Sun™ Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide

Sun Microsystems, Inc.
www.sun.com

Part No. 820-5523-10
December 2008, Revision A

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

Please
Recycle

Contents

Preface

Sun Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide describes how to perform the required procedures to access ILOM for the first time on your system. These procedures include ILOM network connection, login, user account creation, directory service configuration, and firmware upgrade.

This Getting Started Guide is written for system administrators who are familiar with networking concepts and basic system management protocols.

Related Documentation

To fully understand the information that is presented in this guide, use this document in conjunction with the documents listed in the following table. These documents are available online at:

`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

These documents are also available with you platform documentation set at:

`http://docs.sun.com/app/docs/prod/servers`

First read the ILOM 3.0 Concepts Guide to learn about ILOM's features and functionality. To set up a new system supported by ILOM, refer to this ILOM 3.0 Getting Started Guide, where you will find the procedures for connecting to the network, logging in to ILOM for the first time, and configuring a user account or directory service. Then, decide which ILOM interface you want to use to perform other ILOM tasks. You can now refer to the the appropriate ILOM 3.0 Procedures Guide for your selected interface.

The following table lists the ILOM 3.0 Documentation Collection.

TABLE P-1 ILOM 3.0 Documentation Collection

Title	Content	Part Number	Format
Sun Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide	Information that describes ILOM features and functionality	820-6410	PDF HTML
Sun Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide	Information and procedures for network connection, logging in to ILOM for the first time, and configuring a user account or a directory service	820-5523	PDF HTML
Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide	Information and procedures for accessing ILOM functions using the ILOM web interface	820-6411	PDF HTML
Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide	Information and procedures for accessing ILOM functions using the ILOM CLI	820-6412	PDF HTML
Sun Integrated Lights Out Manger (ILOM) 3.0 SNMP and IPMI Procedures Guide	Information and procedures for accessing ILOM functions using SNMP or IPMI management hosts	820-6413	PDF HTML

In addition to the ILOM 3.0 Documentation Collection, associated ILOM Supplement documents present ILOM features and tasks that are specific to the server platform you are using. Use the ILOM 3.0 Documentation Collection in conjunction with the ILOM Supplement that comes with your server platform.

Documentation, Support, and Training

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

ILOM 3.0 Version Numbers

ILOM 3.0 has implemented a new version numbering scheme to help you identify which version of ILOM you are running on your system. The numbering scheme includes a five-field string, for example, `a.b.c.d.e`, where:

- `a` – Represents the major version of ILOM.
- `b` – Represents a minor version of ILOM.
- `c` – Represents the update version of ILOM.
- `d` – Represents a micro version of ILOM. Micro versions are managed per platform or group of platforms. See your platform Product Notes for details.
- `e` – Represents a nano version of ILOM. Nano versions are incremental iterations of a micro version.

For example, ILOM 3.1.2.1.a would designate:

- ILOM 3 as the major version of ILOM
- ILOM 3.1 as a minor version of ILOM 3
- ILOM 3.1.2 as the second update version of ILOM 3.1
- ILOM 3.1.2.1 as a micro version of ILOM 3.1.2
- ILOM 3.1.2.1.a as a nano version of ILOM 3.1.2.1

Product Identity Information

Product identity information enables a system to register itself and use certain automated services based on the service contract associated with its identity. You can use product identity information to uniquely identify a system. You also need to supply the product identity information to Sun when you request service for the system. Product identity consists of the following information:

- `product_name`: Name under which a product is sold. For example, "SUN FIRE X4100 M2."
- `product_part_number`: Namespace assigned by manufacturing within which the product serial number is unique. A product part number never maps to more than one product. For example, "602-3098-01."
- `product_serial_number`: Unique identity assigned to each instance of a product by manufacturing. For example, "0615AM0654A."
- `product_manufacturer`: Manufacturer of the product. For example, 'SUN MICROSYSTEMS."

TABLE P-2 describes the common product identity information used by ILOM.

TABLE P-2 Common Product Identity Information

Required Information	Target	Minimal Properties
Basic product information on server (rackmounted and blade)	/SYS	product_name product_part_number product_serial_number product_manufacturer
Basic product information on chassis monitoring module (CMM)	/CH	product_name product_part_number product_serial_number product_manufacturer
Basic chassis information on blade	/SYS/MIDPLANE	product_name product_part_number product_serial_number product_manufacturer
Location of blade within the chassis	/SYS/SLOTID	type class value
Location of chassis within a rack	/CH	rack_location

Third-Party Web Sites

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

Typographic Conventions

Typeface*	Meaning	Examples
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output	Edit your `.login` file. Use `ls -a` to list all files. `% You have mail.`
`AaBbCc123`	What you type, when contrasted with on-screen 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 *Concept'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.

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:

Sun Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide,
part number 820-5523-10.

Getting Started With ILOM

Topics

Description	Links
Learn how to use this guide	• "About This Guide" on page 2
Review the ILOM getting started process and prerequisites, choose an interface, and plan your ILOM setup	• "ILOM Getting Started Process" on page 3 • "Using the `root` Account" on page 3 • "Using the Web Interface or CLI" on page 4 • "Planning the Initial ILOM Setup" on page 4
Connect ILOM to the network and assign an IP address	• "Connecting to ILOM" on page 6
Use the ILOM web interface to log in, set up user accounts, configure ILOM, and log out	• "Initial ILOM Setup Procedures Using the Web Interface" on page 10
Use the ILOM CLI to log in, set up user accounts, configure ILOM, and log out	• "Initial ILOM Setup Procedures Using the CLI" on page 30
Identify your ILOM firmware version and update firmware	• "Identify ILOM Version Using Web Interface" on page 43 • "Identify ILOM Version Using CLI" on page 43 • "Update ILOM Firmware to Latest Version" on page 44
Find information about your next ILOM configuration steps	• "What Next?" on page 48

About This Guide

Sun Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide provides easy-to-use setup and configuration procedures that will enable you to start using ILOM even before your host system is powered on.

With ILOM, you can remotely monitor and manage your Sun system without consuming operating system resources. ILOM provides fully featured interfaces, including a browser-based web interface, a command-line interface, an SNMP interface, and an IPMI interface. These interfaces are based on industry standards and are intuitive to use.

The getting started procedures describe how to connect to ILOM and configure the required initial settings. The procedures to verify and update the ILOM firmware version are also provided. You can find more in-depth descriptions of ILOM's features and functions in the other documents that comprise the ILOM 3.0 Documentation Collection. For a list of those documents, see TABLE P-1 in the Preface.

ILOM Getting Started Process

You can use ILOM's default configuration and settings to access many of ILOM's features, or you can customize certain ILOM settings to work in your specific environment. Before you begin the initial setup of ILOM, determine how you want to access ILOM and then how to configure ILOM for your system and data center environment.

Using the `root` Account

ILOM 3.0 provides the preconfigured `root` user account. You will use the `root` account for initial login to ILOM. This `root` user account will be familiar to users who are migrating from ILOM 2.x to ILOM 3.0 and who know how to log in using the `root` user account.

The `root` user account is persistent and is available on all interfaces (web interface, CLI, SSH, serial console, and IPMI) unless you choose to delete the `root` account. The `root` account provides built-in administrative privileges (read and write) for all ILOM features, functions, and commands.

To log in to ILOM using the `root` account:

- User name: **`root`**
- Password: **`changeme`**

To prevent unauthorized access to your system, you should change the `root` password (`changeme`) on each service processor (SP) or chassis monitoring module (CMM) installed in your system. Alternatively, you can delete the `root` account to secure access to your system. However, before you delete the `root` account, you must set up a new user account or configure a directory service so that you will be able to log in to ILOM.

If you delete the `root` account before you have configured a new user account or directory service to log in to ILOM, you can use another preconfigured account, the `default` user account, as an alternative way to to log in and re-create the `root` account. For information about the `default` user account, see the *Sun Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide*.

Using the Web Interface or CLI

You can access ILOM's features and functions using either the web interface or the command-line interface (CLI), as well as using an SNMP interface or IPMI interface. You can complete all ILOM tasks in either the web interface or the CLI.

The getting started procedures in this guide are divided into two parts. The first part explains how to perform the initial setup and configuration tasks using the web interface. The second part explains how to perform the same tasks, but using the CLI. Before you begin the setup and configuration, choose one of the interfaces and follow the respective procedures.

Planning the Initial ILOM Setup

Here are some tasks to consider when you start to use ILOM for the first time. Each task is described in more detail in the procedures that follow.

