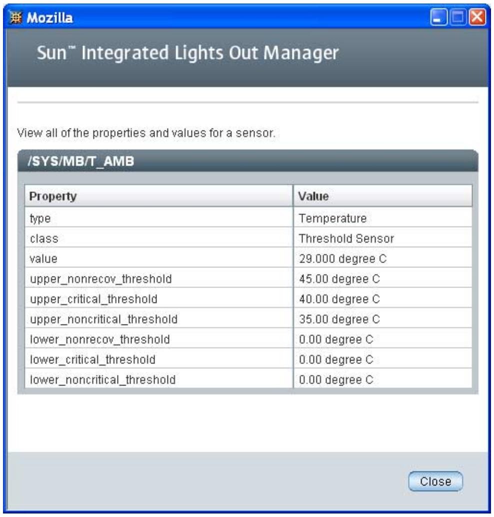
Name	Type	Reading
/SYS/MB/T_AMB	Temperature	29.000 degrees C
/SYS/MB/V_BAT	Voltage	3.152 Volts
/SYS/MB/V_+3V3STBY	Voltage	3.166 Volts
/SYS/MB/V_+3V3	Voltage	3.322 Volts
/SYS/MB/V_+5V	Voltage	4.966 Volts
/SYS/MB/V_+12V	Voltage	12.096 Volts
/SYS/MB/V_-12V	Voltage	-12.350 Volts
/SYS/MB/V_+2V5	Voltage	2.556 Volts
/SYS/MB/V_+1V8	Voltage	1.830 Volts
/SYS/MB/V_+1V2	Voltage	1.220 Volts
/SYS/FIOBD/T_AMB	Temperature	23.000 degrees C
/SYS/PDB/T_AMB	Temperature	23.000 degrees C
/SYS/SASBP/T_AMB	Temperature	21.000 degrees C
/SYS/FIOBD/PRSNT	Entity Presence	Present
/SYS/FIOBD/USBFAIL	Entity Fault	Predictive Failure Deasserted
/SYS/FIOBD/LEDBD/PRSNT	Entity Presence	Present
/SYS/PS0/PRSNT	Entity Presence	Present
/SYS/PS0/VINOK	Power Supply	State Asserted
/SYS/PS0/PWROK	Power Supply	State Asserted
/SYS/PS1/PRSNT	Entity Presence	Absent
/SYS/PS1/VINOK	Power Supply	State Asserted
/SYS/PS1/PWROK	Power Supply	State Asserted

3. **Scroll down the list to find the sensor you wish to view.**

4. **To see details about a particular sensor, click its name.**

   The details view appears. This view provides detailed information about the sensor, such as thresholds.

FIGURE 9-5 Sample Sensor Details View



View all of the properties and values for a sensor.

/SYS/MB/T_AMB

Property	Value
type	Temperature
class	Threshold Sensor
value	29.000 degree C
upper_nonrecov_threshold	45.00 degree C
upper_critical_threshold	40.00 degree C
upper_noncritical_threshold	35.00 degree C
lower_nonrecov_threshold	0.00 degree C
lower_critical_threshold	0.00 degree C
lower_noncritical_threshold	0.00 degree C

Note – The sensors shown in FIGURE 9-4 and FIGURE 9-5 are examples only. The actual sensor names, ranges, and functions might be different on your platform. For details, see your platform supplement.

9.4 Viewing Indicator LEDs and Controlling the Locate LED

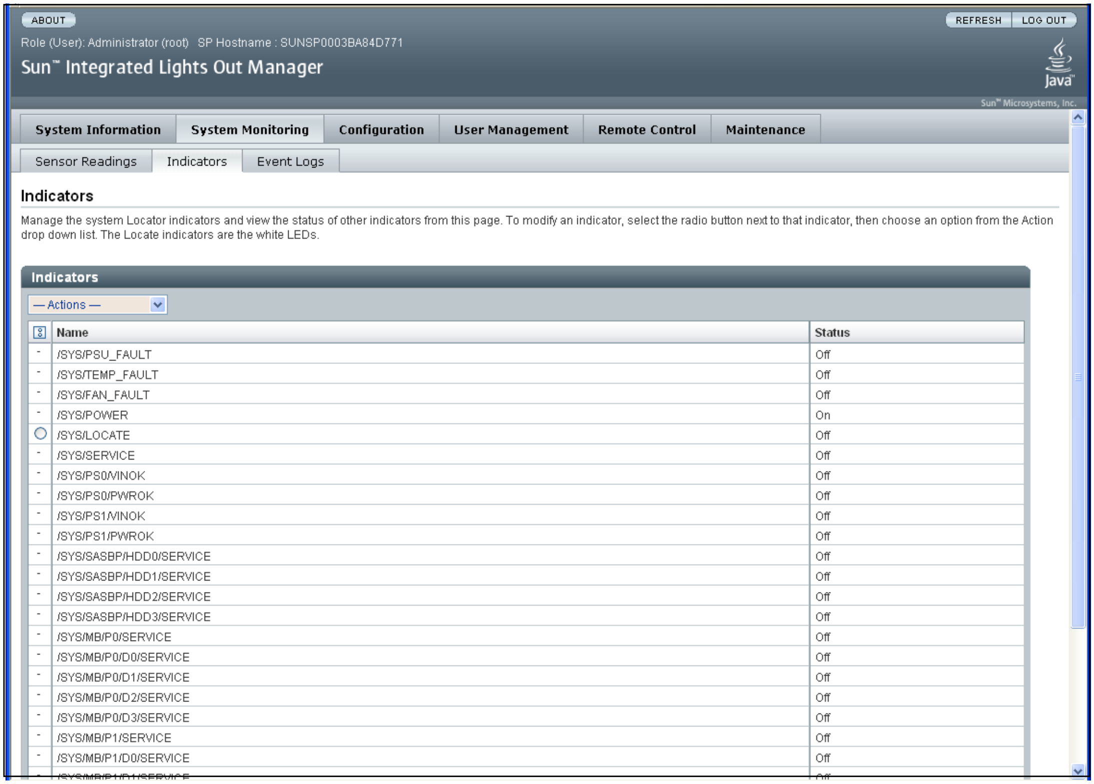
The Indicators view shows the state of the LEDs in the system.

1. **Log in to the ILOM as administrator or operator.**

2. **Select System Monitoring => Indicators.**

   The Indicators display appears.

FIGURE 9-6 Sample Indicators Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Sun™ Integrated Lights Out Manager

Indicators

Manage the system Locator indicators and view the status of other indicators from this page. To modify an indicator, select the radio button next to that indicator, then choose an option from the Action drop down list. The Locate indicators are the white LEDs.

Indicators

	Name	Status
-	/SYS/PSU_FAULT	Off
-	/SYS/TEMP_FAULT	Off
-	/SYS/FAN_FAULT	Off
-	/SYS/POWER	On
○	/SYS/LOCATE	Off
-	/SYS/SERVICE	Off
-	/SYS/PS0/VINOK	Off
-	/SYS/PS0/PWROK	Off
-	/SYS/PS1/VINOK	Off
-	/SYS/PS1/PWROK	Off
-	/SYS/SASBP/HDD0/SERVICE	Off
-	/SYS/SASBP/HDD1/SERVICE	Off
-	/SYS/SASBP/HDD2/SERVICE	Off
-	/SYS/SASBP/HDD3/SERVICE	Off
-	/SYS/MB/P0/SERVICE	Off
-	/SYS/MB/P0/D0/SERVICE	Off
-	/SYS/MB/P0/D1/SERVICE	Off
-	/SYS/MB/P0/D2/SERVICE	Off
-	/SYS/MB/P0/D3/SERVICE	Off
-	/SYS/MB/P1/SERVICE	Off
-	/SYS/MB/P1/D0/SERVICE	Off
-	/SYS/MB/P1/D1/SERVICE	Off

Note – The sensors shown in FIGURE 9-6 are examples only. The actual sensor names, ranges, and functions might be different on your platform. For details, see your platform supplement.

---

3. **Use the scrollbar to view the list.**

4. **To toggle the state of the locate LED:**

   a. **Click the radio button next to /SYS/LOCATE.**

   b. **Select a state from the drop-down menu.**

      The states are Turn LED Off or Set LED to Fast Blink.

      A dialog asks you to confirm.

   c. **Click OK.**

      The locate LED changes states, and the new state appears in the Status column.

9.5 Managing Alerts

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

The mapping between alert levels and sensors is:

TABLE 9-1 Mapping between Alerts and Sensors

Alert	Sensor
Warning	Upper non-critical, lower non-critical
Critical	Upper critical, lower critical
Non-recoverable	Upper non-recoverable, lower non-recoverable
Informational	System events not related to sensors

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.

