Ce logiciel et la documentation qui l’accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d’utilisation et de divulgation. Saut disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d’interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu’elles soient exemptes d’erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l’accompagne, est concédé sous licence au Gouvernement des États-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l’utilise pour le compte du Gouvernement des États-Unis, la notice suivante s’applique :

U.S. GOVERNMENT RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are “commercial computer software” or “commercial technical data” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Ce logiciel et matériel a été développé pour un usage général dans le cadre d’applications de gestion des informations. Ce logiciel ou matériel n’est pas conçu ni n’est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d’applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de securité, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l’utilisation de ce logiciel ou matériel pour ce type d’applications.

Oracle et Java sont des marques déposées d’Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d’autres propriétaires qu’Oracle.

AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d’Advanced Micro Devices. Intel et Intel Xeon sont des marques ou des marques déposées d’Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. UNIX est une marque déposée concédée sous licence par X/Open Company, Ltd.
Contents

Using This Documentation  v

Getting Started With ILOM  1
About This Guide  2
ILOM Getting Started Process  2
Connecting Your System to ILOM  5
  Connection Requirements  5
Using the Web Interface or CLI  6
Using the root Account  6

1. Initial ILOM Setup Procedures Using the Web Interface  7
  Logging In to ILOM for the First Time Using the Web Interface  8
    ▼ Log In to ILOM Using the root User Account  8
  Configuring an IPv4 and IPv6 Network Environment  10
    ▼ Configure IPv4 and IPv6 Settings Using the Web Interface  10
  Adding User Accounts or Configuring a Directory Service  13
    ▼ Add User Account and Assign Privileges  14
    ▼ Configure ILOM for Active Directory  16
    ▼ Configure LDAP Server  22
    ▼ Configure ILOM for LDAP  23
    ▼ Configure ILOM for LDAP/SSL  24
2. Initial ILOM Setup Procedures Using the ILOM CLI 33
   Logging In to ILOM for the First Time Using the CLI 34
     ▼ Log In to ILOM Using the root User Account 34
   Configuring an IPv4 and IPv6 Network Environment 35
     ▼ Configure IPv4 and IPv6 Settings Using the CLI 35
   Adding User Accounts or Configuring a Directory Service 40
     ▼ Add User Account and Assign Privileges 40
     ▼ Configure ILOM for Active Directory 41
     ▼ Configure ILOM for LDAP 45
     ▼ Configure ILOM for LDAP/SSL 46
     ▼ Configure ILOM for RADIUS 49
   ▼ Log In to ILOM Using a New User Account 51
   ▼ Log Out of ILOM 51
What Next? 52

3. ILOM Firmware 53
   Identifying ILOM Version Information 54
     ▼ Identify ILOM Version Using the Web Interface 54
     ▼ Identify ILOM Version Using the CLI 54
   Updating ILOM Firmware to Latest Version 55
     Before You Begin 55
     ▼ Update ILOM Firmware Using the Web Interface 55
     ▼ Update ILOM Firmware Using the CLI 57
Using This Documentation

This Getting Started Guide describes how to perform the required procedures to access the Oracle Integrated Lights Out Manager (ILOM) 3.0 firmware for the first time on your system.

These procedures include ILOM log in, network connection, user account creation, directory service configuration, and firmware upgrade. This guide is written for technicians, system administrators, authorized service providers, and users who have experience managing system hardware.

To fully understand the information that is presented in this guide, use this Getting Started Guide in conjunction with other guides in the Oracle Integrated Lights Out Manager (ILOM) 3.0 Documentation Collection. For a description of the guides that comprise the ILOM 3.0 Documentation Collection, see “Related Documentation” on page vi.

This preface contains the following topics:
- “Related Documentation” on page vi
- “Documentation, Support, and Training” on page vii
- “ILOM 3.0 Version Numbers” on page vii
- “Documentation Feedback” on page viii
Related Documentation

The following table lists the guides that comprise the ILOM 3.0 Documentation Collection. You can access or download these guides online at:

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

**Note** — The documents comprising the collection were formerly referred to as Sun Integrated Lights Out Manager (ILOM) 3.0 guides.

<table>
<thead>
<tr>
<th>Title</th>
<th>Content</th>
<th>Part Number</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts</td>
<td>Information that describes ILOM features and functionality</td>
<td>820-6410</td>
<td>PDF</td>
</tr>
<tr>
<td>Guide</td>
<td></td>
<td></td>
<td>HTML</td>
</tr>
<tr>
<td>Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting</td>
<td>Information and procedures for network connection, logging in to ILOM for the first time, and configuring a user account or a directory service</td>
<td>820-5523</td>
<td>PDF</td>
</tr>
<tr>
<td>Started Guide</td>
<td></td>
<td></td>
<td>HTML</td>
</tr>
<tr>
<td>Oracle Integrated Lights Out Manager (ILOM) 3.0 Web</td>
<td>Information and procedures for accessing ILOM functions using the ILOM web interface</td>
<td>820-6411</td>
<td>PDF</td>
</tr>
<tr>
<td>Interface Procedures Guide</td>
<td></td>
<td></td>
<td>HTML</td>
</tr>
<tr>
<td>Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI</td>
<td>Information and procedures for accessing ILOM functions using the ILOM CLI</td>
<td>820-6412</td>
<td>PDF</td>
</tr>
<tr>
<td>Procedures Guide</td>
<td></td>
<td></td>
<td>HTML</td>
</tr>
<tr>
<td>Oracle Integrated Lights Out Manager (ILOM) 3.0 Management</td>
<td>Information and procedures for accessing ILOM functions using SNMP, IPMI, or WS-Man and CIM</td>
<td>820-6413</td>
<td>PDF</td>
</tr>
<tr>
<td>Protocols Reference Guide</td>
<td></td>
<td></td>
<td>HTML</td>
</tr>
<tr>
<td>Oracle Integrated Lights Out Manager (ILOM) 3.0 Feature</td>
<td>Late-breaking information about new ILOM 3.0 features, as well as known problems and workarounds</td>
<td>820-7329</td>
<td>PDF</td>
</tr>
<tr>
<td>Updates and Release Notes</td>
<td></td>
<td></td>
<td>HTML</td>
</tr>
<tr>
<td>Oracle Integrated Lights Out Manager (ILOM) CMM Administration Guide for Sun Blade 6000 and Sun Blade 6048 Modular Systems</td>
<td>Information and procedures for accessing CMM-specific ILOM functions</td>
<td>820-0052</td>
<td>PDF</td>
</tr>
</tbody>
</table>
In addition to the ILOM 3.0 Documentation Collection, associated ILOM Supplement guides or platform Administration guides 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 or platform Administration guide that comes with your server platform.