TABLE 1 Initial ILOM Setup and Configuration Tasks

Task	Information to Consider	Refer to This Procedure
Configure ILOM for Network Access		
Connect to ILOM	You can connect to ILOM using an Ethernet connection or a serial connection.	Refer to your platform documentation
Configure the network settings	The way you configure network settings depends on your server platform: • Use DHCP – for all platforms • Use serial login – for all platforms • Use BIOS – for x64-based servers or server modules • Use IPMItool running host OS – for x64-based servers or server modules • Use chassis monitoring module (CMM) – for server module (blade) systems only	"Configure SP Network Settings Using DHCP" on page 6 "Configure Static Network Settings Using Serial Connection" on page 8
Log In to ILOM for the First Time		
Log in to ILOM using the `root` user account	ILOM boots automatically when power is applied to your Sun system. ILOM is preconfigured with the `root` user account and its password. You can use this special account for initial login and account setup. To log in using the `root` account: • User name: **`root`** • Password: **`changeme`**	"Log In to ILOM 3.0 Using `root` User Account" on page 11 (web) "Log In to ILOM 3.0 Using `root` User Account" on page 30 (CLI)

TABLE 1 Initial ILOM Setup and Configuration Tasks *(Continued)*

Task	Information to Consider	Refer to This Procedure
Create Local User Accounts or Use a Directory Service		
Note - You can choose either to create a local user account or to configure a directory service.		
Add local user account and assign roles	After you have logged in to ILOM, you can create and configure up to 10 local user accounts.	"Add User Account and Assign Privileges" on page 12 (web) "Add User Account and Assign Privileges" on page 31 (CLI)
Configure ILOM for Active Directory	Before you can use Active Directory, you need to enter basic data, such as primary server, port number, and certificate mode, and optional data, such as alternate server and event or severity levels.	"Configure ILOM for Active Directory" on page 14 (web) "Configure ILOM for Active Directory" on page 31 (CLI)
Configure ILOM for LDAP	ILOM can use LDAP and can be an LDAP client for authentication purposes. To use LDAP authentication, you need to create a user account on your LDAP server that ILOM can authenticate with, or bind to, so that the client has permission to search the proper directory on the LDAP server.	"Configure LDAP Server" on page 20 (web) "Configure ILOM for LDAP" on page 21 (web) "Configure ILOM for LDAP" on page 35 (CLI)
Configure ILOM for LDAP SSL	To configure LDAP with Secure Socket Layer (SSL), you need to enter basic data, such as primary server, port number, and certificate mode, and optional data such as alternate server and event or severity levels.	"Configure ILOM for LDAP/SSL" on page 22 (web) "Edit LDAP/SSL Tables" on page 26 (web) "Configure ILOM for LDAP/SSL" on page 36 (CLI)
Configure ILOM for RADIUS	To use RADIUS authentication, you must first set the IP address and port number of the RADIUS server, as well as set the shared secret, which you use to access the RADIUS server.	"Configure ILOM for RADIUS" on page 27 (web) "Configure ILOM for RADIUS" on page 41 (CLI)
Log In and Out of ILOM Using an Administrative User Account		
Log in to ILOM using a local, administrative user account	Once you have created a local user account or configured a directory service, log in to ILOM using that local, administrative user account.	"Log In to ILOM as a User" on page 28 (web) "Log In to ILOM as a User" on page 42 (CLI)

TABLE 1 Initial ILOM Setup and Configuration Tasks *(Continued)*

Task	Information to Consider	Refer to This Procedure
Log out of ILOM	You can log out of your ILOM session while preserving your configuration settings.	"Log Out of ILOM" on page 29 (web) "Log Out of ILOM" on page 42 (CLI)
Identify ILOM Version and Upgrade Firmware		
Identify ILOM version	You can quickly identify which version of ILOM is running on the service processor or chassis monitoring module.	"Identify ILOM Version Using Web Interface" on page 43 "Identify ILOM Version Using CLI" on page 43
Update ILOM firmware	You can easily update your ILOM firmware to the latest version.	"Update ILOM Firmware Using Web Interface" on page 45 "Update ILOM Firmware Using CLI" on page 46

Connecting to ILOM

You can log in to ILOM over the serial port without a network connection, or you can log in to ILOM over the network. To log in using a direct serial connection, attach a serial cable to the workstation, terminal, or terminal emulator and to the SER MGT port on the server or, if you are using a modular chassis system, on the chassis monitoring module (CMM). To log in using a network connection, attach an Ethernet cable to the NET MGT port on the server or on the CMM. Then, configure the SP network interface using static or dynamic settings.

If your network infrastructure uses a firewall, or non-standard ports for common services, you should review the default network port assignments that are documented in the *Sun Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.*

▼ Configure SP Network Settings Using DHCP

This procedure assumes that you are setting up a new system or setting up a system that was previously configured to use DHCP. If your system is not set up to use DHCP, you need to set the DHCP option using the web interface or the CLI. See the *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide* or the *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide* for more information.

Follow these steps to configure SP network settings using DHCP:

1. **Connect your network to the management Ethernet port on your server:**

   By default, ILOM will attempt to obtain network settings using DHCP.

   Refer to your platform documentation to locate the management Ethernet port on your server.

2. **Use one of the following methods to obtain the IP address assigned to the SP.**

   - **DHCP server logs:**

     Refer to your DHCP server documentation for information.

   - Connect to the SP serial port and type the following command:

     -> **show /SP/network**

   - Observe the IP address displayed by the BIOS during host startup of x64 servers.

   - Using IPMItool for your host OS, type the following command:

     #**ipmitool -I** <*interface*> **lan print 1**

     Where *interface* is `bmc` on Solaris systems, `open` on Linux systems, and `ms` on Windows 2003 Server R2 Enterprise systems.

Note – When you use the `ipmitool` command on a Microsoft Windows system, you need to add the `.exe` extension to the `ipmitool` command. For example, **`ipmitool.exe -I ms lan print 1`**

▼ Configure SP Network Settings Using BIOS

This procedure assumes you are accessing the server host side BIOS and that you have connected a keyboard and terminal to the keyboard and VGA ports on the server.

Follow these steps for x64 servers and server modules (blades) in a modular chassis system:

1. **Enter the BIOS Setup utility by pressing the F2 key while the system is powering on and performing the power-on self-test (POST).**

2. **When the BIOS Main menu screen is displayed, select Advanced --> IPMI 2.0 Configuration --> LAN Configuration.**

3. **On the LAN Configuration screen, under IP Assignment, select DHCP or Static.**

   - If you selected DHCP, the SP will obtain its network configuration from the DHCP server.

   - If you selected Static, fill in the fields for IP address, subnet mask, and default gateway. Select Commit to save your changes.

▼ Configure Static Network Settings Using Serial Connection

Follow these steps to configure static network settings using a serial connection:

1. **Establish a serial connection to the server SP or CMM.**

   Attach a terminal or PC running terminal emulation software to the serial port on the server or chassis monitoring module (CMM).

2. **Configure the following settings in the terminal window:**
   - 8N1: eight data bits, no parity, one stop bit
   - 9600 baud
   - Disable hardware flow control
   - Disable software flow control

3. **Press Enter to obtain the ILOM login prompt.**

   The ILOM login prompt appears:

   <*hostname*> `login:`

4. **Log in to the ILOM CLI using the `root` user account and password.**

   <*hostname*> `login:` **`root`**

   `Password:` **`changeme`**

   The ILOM CLI prompt appears (`->`).

5. **Type one of the following commands to set the working directory.**
   - For a server SP:

   `->` **`cd /SP/network`**
   - For a CMM:

   `->` **`cd /CMM/network`**

6. **Use the following commands to configure the network.**
   - **`set pendingipdiscovery=static`**
   - **`set pendingipaddress=`***ip_address*
   - **`set pendingipnetmask=`***ip_netmask*
   - **`set prendingipgateway=`***ip_gateway*
   - **`set commitpending=true`**

▼ Configure Network Settings Using IPMItool

Detailed information about IPMItool is provided in a man page that is available from this site:

http://ipmitool.sourceforge.net/manpage.html

Follow these steps to configure network settings using IPMItool:

1. **Determine the appropriate static network settings that you want to use.**
2. **To assign static IP network settings, while running IPMItool on the host, type the following commands:**

   #**ipmitool -I** <*interface*> **lan set 1 ipsrc static**
   #**ipmitool -I** <*interface*> **lan set 1 ipaddr** <*ipaddress*>
   #**ipmitool -I** <*interface*> **lan set 1 netmask** <*netmask*>
   #**ipmitool -I** <*interface*> **lan set 1 defgw ipaddr** <*gateway*>

   Where *interface* is `bmc` on Solaris systems, `open` on Linux systems, and `ms` on Windows 2003 Server R2 Enterprise systems.