9.5.1 Viewing Alert Destinations

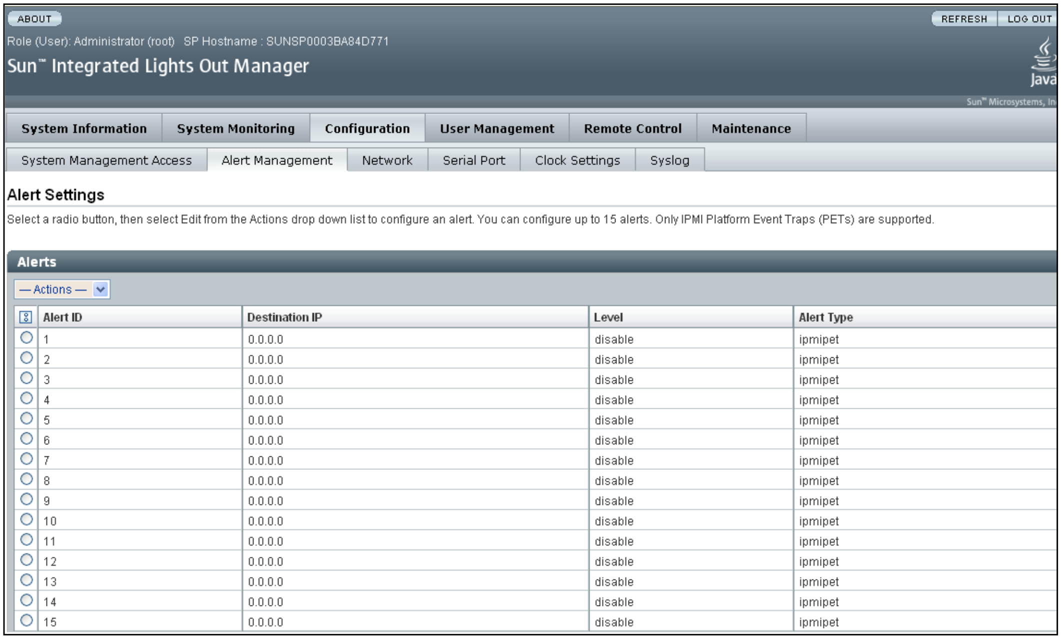
Users with operator privileges can view the alert settings. Changing them requires administrator privileges.

1. **Log in to the ILOM as administrator or operator**

2. **Select Configuration => Alert Management.**

   The Alert Settings page displays a list of alerts.

FIGURE 9-7 Alert Destination Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Sun™ Integrated Lights Out Manager

Alert Settings

Select a radio button, then select Edit from the Actions drop down list to configure an alert. You can configure up to 15 alerts. Only IPMI Platform Event Traps (PETs) are supported.

Alerts

	Alert ID	Destination IP	Level	Alert Type
○	1	0.0.0.0	disable	ipmipet
○	2	0.0.0.0	disable	ipmipet
○	3	0.0.0.0	disable	ipmipet
○	4	0.0.0.0	disable	ipmipet
○	5	0.0.0.0	disable	ipmipet
○	6	0.0.0.0	disable	ipmipet
○	7	0.0.0.0	disable	ipmipet
○	8	0.0.0.0	disable	ipmipet
○	9	0.0.0.0	disable	ipmipet
○	10	0.0.0.0	disable	ipmipet
○	11	0.0.0.0	disable	ipmipet
○	12	0.0.0.0	disable	ipmipet
○	13	0.0.0.0	disable	ipmipet
○	14	0.0.0.0	disable	ipmipet
○	15	0.0.0.0	disable	ipmipet

The alert table includes five columns:

- Radio buttons – Use to select an alert.
- Alert ID – The number of the alert rule. A number from 1 to 15.
- Destination IP – The IP address of the machine where the alert will be sent.
- Alert Level – Displays the severity level of the alert. Possible levels include:

TABLE 9-2 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.

TABLE 9-2 Alert Levels *(Continued)*

Alert Levels	Name in Sensor Readings View	Description
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.

- Alert Type – ipmipet, indicating that all alerts are sent as IPMI PET traps.

9.5.2 Configuring an Alert

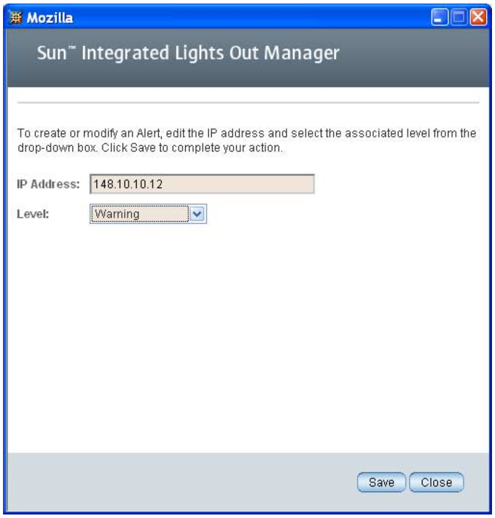
Configuring an alert requires administrator privileges.

1. **Select a radio button for an alert in the table.**

2. **Select Edit from the drop-down menu.**

   The Alert dialog box appears.

FIGURE 9-8 Alert Dialog Box



To create or modify an Alert, edit the IP address and select the associated level from the drop-down box. Click Save to complete your action.

IP Address: 148.10.10.12

Level: Warning

3. **Type the destination IP address for the alert.**

4. **Select an event severity from the drop-down menu.**

5. **Click Save.**

   The modified alert appears in the Alert Destinations table.

9.6 Viewing and Clearing the System Event Log

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

The system event log accumulates various events, including administration changes to the ILOM, software events, and warnings and alerts. It also accumulates events from the IPMI log.

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 as local time.

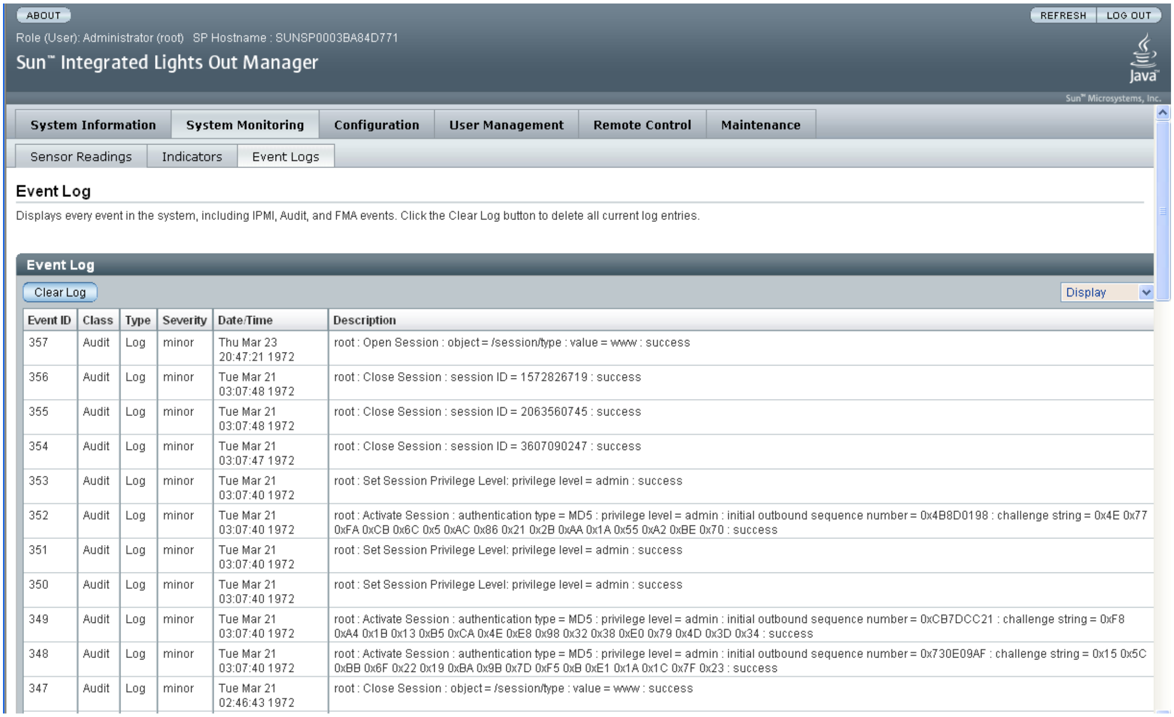
---

1. **Log in to the ILOM as administrator or operator.**

2. **Select System Monitoring => Event Logs.**

   The System Event Logs page appears.

FIGURE 9-9 System Event Log Page



Event Log

Displays every event in the system, including IPMI, Audit, and FMA events. Click the Clear Log button to delete all current log entries.