Translated versions of some of these documents are available at the web site listed above the table. English documentation is revised more frequently and might be more up-to-date than the translated documentation.

---

**Documentation, Support, and Training**

These web sites provide additional resources:
- Documentation [http://docs.sun.com](http://docs.sun.com)

---

**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
Documentation Feedback

Submit comments about this document by clicking the Feedback[+] link at:

http://docs.sun.com

Include the title and part number of your document with your feedback:

Oracle Integrated Lights Out Manager (ILOM) 3.0 Getting Started Guide,
part number 820-5523-12
Getting Started With ILOM

**Topics**

<table>
<thead>
<tr>
<th>Description</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn how to use this guide</td>
<td>• “About This Guide” on page 2</td>
</tr>
<tr>
<td>Review the ILOM getting started process and prerequisites, choose an interface, and plan your ILOM setup</td>
<td>• “ILOM Getting Started Process” on page 2</td>
</tr>
<tr>
<td></td>
<td>• “Connecting Your System to ILOM” on page 5</td>
</tr>
<tr>
<td>Review the requirements for connecting to ILOM</td>
<td>• “Connecting Your System to ILOM” on page 5</td>
</tr>
<tr>
<td></td>
<td>• “Using the Web Interface or CLI” on page 6</td>
</tr>
<tr>
<td></td>
<td>• “Using the root Account” on page 6</td>
</tr>
</tbody>
</table>
About This Guide

*Oracle 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 Oracle Sun server platform 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 your system to ILOM and how to configure the required initial ILOM 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 “Related Documentation” on page vi.

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 how to configure ILOM for your system and data center environment.

*TABLE 1-1* presents 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.
## Chapter 1 Getting Started With ILOM

### TABLE 1-1 Initial ILOM Setup and Configuration Tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Information to Consider</th>
<th>Refer to This Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prerequisite Information for Logging In to ILOM</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connect your system to ILOM, choose to use either the ILOM web interface or the CLI, then learn about the preconfigured root user account</td>
<td>You can connect to ILOM using an Ethernet connection or a serial connection. As of ILOM 3.0.12 and later releases, you can use a dual-stack IPv4 and IPv6 network environment. You can set up ILOM for the first time using either the web interface or the command-line interface (CLI). For initial login, you will use the preconfigured root user account.</td>
<td>“Connecting Your System to ILOM” on page 5 “Using the Web Interface or CLI” on page 6 “Using the root Account” on page 6 Also refer to your platform documentation</td>
</tr>
<tr>
<td><strong>Log In to ILOM for the First Time</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log in to ILOM using the root user account</td>
<td>ILOM boots automatically when power is applied to your Oracle Sun server platform. 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:</td>
<td>“Logging In to ILOM for the First Time Using the Web Interface” on page 8 “Logging In to ILOM for the First Time Using the CLI” on page 34</td>
</tr>
<tr>
<td><strong>Configure ILOM for Network Access</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure the IPv4 or IPv6 network settings</td>
<td>You can accept the default dual-stack IPv4 (DHCPv4) and IPv6 (stateless) settings that are provided, or you can change the settings using the ILOM web interface or command-line interface (CLI). If your network only supports IPv4, you can also change the default IPv4 settings from the host operating system using the BIOS utility or IPMItool.</td>
<td>“Configuring an IPv4 and IPv6 Network Environment” on page 10 (web) “Configuring an IPv4 and IPv6 Network Environment” on page 35 (CLI)</td>
</tr>
<tr>
<td><strong>Create Local User Accounts or Use a Directory Service</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note - You can choose either to create a local user account or to configure a directory service. Add local user account and assign roles</td>
<td>After you have logged in to ILOM, you can create and configure up to 10 local user accounts.</td>
<td>“Adding User Accounts or Configuring a Directory Service” on page 13 (web) “Adding User Accounts or Configuring a Directory Service” on page 40 (CLI)</td>
</tr>
</tbody>
</table>
### TABLE 1-1 Initial ILOM Setup and Configuration Tasks (Continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Information to Consider</th>
<th>Refer to This Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure ILOM for Active Directory</td>
<td>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.</td>
<td>“Configure ILOM for Active Directory” on page 16 (web) &lt;br&gt;“Configure ILOM for Active Directory” on page 41 (CLI)</td>
</tr>
<tr>
<td>Configure ILOM for LDAP</td>
<td>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.</td>
<td>“Configure LDAP Server” on page 22 (web) &lt;br&gt;“Configure ILOM for LDAP” on page 45 (CLI)</td>
</tr>
<tr>
<td>Configure ILOM for LDAP/SSL</td>
<td>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.</td>
<td>“Configure ILOM for LDAP/SSL” on page 24 (web) &lt;br&gt;“Configure ILOM for LDAP/SSL” on page 46 (CLI)</td>
</tr>
<tr>
<td>Configure ILOM for RADIUS</td>
<td>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.</td>
<td>“Configure ILOM for RADIUS” on page 29 (web) &lt;br&gt;“Configure ILOM for RADIUS” on page 49 (CLI)</td>
</tr>
</tbody>
</table>

### Log In and Out of ILOM Using an Administrative User Account

<table>
<thead>
<tr>
<th>Task</th>
<th>Information to Consider</th>
<th>Refer to This Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log in to ILOM using a local, administrative user account</td>
<td>Once you have created a local user account or configured a directory service, log in to ILOM using that local, administrative user account.</td>
<td>“Log In to ILOM Using a New User Account” on page 30 (web) &lt;br&gt;“Log In to ILOM Using a New User Account” on page 51 (CLI)</td>
</tr>
<tr>
<td>Log out of ILOM</td>
<td>You can log out of your ILOM session while preserving your configuration settings.</td>
<td>“Log Out of ILOM” on page 31 (web) &lt;br&gt;“Log Out of ILOM” on page 51 (CLI)</td>
</tr>
</tbody>
</table>

### Identify ILOM Version and Upgrade Firmware

<table>
<thead>
<tr>
<th>Task</th>
<th>Information to Consider</th>
<th>Refer to This Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify ILOM version</td>
<td>You can quickly identify which version of ILOM is running on the service processor or chassis monitoring module.</td>
<td>“Identifying ILOM Version Information” on page 54</td>
</tr>
<tr>
<td>Update ILOM firmware</td>
<td>You can easily update your ILOM firmware to the latest version.</td>
<td>“Updating ILOM Firmware to Latest Version” on page 55</td>
</tr>
</tbody>
</table>
Connecting Your System to ILOM

You can connect your system to ILOM without a network connection using the serial port, or you can connect your system to ILOM over a network using the network management port.

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 Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.