Note – When you use the `ipmitool` command on a Microsoft Windows system, you need to add the `.exe` extension to the `ipmitool` command. For example, **`ipmitool.exe -I ms lan set 1 ipsrc static`**

Initial ILOM Setup Procedures Using the Web Interface

Topics

Step	Description	Links
1	Log in to ILOM to the first time using the web interface	• "Log In to ILOM 3.0 Using `root` User Account" on page 11
2	Add a local user account, or configure a directory service	• "Add User Account and Assign Privileges" on page 12 • "Configure ILOM for Active Directory" on page 14 • "Configure LDAP Server" on page 20 • "Configure ILOM for LDAP" on page 21 • "Edit LDAP/SSL Tables" on page 26 • "Configure ILOM for RADIUS" on page 27
3	Confirm your authentication configuration	• "Log In to ILOM as a User" on page 28
4	Log out of ILOM	• "Log Out of ILOM" on page 29

▼ Log In to ILOM 3.0 Using `root` User Account

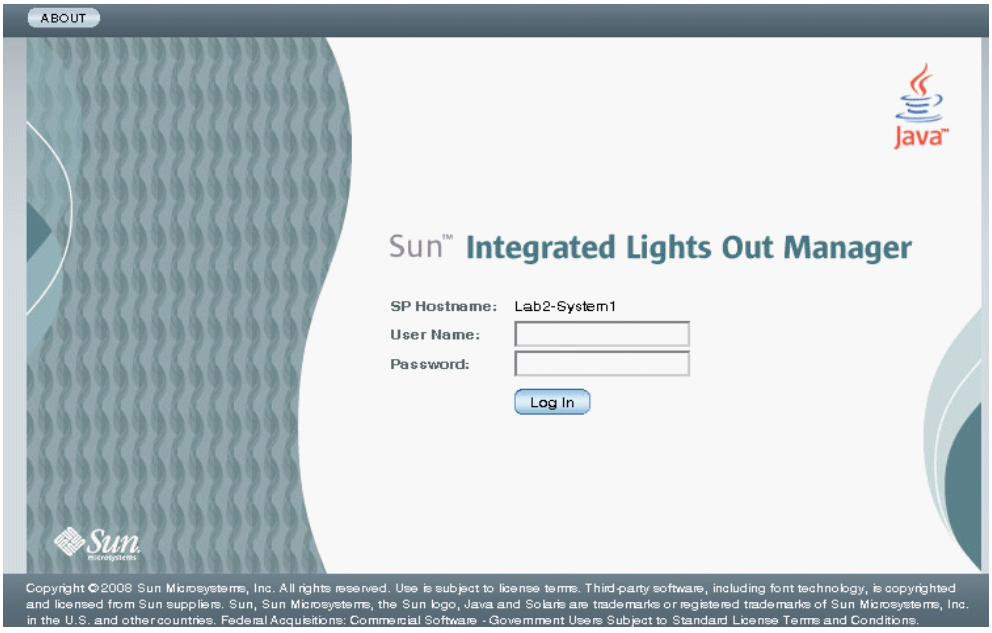
Before You Begin

- Open a web browser.

Follow these steps to log in to the ILOM web interface for the first time using the `root` user account:

1. **Type `http://`*system_ipaddress* into the web browser.**

   The web interface Login page appears.



2. **Type the user name and password for the `root` user account:**

   User Name: **`root`**

   Password: **`changeme`**

3. **Click Log In.**

   The Version page in the web interface appears.

▼ Add User Account and Assign Privileges

Before You Begin

- Log in to the ILOM web interface using the `root` user account.
- Choose either to create a local user account or to configure a directory service.

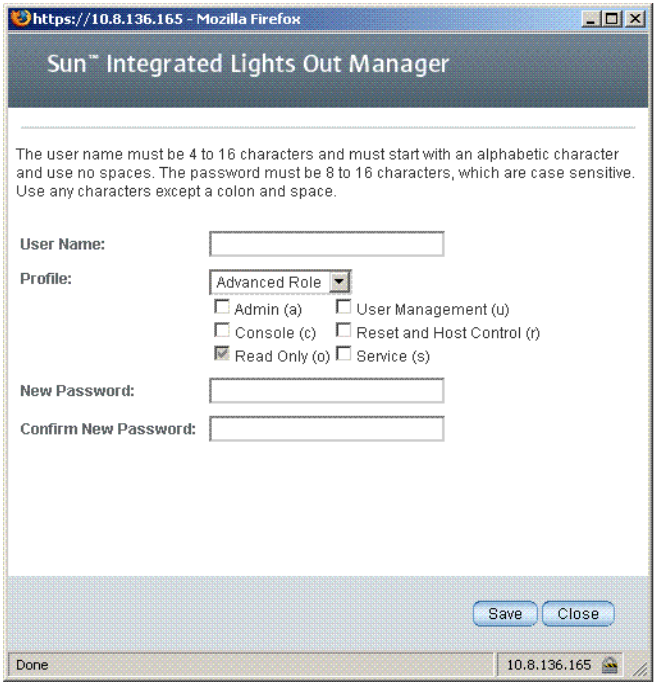
Follow these steps to add a local user account and assign privileges (roles):

1. **Select User Management --> User Accounts.**

   The User Account Settings page appears.

2. **In the Users table, click Add.**

   The Add User dialog appears.



3. **Complete the following information:**

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

   b. **Choose a profile. Options include `Advanced Role` for all new ILOM 3.0 installations.**

c. Select the appropriate roles.

See the following table for descriptions of advanced roles for user accounts.

Roles	Definition	Privileges
a	Admin	A user who is assigned the Admin (a) role is authorized to view and change the state of ILOM configuration variables. With the exception of tasks that users who have User Management, Console, and Reset and Host Control roles, users assigned the Admin role are authorized to perform all other ILOM functions.
u	User Management	A user who is assigned the User Management (u) role is authorized to create and delete user accounts, change user passwords, change roles assigned to other users, and enable/disable the physical-access requirement for the default user account. This role also includes authorization to set up LDAP, LDAP/SSL, RADIUS, and Active Directory.
c	Console	A user who is assigned the Console (c) role is authorized to access the ILOM Remote Console and the SP console and to view and change the state of the ILOM console configuration variables.
r	Reset and Host Control	A user who is assigned the Reset and Host Control (r) role is authorized to operate the system, which includes power control, reset, hot-plug, enabling and disabling components, and fault management. This role maps very closely to the ILOM 2.0 user with Operator privileges.
o	Read Only	A user who is assigned the Read Only (o) role is authorized to view the state of the ILOM configuration variables but cannot make any changes. Users assigned this role can also change the password and the Session Time-Out setting for their own user account.
s	Service	A user who is assigned the Service (s) role can assist Sun service engineers in the event that on-site service is required.

d. Type a password in the New 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.

e. Retype the password in the Confirm New Password field to confirm the password.

f. When you are done entering the new user's information, click Save.

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

▼ Configure ILOM for Active Directory

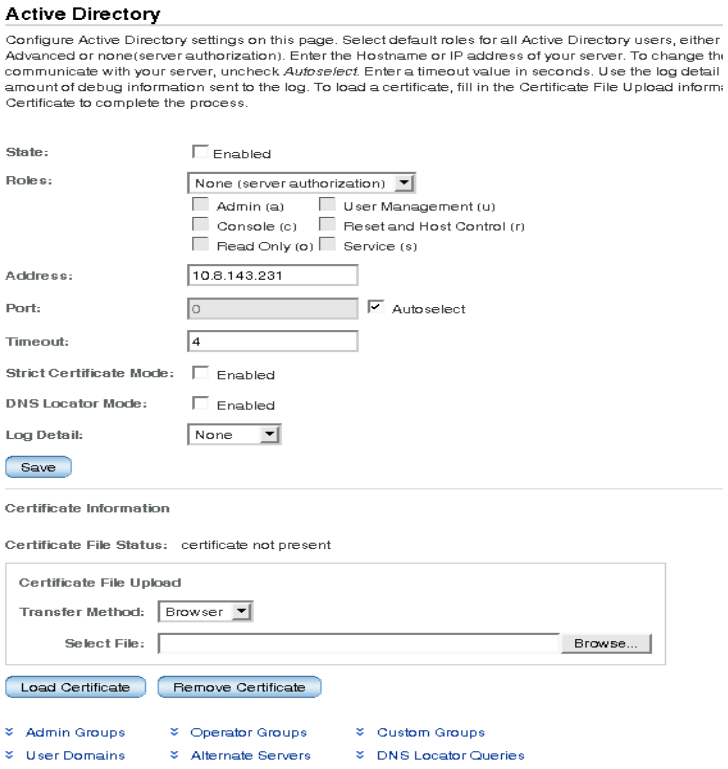
Before You Begin

- Log in to the ILOM web interface using the `root` user account.
- Choose either to create a local user account or to configure a directory service.