Event Log

Event ID	Class	Type	Severity	Date/Time	Description
357	Audit	Log	minor	Thu Mar 23 20:47:21 1972	root : Open Session : object = /session/type : value = www : success
356	Audit	Log	minor	Tue Mar 21 03:07:48 1972	root : Close Session : session ID = 1572826719 : success
355	Audit	Log	minor	Tue Mar 21 03:07:48 1972	root : Close Session : session ID = 2063560745 : success
354	Audit	Log	minor	Tue Mar 21 03:07:47 1972	root : Close Session : session ID = 3607090247 : success
353	Audit	Log	minor	Tue Mar 21 03:07:40 1972	root : Set Session Privilege Level: privilege level = admin : success
352	Audit	Log	minor	Tue Mar 21 03:07:40 1972	root : Activate Session : authentication type = MD5 : privilege level = admin : initial outbound sequence number = 0x4B8D0198 : challenge string = 0x4E 0x77 0xFA 0xCB 0x6C 0x5 0xAC 0x86 0x21 0x2B 0xAA 0x1A 0x55 0xA2 0xBE 0x70 : success
351	Audit	Log	minor	Tue Mar 21 03:07:40 1972	root : Set Session Privilege Level: privilege level = admin : success
350	Audit	Log	minor	Tue Mar 21 03:07:40 1972	root : Set Session Privilege Level: privilege level = admin : success
349	Audit	Log	minor	Tue Mar 21 03:07:40 1972	root : Activate Session : authentication type = MD5 : privilege level = admin : initial outbound sequence number = 0xCB7DCC21 : challenge string = 0xF8 0xA4 0x1B 0x13 0xB5 0xCA 0x4E 0xE8 0x98 0x32 0x38 0xE0 0x79 0x4D 0x3D 0x34 : success
348	Audit	Log	minor	Tue Mar 21 03:07:40 1972	root : Activate Session : authentication type = MD5 : privilege level = admin : initial outbound sequence number = 0x730E09AF : challenge string = 0x15 0x5C 0xBB 0x6F 0x22 0x19 0xBA 0x9B 0x7D 0xF5 0xB 0xE1 0x1A 0x1C 0x7F 0x23 : success
347	Audit	Log	minor	Tue Mar 21 02:46:43 1972	root : Close Session : object = /session/type : value = www : success

3. **Use the Display drop-down menu to determine how many events to display.**

   Selecting a larger number might cause the WebGUI to respond more slowly.

   The WebGUI displays the most recent events first. To see later events, select a larger number.

4. **Use the scrollbar to scroll through the list.**

The fields in the Event Log table are described in TABLE 9-3.

TABLE 9-3 Event Log Fields

Field	Description
Event ID	The number of the event, in sequence from number 1.
Class/Type	• Audit/ Log – Commands that result in a configuration change. Description includes user, command, command parameters and success/fail. • IPMI/Log – Any event that is placed in the IPMI SEL is also put in the management log. • Chassis/State – For changes to the SC/SP's state. (e.g. initializing to master). • Chassis/Action – Category for shutdown events for server module/chassis, hot insert/removal of a FRU and reset parameters button pushed. • FMA/Fault – For FMA faults. Description gives time of fault as detected by FMA and suspect component. • FMA/Repair – For FMA repairs. Description gives component.
Severity	Critical, Major or Minor
Date/Time	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).
Description	A description of the event.

5. **To clear the event log, click Clear Event Log.**

   A confirmation dialog box appears.

Note – The SEL accumulates many types of events, including copies of entries that IPMI posts the IPMI log. Clearing the SEL clears all entries, including the copies of the IPMI log entries. However, clearing the SEL does NOT clear the actual IPMI log. You must use IPMI commands to view and clear the IPMI log.

---

6. **Click OK to clear all entries in the log.**

9.6.1 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`
- A 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 user 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 6-5.

9.7 Viewing ILOM Hardware, Firmware, and IPMI Versions

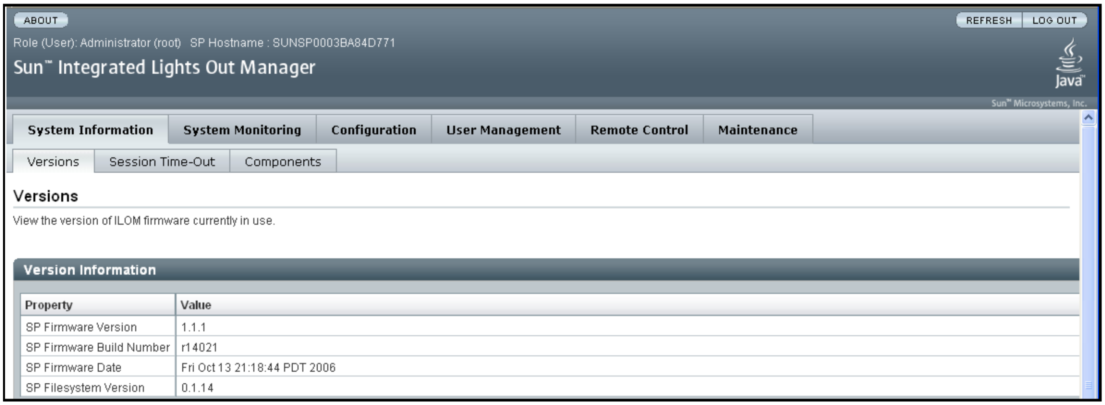
This section describes how to view the ILOM hardware and firmware revisions, as well as the Intelligent Platform Management Interface (IPMI) version.

1. **Log in to the ILOM as administrator or operator.**

2. **Select System Information => Versions.**

   The Version Information page appears (see FIGURE 9-10). This page displays the ILOM hardware and software revisions.

FIGURE 9-10 Version Information Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Versions

View the version of ILOM firmware currently in use.

Version Information

Property	Value
SP Firmware Version	1.1.1
SP Firmware Build Number	r14021
SP Firmware Date	Fri Oct 13 21:18:44 PDT 2006
SP Filesystem Version	0.1.14

CHAPTER 10

Using The Remote Console Application

This chapter describes how to use the remote console application.

It includes the following sections:

- Section 10.1, "About the Remote Console Application" on page 10-1
- Section 10.2, "Starting the Remote Console Application From the WebGUI" on page 10-5
- Section 10.3, "Redirecting Keyboard, Video, Mouse, or Storage Devices" on page 10-10

10.1 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 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.

10.1.1 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 10-1.

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

TABLE 10-1 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 10-2 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 10-2 Remote Console Ports and Interfaces *(Continued)*

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

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

10.1.2 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 10-3 describes different case scenarios in which the remote console application and CD drive and diskette drive redirection operate.

TABLE 10-3 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.
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.

10.1.3 Remote Console Security

Only users with administrator privilege can use the remote console application.

- When users with operator privilege select Remote Console => Redirection, a login window prompts them for a user name and password. They must enter the user name and password for an account with administrator privilege to proceed.
- Normally, when users with administrator privilege click Remote Console => Redirection, the Launch Redirection page appears.

  However, this can be configured. If `/SP/services/sso` is set to `disabled`, even users with administrator privilege are prompted to login again. They can log in using the same user name and password, or a different user name and password, as long as it accesses a valid user account with administrator privilege.

To change the `/SP/services/sso`:

1. **Log in to the CLI using an account with administrator privileges.**
2. **Navigate to /SP/services.**
3. **Enter the command:**
   - **`sso state = enabled`**

     to allow users with administrator privileges to start the remote console operation without a login prompt.
   - **`sso state = disabled`**

     to require users with administrator privileges to log in again when starting the remote console application

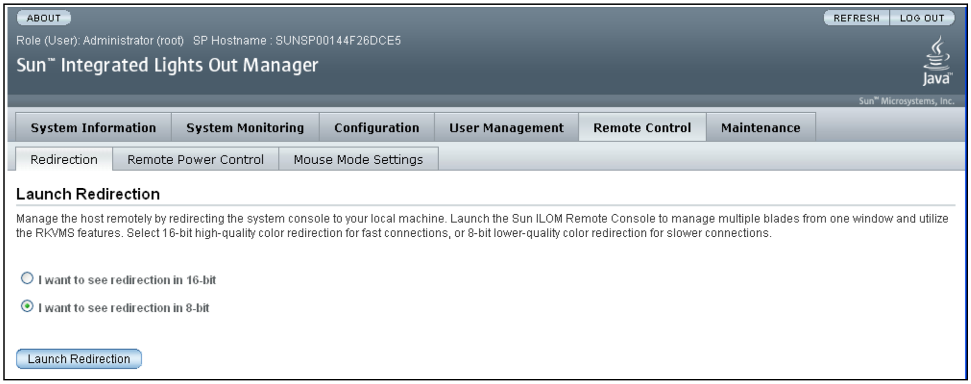
10.2 Starting the Remote Console Application From the WebGUI

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

1. **Log in to the ILOM as administrator.**
2. **Select Remote Control => Redirection.**

   The Launch Redirection page appears.
3. **If a login screen appears, enter the user name and password of an account that has administrator privileges. See** Section 10.1.3, "Remote Console Security" on page 10-5 **for details.**

FIGURE 10-1 Launch Redirection Page



Role (User): Administrator (root) SP Hostname : SUNSP00144F26DCE5

Launch Redirection

Manage the host remotely by redirecting the system console to your local machine. Launch the Sun ILOM Remote Console to manage multiple blades from one window and utilize the RKVMS features. Select 16-bit high-quality color redirection for fast connections, or 8-bit lower-quality color redirection for slower connections.

○ I want to see redirection in 16-bit

● I want to see redirection in 8-bit

4. **If necessary, set the mouse mode.**

   If you are not changing the mouse mode, skip to Step 5.

