HP iLO 3 User Guide

Abstract

This guide provides information about configuring, updating, and operating HP ProLiant servers by using the HP iLO 3 firmware. This document is intended for system administrators, HP representatives, and HP Authorized Channel Partners who are involved in configuring and using HP iLO 3 and HP ProLiant servers.

This guide discusses HP iLO for HP ProLiant servers and HP ProLiant BladeSystem server blades. For information about iLO for Integrity servers and server blades, see the HP website at http://www.hp.com/go/integrityiLO.

HP Part Number: 616301-006
Published: March 2014
Edition: 1

Acknowledgements

Contents

1 Introduction to iLO

The iLO software can remotely perform most functions that otherwise require a visit to the servers at the data center, computer room, or remote location. iLO allows you to do the following:

- Monitor server health. iLO monitors temperatures in the server and sends corrective signals to the fans to maintain proper server cooling. iLO also monitors firmware versions and the status of fans, memory, the network, processors, power supplies, and server hard drives.
- Access a high-performance and secure Integrated Remote Console to the server from anywhere in the world if you have a network connection to the server.

  There are two versions of the Integrated Remote Console:

  - .NET IRC
  - Java IRC

  General references to the Remote Console apply to both the .NET IRC and Java IRC, unless otherwise specified.
- Use the shared .NET IRC to collaborate with multiple server administrators.
- Remotely mount high-performance Virtual Media devices to the server.
- Use Virtual Power and Virtual Media from the GUI, the CLI, or the iLO scripting toolkit for many tasks, including the automation of deployment and provisioning.
- Securely and remotely control the power state of the managed server.
- Monitor the power consumption and server power settings.
- Use local or directory-based user accounts to log in to iLO.
- Configure Kerberos authentication, which adds the **HP Zero Sign In** button to the login screen.
- Use iLO language packs to switch between English and another supported language.

For more information about the iLO 3 features, see http://www.hp.com/go/iLO3.

iLO web interface

The iLO web interface groups similar tasks for easy navigation and workflow. It is organized in a navigational tree view located on the left side of the page. The top-level branches are **Information**, **Remote Console**, **Virtual Media**, **Power Management**, **Network**, and **Administration**. If you have a ProLiant server blade, the **BL c-Class** branch is included.

When using the iLO web interface, note the following:

- Each high-level iLO branch has a submenu that you can display by clicking the + icon to the left of that branch. Each menu topic displays a page title that describes the information or settings available on that page. The page title might not reflect the name that is displayed on the menu option.
- Assistance for all iLO pages is available from the iLO help pages. To access page-specific help, click the ? icon on the upper right side of the page.
- Typical administrator tasks are available from the **Administration** and **Network** branches of the iLO web interface. These tasks are described in "Setting up iLO" (page 14) and "Configuring iLO" (page 25).
- Typical user tasks are available from the **Information**, **Remote Console**, **Virtual Media**, **Power Management**, and **BL c-Class** branches of the iLO web interface. These tasks are described in "Using iLO" (page 92).

For more information about iLO functionality and integration, see the following:

- "Integrating HP Systems Insight Manager" (page 157)
- "Directory services" (page 160)
- "Troubleshooting" (page 209)

iLO RBSU

You can use the iLO ROM-based setup utility to configure network parameters, global settings, and user accounts. iLO RBSU is designed for the initial iLO setup, and is not intended for continued iLO administration. iLO RBSU is available whenever the server is booted, and can be run remotely through the Remote Console. Press **F8** during POST to enter iLO RBSU.

You can disable iLO RBSU in the iLO RBSU Global Settings preferences or in the iLO web interface. Disabling iLO RBSU prevents reconfiguration from the host unless the iLO Security Override Switch is set.

For more information about using iLO RBSU, see the following:

- "Setting up iLO by using iLO RBSU" (page 16)
- "iLO RBSU security" (page 44)
- "Using the iLO RBSU" (page 87)

iLO mobile app

The HP iLO mobile app provides access to the Remote Console of your HP ProLiant server from your mobile device. The mobile app interacts directly with the iLO processor on HP ProLiant servers, providing total control of the server at all times as long as the server is plugged in. For example, you can access the server when it is in a healthy state or when it is powered off with a blank hard drive. As an IT administrator, you can troubleshoot problems and perform software deployments from almost anywhere.