Follow these steps to configure ILOM for Active Directory:

1. **Select User Management --> Active Directory.**

   The Active Directory page appears.



2. **Configure the Active Directory settings.**

   See the following table for a description of the Active Directory settings.

Property (Web)	Property (CLI)	Default	Description
State	`state`	Disabled	Enabled | Disabled Specifies whether the Active Directory client is enabled or disabled.
Roles	`defaultRole (a|u|c|r|o|s)`	(none)	Administrator | Operator | Advanced roles | none Access role granted to all authenticated Active Directory users. This property supports the legacy roles of Administrator or Operator, or any of the individual role ID combinations of 'a', 'u', 'c', 'r', 'o' and 's'. For example, `aucros`, where `a`=Admin, `u`=User Management, `c`=Console, `r`=Reset and Host Control, `o`=Read Only, and `s`=Service. If you do not configure a role, the Active Directory server is used to determine the role.
Address	`address`	0.0.0.0	IP address or DNS name of the Active Directory server. If the DNS name is used, DNS must be configured and functional.
Port	`port`	0	Port used to communicate with the server or enable `autoselect` (which assigns the port to 0). Available in the unlikely event of a non-standard TCP port being used.
Timeout	`timeout`	4	Timeout value in seconds. Number of seconds to wait for individual transactions to complete. The value does not represent the total time of all transactions because the number of transactions can differ depending on the configuration. This property allows for tuning the time to wait when a server is not responding or is unreachable.
Strict Certificate Mode	`strictcertmode`	Disabled	Enabled | Disabled If enabled, the server certificate contents are verified by digital signatures at the time of authentication. Certificate must be loaded before Strict Certificate Mode can be set to enabled.
DNS Locator Mode	`dnslocatormode`	Disabled	Enabled | Disabled If enabled, an attempt to locate the Active Directory server is performed, based on the DNS locator queries that are configured.
Log Detail	`logdetail`	None	None | High | Medium | Low Specifies the amount of diagnostics that go into the event log.

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

4. **View the Active Directory certificate information.**

   See the following table for a description of Active Directory certificate settings:

Property (Web)	Property (CLI)	Displays	Description
Certificate File Status	`certstatus`	`certificate not present`	Read-only indicator of whether a certificate exists.
Certificate File Status	`certstatus`	`certificate present (details)`	Click on "details" for information about issuer, subject, serial number, valid_from, valid_to, and version.

5. **Complete the "Certificate File Upload" section by selecting a transfer method for uploading the certificate file and the requested parameters.**

Note – This section is required only if Strict Certificate Mode is used.

The following table describes the required parameters for each transfer method:

Transfer Method	Required Parameters
Browser	File Name
TFTP	Host Filepath
FTP	Host Filepath Username Password
SCP	Host Filepath Username Password

6. **Click the Load Certificate button or Remove Certificate button.**

7. **If a certificate is loaded, the following read-only details appear if you selected "certificate present (details)":**

`issuer`	Certificate Authority who issued the certificate.
`subject`	Server or domain for which the certificate is intended.
`valid_from`	Date when the certificate becomes valid.
`valid_until`	Date when the certificate becomes invalid.
`serial_number`	Serial number of the certificate.
`version`	Version number of the certificate.

8. **At the bottom of the Active Directory page, click the radio button next to the configuration option you want to configure:**
   - Admin Groups
   - Operator Groups
   - Custom Groups
   - User Domains
   - Alternate Servers
   - DNS Locator Queries
9. **Enter the required data in the tables.**

   The Admin Groups, Operator Groups, and Custom Groups tables contain the names of the Microsoft Active Directory groups in the Distinguished Name (DN) format, Simple Name format, or NT-Style Name. Custom Groups require the configuration of user roles to have Advanced Roles or Administrator/Operator privileges to perform various tasks.

   User Domains are the authentication domains used to authenticate a user. When the user logs in, the name used is formatted in the specific domain name format template that appears in the cell. `<USERNAME>` will be replaced by the user's login name during authentication. Either the principle or Distinguished Name format is supported. User authentication is attempted based on the user name that is entered and the configured user domains.

The Alternate Servers table provides redundancy for authentication. If a certificate is not supplied, a top-level primary certificate is used. The alternate servers have the same rules and requirements as the top-level certificate mode. Each server has its own certificate status, and its own certificate command to retrieve the certificate if it is needed.

The DNS Locator Queries table is used to query DNS servers to learn about the hosts to use for authentication. The DNS Locator queries are only used when DNS Locator is enabled and DNS is configured and functioning.

In the following tables, default data shows the expected format of the Active Directory data.

- **Admin Groups Table:**

  The name listed in entry 1 uses the Distinguished Name format.

ID	Name
1	`CN=SpSuperAdmin,OU=Groups,DC=sales,DC=east,DC=sun,DC=com`
2	

- **Operator Groups Table:**

  The name listed in entry 1 uses the Distinguished Name format.

ID	Name
1	`CN=SpSuperOper,OU=Groups,DC=sales,DC=east,DC=sun,DC=com`
2	

- **Custom Groups Table**:

  The name listed in entry 1 uses the Simple Name format.

ID	Name	Roles
1	`custom_group_1`	`Admin, User Management, Console, Reset and Host Control, Read Only (aucro)`

- **User Domains Table:**

  The domain listed in entry 1 shows the principle format that is used in the first attempt to authenticate the user. Entry 2 shows the complete Distinguished Name, which Active Directory would use if the attempt to authenticate with the first entry failed.

Note – In the example below, <USERNAME> represents a user's login name. During authentication, the user's login name replaces <USERNAME>.

ID	Domain
1	<USERNAME>@sales.east.sun.com
2	CN=<USERNAME>,OU=Users,DC=sales,DC=east,DC=sun,DC=com

- **Alternate Servers Table:**

ID	Address	Port	Certificate Status
1	10.8.168.99	0	Certificate not present
2	10.8.143.230	0	Certificate not present

- **DNS Locator Queries Table:**

  The DNS Locator service query identifies the named DNS service. The port ID is generally part of the record, but it can be overridden by using the format <PORT:636>. Also, named services specific for the domain being authenticated can be specified by using the <DOMAIN> substitution marker.

Name	Domain
1	_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269>
2	_ldap._tcp.dc._msdcs.<DOMAIN>.<PORT:636>

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

▼ Configure LDAP Server

Follow these steps to configure the LDAP server. Refer to your LDAP documentation for detailed instructions.