Connection Requirements

As of ILOM 3.0.12, new network configuration settings have been added to the ILOM web interface and CLI to support the configuration of a dual-stack IPv4 and IPv6 network environment. For information about dual-stack IPv4 and IPv6 networks, refer to the Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.

Prior to performing the procedures for logging in to ILOM and configuring network settings, you should ensure that the following requirements are met.

- Plan how you want to set up ILOM on your server to work in your data center environment. Refer to the section for establishing communication with ILOM in the Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.

- Connect to ILOM over a serial port without a network connection, or log in to ILOM over a 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 Sun Blade Modular System chassis, to the chassis monitoring module (CMM) port. To log in using a network connection, attach an Ethernet cable to the NET MGT port on the server or CMM. Refer to your platform documentation for more information.

- Determine the method to use to configure the network settings. As of ILOM 3.0.12, new dual-stack IPv4 and IPv6 settings are provided that enable ILOM to fully operate in an IPv4 and IPv6 network environment. Prior to ILOM 3.0.12, network configuration settings for IPv4 were provided. You can use either dual-stack IPv4 and IPv6 network settings, DHCP for IPv4 settings, or Stateless settings for IPv6. By default, ILOM will attempt to obtain network settings using DHCP.

- Verify that network addresses were accepted by ILOM for IPv4 network environments or that DNS and host names were accepted by ILOM for IPv6 network environments.
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 chapters. Chapter 2 explains how to perform the initial setup and configuration tasks using the web interface. Chapter 3 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.

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) 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 in order 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 log in and re-create the root account. For information about the default user account, refer to the Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.
Initial ILOM Setup Procedures Using the Web Interface

<table>
<thead>
<tr>
<th>Topics</th>
<th>Description</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log in to ILOM for the first time</td>
<td>• “Logging In to ILOM for the First Time Using the Web Interface” on page 8</td>
<td></td>
</tr>
<tr>
<td>Configure the network environment</td>
<td>• “Configuring an IPv4 and IPv6 Network Environment” on page 10</td>
<td></td>
</tr>
<tr>
<td>Add user accounts or configure a directory service</td>
<td>• “Adding User Accounts or Configuring a Directory Service” on page 13</td>
<td></td>
</tr>
<tr>
<td>Find information about your next ILOM configuration steps</td>
<td>• “What Next?” on page 31</td>
<td></td>
</tr>
</tbody>
</table>
Logging In to ILOM for the First Time Using the Web Interface

To log in to the ILOM web interface for the first time, you use the default root user account and its default password changeme.

▼ Log In to ILOM Using the root User Account

To log in to the ILOM web interface for the first time using the root user account, open a web browser and do the following:

1. Type **http://system_ipaddress** into the web browser.
   If ILOM is operating in a dual-stack network environment, the system_ipaddress can be entered using either an IPv4 or IPv6 address format.
   For example:
   For IPv4 - http://10.8.183.106
   or
   For IPv6 - http://[fec0:a:8:b7:214:4ff:5eca:5f7e/64]
   The web interface Login page appears.
   For more information about entering IP addresses in a dual-stack environment, and for diagnosing connection issues, refer to the **Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide**.
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.

You are now ready to configure your network settings and to access all of ILOM’s features and functionality. 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. You can access the ILOM 3.0 Documentation Collection at:

http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic
Configuring an IPv4 and IPv6 Network Environment

The following web interface procedure provides instructions for configuring ILOM 3.0.12 and later versions to operate in a dual-stack IPv4 and IPv6 network environment. For a detailed description about configuring ILOM in the IPv4 and IPv6 network environment, refer to the Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.

If you are configuring ILOM to operate in an IPv4-only network environment, as is supported in ILOM 3.0.10 and earlier versions of ILOM, refer to the Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide.

By default, ILOM will attempt to obtain the IPv4 address using DHCPv4 and the IPv6 address using IPv6 stateless.

▼ Configure IPv4 and IPv6 Settings Using the Web Interface

1. Log in to the ILOM SP web interface or the CMM ILOM web interface.
2. Navigate to the IPv4 and IPv6 network settings that are available on the Network tab.
   For example:
   - On a server SP, click Configuration --> Network.
   - On a CMM, do the following:
     - Select the blade (in the left pane), then (in the right pane) click Configuration --> Network.
     - In the Network Settings table, select the radio button for either the CMM or the blade SP, then click Edit.

   Note – The Network Settings page at the CMM level of the web interface does not support the dual-stack IPv4 and IPv6 properties. However, it does support IPv4 only properties. To change the IPv6 network settings for a CMM, see “Configure IPv4 and IPv6 Settings Using the CLI” on page 35.

3. Verify that the network State is enabled.
Chapter 2 Initial ILOM Setup Procedures Using the Web Interface

Note – The setting for network State is enabled by default for both IPv4 and IPv6. If necessary, you can optionally disable (uncheck) the network State for IPv6. However, the IPv4 network State must always be enabled in order for ILOM to operate in an IPv4 network environment or within a dual-stack IPv4 and IPv6 network environment.

4. Perform the network configuration instructions below that apply to your network environment.

- To manually configure a static IP, see the steps below for IPv4 and/or see the steps for IPv6.
  - Steps to manually configure a static IPv4 address:
    
    | Steps | Description |
    |-------|-------------|
    | a.    | Enable the radio button for Static IP. |
    | b.    | Type the IP address for the device in the IP address text box. |
    | c.    | Type the subnet mask of the network on which the device resides. |
    | d.    | Type the device gateway access address. |

- Steps to manually configure a static IPv6 address:

<table>
<thead>
<tr>
<th>Steps</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>•</td>
<td>Type the IP address for the device in the IP address text box.</td>
</tr>
<tr>
<td></td>
<td>The input parameters for specifying the IPv6 static IP and netmask are:</td>
</tr>
<tr>
<td></td>
<td>(&lt;IPv6_address&gt;/&lt;subnet_mask_length_in_bits&gt;)</td>
</tr>
<tr>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td>[fec0:a:8:b7:214:4fff:feca:5f7e/64]</td>
</tr>
<tr>
<td>Note</td>
<td>IPv6 supports the assignment of multiple IP addresses for a device. Therefore, you can manually configure a single static IPv6 address in ILOM, as well as enable one or more of the IPv6 auto-configuration options in ILOM, if desired.</td>
</tr>
</tbody>
</table>

- To enable DHCP to automatically assign an IPv4 address, select the IPv4 DHCP radio button.

- To enable one or more of the IPv6 auto-configuration options, select the appropriate option(s) described below.
Note – As of ILOM 3.0.14 or later, you can enable the option for Stateless auto-configuration to run at the same time as when the option for DHCPv6 Stateless is enabled or when the option for DHCPv6 Stateful is enabled. However, the auto-configuration options for DHCPv6 Stateless and DHCPv6 Stateful should not be enabled to run at the same time.