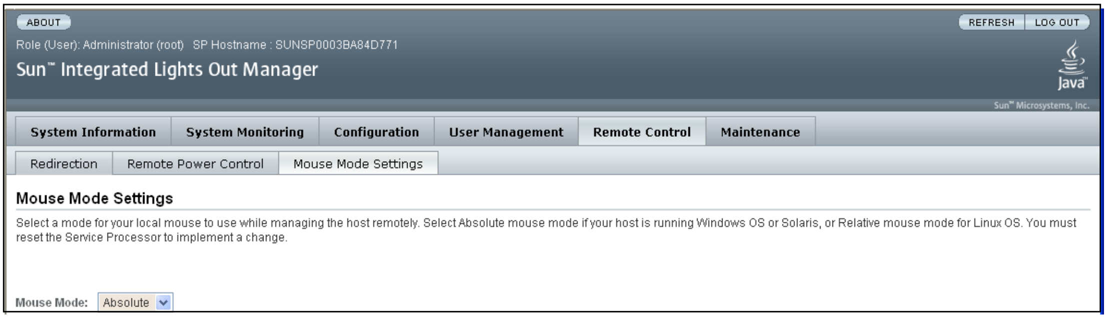
- **Absolute mouse mode** – Select this setting for best performance when you are using a Solaris or Microsoft Windows operating system.
- **Relative mouse mode** – Select this setting for best performance when you are using a Linux operating system. Linux currently does not support Absolute mode.

   a. **Select Remote Control => Mouse Mode Settings.**

      The Mouse Mode Settings page appears.

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

FIGURE 10-2 Mouse Mode Settings Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Mouse Mode Settings

Select a mode for your local mouse to use while managing the host remotely. Select Absolute mouse mode if your host is running Windows OS or Solaris, or Relative mouse mode for Linux OS. You must reset the Service Processor to implement a change.

Mouse Mode: Absolute

   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 menu.**

A confirmation dialog box appears.

d. **Click OK 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 and Step 2, 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 the 8-bit or 16-bit color option.**

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

---

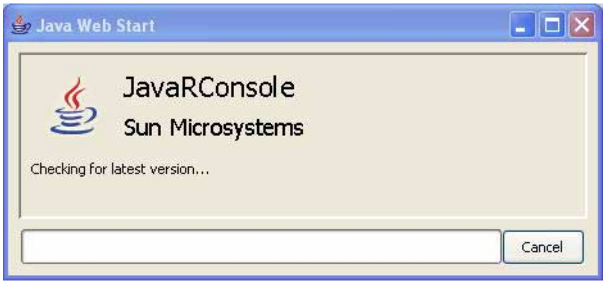
6. **Click Launch Redirection.**

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 10-3 JavaRConsole Page

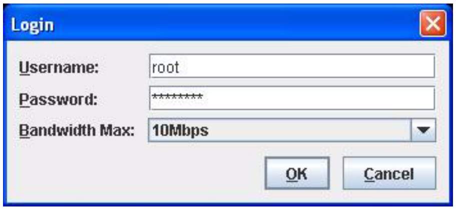


Checking for latest version...

7. **When you see the Login dialog box, type the user name and password.**

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

FIGURE 10-4 Login Dialog Box



Username: root

Password: ********

Bandwidth Max: 10Mbps

8. **Select a bandwidth from the drop-down menu (optional).**

   Select bandwidth that matches your actual bandwidth.

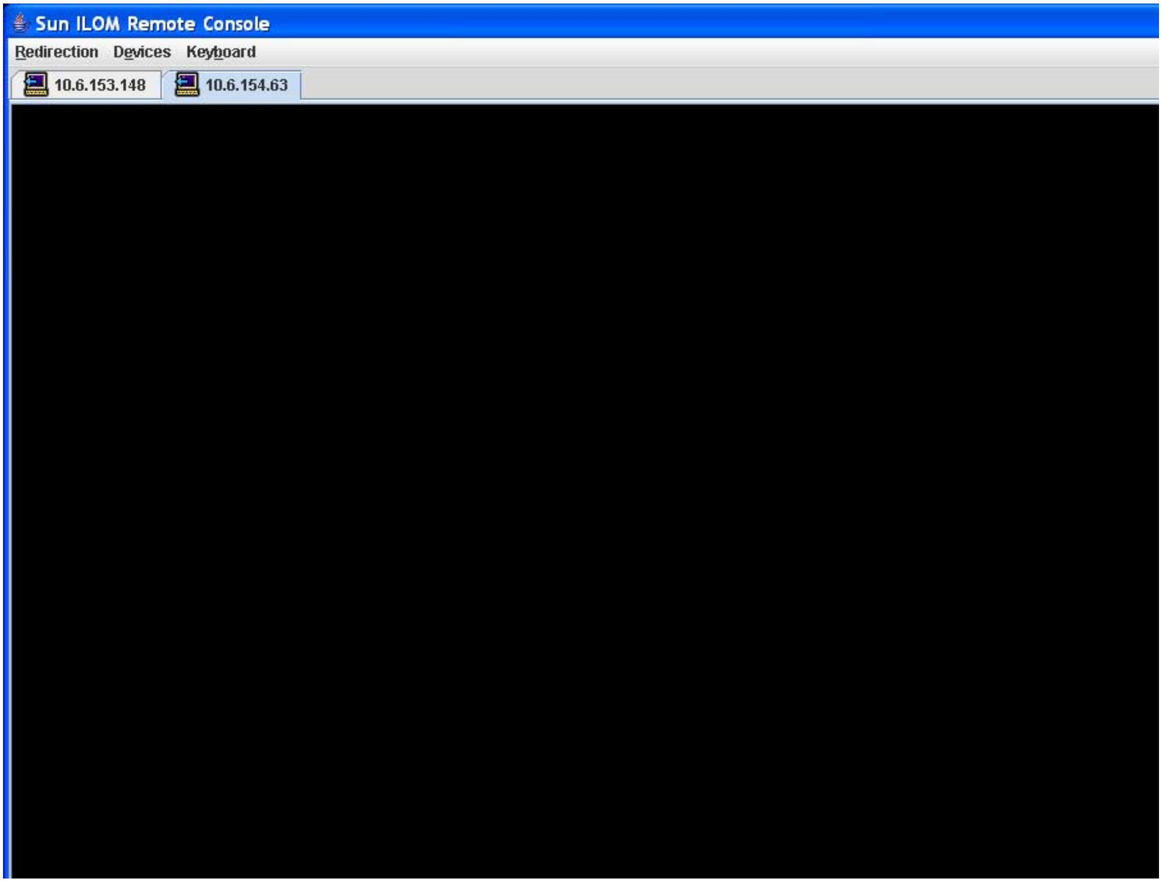
Note – Setting the bandwidth higher than what is actually available can degrade performance. Sometimes you can improve performance by setting the bandwidth lower.

---

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

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

FIGURE 10-5 Remote Console Screen



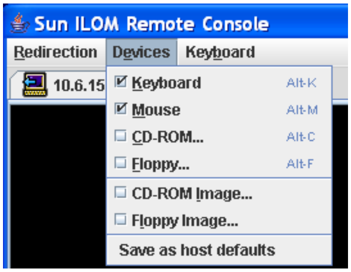
The Remote Console application starts with the video and keyboard enabled.

Note – You can open multiple Remote Console sessions and use the tabs to switch between them.

---

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

FIGURE 10-6 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 10.3, "Redirecting Keyboard, Video, Mouse, or Storage Devices" on page 10-10.

10.3 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.

10.3.1 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 10.2, "Starting the Remote Console Application From the WebGUI" on page 10-5.

---

1. **Start the remote console application as described in** Section 10.2, "Starting the Remote Console Application From the WebGUI" on page 10-5**.**

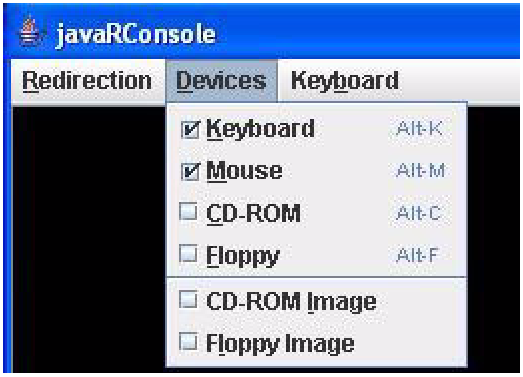
   The Remote Console screen appears.

2. **Choose Devices => Mouse to enable mouse redirection.**

3. **If keyboard redirection is disabled, choose Devices => Keyboard to enable it.**

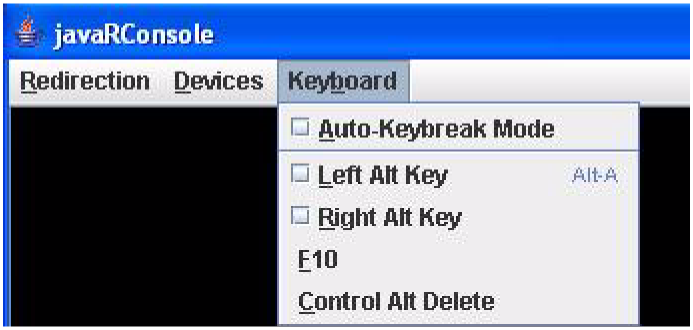
Note – Keyboard redirection is selected by default.