For more information about the iLO mobile app, see http://www.hp.com/go/ilo/mobileapp.

iLO scripting and command line

You can use the iLO scripting tools to configure multiple iLO systems, to incorporate a standard configuration into the deployment process, and to control servers and subsystems.

The *HP iLO Scripting and Command Line Guide* describes the syntax and tools available to use iLO 3 through a command line or scripted interface.

2 Setting up iLO

The iLO default settings enable you to use most features without additional configuration. However, the configuration flexibility of iLO enables customization for multiple enterprise environments. This chapter discusses the initial iLO setup steps. For information about additional configuration options, see "Configuring iLO" (page 25).

Complete the initial setup steps:

1. Decide how you want to handle networking and security. For more information, see "Preparing to set up iLO" (page 14).
2. Connect iLO to the network. For more information, see "Connecting iLO to the network" (page 16).
3. If you are not using dynamic IP addressing, configure a static IP address by using iLO RBSU. For more information, see "Setting up iLO by using iLO RBSU" (page 16).
4. If you are using the local accounts feature, set up your user accounts by using iLO RBSU or the iLO web interface. For more information, see "Setting up iLO by using iLO RBSU" (page 16) or "Setting up iLO by using the iLO web interface" (page 21).
5. Install an iLO license. For more information, see "Activating iLO licensed features" (page 22).
6. If required, install the iLO drivers. For more information, see "Installing the iLO drivers" (page 22).

Preparing to set up iLO

Before setting up an iLO management processor, you must decide how to handle networking and security. The following questions can help you configure iLO:

1. **How should iLO connect to the network?**

   For a graphical representation and explanation of the available connections, see "Connecting iLO to the network" (page 16).

   Typically, iLO is connected to the network through one of the following:

   - A **corporate network** that both the NIC and the iLO port are connected to. This connection enables access to iLO from anywhere on the network and reduces the amount of networking hardware and infrastructure required to support iLO. However, on a corporate network, traffic can hinder iLO performance.
   - A **dedicated management network** with the iLO port on a separate network. A separate network improves performance and security because you can physically control which workstations are connected to the network. A separate network also provides redundant access to the server when a hardware failure occurs on the corporate network. In this configuration, iLO cannot be accessed directly from the corporate network.

2. **How will iLO acquire an IP address?**

   To access iLO after connecting it to the network, the iLO management processor must acquire an IP address and subnet mask by using either a dynamic or static process.

   - A **dynamic IP address** is set by default. iLO obtains the IP address and subnet mask from DNS or DHCP servers. This method is the simplest.
   - A **static IP address** is used if DNS or DHCP servers are not available on the network. A static IP address can be configured by using iLO RBSU. For more information, see "Configuring a static IP address by using iLO RBSU" (page 17).

IMPORTANT: If you plan to use a static IP address, you must have the IP address before starting the iLO setup process.

3. **What access security is required, and what user accounts and privileges are needed?**

   iLO provides several options to control user access. Use one of the following methods to prevent unauthorized access:

   - **Local accounts**—Up to 12 user names and passwords can be stored in iLO. This is ideal for small environments such as labs and small-sized or medium-sized businesses.
   - **Directory services**—Use the corporate directory to manage iLO user access. This is ideal for environments with a large number of users. If you plan to use directory services, consider enabling at least one local administrator account for alternate access.

   For more information about iLO access security, see "Configuring iLO security" (page 43).

4. **How do you want to configure iLO?**

   iLO supports various interfaces for configuration and operation. This guide discusses the following interfaces:

   - Use **iLO RBSU** when the system environment does not use DHCP, DNS, or WINS. For more information, see "Setting up iLO by using iLO RBSU" (page 16).
   - Use the **iLO web interface** when you can connect to iLO on the network by using a web browser. You can also use this method to reconfigure an iLO management processor. For more information, see "Setting up iLO by using the iLO web interface" (page 21).