Note – When you enable the auto-configuration for either DHCPv6 Stateful or DHCPv6 Stateless, ILOM will identify in the Network Settings page the DHCP Unique ID for the DHCPv6 server that was last used to retrieve the DHCP information.

5. Click Save to apply the changes made.

All changes to the network settings are considered pending within the ILOM session until you click Save.

Note – Changing the static IP address on the device (SP or CMM) will end all active ILOM sessions to the device. A message will appear prompting you to close your browser session. You will need to log back in to ILOM using the newly assigned static IP address.
Note – IPv6 addresses learned for the device from any of the IPv6 auto-
configuration options will not affect any of the active ILOM sessions to the device.
You can verify the newly learned auto-configured addresses on the Network tab.

To test the IPv4 or IPv6 network configuration from ILOM, use the Network Test Tools (Ping or Ping6). For details, refer to the Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Interface Procedures Guide.

Adding User Accounts or Configuring a Directory Service

After you log in to ILOM using the root user account, you can choose either to create a local user account or to configure a directory service. For detailed information about ILOM user accounts and directory services, refer to the Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.

<table>
<thead>
<tr>
<th>Topics</th>
<th>Description</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn how to add a user account and assign user roles (privileges)</td>
<td>• “Add User Account and Assign Privileges” on page 14</td>
<td></td>
</tr>
<tr>
<td>Learn how to configure ILOM for Active Directory</td>
<td>• “Configure ILOM for Active Directory” on page 16</td>
<td></td>
</tr>
<tr>
<td>Learn how to configure the LDAP server</td>
<td>• “Configure LDAP Server” on page 22</td>
<td></td>
</tr>
<tr>
<td>Learn how to configure ILOM for LDAP</td>
<td>• “Configure ILOM for LDAP” on page 23</td>
<td></td>
</tr>
<tr>
<td>Learn how to configure ILOM for LDAP/SSL</td>
<td>• “Configure ILOM for LDAP/SSL” on page 24</td>
<td></td>
</tr>
<tr>
<td>Learn how to edit the SSL tables</td>
<td>• “Edit LDAP/SSL Tables” on page 28</td>
<td></td>
</tr>
<tr>
<td>Learn how to configure ILOM for RADIUS</td>
<td>• “Configure ILOM for RADIUS” on page 29</td>
<td></td>
</tr>
<tr>
<td>Learn how to verify that the new user account or directory service is working properly</td>
<td>• “Log In to ILOM Using a New User Account” on page 30</td>
<td></td>
</tr>
<tr>
<td>Learn how to log out of ILOM</td>
<td>• “Log Out of ILOM” on page 31</td>
<td></td>
</tr>
</tbody>
</table>
Add User Account and Assign Privileges

1. Log in to the ILOM web interface.

   The User Account Settings page appears.

3. In the Users table, click Add.
   The Add User dialog appears.

4. 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.

<table>
<thead>
<tr>
<th>Roles</th>
<th>Definition</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Admin</td>
<td>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.</td>
</tr>
<tr>
<td>u</td>
<td>User Management</td>
<td>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.</td>
</tr>
<tr>
<td>c</td>
<td>Console</td>
<td>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.</td>
</tr>
<tr>
<td>r</td>
<td>Reset and Host Control</td>
<td>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.</td>
</tr>
<tr>
<td>o</td>
<td>Read Only</td>
<td>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.</td>
</tr>
<tr>
<td>s</td>
<td>Service</td>
<td>A user who is assigned the Service (s) role can assist Oracle service engineers in the event that on-site service is required.</td>
</tr>
</tbody>
</table>

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

1. Log in to the ILOM web interface

   The Active Directory page appears.
3. Configure the Active Directory settings.

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

<table>
<thead>
<tr>
<th>Property (Web)</th>
<th>Property (CLI)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>state</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies whether the Active Directory client is enabled or disabled.</td>
</tr>
<tr>
<td>Roles</td>
<td>defaultRole</td>
<td>(none)</td>
<td>Administrator</td>
</tr>
<tr>
<td></td>
<td>(a</td>
<td>u</td>
<td>c</td>
</tr>
<tr>
<td>Address</td>
<td>address</td>
<td>0.0.0.0</td>
<td>IP address or DNS name of the Active Directory server. If the DNS name is used, DNS must be configured and functional.</td>
</tr>
<tr>
<td>Port</td>
<td>port</td>
<td>0</td>
<td>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.</td>
</tr>
<tr>
<td>Timeout</td>
<td>timeout</td>
<td>4</td>
<td>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 adjusting the time to wait when a server is not responding or is unreachable.</td>
</tr>
<tr>
<td>Strict Cert</td>
<td>strictcertmode</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Certificate Mode</td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>DNS Locator Mode</td>
<td>dnslocatormode</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If enabled, an attempt to locate the Active Directory server is performed, based on the DNS locator queries that are configured.</td>
</tr>
<tr>
<td>Log Detail</td>
<td>logdetail</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies the amount of diagnostics that go into the event log.</td>
</tr>
</tbody>
</table>
4. Click Save for your settings to take effect.

5. View the Active Directory certificate information.

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

<table>
<thead>
<tr>
<th>Property (Web)</th>
<th>Property (CLI)</th>
<th>Displays</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate File Status</td>
<td>certstatus</td>
<td>certificate not present</td>
<td>Read-only indicator of whether a certificate exists.</td>
</tr>
<tr>
<td>Certificate File Status</td>
<td>certstatus</td>
<td>certificate present (details)</td>
<td>Click on “details” for information about issuer, subject, serial number, valid_from, valid_to, and version.</td>
</tr>
</tbody>
</table>

6. 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:

<table>
<thead>
<tr>
<th>Transfer Method</th>
<th>Required Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser</td>
<td>File Name</td>
</tr>
<tr>
<td>TFTP</td>
<td>Host, Filepath</td>
</tr>
<tr>
<td>FTP</td>
<td>Host, Filepath, Username, Password</td>
</tr>
<tr>
<td>SCP</td>
<td>Host, Filepath, Username, Password</td>
</tr>
</tbody>
</table>

7. Click the Load Certificate button or Remove Certificate button.
8. If a certificate is loaded, the following read-only details appear if you selected “certificate present (details)”: 

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>issuer</td>
<td>Certificate Authority who issued the certificate.</td>
</tr>
<tr>
<td>subject</td>
<td>Server or domain for which the certificate is intended.</td>
</tr>
<tr>
<td>valid_from</td>
<td>Date when the certificate becomes valid.</td>
</tr>
<tr>
<td>valid_until</td>
<td>Date when the certificate becomes invalid.</td>
</tr>
<tr>
<td>serial_number</td>
<td>Serial number of the certificate.</td>
</tr>
<tr>
<td>version</td>
<td>Version number of the certificate.</td>
</tr>
</tbody>
</table>

9. 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

10. 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.