FIGURE 10-7 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 10-8 Keyboard Menu 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.

10.3.2 Redirecting Storage Devices

This section describes how 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.

---

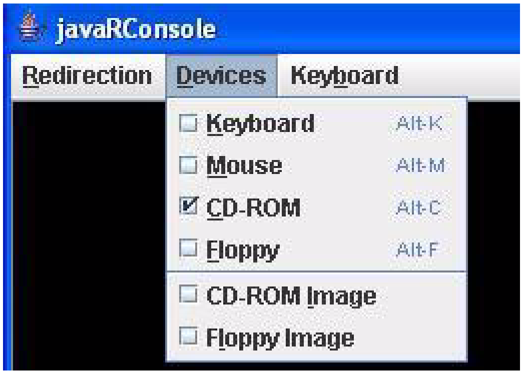
1. **Start the remote console application as described in** Section 10.2, "Starting the Remote Console Application From the WebGUI" on page 10-5**.**

   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 10-9 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 OK.**

5. **To disconnect a device from the server, deselect the corresponding menu item.**

CHAPTER 11

Using Intelligent Platform Management Interface (IPMI)

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

This chapter includes the following sections:

- Section 11.1, "About IPMI" on page 11-1
- Section 11.2, "Supported IPMI 2.0 Commands" on page 11-3

11.1 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 though 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:

- It allows for out-of-band server management.
- The operating system is not burdened with transporting system status data.

Note – VMware EFX Server does not virtualize the Baseboard Management Controller (BMC) interface. That means that guest operating systems cannot load their BMC interface drivers. Also, IPMI utilities cannot use the BMC interface to interact with the Service Processor.

When run under a guest operating system, IPMI utilities must access the Service Processor over the network instead of using the BMC interface. Error messages that occur when the BMC interface driver fails to load can be safely ignored.

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.

11.1.1 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 the system environment, independent of the operating system.

You can download IPMItool from `http://ipmitool.sourceforge.net/`. Also, a copy of IMPItool and its related documentation is provided on your server Tools and Drivers CD.

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

```
man ipmitool
```

11.2 Supported IPMI 2.0 Commands

TABLE 11-1 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 11-1 Supported IPMI 2.0 Commands

Supported IPMI 2.0 Commands
General Commands
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

TABLE 11-1 Supported IPMI 2.0 Commands *(Continued)*

Supported IPMI 2.0 Commands ***(Continued)***
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
Set/Get System Boot Options
Set/Get Event Receiver IPMI
System Interface Support
KCS
BT
RCMP
• Multiple Payloads
• Enhanced Authentication
• Encryption
PEF and Alerting Commands
Get PEF Capabilities
Arm PEF Postpone Timer
Set/Get PEF Configuration Parameters
Set/Get Last Processed Event ID
Alert Immediate
PET Acknowledge

TABLE 11-1 Supported IPMI 2.0 Commands *(Continued)*

Supported IPMI 2.0 Commands ***(Continued)***
Sensor Device Commands
Get Sensor Reading Factors
Set/Get Sensor Hysteresis
Set/Get Sensor Threshold
Set/Get Sensor Event Enable
Get Sensor Reading
Set Sensor Type
FRU Device Commands
Get FRU Inventory Area Info
Read/Write FRU Data SDR Device Commands
Get SDR Repository Info
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
SEL Device Commands
Get SEL Info
Get SEL Allocation Info
Reserve SEL
Get/Add SEL Entry
Clear SEL
Set/Get SEL Time

TABLE 11-1 Supported IPMI 2.0 Commands *(Continued)*

Supported IPMI 2.0 Commands ***(Continued)***
LAN Device Commands
Get LAN Configuration Parameters
Suspend BMC ARPs
Serial/Modem Device Commands
Set/Get Serial Modem Configuration
Set Serial Modem MUX
Get TAP Response Codes
Serial/Modem Connection Active
Callback
Set/Get User Callback Options
Event Commands
Get Event Count
Set/Get Event Destination
Set/Get Event Reception State
Send ICMB Event Message

CHAPTER 12

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, go to `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.

This chapter includes the following sections:

12.1 LDAP Servers Directory Organization

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.

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.