   Other configuration options not discussed in this guide follow:

   - **HP Scripting Toolkit**—This toolkit is a server deployment product for IT experts that provides unattended automated installation for high-volume server deployments. For more information, see the *HP Scripting Toolkit for Linux User Guide* and the *HP Scripting Toolkit for Windows User Guide*.
   - **Scripting**—You can use scripting for advanced setup of multiple iLO management processors. Scripts are XML files written for a scripting language called RIBCL. You can use RIBCL scripts to configure iLO on the network during initial deployment or from an already deployed host.

     The following methods are available:

     - **HP Lights-Out Configuration Utility (HPQLOCFG)**—The HPQLOCFG.EXE utility replaces the previously used CPQLOCFG.EXE utility. It is a Windows command line utility that sends XML configuration and control scripts over the network to iLO.
     - **HP Lights-Out Online Configuration Utility (HPONCFG)**—A local online scripted setup utility that runs on the host and passes RIBCL scripts to the local iLO. HPONCFG requires the HP iLO Channel Interface Driver.
     - **Custom scripting environments**—The iLO scripting samples include a Perl sample that can be used to send RIBCL scripts to iLO over the network.
     - **SMASH CLP**—A command-line protocol that can be used when a command line is accessible through SSH or the physical serial port.

     For more information about these methods, see the *HP iLO 3 Scripting and Command Line Guide*.

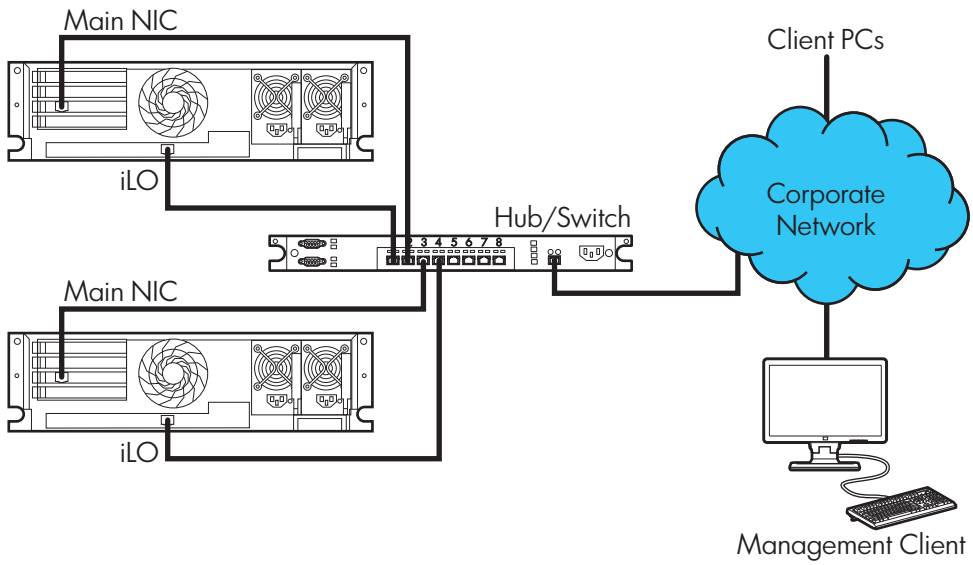
     iLO sample scripts are available at the following website: http://www.hp.com/support/iLO3.

Connecting iLO to the network

You can connect iLO to the network through a corporate network or a dedicated management network.

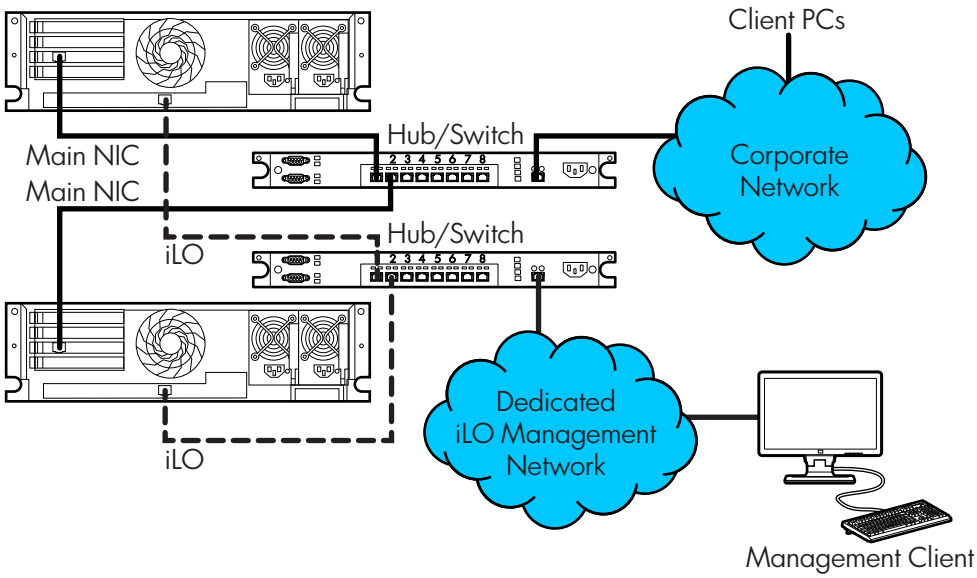
- In a **corporate network**, the server has two network port types (server NICs and one iLO NIC) connected to the corporate network, as shown in Figure 1 (page 16).