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CN=SpSuperAdmin,OU=Groups,DC=sales,DC=east,DC=oracle,DC=com</td>
</tr>
</tbody>
</table>

- **Operator Groups Table:**
  - The name listed in entry 1 uses the Distinguished Name format.

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CN=SpSuperOper,OU=Groups,DC=sales,DC=east,DC=oracle,DC=com</td>
</tr>
</tbody>
</table>

- **Custom Groups Table:**
  - The name listed in entry 1 uses the Simple Name format.

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>custom_group_1</td>
<td>Admin, User Management, Console, Reset and Host Control, Read Only (aucro)</td>
</tr>
</tbody>
</table>

- **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>.

<table>
<thead>
<tr>
<th>ID</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>&lt;USERNAME&gt;@sales.east.oracle.com</td>
</tr>
<tr>
<td>2</td>
<td>CN=&lt;USERNAME&gt;,OU=Users,DC=sales,DC=east,DC=oracle,DC=com</td>
</tr>
</tbody>
</table>

- **Alternate Servers Table:**
  The entries below provide redundancy for authentication.

<table>
<thead>
<tr>
<th>ID</th>
<th>Address</th>
<th>Port</th>
<th>Certificate Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.8.168.99</td>
<td>0</td>
<td>Certificate not present</td>
</tr>
<tr>
<td>2</td>
<td>10.8.143.230</td>
<td>0</td>
<td>Certificate not present</td>
</tr>
</tbody>
</table>

- **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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>_ldap._tcp.gc._msdcs.&lt;DOMAIN&gt;..<a href="">PORT:3269</a></td>
</tr>
<tr>
<td>2</td>
<td>_ldap._tcp.dc._msdcs.&lt;DOMAIN&gt;..<a href="">PORT:636</a></td>
</tr>
</tbody>
</table>

11. 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).

<table>
<thead>
<tr>
<th>Required Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>User name for logging in to ILOM</td>
</tr>
<tr>
<td>uidNumber</td>
<td>Any unique number</td>
</tr>
<tr>
<td>gidNumber</td>
<td>Any unique number</td>
</tr>
<tr>
<td>userPassword</td>
<td>Password</td>
</tr>
<tr>
<td>homeDirectory</td>
<td>Any value (this property is ignored by ILOM)</td>
</tr>
<tr>
<td>loginShell</td>
<td>Any value (this property is ignored by ILOM)</td>
</tr>
</tbody>
</table>

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 23.
Configure ILOM for LDAP

1. Log in to the ILOM web interface.

2. Select User Management --> LDAP.
   The LDAP Settings page appears.

3. 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.
4. Click Save for your changes to take effect.

5. 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**

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. Log in to the ILOM web interface.

2. Select User Management --> LDAP/SSL.

   The LDAP/SSL page appears, displaying the configuration settings and the LDAP/SSL tables.
3. Configure the LDAP/SSL settings.
See the following table for a description of the LDAP/SSL settings.
<table>
<thead>
<tr>
<th>Property (Web)</th>
<th>Property (CLI)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>state</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies whether the LDAP/SSL client is enabled or disabled.</td>
</tr>
<tr>
<td>Roles</td>
<td>defaultRole</td>
<td>(none)</td>
<td>Administrator</td>
</tr>
<tr>
<td></td>
<td>(a</td>
<td>u</td>
<td>c</td>
</tr>
<tr>
<td>Address</td>
<td>address</td>
<td>0.0.0.0</td>
<td>IP address or DNS name of the LDAP/SSL server. If the DNS name is used, DNS must be configured and functional.</td>
</tr>
<tr>
<td>Port</td>
<td>port</td>
<td>0</td>
<td>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.</td>
</tr>
<tr>
<td>Timeout</td>
<td>timeout</td>
<td>4</td>
<td>Timeout value in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This property allows for adjusting the time to wait when a server is not responding or is unreachable.</td>
</tr>
<tr>
<td>Strict Certificate Mode</td>
<td>strictcertmode</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Log Detail</td>
<td>logdetail</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies the amount of diagnostics that go into the event log.</td>
</tr>
</tbody>
</table>

4. Click Save for your settings to take effect.
5. 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.

<table>
<thead>
<tr>
<th>Property (Web)</th>
<th>Property (CLI)</th>
<th>Displays</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate File Status</td>
<td>certstatus</td>
<td>certificate not present</td>
<td>Read-only indicator of whether a certificate exists.</td>
</tr>
<tr>
<td>Certificate File Status</td>
<td>certstatus</td>
<td>certificate present (details)</td>
<td>Click on “details” for information about issuer, subject, serial number, valid_from, valid_to, and version.</td>
</tr>
</tbody>
</table>

6. 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.

<table>
<thead>
<tr>
<th>Transfer Method</th>
<th>Required Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser</td>
<td>File Name</td>
</tr>
</tbody>
</table>
| TFTP            | Host
|                 | Filepath            |
| FTP             | Host
|                 | Filepath
|                 | Username
|                 | Password            |
| SCP             | Host
|                 | Filepath
|                 | Username
|                 | Password            |

7. Click the Load Certificate button or Remove Certificate button.
8. If a certificate is loaded, the following read-only details will appear if you selected “certificate present (details)”: 

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>issuer</td>
<td>Certificate Authority who issued the certificate.</td>
</tr>
<tr>
<td>subject</td>
<td>Server or domain for which the certificate is intended.</td>
</tr>
<tr>
<td>valid_from</td>
<td>Date when the certificate becomes valid.</td>
</tr>
<tr>
<td>valid_until</td>
<td>Date when the certificate becomes invalid.</td>
</tr>
<tr>
<td>serial_number</td>
<td>Serial number of the certificate.</td>
</tr>
<tr>
<td>version</td>
<td>Version number of the certificate.</td>
</tr>
</tbody>
</table>

▼ Edit LDAP/SSL Tables

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

1. Log in to the ILOM web interface.

2. Select User Management --> LDAP/SSL.

   The LDAP/SSL page appears.

3. 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
   - Alternate Servers

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

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

See the procedure “Configure ILOM for Active Directory” on page 16 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=oracle, DC=com

You would be authenticated to ILOM with the supplied name.