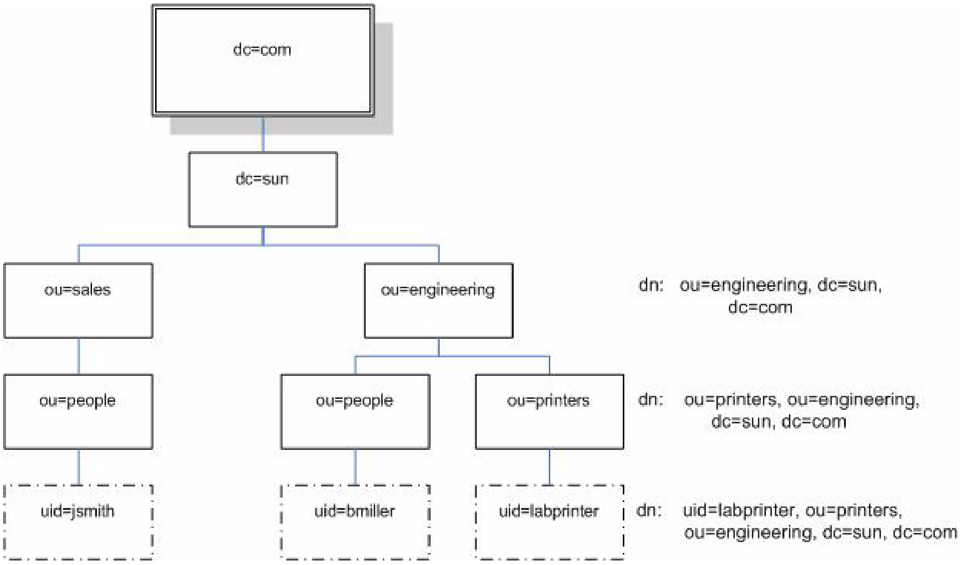
For example, the distinguished name for jsmith is:

```
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.

FIGURE 12-1 shows how distinguished names are used to identify entries uniquely in the directory hierarchy.

FIGURE 12-1 LDAP Distinguished Names


dc=com
dc=sun
ou=sales
ou=engineering
dn: ou=engineering, dc=sun, dc=com
ou=people
ou=people
ou=printers
dn: ou=printers, ou=engineering, dc=sun, dc=com
uid=jsmith
uid=bmiller
uid=labprinter
dn: uid=labprinter, ou=printers, ou=engineering, dc=sun, dc=com

12.2 LDAP Clients and Servers

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 the following 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. To use LDAP authentication, you need to create a user on your LDAP server that your Sun server can authenticate, or bind to, so that the client has permission to search the proper directory on the LDAP server.

12.3 Configuring LDAP

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

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

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

12.3.1 Configuring the LDAP Server

1. **Ensure that all users authenticating to the CMM ILOM have passwords stored in `crypt` format or the GNU extension to `crypt`, commonly referred to as `MD5 crypt`.**

   For example,

   ```
   userPassword: {CRYPT}ajCa2He4PJhNo
   ```

   or

   ```
   userPassword: {CRYPT}$1$pzKng1$du1Bf0NWBjh9t3FbUgf46.
   ```

   The ILOM supports LDAP authentication only, for passwords stored in these two variations of the crypt format.

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

TABLE 12-1 LDAP Property Values

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

12.3.2 Configuring the ILOM

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

12.3.2.1 Configuring the ILOM 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 it searches LDAP users. If an LDAP user name exists as a local user, the ILOM uses the local account for authentication.

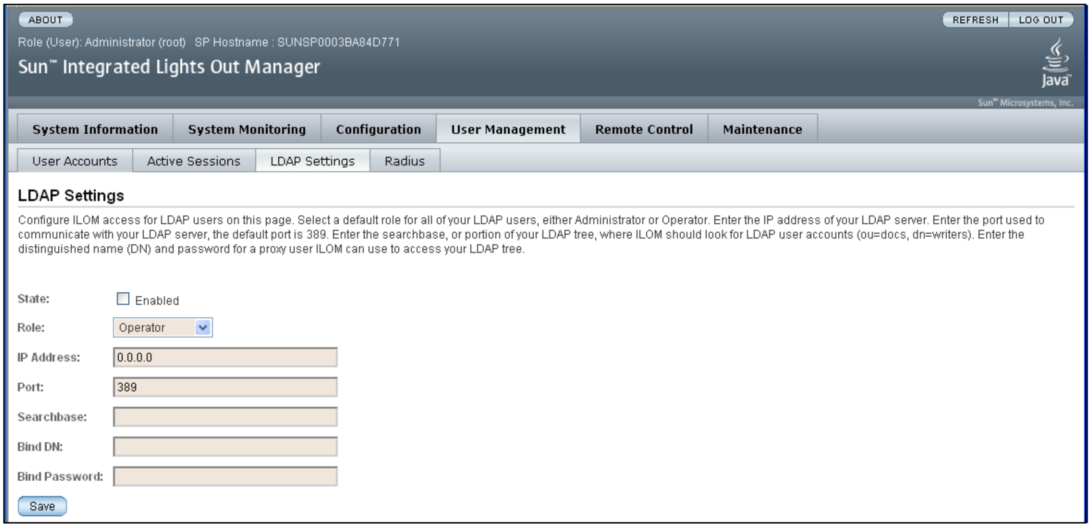
12.3.2.2 Configuring the ILOM Using the WebGUI

1. **Log in to the ILOM as administrator or operator.**

2. **Select User Management => LDAP Settings.**

   The LDAP Settings page appears.

FIGURE 12-2 LDAP Settings Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

LDAP Settings

Configure ILOM access for LDAP users on this page. Select a default role for all of your LDAP users, either Administrator or Operator. Enter the IP address of your LDAP server. Enter the port used to communicate with your LDAP server, the default port is 389. Enter the searchbase, or portion of your LDAP tree, where ILOM should look for LDAP user accounts (ou=docs, dn=writers). Enter the distinguished name (DN) and password for a proxy user ILOM can use to access your LDAP tree.

State: □ Enabled

Role: Operator

IP Address: 0.0.0.0

Port: 389

Searchbase:

Bind DN:

Bind Password:

3. **Enter the following values:**

- State – Select the Enabled check box to authenticate LDAP users.
- Role – The default role of LDAP users. Select operator or administrator from the drop-down menu.
- 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 authenticate users.
- Bind Password – Type the password of the read-only user.

4. **Click Save.**

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.

CHAPTER 13

RADIUS

ILOM supports Remote Authentication Dial-In User Service (RADIUS) authentication for users, based on RFC 2058 and RFC 2059. RADIUS is an authentication protocol that facilitates centralized user administration. RADIUS allows many servers shared access to user data in a central database, providing better security and easier administration.

This chapter contains the following sections:

13.1 RADIUS Overview

RADIUS is based on a client/server model. The RADIUS server provides the user authentication data and can grant or deny access, and the clients send user data to the server and receive an accept or deny response. A RADIUS server can work in conjunction with multiple RADIUS servers and other types of authentication servers.

In the RADIUS client-server model, the client sends an Access-Request query to the RADIUS server. When the server receives an Access-Request message from a client, it searches the database for that user’s authentication information. If the user’s information is not found, the server sends an Access-Reject message and the user is denied access to the requested service. If the user’s information is found, the server responds with an Access-Accept message. The Access-Accept message confirms the user’s authentication data and grants the user access to the requested service.

All transactions between the RADIUS client and server are authenticated by the use of a shared secret. The client and server must each know the secret because it is never passed over the network. You must know the shared secret to configure RADIUS authenticating for ILOM.

To use RADIUS configuration with ILOM, you must configure ILOM as a RADIUS client. For more information, see Section 13.2, "Configuring RADIUS Settings" on page 13-2.

13.2 Configuring RADIUS Settings

If you need to provide ILOM access beyond the 10 local user accounts, you can configure ILOM to use RADIUS authentication. You must have a properly configured RADIUS server before you can use RADIUS authentication with ILOM.

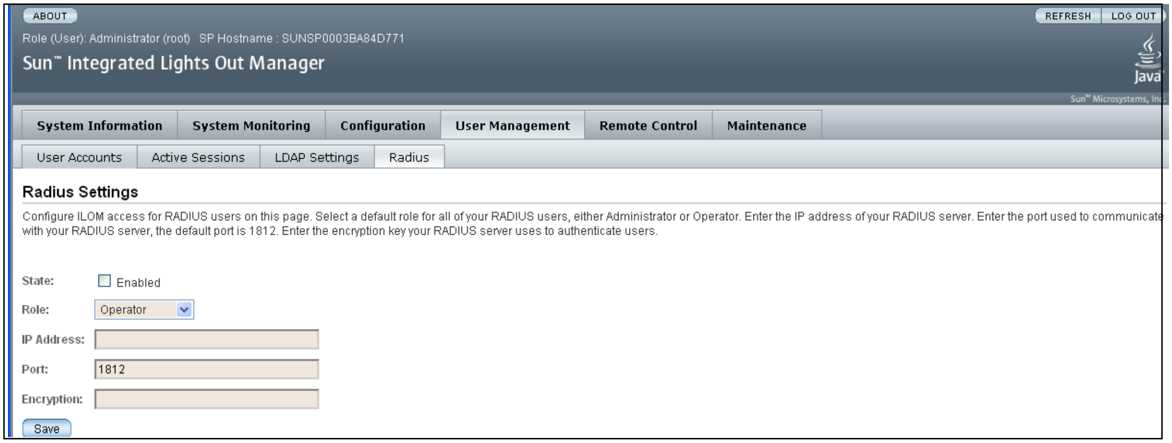
Before completing this procedure, collect the appropriate information about your RADIUS environment, as described in Section 13.1, "RADIUS Overview" on page 13-1.

13.2.1 Configuring RADIUS Using the WebGUI

1. **Log in to the WebGUI as administrator.**
2. **Select User Management => RADIUS.**

   The RADIUS Settings page appears.

FIGURE 13-1 RADIUS Page



Role (User): Administrator (root) SP Hostname : SUNSP0003BA84D771

Radius Settings

Configure ILOM access for RADIUS users on this page. Select a default role for all of your RADIUS users, either Administrator or Operator. Enter the IP address of your RADIUS server. Enter the port used to communicate with your RADIUS server, the default port is 1812. Enter the encryption key your RADIUS server uses to authenticate users.

State: □ Enabled

Role: Operator

IP Address:

Port: 1812

Encryption:

3. **Complete the settings. For details, see TABLE 13-1.**
4. **Click Save for your changes to take effect.**

13.2.2 Configuring RADIUS Using the CLI

1. **Log in to the CLI as administrator.**
2. **Navigate to** `/SP/clients/radius`**.**
3. **Set the parameters shown in TABLE 13-1.**

13.2.3 RADIUS Parameters

TABLE 13-1 describes the RADIUS parameters for the WebGUI and the CLI.

TABLE 13-1 RADIUS WebGUI and CLI Settings

WebGUI	CLI	Description
Default Role	`defaultrole` *administrator* | *operator*	Sets the default role for all RADIUS users: administrator or operator
IP Address	`ipaddress` *ipaddress*	The IP address of the RADIUS server
Port	`port` *portnum*	The port number used to communicate with the RADIUS server. The default port is 1812.

TABLE 13-1 RADIUS WebGUI and CLI Settings

WebGUI	CLI	Description
State	`state` *enabled*|*disabled*	Enable to authenticate RADIUS users
Encryption Key		Type the encryption key used by your RADIUS server.
	`secret` *text*	The shared secret used to gain access to RADIUS

13.3 RADIUS Commands

This section describes the RADIUS commands.

13.3.1 `show /SP/clients/radius`

This command is available to administrators and operators.

Purpose

Use this command to view the properties associated with RADIUS authentication.

Syntax

```
show /SP/clients/radius
```

Properties

defaultrole – This is the role assigned to all RADIUS users. It is either administrator or operator.

ipaddress – The IP address of your RADIUS server.

port – The port number used to communicate with your RADIUS server. The default port is 1812.

secret – Enter the shared secret used to gain access to your RADIUS server.

state – Choose `enabled` or `disabled` to allow or deny access to your RADIUS users.

Example

```
  -> show /SP/clients/radius

    /SP/clients/radius
     Targets:

     Properties:
         defaultrole = Operator
         ipaddress = 129.144.36.142
         port = 1812
         secret = (none)
         state = enabled

     Commands:
         cd
         set
         show

 ->
```

13.3.2 set /SP/clients/radius

This command is available to administrators.

Purpose

Use this command to configure the properties associated with RADIUS authentication on a service processor.

Syntax

```
set /SP/clients/radius [defaultrole=[Administrator|Operator]
ipaddress=radiusserverIP port=port# secret=radiussecret state=
[enabled|disabled]]
```

Properties

- defaultrole – Assign a permission level that will apply to all RADIUS users.
- ipaddress – The IP address of your RADIUS server.
- port – The port number used to communicate with your RADIUS server. The default port is 1812.
- secret – Enter the shared secret used to gain access to your RADIUS server. This is also known as an encryption key.
- state – Choose enabled or disabled to allow or deny access to your RADIUS users.

Example

```
 -> set /SP/clients/radius state=enabled ipaddress=10.8.145.77
Set 'state' to 'enabled'
Set 'ipaddress' to '10.8.145.77
```

13.3.3 show /SP/clients

This command is available to administrators and operators.

Purpose

Use this command to view clients that can receive data from a service processor, including LDAP, NTP, RADIUS, and SYSLOG clients.

Syntax

```
show /SP/clients
```

Example

```
-> show /SP/clients

 /SP/clients
   Targets:
 ldap
 ntp
 radius
 syslog

   Properties:

   Commands:
       cd
       show
```

Note – Users with operator privileges can only view the ntp and syslog targets. The radius and ldap targets remain hidden.

CHAPTER 14

Using Simple Network Management Protocol (SNMP)

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

14.1 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.

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

The SNMP agent is preinstalled and runs on the 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.

14.2 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 MIB files.

Standard:

- SNMP-FRAMEWORK-MIB
- SNMP-USER-BASED-MIB
- SNMP-MPD-MIB
- ENTITY-MIB

Sun Specific:

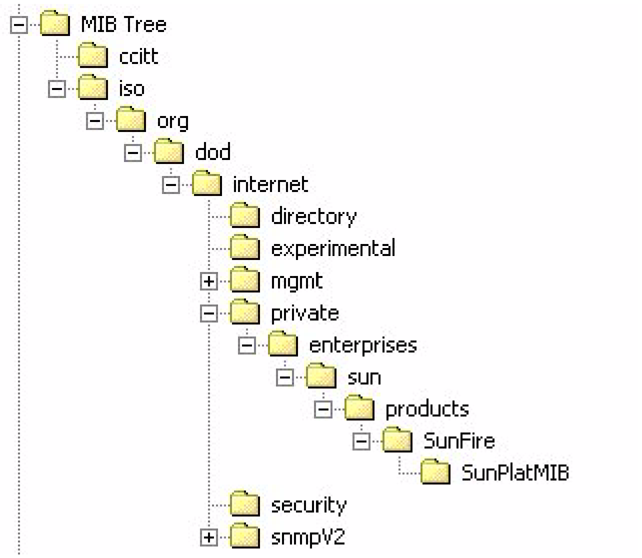
- SUN-PLATFORM-MIB
- SUN-ILOM-CONTROL-MIB
- SUN-ILOM-PET-MIB

Download and install the product-specific MIB files from your Tools and Drivers CD for your platform.

14.3 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 14-1 shows the arrangement. The standard SNMP port (port 161) is used by the SNMP agent on the ILOM.

FIGURE 14-1 Sun server MIB Tree



14.4 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 might provide this functionality, or you can use an open source tool like net-SNMP, which is available at:

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

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

14.5 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, and (3) configure the specific traps.

The Sun server MIB tree appears in FIGURE 14-1.

14.5.1 Integrating the MIBs

Use a third-party SNMP management application to load the SUN-PLATFORM-MIB listed in Section 14.2, “SNMP Management Information Base (MIB) Files” on page 14-2.

14.5.2 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 more details.

14.5.3 Configuring Receipt of SNMP Traps

To configure a trap in your ILOM, see Section 8.5, "Managing ILOM Alerts" on page 8-6 for CLI instructions, and Section 9.5, "Managing Alerts" on page 9-10 for WebGUI instructions.

14.6 Managing SNMP Users With the CLI

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 14.7, "Managing SNMP With the WebGUI" on page 14-7.

14.6.1 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 the following command:

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

14.6.2 Deleting a User Account

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

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

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

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

14.6.3 Configuring User Accounts

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

14.6.3.1 Syntax

set target *[propertyname=value]*

14.6.3.2 Targets, Properties, and Values

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

TABLE 14-1 SNMP User Account Targets, Properties, and Values

Target	Property	Value	Default
`/SP/services/snmp/communities/communityname`	permissions	ro|rw	ro
`/SP/services/snmp/users/username`	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.

14.6.3.3 Examples

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

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

Your changes would be invalid if you typed:

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

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

14.7 Managing SNMP With the WebGUI

This section describes how to use the WebGUI to manage SNMP users.

For more information about SNMP and the classes of MIB files that the Sun server supports, see Section 14.1, "About SNMP" on page 14-1.

14.7.1 Configuring SNMP Settings

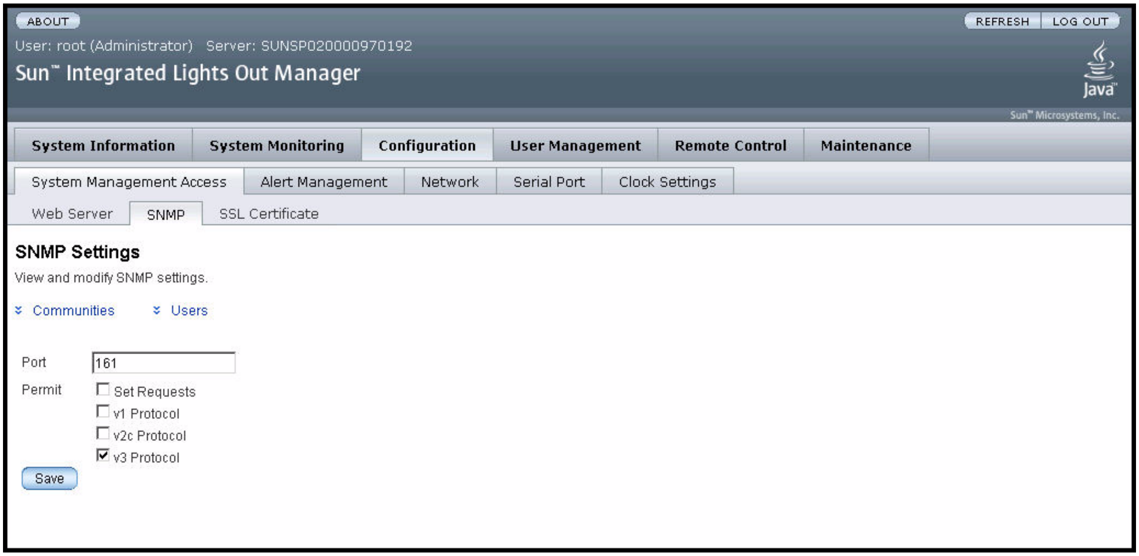
1. **Log in to the ILOM as administrator.**

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

2. **Select Configuration =>System Management Access => SNMP.**

   The SNMP Settings page appears.

FIGURE 14-2 SNMP Settings



SNMP Settings

View and modify SNMP settings.

Port 161

Permit
- □ Set Requests
- □ v1 Protocol
- □ v2c Protocol
- ☑ v3 Protocol

3. **Type the port number in the Port field.**

4. **Enable or disable Set Requests by selecting or clearing the Set Requests check box.**

   If Set Requests is disabled, all SNMP objects are read-only.

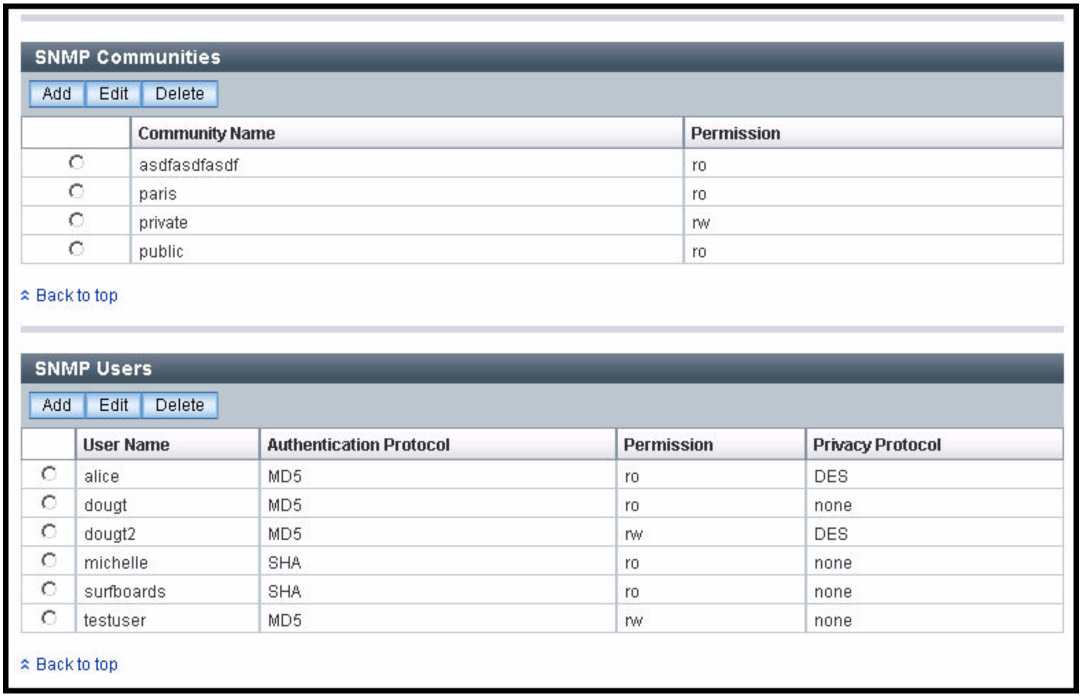
5. **Select a check box to enable SNMP v1, v2c, or v3.**

   SNMP v3 is enabled by default. You can independently enable or disable v1, v2c, and v3 protocol versions.

6. **Click Save for your settings to take effect.**

7. **At the bottom of the page, you can also add, edit, or delete SNMP communities, as well as SNMP users. See** FIGURE 14-3**.**

FIGURE 14-3 SNMP Communities and Users



SNMP Communities

	Community Name	Permission
○	asdfasdfasdf	ro
○	paris	ro
○	private	rw
○	public	ro

SNMP Users

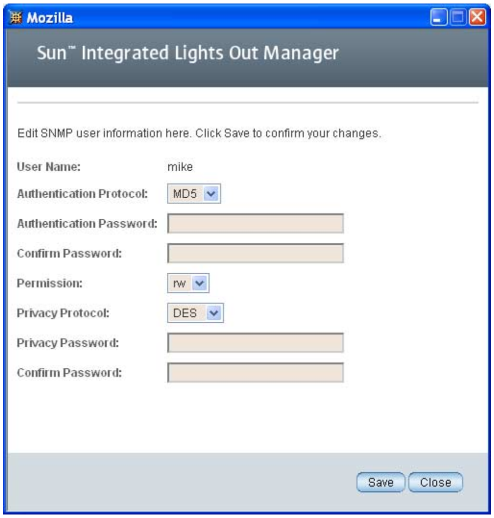
	User Name	Authentication Protocol	Permission	Privacy Protocol
○	alice	MD5	ro	DES
○	dougt	MD5	ro	none
○	dougt2	MD5	rw	DES
○	michelle	SHA	ro	none
○	surfboards	SHA	ro	none
○	testuser	MD5	rw	none

14.7.2 Adding or Editing SNMP Users

1. **Click the Users link or scroll down to the SNMP Users list.**
2. **Click Add or Edit under the SNMP Users list.**

   The Add dialog box, or the Edit dialog box appears. **See** FIGURE 14-4**.**

FIGURE 14-4 Edit SNMP User Dialog Box



Edit SNMP user information here. Click Save to confirm your changes.

User Name:	mike
Authentication Protocol:	MD5
Authentication Password:	
Confirm Password:	
Permission:	rw
Privacy Protocol:	DES
Privacy Password:	
Confirm Password:	

3. **Add or change the information in the fields as follows:**

   a. **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.

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

   c. **Type an authentication password.**

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

   d. **Type the authentication password again in the Confirm Password field.**

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

   f. **Select DES or none for a privacy protocol.**

   g. **Type a privacy password.**

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

   h. **Type the privacy password again in the Confirm Password field.**

4. **Click Save.**

14.7.3 Deleting an SNMP user

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

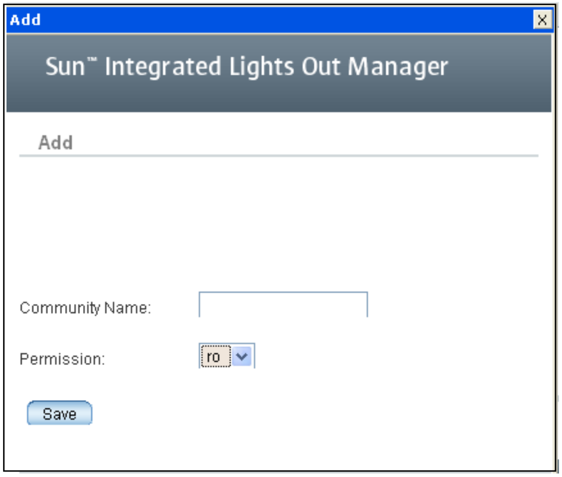
   A confirmation dialog box appears.
4. **Click OK to delete the SNMP user.**

14.7.4 Adding and Editing SNMP Communities

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

   The Add or Edit dialog box appears. See FIGURE 14-5.

FIGURE 14-5 Add Community Dialog Box



Add

Sun™ Integrated Lights Out Manager

Add

Community Name:

Permission: ro

3. **Type the community name in the 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 read-only (ro) or read-write (rw) permissions.**
5. **Click Save.**

14.7.5 Deleting 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 Delete under the SNMP Communities list.**

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

APPENDIX **A**

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-6

A.1 CLI Command Quick Reference

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

TABLE A-2 General Commands

Description	Command
Show all valid targets.	`help targets`
Log out of the CLI.	`exit`
Display the version of the ILOM firmware running on the ILOM.	`version`
Display clock information.	`show /SP/clock`
Display all of the CLI commands.	`show /SP/cli/commands`
Display the active ILOM sessions.	`show /SP/sessions`
Display information about commands and targets.	`help`
Display information about a specific command.	`help` *create*
Update the ILOM and BIOS firmware.	`load -source` *tftp://newSPimage*
Display a list of the ILOM event logs.	`show /SP/logs/event/list`

TABLE A-3 User Commands

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

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=`***ipaddress* **`pendingipdiscovery=dchp|static`** **`pendingipgateway=`***ipgateway* **`pendingipnetmask=`***ipnetmask* **`commitpending=true`**
Display information about the external serial port.	**`show /SP/serial/external`**
Change the external serial port configuration.	**`set /SP/serial/external pendingspeed=`***integer* **`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=`***integer* **`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=`***ipaddress* **`level=`**`down|critical|major|minor`

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**

TABLE A-7 SNMP Commands *(Continued)*

Description	Command
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*
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] [-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] [-h|help]`

Targets, Properties, and Values

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

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

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

Targets

TABLE A-11 Targets for the `delete` Command

Valid Targets
/SP/users/*username*
/SP/services/snmp/community/*communityname*
/SP/services/snmp/user/*username*

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

[-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

[-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

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

Examples

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

-> load -source tftp://10.6.22.32/tftp_files/file.ima

-> load -source tftp://tftpserver.sun.com/file.ima
```