Figure 1 Corporate network diagram



- In a **dedicated management network**, the iLO port is on a separate network, as shown in Figure 2 (page 16).

Figure 2 Dedicated management network diagram



Setting up iLO by using iLO RBSU

HP recommends using iLO RBSU to set up iLO for the first time and to configure iLO network parameters for environments that do not use DHCP, DNS, or WINS.

Configuring a static IP address by using iLO RBSU

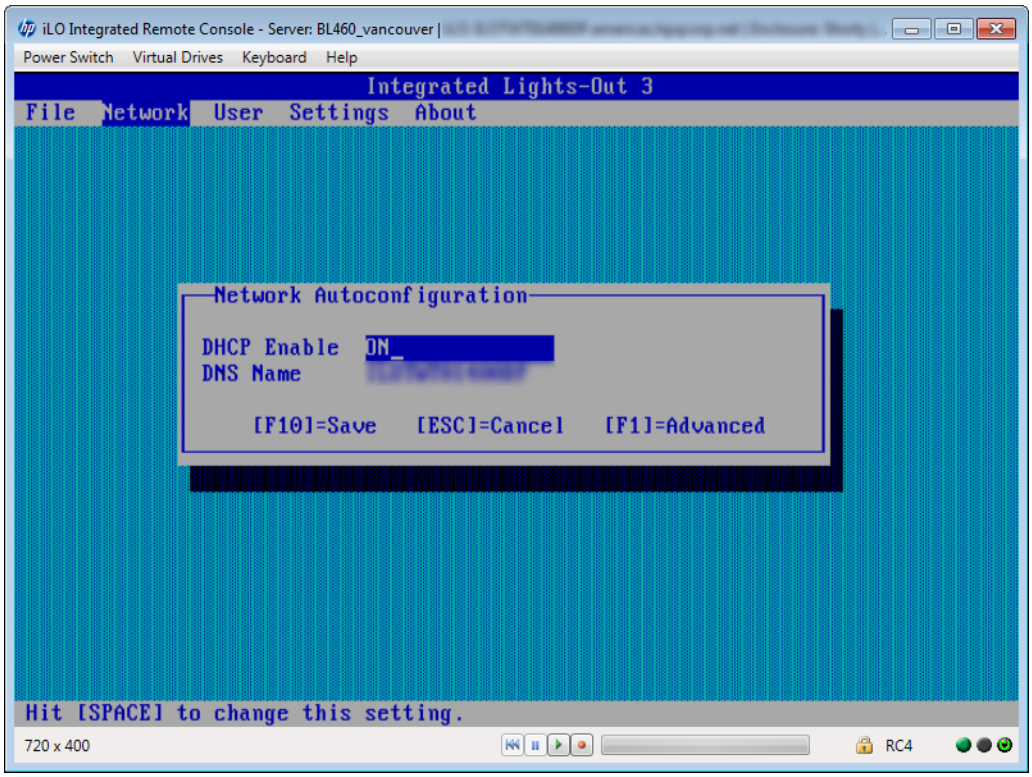
This procedure is required only if you are using a static IP address. When you are using dynamic IP addressing, your DHCP server automatically assigns an IP address for iLO.

NOTE: To simplify installation, HP recommends using DNS or DHCP with iLO.