6. Click Save for your changes to take effect.

▼ Configure ILOM for RADIUS

1. Log in to the ILOM web interface.

2. Select User Management --> RADIUS.

The RADIUS Settings page appears.
3. Complete the RADIUS settings.

<table>
<thead>
<tr>
<th>Property (Web)</th>
<th>Property (CLI)</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>state</td>
<td>Disabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Role</td>
<td>defaultrole</td>
<td>Read Only</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a</td>
<td>u</td>
<td>c</td>
</tr>
<tr>
<td>Address</td>
<td>ipaddress</td>
<td>0.0.0.0</td>
<td>IP address or DNS name of the RADIUS server. If the DNS name is used, DNS must be configured and functional.</td>
</tr>
<tr>
<td>Port</td>
<td>port</td>
<td>1812</td>
<td>Specifies the port number used to communicate with the RADIUS server. The default port is 1812.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>secret</td>
<td>(none)</td>
<td>Specifies the shared secret that is used to protect sensitive data and to ensure that the client and server recognize each other.</td>
</tr>
</tbody>
</table>

4. Click Save for your settings to take effect.

Log In to ILOM Using a New User Account

To log in to the ILOM web interface using a non-root user account, open a web browser and do the following:

1. Type [http://system_ipaddress into the web browser.](http://system_ipaddress]

   If ILOM is operating in a dual-stack network environment, the `system_ipaddress` can be entered using either an IPv4 or IPv6 address format.

   For example:

   **For IPv4** - [http://10.8.183.106](http://10.8.183.106)
   or

   **For IPv6** - [http://[fec0:a:8:b7:214:4ff:5eca:5f7e/64](http://[fec0:a:8:b7:214:4ff:5eca:5f7e/64]

   The web interface Login page appears.

   For more information about entering IP addresses in a dual-stack environment, and for diagnosing connection issues, refer to the [Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide](http://oracle.com/iloм).
2. Type the user name and password for the user account:
   User Name: <assigned_username>
   Password: <assigned_password>

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.

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 Oracle 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 Oracle ILOM 3.0 Procedures Guides for descriptions of how to perform ILOM tasks using a specific user interface and to your platform ILOM Supplement or platform Administration guide for platform-specific configuration instructions.

The ILOM 3.0 Documentation Collection can be found at:

http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic
CHAPTER 3

Initial ILOM Setup Procedures Using the ILOM CLI

<table>
<thead>
<tr>
<th>Topics</th>
<th>Description</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log in to ILOM for the first time</td>
<td></td>
<td>• “Logging In to ILOM for the First Time Using the CLI” on page 34</td>
</tr>
<tr>
<td>Configure the network environment</td>
<td></td>
<td>• “Configuring an IPv4 and IPv6 Network Environment” on page 35</td>
</tr>
<tr>
<td>Add user accounts or configure a</td>
<td></td>
<td>• “Adding User Accounts or Configuring a Directory Service” on page 40</td>
</tr>
<tr>
<td>directory service</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Find information about your next</td>
<td></td>
<td>• “What Next?” on page 52</td>
</tr>
<tr>
<td>ILOM configuration steps</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Logging In to ILOM for the First Time Using the CLI

To log in to the ILOM CLI for the first time, you use the default root user account and its default password changeme. After you set up your network environment, you can establish an Administrative user account using an assigned user account name and password.

▼ Log In to ILOM Using the root User Account

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

1. To log in to the ILOM CLI using the root user account, type:

```
$ ssh root@system_ipaddress
```

If ILOM is operating in a dual-stack network environment, the system_ipaddress can be entered using either an IPv4 or IPv6 address format.

For example:

- **For IPv4** - 10.8.183.106
- **For IPv6** - [fec0:a:8:b7:214:4fff:5eca:5f7e/64]

The ILOM Login prompt appears.

For more information about entering IP addresses in a dual-stack environment, refer to the Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.

2. Type the default user name and password:

```
<hostname>: root
Password: changeme
```

The ILOM CLI prompt appears (\->).
Configuring an IPv4 and IPv6 Network Environment

The following CLI procedure provides instructions for configuring ILOM to operate in a dual-stack IPv4 and IPv6 network environment. For a detailed description about configuring ILOM in the IPv4 and IPv6 network environment, refer to the Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.

If you are configuring ILOM to operate in an IPv4-only network environment, as is supported in ILOM 3.0.10 and earlier versions of ILOM, refer to the Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide.

By default, ILOM will attempt to obtain the IPv4 address using DHCPv4 and the IPv6 address using IPv6 stateless.

▼ Configure IPv4 and IPv6 Settings Using the CLI

1. Log in to the ILOM SP CLI or the CMM CLI.
   Establish a local serial console connection or SSH connection to the server SP or CMM.

2. Perform the network configuration instructions that apply to your network environment:
   ■ To configure IPv4 network settings, perform Step 3 through Step 5 in this procedure.
   ■ To configure IPv6 network settings, perform Step 6 to Step 10 in this procedure.

3. For IPv4 network configurations, use the cd command to navigate to the /x/network working directory for the device.
   For example:
   ■ For a rackmount server SP type: cd /SP/network
   ■ For a chassis CMM type: cd /CMM/network
   ■ For a chassis blade server SP type: cd /CH/BL/n/network
   ■ For a chassis blade server with multiple SP nodes type: cd /CH/BL#Node/n/network

4. Type the show command to view the configured IPv4 network settings configured on the device.

5. To set IPv4 network settings for DHCP or static, perform one of the following:
To configure DHCP IPv4 network settings, set values for the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Set Property Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>state</td>
<td>set state=enabled</td>
<td>The network state is enabled by default for IPv4.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> - To enable the DHCP network option for IPv4 the state must be set to enabled.</td>
</tr>
<tr>
<td>pendingipdiscovery</td>
<td>set pendingipdiscovery=dhcp</td>
<td>The property value for ipdiscovery is set to dhcp by default for IPv4.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> - If the dhcp default property value was changed to static, you will need to set the property value to dhcp.</td>
</tr>
<tr>
<td>commitpending=</td>
<td>set commitpending=true</td>
<td>Type set commitpending=true to commit the changes made to the state and ipdiscovery property values.</td>
</tr>
</tbody>
</table>

To configure static IPv4 network settings, set values for the following properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Set Property Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>state</td>
<td>set state=enabled</td>
<td>The network state is enabled by default for IPv4.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> - To enable the static IPv4 network option the state must be set to enabled.</td>
</tr>
<tr>
<td>pendingipdiscovery</td>
<td>set pendingipdiscovery=static</td>
<td>To enable a static IPv4 network configuration, you need to set the pendingipdiscovery property value to static.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> - The property value for ipdiscovery is set to dhcp by default for IPv4.</td>
</tr>
<tr>
<td>pendingipaddress</td>
<td>set pendingipaddress=</td>
<td>To assign multiple static network settings, type the set command followed by the pending command for each property value (IP address, netmask, and gateway), then type the static value that you want to assign.</td>
</tr>
<tr>
<td>pendingipnetmask</td>
<td>&lt;ip_address&gt; pendingipnetmask=</td>
<td></td>
</tr>
<tr>
<td>pendingipgateway</td>
<td>&lt;netmask&gt; pendingipgateway=</td>
<td></td>
</tr>
<tr>
<td>commitpending=</td>
<td>set commitpending=true</td>
<td>Type set commitpending=true to commit the changes made to the state, ipdiscovery, and network settings property values.</td>
</tr>
</tbody>
</table>
6. For IPv6 network configurations, use the `cd` command to navigate to the `/x/network/ipv6` working directory for the device.