1. **Ensure that all users authenticating to 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.
   ```

   ILOM only supports LDAP authentication 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).**

Required Property	Description
uid	User name for logging in to ILOM
uidNumber	Any unique number
gidNumber	Any unique number
userPassword	Password
homeDirectory	Any value (this property is ignored by ILOM)
loginShell	Any value (this property is ignored by ILOM)

3. **Configure the LDAP server to enable LDAP server access to ILOM user accounts.**

   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 ILOM.

   See "Configure ILOM for LDAP" on page 21.

▼ Configure ILOM for LDAP

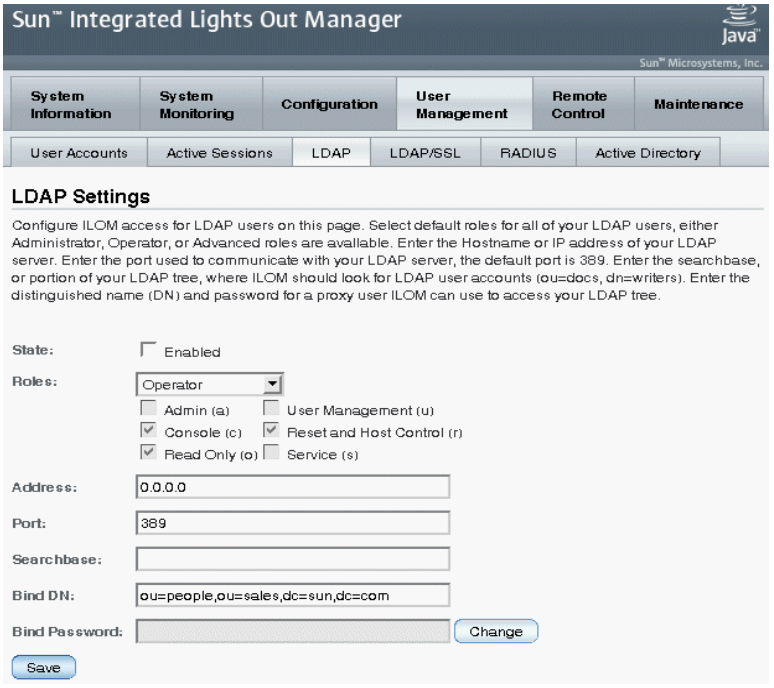
Before You Begin

- Log in to the ILOM web interface using the `root` user account.
- Choose either to create a local user account or to configure a directory service.

Follow these steps to configure ILOM for LDAP:

1. **Select User Management --> LDAP.**

   The LDAP Settings page appears.



2. **Enter the following values:**
   - **State** – Select the Enabled check box to authenticate LDAP users.
   - **Role** – Select either Administrator or Operator, or any of the individual ID role combinations of a, u, c, r, o, and s.
   - **Address** – The address of the LDAP server or DNS name. If the DNS name is used, DNS must be configured and functional.
   - **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.

3. **Click Save for your changes to take effect.**
4. **To verify that LDAP authentication works, log in to the ILOM using an LDAP user name and password.**

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

▼ Configure ILOM for LDAP/SSL

Before You Begin

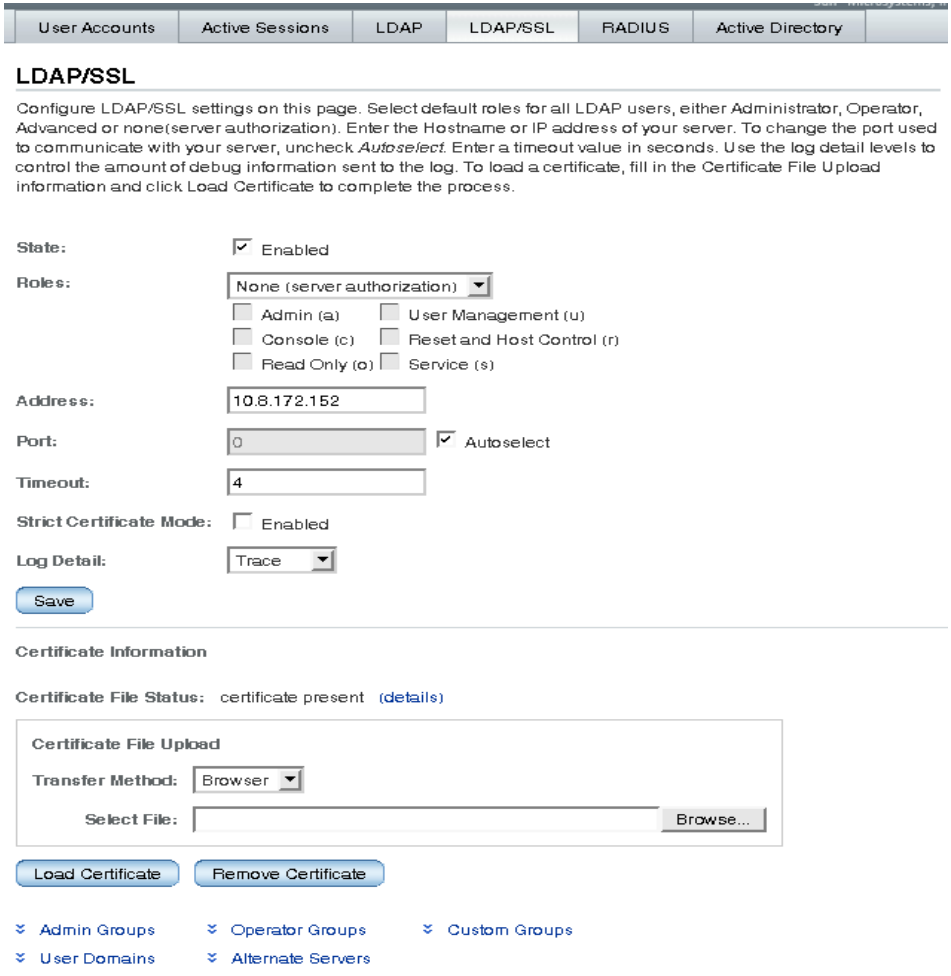
- Log in to the ILOM web interface using the `root` user account.
- Choose either to create a local user account or to configure a directory service.

LDAP/SSL offers enhanced security to LDAP users by way of Secure Socket Layer (SSL) technology. Certificates are optional if Strict Certificate Mode is used.

Follow these steps to configure ILOM for LDAP/SSL:

1. **Select User Management --> LDAP/SSL.**

   The LDAP/SSL page appears, displaying the configuration settings and the LDAP/SSL tables.



2. **Configure the LDAP/SSL settings.**

See the following table for a description of the LDAP/SSL settings.

Property (Web)	Property (CLI)	Default	Description
State	`state`	Disabled	Enabled | Disabled Specifies whether the LDAP/SSL client is enabled or disabled.
Roles	`defaultRole (a|u|c|r|o|s)`	(none)	Administrator | Operator | Advanced roles | none Access role granted to all authenticated LDAP/SSL users. This property supports the legacy roles of Administrator or Operator, or any of the individual role ID combinations of 'a', 'u', 'c', 'r', 'o' and 's'. For example, `aucros`, where `a`=Admin, `u`=User Management, `c`=Console, `r`=Reset and Host Control, `o`=Read Only, and `s`=Service. If you do not configure a role, the LDAP/SSL server is used to determine the role.
Address	`address`	0.0.0.0	IP address or DNS name of the LDAP/SSL server. If the DNS name is used, DNS must be configured and functional.
Port	`port`	0	Port used to communicate with the server or enable `autoselect` (which assigns the port to 0). Available in the unlikely event of a non-standard TCP port being used.
Timeout	`timeout`	4	Timeout value in seconds. Number of seconds to wait for individual transactions to complete. The value does not represent the total time of all transactions because the number of transactions can differ depending on the configuration. This property allows for tuning the time to wait when a server is not responding or is unreachable.
Strict Certificate Mode	`strictcertmode`	Disabled	Enabled | Disabled If enabled, the server certificate contents are verified by digital signatures at the time of authentication. Certificate must be loaded before Strict Certificate Mode can be set to enabled.
Log Detail	`logdetail`	None	None | High | Medium | Low Specifies the amount of diagnostics that go into the event log.

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

4. **View the LDAP/SSL certificate information in the middle section of the LDAP/SSL page.**

   See the following table for a description of LDAP/SSL certificate settings.

Property (Web)	Property (CLI)	Displays	Description
Certificate File Status	`certstatus`	`certificate not present`	Read-only indicator of whether a certificate exists.
Certificate File Status	`certstatus`	`certificate present (details)`	Click on "details" for information about issuer, subject, serial number, valid_from, valid_to, and version.

5. **Complete the "Certificate File Upload" section by selecting a transfer method for uploading the certificate file and the required parameters.**

Note – This section is required only if Strict Certificate Mode is used.

The following table describes the required parameters for each transfer method.

Transfer Method	Required Parameters
Browser	File Name
TFTP	Host Filepath
FTP	Host Filepath Username Password
SCP	Host Filepath Username Password

6. **Click the Load Certificate button or Remove Certificate button.**

7. **If a certificate is loaded, the following read-only details will appear if you selected "certificate present (details)":**

`issuer`	Certificate Authority who issued the certificate.
`subject`	Server or domain for which the certificate is intended.
`valid_from`	Date when the certificate becomes valid.
`valid_until`	Date when the certificate becomes invalid.
`serial_number`	Serial number of the certificate.
`version`	Version number of the certificate.

▼ Edit LDAP/SSL Tables

Before You Begin

- Log in to the ILOM web interface using the `root` user account.
- Choose either to create a local user account or to configure a directory service.

Follow these steps to modify information for Admin Groups, Operator Groups, Custom Groups, User Domains, or Alternate Servers:

1. **Select User Management --> LDAP/SSL.**

   The LDAP/SSL page appears.

2. **At the bottom of the LDAP/SSL page, select the links next to the type of information you want to edit:**
   - Admin Groups
   - Operator Groups
   - Custom Groups
   - User Domains
   - Alernate Servers

3. **Select the radio button next to the individual table you want to edit, then click Edit.**

   The appropriate page appears: Edit LDAP/SSL **Admin Groups** page, Edit LDAP/SSL **Operator Groups** page, Edit LDAP/SSL **Custom Groups** page, Edit LDAP/SSL **User Domains** page, or Edit LDAP/SSL **Alternate Servers** page.

4. **In each Edit page, edit the information you want to modify.**

   Refer to the procedure "Configure ILOM for Active Directory" on page 14 for examples of the information you can add or edit in the LDAP/SSL tables. Information in the Active Directory tables is similar to LDAP/SSL tables.

   For example, in the User Domains table, enter the information in the Name field as text. Use the `<USERNAME>` substitution marker to hold a place for the user's name.

   ```
   domain=uid=<USERNAME>,OU=people,DC=sales,DC=east,DC=sun,DC=com
   ```

   You would be authenticated to ILOM with the supplied name.

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

▼ Configure ILOM for RADIUS

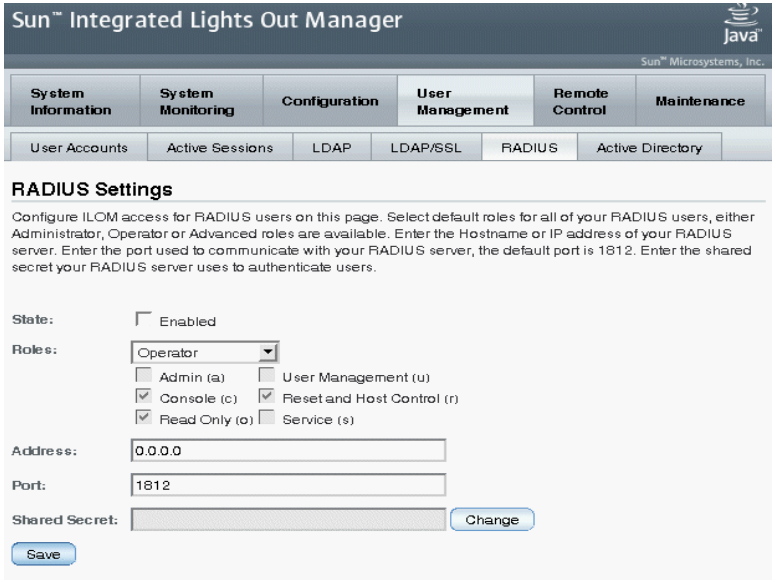
Before You Begin

- Log in to the ILOM web interface using the `root` user account.
- Choose either to create a local user account or to configure a directory service.

Follow these steps to configure ILOM for RADIUS:

1. **Select User Management --> RADIUS.**

   The RADIUS Settings page appears.



2. **Complete the RADIUS settings.**

Property (Web)	Property (CLI)	Default	Description
State	`state`	Disabled	Enabled | Disabled Specifies whether the RADIUS client is enabled or disabled.
Role	`defaultrole` `a|u|c|r|o|s`	Read Only (`o`)	Administrator | Operator | Advanced Roles Access role granted to all authenticated RADIUS users. This property supports the legacy roles of Administrator or Operator, or any of the individual role ID combinations of 'a', 'u', 'c', 'r', 'o' and 's'. For example, `aucros`, where `a`=Admin, `u`=User Management, `c`=Console, `r`=Reset and Host Control, `o`=Read Only, and `s`=Service.
Address	`ipaddress`	0.0.0.0	IP address or DNS name of the RADIUS server. If the DNS name is used, DNS must be configured and functional.
Port	`port`	1812	Specifies the port number used to communicate with the RADIUS server. The default port is 1812.
Shared Secret	`secret`	(none)	Specifies the shared secret that is used to protect sensitive data and to ensure that the client and server recognize each other.

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

▼ Log In to ILOM as a User

Before You Begin

- Open a web browser.

Follow these steps to log in to ILOM as a non-`root` account user:

1. **Type `http://`*system_ipaddress* into the web browser.**
   The web interface Login page appears.
2. **Type the user name and password of a user account that you previously configured.**
3. **Click Log In.**
   The ILOM web interface appears, displaying the Version page.

▼ Log Out of ILOM

- **Click the Log Out button in the ILOM web interface.**

  The Log Out button is located in the top right corner of the ILOM web interface. Do not use the Log Out button on your web browser to exit ILOM.

You are now ready to configure ILOM as a regular ILOM user. To learn about ILOM's features and the procedures you can perform to access ILOM's functions, refer to the other documents in the ILOM 3.0 Documentation Collection. See TABLE P-1. You can access the ILOM 3.0 Documentation Collection at:

`http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic`

Initial ILOM Setup Procedures Using the CLI

Topics

Step	Description	Links
1	Log in to ILOM to the first time using the CLI	• "Log In to ILOM 3.0 Using `root` User Account" on page 30
2	Add a local user account, or configure a directory service	• "Add User Account and Assign Privileges" on page 31 • "Configure ILOM for Active Directory" on page 31 • "Configure LDAP Server" on page 35 • "Configure ILOM for LDAP" on page 35 • "Configure ILOM for LDAP/SSL" on page 36 • "Configure ILOM for RADIUS" on page 41
3	Confirm your authentication configuration	• "Log In to ILOM as a User" on page 42
4	Log out of ILOM	• "Log Out of ILOM" on page 42

▼ Log In to ILOM 3.0 Using `root` User Account

To log in to the ILOM CLI for the first time, use SSH and the `root` user account.

- **To log in to the ILOM CLI using the `root` user account, type:**