To configure a static IP address:

1. Optional: If you access the server remotely, start an iLO remote console session.
   You can use the .NET IRC or Java IRC.
2. Restart or power on the server.
3. Press **F8** in the HP ProLiant POST screen.
   The iLO RBSU screen appears.
4. Disable DHCP:
   a. Select **Network→DNS/DHCP**, and then press **Enter**.
      The **Network Autoconfiguration** window opens.
   b. Select **DHCP Enable**, as shown in Figure 3 (page 17).

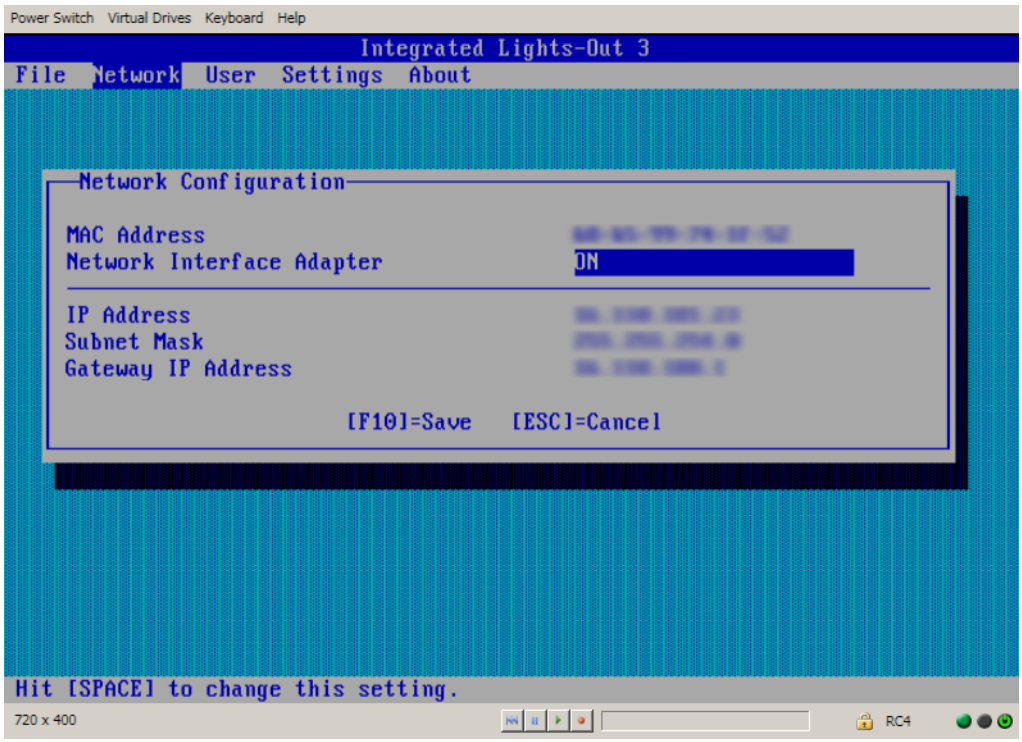
Figure 3 iLO RBSU Network Autoconfiguration window



   c. Press the spacebar to set **DHCP Enable** to **OFF**, and then press **F10** to save the changes.

5. Enter the network settings:
   a. Select **Network→NIC and TCP/IP**, and then press **Enter**.
      The **Network Configuration** window opens.
   b. Enter the appropriate information in the **IP Address**, **Subnet Mask**, and **Gateway IP Address** fields, as shown in Figure 4 (page 18).

Figure 4 iLO RBSU Network Configuration window



   c. Press **F10** to save the changes.
6. Select **File→Exit** to exit iLO RBSU.
   The changes take effect when you exit iLO RBSU.