   For example:
   - For a rackmount server SP type: `cd /SP/network/ipv6`
   - For a chassis CMM type: `cd /CMM/network/ipv6`
   - For a chassis blade server SP type: `cd /CH/BL/network/ipv6`
   - For a chassis blade server with multiple SP nodes type: `cd /CH/BL/Node/network/ipv6`

7. Type the `show` command to view the configured IPv6 network settings configured on the device.

   For example, see the following sample output values for the IPv6 properties on a server SP device:

   ```
   -> show

   /SP/network/ipv6
   Targets:

   Properties:
   state = enabled
   autoconfig = stateless
   dhcpv6_server_duid = (none)
   link_local_ipaddress = fe80::214:4fff:feca:5f7e/64
   static_ipaddress = ::/128
   ipgateway = fe80::211:5dff:febe:5000/128
   pending_static_ipaddress = ::/128
   dynamic_ipaddress_1 = fec0:a:8:b7:214:4fff:feca:5f7e/64

   Commands:
   cd
   show
   ```

**Note** – The default IPv6 autoconfig= property value provided in ILOM 3.0.14 (and later) is autoconfig=stateless. However, if you have ILOM 3.0.12 installed on your CMM or server, the default property value for autoconfig appears as autoconfig=stateless_only.

**Note** – When the autoconfig= property is set to dhcpv6_stateful or dhcpv6_stateless, the read-only property for dhcpv6_server_duid will identify the DHCP Unique ID of the DHCPv6 server that was last used by ILOM to retrieve the DHCP information.
8. To configure an IPv6 auto-configuration option, use the `set` command to specify the following auto-configuration property values.

<table>
<thead>
<tr>
<th>Property</th>
<th>Set Property Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>state</td>
<td>set state=enabled</td>
<td>The IPv6 network state is enabled by default. To enable an IPv6 auto-configuration option, this state must be set to enabled.</td>
</tr>
</tbody>
</table>
| autoconfig | set autoconfig=<value> | Specify this command followed by the `autoconf` value you want to set. Options include:  
  - stateless (default setting provided in ILOM 3.0.14 or later)  
    or stateless_only (default setting provided in ILOM 3.0.12)  
    Automatically assigns IP address learned from the IPv6 network router.  
  - dhcpv6_stateless  
    Automatically assigns DNS information learned from the DHCP server.  
    The `dhcpv6_stateless` property value is available in ILOM as of 3.0.14.  
  - dhcpv6_stateful  
    Automatically assigns the IPv6 address learned from the DHCPv6 server.  
    The `dhcpv6_stateful` property value is available in ILOM as of 3.0.14.  
  - disable  
    Disables all auto-configuration property values and sets the read-only property value for link local address. |

The following information is relevant to the IPv6 autoconfig options:

- IPv6 auto-config options take affect after they are set. You do not need to commit these changes under the `/network` target.
- IPv6 auto-config addresses learned for the device will not affect any of the active ILOM sessions to the device. You can verify the newly learned auto-configured addresses under the `/network/ipv6` target.
- As of ILOM 3.0.14 or later, you can enable the stateless auto-config option to run at the same time as when the option for `dhcpv6_stateless` is enabled or as when the option for `dhcpv6_stateful` is enabled. However, the auto-config options for `dhcpv6_stateless` and `dhcpv6_stateful` should not be enabled to run at the same time.
9. To set a pending static IPv6 address, specify the following property values:

<table>
<thead>
<tr>
<th>Property</th>
<th>Set Property Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>state</td>
<td>set state=enabled</td>
<td>The IPv6 network state is enabled by default. To enable a static IP address the state must be set to enabled.</td>
</tr>
<tr>
<td>pendingipaddress</td>
<td>set pending_static_ipaddress=&lt;ip_address&gt;/&lt;subnet_mask_length_in_bits&gt;</td>
<td>Type this command followed by the property value for the static IPv6 address and net mask that you want to assign to the device. IPv6 address example: fec0:a:8:b7:214:4ff:00:4fca:5f7e/64</td>
</tr>
</tbody>
</table>

10. To commit the pending IPv6 static network parameters, perform the following steps:

   a. Use the cd command to change the directory to the device network target.
      For example:
      - For rackmount server type: cd /SP/network
      - For chassis CMM type: cd /CMM/network
      - For chassis blade server SP type: cd /CH/BL/n/network
      - For chassis blade server SP with multiple nodes type: cd /CH/BL/n/Node/n/network

   b. Type the following command to commit the changed property values for IPv6:
      ```
      set commitpending=true
      ```

**Note** – Assigning a new static IP address to the device (SP or CMM) will end all active ILOM sessions to the device. To log back in to ILOM, you will need to create a new browser session using the newly assigned IP address.

To test the IPv4 or IPv6 network configuration from ILOM use the Network Test Tools (Ping and Ping6). For details, refer to the *Oracle Integrated Lights Out Manager (ILOM) 3.0 CLI Procedures Guide.*
Adding User Accounts or Configuring a Directory Service

After you log in to ILOM using the root user account, you can choose either to create a local user account or to configure a directory service. For detailed information about ILOM user accounts and directory services, refer to the Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.