```
$ ssh root@system_ipaddress
Password: changeme
```

The ILOM CLI prompt appears (->).

▼ Add User Account and Assign Privileges

Before You Begin

- Log in to the ILOM CLI using the `root` user account.
- Choose either to create a local user account or to configure a directory service.

Follow these steps to add a local user account and assign user privileges (roles):

1. **Type the following command and your password to add a local user account:**

   –> **create /SP/users/***username* **password=***password*

   For example:

   ```
   -> create /SP/users/user5
   Creating user...
   Enter new password: ********
   Enter new password again: ********
   Created /SP/users/user5
   ```

2. **Type the following command to assign roles to a user account:**

   –> **set /SP/users/***username* **role=aucr**

   For example:

   ```
   -> set /SP/users/user5 role=aucr
   Set 'role' to 'aucr'
   ```

   For a description of the user account roles, see "Add User Account and Assign Privileges" on page 12.

▼ Configure ILOM for Active Directory

Before You Begin

- Log in to the ILOM CLI using the `root` user account.
- Choose either to create a local user account or to configure a directory service.

You can configure Active Directory to authenticate user credentials and authorize user access levels to the service processor.

Follow thse steps to configure ILOM for Active Directory:

1. **Use the** `show` **command to view the top-level properties. Type:**

```
-> cd /SP/clients/activedirectory
/SP/clients/activedirectory

-> show

 /SP/clients/activedirectory
    Targets:
        admingroups
        alternateservers
        cert
        customgroups
        dnslocatorqueries
        opergroups
        userdomains

    Properties:
        address = 10.5.121.321
        defaultrole = Administrator
        dnslocatormode = enabled
        logdetail = trace
        port = 0
        state = disabled
        strictcertmode = disabled
        timeout = 4

    Commands:
        cd
        set
        show
```

2. **Use the** `show` **command to view information in the tables. Type:**

   -> **show /SP/clients/activedirectory/***name***/***n*

   Where *n* is **1** through **5**, and where *name* is one of the following:

   - **admingroups** (for Admin Groups properties)
   - **opergroups** (for Operator Groups properties)
   - **customgroups** (for Custom Groups properties)
   - **userdomains** (for User Domains properties)
   - **alternateservers** (for Alternate Servers properties)
   - **dnslocatorqueries** (for DNS Locator Queries properties)
   - **cert** (for certificate properties - `cert` is not a table; therefore the value of 1 through 5 for *n* does not apply)

You can use the `show` command to retrieve the certificate properties:

```
-> show /SP/clients/activedirectory/cert
 /SP/clients/activedirectory/cert
    Targets:

    Properties:
        certstatus = certificate not present
        clear_action = (none)
        issuer = (none)
        load_uri = (none)
        serial_number = (none)
        subject = (none)
        valid_from = (none)
        valid_until = (none)
        version = (none)
```

You can also use the `show` command to retrieve the alternate server certificate properties:

```
-> show /SP/clients/activedirectory/alternateservers/1/cert
 /SP/clients/activedirectory/alternateservers/1/cert
    Targets:

    Properties:
        certstatus = certificate not present
        clear_action = (none)
        issuer = (none)
        load_uri = (none)
        serial_number = (none)
        subject = (none)
        valid_from = (none)
        valid_until = (none)
        version = (none)
```

3. **Use the `set` command to configure top-level properties.**

   For example:

```
-> set address=10.5.121.321
Set 'address' to 10.5.121.321
->set ...etc. for defaultrole, dnslocator, logdetail, port, state,
stricmode, timeout
```

4. **Use the `set` command to load a certificate or to modify properties.**

   For example:

- **To load an Active Directory certificate:**

```
-> set /SP/clients/activedirectory/cert load_uri=
tftp://10.6.143.192/sales/cert.cert
Set 'load_uri' to 'tftp://10.6.143.192/sales/cert.cert'
```

- **To load an alternate server certificate:**

```
-> set /SP/clients/activedirectory/alternateservers/1/cert
load_uri=tftp://10.6.143.192/sales/cert.cert
Set 'load_uri' to 'tftp://10.6.143.192/sales/cert.cert'
```

- **To modify Admin Groups table properties:**

```
-> set /SP/clients/activedirectory/admingroups/1 name=CN=
spSuperAdmin,OU=Groups,DC=sales,DC=sun,DC=com
Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=sun,DC=com'
```

- **To modify Operator Groups table properties:**

```
-> set /SP/clients/activedirectory/opergroups/1 name=CN=
spSuperOper,OU=Groups,DC=sales,DC=sun,DC=com
Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=sun,DC=com'
```

- **To modify Custom Groups table properties**:

Note – You can set the role to any one or a combination of Admin (a), User Management (u), Console (c), Reset and Host Control (r), or Read Only (o). The legacy roles Administrator or Operator are also supported.

```
-> set /SP/clients/activedirectory/customgroups/1 name=CN=
spSuperCust,OU=Groups,DC=sales,DC=sun,DC=com
Set 'name' to 'CN=spSuperCust,OU=Groups,DC=sales,DC=sun,DC=com'
-> set /SP/clients/activedirectory/customgroups/1 roles=au
Set 'roles' to au
```

- **To modify User Domains table properties:**

```
-> set /SP/clients/activedirectory/userdomains/1 domain=
username@sales.sun.com
Set 'domain' to 'username@sales.sun.com'
```

- **To modify Alternate Servers table properties:**

```
-> set /SP/clients/activedirectory/alternateservers/1 address=
ip_address
```

- **To modify DNS Locator Queries table properties:**

```
-> set /SP/clients/activedirectory/dnslocatorqueries/1 service=
_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269>
```

Note – The DNS Locator service query identifies the named DNS service. The port ID is generally part of the record, but it can be overridden by using the format <PORT:636>. Also, named services specific for the domain being authenticated can be specified by using the <DOMAIN> substitution marker.

▼ Configure LDAP Server

To use LDAP, you first need to configure the LDAP server. See "Configure LDAP Server" on page 20 in the web interface section.

▼ Configure ILOM for LDAP

Before You Begin

- Log in to the ILOM CLI using the root user account.
- Choose either to create a local user account or to configure a directory service.

Follow these steps to configure ILOM for LDAP:

1. **Use the** set **command to enter the proxy user name and password.**

   For example:

   –> set /SP/clients/ldap binddn="cn=proxyuser, ou=people, ou=sales, dc=sun, dc=com" bindpw=*password*

2. **Enter the IP address or DNS name of the LDAP server. Type:**

   –> **set /SP/clients/ldap address=***ldap_ipaddress* | *DNS_name*

3. **(Optional) Assign the port used to communicate with the LDAP server; the default port is 389. Type:**

   –> **set /SP/clients/ldap port=***ldap_port*

4. **Enter the Distinguished Name of the branch of your LDAP tree that contains users and groups. 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.

5. **Set the state of the LDAP service to enabled. Type:**

   –> **set /SP/clients/ldap state=enabled**

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

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

▼ Configure ILOM for LDAP/SSL

Before You Begin

- Log in to the ILOM CLI using the `root` user account.
- Choose either to create a local user account or to configure a directory service.

LDAP/SSL offers enhanced security to LDAP users by way of Secure Socket Layer (SSL) technology. Certificates are optional if Strict Certificate Mode is used.

Follow these steps to configure ILOM for LDAP/SSL:

1. Use the `show` **command to view top-level properties. Type:**

```
-> cd /SP/clients/ldapssl
/SP/clients/ldapssl

-> show

 /SP/clients/ldapssl
    Targets:
        admingroups
        alternateservers
        cert
        customgroups
        opergroups
        userdomains

    Properties:
        address = 10.5.121.321
        defaultrole = Administrator
        logdetail = trace
        port = 0
        state = disabled
        strictcertmode = disabled
        timeout = 4

    Commands:
        cd
        set
        show
```

2. **Use the** `show` **command to view information in the tables. Type:**

   -> **show /SP/clients/ldapssl/***name***/***n*

   Where *n* is **1** through **5**, and where *name* is one of the following:

   - **admingroups** (for Admin Groups properties)
   - **opergroups** (for Operator Groups properties)
   - **customgroups** (for Custom Groups properties)
   - **userdomains** (for User Domains properties)
   - **alternateservers** (for Alternate Servers properties)
   - **cert** (for certificate properties - `cert` is not a table; therefore the value of 1 through 5 for *n* does not apply)

   You can use the `show` command to retrieve the certificate properties:

```
-> show /SP/clients/ldapssl/cert
 /SP/clients/ldapssl/cert
    Targets:

    Properties:
        certstatus = certificate not present
        clear_action = (none)
        issuer = (none)
        load_uri = (none)
        serial_number = (none)
        subject = (none)
        valid_from = (none)
        valid_until = (none)
        version = (none)
```

   You can also use the `show` command to retrieve the alternate server certificate properties:

```
-> show /SP/clients/ldapssl/alternateservers/1/cert
 /SP/clients/ldapssl/alternateservers/1/cert
    Targets:

    Properties:
        certstatus = certificate not present
        clear_action = (none)
        issuer = (none)
        load_uri = (none)
        serial_number = (none)
        subject = (none)
        valid_from = (none)
        valid_until = (none)
        version = (none)
```

3. **Use the** `set` **command to configure top-level properties.**

   For example:

```
-> set address=10.5.121.321
Set 'address' to 10.5.121.321
->set ...etc. for defaultrole, logdetail, port, state, stricmode,
timeout
```

4. **Use the** `set` **command to load a certificate or to modify properties.**

   For example:

   - **To load an LDAP/SSL certificate:**

```
-> set /SP/clients/ldapssl/cert load_uri=
tftp://10.6.142.192/sales/cert.cert
Set 'load_uri' to 'tftp://10.6.142.192/sales/cert.cert'
```

   - **To load an alternate server certificate:**

```
-> set /SP/clients/ldapssl/alternateservers/1/cert load_uri=
tftp://10.6.142.192/sales/cert.cert
Set 'load_uri' to 'tftp://10.6.142.192/sales/cert.cert'
```

   - **To modify Admin Groups properties:**

```
-> set /SP/clients/ldapssl/admingroups/1 name=CN=
spSuperAdmin,OU=Groups,DC=sales,DC=sun,DC=com
Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=sun,DC=com'
```

   - **To modify Operator Groups properties:**

```
-> set /SP/clients/ldapssl/opergroups/1 name=CN=spSuperOper,OU=
Groups,DC=sales,DC=sun,DC=com
Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=sun,DC=com'
```

   - **To modify Custom Groups table properties**:

Note – You can set the role to any one or a combination of Admin (`a`), User Management (`u`), Console (`c`), Reset and Host Control (`r`), or Read Only (`o`). The legacy roles Administrator or Operator are also supported.

```
-> set /SP/clients/ldapssl/customgroups/1 name=CN=
spSuperCust,OU=Groups,DC=sales,DC=sun,DC=com
Set 'name' to 'CN=spSuperCust,OU=Groups,DC=sales,DC=sun,DC=com'
-> set /SP/clients/ldapssl/customgroups/1 roles=au
Set ‘roles’ to au
```

- **To modify User Domains properties:**

Note – In the example below, <USERNAME> represents a user’s login name. During authentication, the user’s login name replaces <USERNAME>.