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 enters 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

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

Targets

TABLE A-12 Targets for the `reset` Command

Valid Targets
/SP
/SYS

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 the `set` Command

Valid Targets	Properties	Values	Default
/SP/users/*username*	password role	<string> administrator | operator	(none) operator
/SP/alert/rules/*rulename* (rulename = 1 through 15)	level	disable | information | warnin g | critical | non-recoverable	critical
	destination	<ipaddress>	(none)
/SP/clock	usentpserver	enabled | disabled	/SP/clock

TABLE A-13 Targets, Properties, and Values for the `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/radius	defaultrole	administrator | operator<ipaddress> | none	operator
	ipaddress		none
	port	<decimal>	1812
	secret	<string> | none	none
	state	enable | disabled	disabled
/SP/clients/servers/[1|2]	address	<IP address> | <hostname> | none	(none)

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

Valid Targets	Properties	Values	Default
`/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 the `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/radius	defaultrole ipaddress port secret state
/SP/clients/ntp	
/SP/clients/ntp/server	
/SP/clients/ntp/server/[1|2]	
/SP/clock	datetime usentpserver
/SP/logs	

TABLE A-14 Targets for the `show` Command *(Continued)*

Valid Targets	Properties
`/SP/logs/event`	clear
`/SP/logs/event/list`	
`/SP/network`	commitpending ipaddress ipdiscovery ipgateway ipnetmask linkstatus macaddress pendingipaddress pendingdiscovery pendingipgateway pendingipnetmask
`/SP/serial`	
`/SP/serial/external`	commitpending flowcontrol pendingspeed speed
`/SP/serial/host`	commitpending pendingspeed speed
`/SP/services`	
`/SP/services/http`	port securedirect 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

TABLE A-14 Targets for the `show` Command *(Continued)*

Valid Targets	Properties
/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	
/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
```

TABLE A-15

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

/SP/clients

                  Targets:

                                 ldap
                                 ntp

                  Properties:
```

TABLE A-15

	`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`
	`Commands:`	
		`cd`
		`show`
`/SP/clients/ntp`		
	`Targets:`	
		`server`
	`Properties:`	

	`Commands:`
	`cd`
	`show`	

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

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

Targets

TABLE A-16 Targets for the `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

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

Targets

TABLE A-17 Targets for the `stop` Command

Valid Targets	Description
`/SYS`	Perform an orderly shutdown, followed by a power off of the specified hardware. Use the `-force` option to skip the orderly shutdown and force an immediate power off.
`/SP/console`	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

```
[-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
```

APPENDIX **B**

ILOM Ports

This appendix lists the ports in the ILOM.

When configuring firewall access to the ILOM, you must allow access to all relevant ports.

TABLE B-1 ILOM Ports

Ports	Protocols	Applications
80	HTTP over TCP	SP - ILOM user-configurable port
443	HTTPS over TCP	SP - ILOM user-configurable port
5120	TCP	SP - ILOM remote console: CD
5123	TCP	SP - ILOM remote console: diskette
5121	TCP	SP - ILOM remote console: keyboard and mouse
7578	TCP	SP - ILOM remote console: video
22	ssh over TCP	ssh - secure shell
69	TFTP over UDP	TFTP - trivial file transfer protocol
123	NTP over UDP	NTP - network time protocol
161	SNMP over UDP	SNMP - simple network management protocol
162	IPMI over UDP	IPMI - platform event trap (PET) (outgoing port)
389	LDAP over UDP/TCP	LDAP - lightweight directory access protocol (user-configurable port)
514	Syslog over UDP	Syslog - (outgoing port)
546	DHCP over UDP	DHCP - dynamic host configuration protocol (client)
623	IPMI over UDP	IPMI - intelligent platform management interface
1812	RADIUS over UDP	RADIUS - remote authentication dial in user service

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 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 than 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 can then 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 by a 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 a 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," which 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(TM) 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.

OpenBoot(TM) 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) 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 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