Add User Account and Assign Privileges

1. Log in to the ILOM CLI.
2. 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
   ```
3. 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 40.

▼ Configure ILOM for Active Directory

1. Log in to the ILOM CLI using the root user account.

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

```bash
-> 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:

```bash
-> 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:

```bash
-> 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)
```

4. Use the `set` command to configure top-level properties.
   For example:

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

5. Use the `set` command to load a certificate or to modify properties.
   For example:
   - To load an Active Directory certificate:

```bash
-> 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:

```bash
-> 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=oracle,DC=com
Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com'
```

■ To modify Operator Groups table properties:

```
-> set /SP/clients/activedirectory/opergroups/1 name=CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperOper,OU=Groups,DC=sales,DC=oracle,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=oracle,DC=com
Set 'name' to 'CN=spSuperCust,OU=Groups,DC=sales,DC=oracle,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.oracle.com
Set 'domain' to 'username@sales.oracle.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>
```

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>_ldap._tcp.gc._msdcs.&lt;DOMAIN&gt;..<a href="">PORT:3269</a></td>
</tr>
<tr>
<td>2</td>
<td>_ldap._tcp.dc._msdcs.&lt;DOMAIN&gt;..<a href="">PORT:636</a></td>
</tr>
</tbody>
</table>

### Configure ILOM for LDAP

1. Log in to the ILOM CLI.

2. 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=oracle, dc=com" bindpw=password
   ```

3. Enter the IP address or DNS name of the LDAP server. Type:
   
   ```
   -> set /SP/clients/ldap address=ldap_ipaddress | DNS_name
   ```

4. (Optional) Assign the port used to communicate with the LDAP server; the default port is 389. Type:
   
   ```
   -> set /SP/clients/ldap port=ldap_port
   ```

5. 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=oracle, dc=com"
   ```
   
   This is the location in your LDAP tree that you want to search for user authentication.

6. Set the state of the LDAP service to enabled. Type:
   
   ```
   -> set /SP/clients/ldap state=enabled
   ```
7. 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**

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. **Log in to the ILOM CLI.**
2. **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
```
3. Use the `show` command to view information in the tables. Type:

```bash
-> 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:

```bash
-> 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:

```bash
-> 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)
```
4. 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, strictmode, timeout
   ```

5. 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=oracle,DC=com
   Set 'name' to 'CN=spSuperAdmin,OU=Groups,DC=sales,DC=oracle,DC=com'
   ```

   - To modify Operator Groups properties:

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

   - To modify Custom Groups 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.

```plaintext
-> set /SP/clients/ldapssl/customgroups/1 name=CN=spSuperCust,OU=Groups,DC=sales,DC=oracle,DC=com
Set 'name' to 'CN=spSuperCust,OU=Groups,DC=sales,DC=oracle,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>`.

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

- To modify Alternate Servers properties:

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

▼ **Configure ILOM for RADIUS**

1. Log in to the ILOM CLI.
2. 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
```

3. 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 49.
Log In to ILOM Using a New User Account

Use this procedure to log in to ILOM to verify that the non-root user account is functioning properly.

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

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

   $ ssh root@system_ipaddress

   Or

   $ ssh -l username ipaddress

   If ILOM is operating in a dual-stack network environment, the system_ipaddress can be entered using either an IPv4 or IPv6 address format.

   For example:

   For IPv4 - 10.8.183.106

   or

   For IPv6 - [fec0:a:8:b7:214:4ff:5eca:5f7e/64]

   The ILOM Login prompt appears.

   For more information about entering IP addresses in a dual-stack environment, and for diagnosing connection issues, refer to the Oracle Integrated Lights Out Manager (ILOM) 3.0 Concepts Guide.

2. Type the user name and password for the user account.

   <hostname>: <assigned_username>

   Password: <assigned_password>

   The ILOM CLI prompt appears (->).

Log Out of ILOM

- At the command prompt, type:

  -> exit
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 Oracle 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 Oracle ILOM 3.0 Procedures Guides for descriptions of how to perform ILOM tasks using a specific user interface and to your platform ILOM Supplement or platform Administration guide for platform-specific configuration instructions.

The ILOM 3.0 Documentation Collection can be found at:

http://docs.sun.com/app/docs/prod/int.lights.mgr30#hic
CHAPTER 4

ILOM Firmware

<table>
<thead>
<tr>
<th>Topics</th>
<th>Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify your ILOM firmware version.</td>
<td>• “Identifying ILOM Version Information” on page 54</td>
</tr>
<tr>
<td>Update your ILOM firmware</td>
<td>• “Updating ILOM Firmware to Latest Version” on page 55</td>
</tr>
</tbody>
</table>
Identifying 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 the 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 the 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
   ```
Updating ILOM Firmware to Latest Version

You can use either the ILOM web interface or the CLI to update ILOM firmware. See:
- “Update ILOM Firmware Using the Web Interface” on page 55
- “Update ILOM Firmware Using the CLI” on page 57

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 platform’s product web site. Refer to the section about Updating the Firmware in either the Oracle Integrated Lights Out Manager (ILOM) 3.0 Web Procedures Guide or the Oracle 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 the 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 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 BIOS prompt only appears on x86 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.

   If you choose to update the BIOS, the system will automatically overwrite the current BIOS settings and then assign the BIOS factory default settings.

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 details 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 using the same user name and password that you provided in Step 1 of this procedure.
   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.

10. Verify that the proper firmware version has been installed. Select System Information --> Version.
    The firmware version on the SP or CMM should correspond to the firmware image you installed.

▼ **Update ILOM Firmware Using the 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.
   For example:
   - To verify network connectivity on a server SP, type:
     ```
     -> show /SP/network
     ```
   - To verify network connectivity on a CMM, type:
     ```
     -> show /CMM/network
     ```

3. Type the following command to load the ILOM firmware image:
   ```
   -> load -source <supported_protocol>://<server_ipaddress>/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 platform.
4. At the prompt for loading the specified file, type \textit{y} for yes or \textit{n} for no. 

   The prompt to preserve the configuration appears.

   For example:
   
   \textit{Do you want to preserve the configuration (y/n)?}

5. At the preserve configuration prompt, type \textit{y} for yes or \textit{n} for no. 

   Type \textit{y} to save your existing ILOM configuration and to restore that configuration when the update process completes.

\textbf{Note} – If you type \textit{n} at the preserve configuration prompt, another platform-specific prompt appears.

6. Do one of the following:

   - If you have a \textbf{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 \textbf{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 \textbf{3.x firmware release installed on an x86 system}, a prompt to postpone the BIOS update will appear.

     For example:
     
     \textit{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 \textit{y} for yes or \textit{n} for no.

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

\textbf{Note} – The BIOS prompt only appears on x86 systems currently running an ILOM 3.x firmware release. If you answer yes (\textit{y}) to the prompt, the system postpones the BIOS upgrade until the next time the system reboots. If you answer no (\textit{n}) to the prompt, the system automatically updates the BIOS, if necessary, when updating the SP firmware.

If you choose to update the BIOS, the system will automatically overwrite the current BIOS settings and then assign the BIOS factory default settings.

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

   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. Verify that the proper firmware version has been installed. At the CLI prompt, type:

   ```
   -> version
   ```

   The firmware version on the SP or CMM should correspond to the firmware image you installed.