```
-> set /SP/clients/ldapssl/userdomains/1 name=<USERNAME>@uid=
<USERNAME>,OU=people,DC=sun,DC=com
Set 'domain' to 'uid=<USERNAME>,OU=people,DC=sun,DC=com’
```

- **To modify Alternate Servers properties:**

```
-> set /SP/clients/ldapssl/alternateservers/1 address=ip_address
```

▼ Configure ILOM for RADIUS

Before You Begin

- Log in to the ILOM CLI using the `root` user account.
- Choose either to create a local user account or to configure a directory service.

Follow these steps to configure ILOM for RADIUS:

1. **To display the properties of RADIUS, type:**

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

   For example:

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

   Properties:
     address = 0.0.0.0
     defaultrole = Operator
     port = 1812
     secret = (none)
     state = disabled
```

2. **Use the `set` command to modify properties.**

   For example:

   -> **`set /SP/clients/radius ipaddress=1.2.3.4 port=1812 state=enabled defaultrole=administrator secret=changeme`**

   For a description of the RADIUS settings, see "Configure ILOM for RADIUS" on page 27.

▼ Log In to ILOM as a User

1. **Using a Secure Shell (SSH) session, log in to ILOM by specifying your user name and the IP address of the server SP or CMM.**

   For example:

   $ **ssh** *username@ip_address*

   Or

   $ **ssh -l** *username ip_address*

   The ILOM login password prompt appears.

2. **Type the user name and password for the user account that you previously configured to access ILOM.**

   <hostname>: *username*

   Password: *password*

   The ILOM CLI prompt appears (->).

▼ Log Out of ILOM

- **At the command prompt, type:**

  -> **exit**

You are now ready to configure ILOM as a regular ILOM user. To learn about ILOM's features and the procedures you can perform to access ILOM's functions, refer to the other documents in the ILOM 3.0 Documentation Collection. See TABLE P-1. You can access the ILOM 3.0 Documentation Collection at:

http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic

Identify ILOM Version Information

You can easily identify the ILOM firmware version that is running on the server SP. To identify the ILOM firmware version, you need the Read Only (o) role enabled.

▼ Identify ILOM Version Using Web Interface

1. **Log in to the ILOM web interface.**
2. **Select System Information --> Version.**

   The current firmware version information appears.

▼ Identify ILOM Version Using CLI

1. **Log in to the ILOM CLI.**
2. **At the command prompt, type** `version`**.**

   The current firmware version information appears. For example:

```
SP firmware 3.0.0.1
SP firmware build number: 38000
SP firmware date: Fri Nov 28 14:03:21 EDT 2008
SP filesystem version: 0.1.22
```

Update ILOM Firmware to Latest Version

Before You Begin

Prior to performing the procedures in this section, the following requirements must be met:

- Identify the version of ILOM that is currently running on your system.
- Download the firmware image for your server or CMM from the Sun platform's product web site. Refer to "Updating the Firmware" in either the *Sun Integrated Lights Out Manager (ILOM) 3.0 Web Procedures Guide* or the *Sun Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide.*
- Copy the firmware image to a server using a supported protocol (TFTP, FTP, HTTP, HTTPS). For a CLI update, copy the image to a local server. For a web interface update, copy the image to the system on which the web browser is running.
- If required by your platform, shut down your host operating system before updating the firmware on your server SP.
- Obtain an ILOM user name and password that has Admin (`a`) role account privileges. You must have Admin (`a`) privileges to update the firmware on the system.
- The firmware update process takes about six minutes to complete. During this time, do not perform other ILOM tasks. When the firmware update is complete, the system will reboot.

▼ Update ILOM Firmware Using Web Interface

1. **Log in to the ILOM web interface as any user with Admin (a) role account privileges.**
2. **Select Maintenance --> Firmware Upgrade.**

   The Firmware Upgrade page appears.
3. **In the Firmware Upgrade page, click Enter Upgrade Mode.**

   An Upgrade Verification dialog appears, indicating that other users who are logged in will lose their session when the update processes completes.
4. **In the Upgrade Verification dialog, click OK to continue.**

   The Firmware Upgrade page appears.
5. **In the Firmware Upgrade page, do the following:**

   a. **Specify the image location by performing one of the following:**

      - Click **Browse** to select the location of the firmware image you want to install.
      - If supported on your system, click **Specify URL** to specify a URL that will locate the firmware image. Then type the URL into the text box.

   b. **Click the Upload button to upload and validate the file.**

      Wait for the file to upload and validate.

      The Firmware Verification page appears.
6. **In the Firmware Verification page, enable any one of the following options:**

   - **Preserve Configuration.** Enable this option if you want to save your existing configuration in ILOM and restore that existing configuration after the update process completes.
   - **Delay BIOS upgrade until next server power-off.** Enable this option if you want to postpone the BIOS upgrade until the next time the system reboots.

Note – The "Delay BIOS upgrade" option appears only for firmware updates to ILOM 3.0 or later on x64 systems.

---

7. **Click Start Upgrade to start the upgrade process or click Exit to cancel the process.**

   When you click Start Upgrade the upload process will start and a prompt to continue the process appears.

8. **At the prompt, click OK to continue.**

   The Update Status page appears providing detail about the update progress. When the update status indicates 100%, the firmware update is complete.

   When the update completes, the system *automatically* reboots.

Note – The ILOM web interface might not refresh properly after the update completes. If the ILOM web page is missing information, or displays an error message, you might be viewing a cached version of the page from the version previous to the update. Clear your browser cache and refresh your browser before continuing.

---

9. **Reconnect to the ILOM web interface. Select System Information --> Version. Verify that the firmware version on the SP or CMM corresponds to the firmware image you installed.**

Note – If you did not preserve the ILOM configuration before the firmware update, you will need to perform the initial ILOM setup procedures to reconnect to ILOM.

▼ Update ILOM Firmware Using CLI

1. **Log in to the ILOM CLI as any user with Admin (`a`) role account privileges.**
2. **Verify that you have network connectivity to update the firmware.**
3. **Type the following command to load the ILOM firmware image:**

   -> **`load -source`** *<supported_protocol>*`://`*<server_ip>*`/`*<path_to_firmware_image>*`/`*<filename.xxx>*

   A note about the firmware update process followed by message prompts to load the image are displayed. The text of the note depends on your platfom.

4. **At prompt for loading the specified file, type `y` for yes or `n` for no.**

   The prompt to preserve the configuration appears.

   For example:

   ```
   Do you want to preserve the configuration (y/n)?
   ```

5. **At the preserve configuration prompt, type `y` for yes or `n` for no.**

   Type `y` to save your existing ILOM configuration and to restore that configuration when the update process completes.

Note – If you type `n` at the preserve configuration prompt, another platform-specific prompt appears.

6. **Do one of the following:**
   - If you have a **2.x firmware release installed** on your system, the system will enter a special mode to load the new firmware. Then the system will automatically reboot to complete the firmware update. Proceed to Step 7.
   - If you have a **3.x firmware release installed** on a **SPARC** system, the system will enter a special mode to load the new firmware. Then the system will automatically reboot to complete the firmware update. Proceed to Step 7.
   - If you have a **3.x firmware release installed** on an **x64 system**, a prompt to postpone the BIOS update will appear.

     For example:
     ```
     Do you want to force the server off if BIOS needs to be upgraded
     (y/n)?
     ```

   a. **At the prompt to postpone the BIOS update, type `y` for yes or n for `n`.**

      The system will enter a special mode to load the new firmware and then the system will automatically reboot to complete the firmware update.

Note – The BIOS prompt only appears on x64 systems currently running an ILOM 3.x firmware release. If you answer yes (`y`) to the prompt,the system postpones the BIOS upgrade until the next time the system reboots. If you answer no (`n`) to the prompt, the system automatically updates the BIOS, if necessary, when updating the SP firmware.

   b. **Proceed to Step 7.**

7. **Reconnect to the ILOM server SP or CMM using the same user name and password that you provided in Step 1 of this procedure.**

Note – If you did not preserve the ILOM configuration before the firmware update, you will need to perform the initial ILOM setup procedures to reconnect to ILOM.

8. **Ensure that the proper firmware version has been installed. At the CLI prompt, type:**

   ```
   -> version
   ```

What Next?

You can now continue to customize your ILOM configuration for your system and data center environment. Before you configure ILOM for your environment, refer to the *Sun Integrated Lights Out Manager 3.0 Concepts Guide* for an overview of the new ILOM 3.0 features and functionality. Knowing how the new ILOM features will affect your environment will help you configure ILOM settings so that you can access all of ILOM's capabilities in your system and data center.

Also refer to the Sun ILOM 3.0 Procedures Guides for descriptions of how to perform ILOM tasks using a specific user interface and your platform ILOM Supplement documentation for platform-specific configuration instructions.

These documents can be found on docs.sun.com at:

http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic

These documents also can be found with your platform documentation on docs.sun.com at:

http://docs.sun.com/app/docs/prod/servers