Managing iLO users by using iLO RBSU

You can use iLO RBSU to perform the following user management tasks:

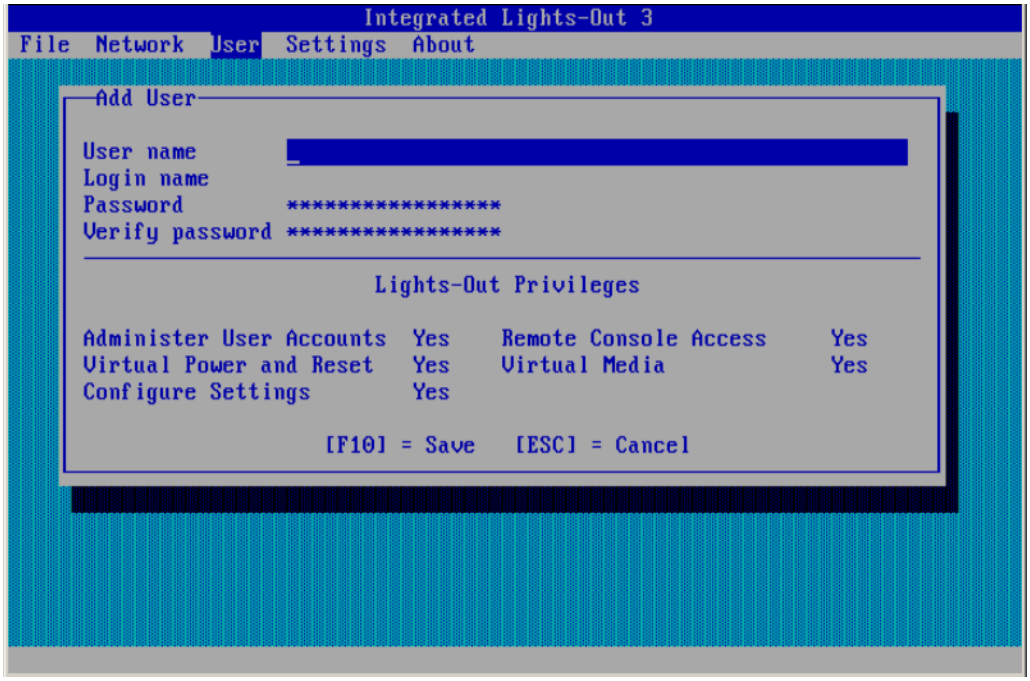
- "Adding user accounts" (page 18)
- "Editing user accounts" (page 20)
- "Removing user accounts" (page 20)

Adding user accounts

To add local iLO user accounts:

1. Optional: If you access the server remotely, start an iLO remote console session.
   You can use the .NET IRC or Java IRC.
2. Restart or power on the server.
3. Press **F8** in the HP ProLiant POST screen.
   iLO RBSU starts.
4. Select **User→Add**, and then press **Enter**.
   The **Add User** screen appears, as shown in Figure 5 (page 19).

Figure 5 iLO RBSU Add User window



5. Enter the following user account details:
   - **User name** appears in the user list on the **User Administration** page. It does not have to be the same as the **Login name**. The maximum length for a user name is 39 characters. The user name must use printable characters. Assigning descriptive user names can help you to easily identify the owner of each login name.
   - **Login name** is the name you must use when logging in to iLO. It appears in the user list on the **User Administration** page, on the **iLO Overview** page, and in iLO logs. The **Login name** does not have to be the same as the **User name**. The maximum length for a login name is 39 characters. The login name must use printable characters.
   - **Password** and **Verify password** set and confirm the password that is used for logging in to iLO. The maximum length for a password is 39 characters. Enter the password twice for verification.
6. Select from the following iLO privileges. To enable a privilege, set it to **Yes**. To disable a privilege, set it to **No**.
   - **Administer User Accounts**—Enables a user to add, edit, and delete local iLO user accounts. A user with this privilege can change privileges for all users. If you do not have this privilege, you can view your own settings and change your own password.
   - **Remote Console Access**—Enables a user to remotely access the host system Remote Console, including video, keyboard, and mouse control.
   - **Virtual Power and Reset**—Enables a user to power-cycle or reset the host system. These activities interrupt the system availability. A user with this privilege can diagnose the system by using the **Generate NMI to System** button.
   - **Virtual Media**—Enables a user to use the Virtual Media feature on the host system.
   - **Configure iLO Settings**—Enables a user to configure most iLO settings, including security settings, and to remotely update the iLO firmware. This privilege does not enable local user account administration.

     After iLO is configured, revoking this privilege from all users prevents reconfiguration using the web interface, HPQLOCFG, or the CLI. Users who have access to iLO RBSU or

HPONCFG can still reconfigure iLO. Only a user who has the Administer User Accounts privilege can enable or disable this privilege.

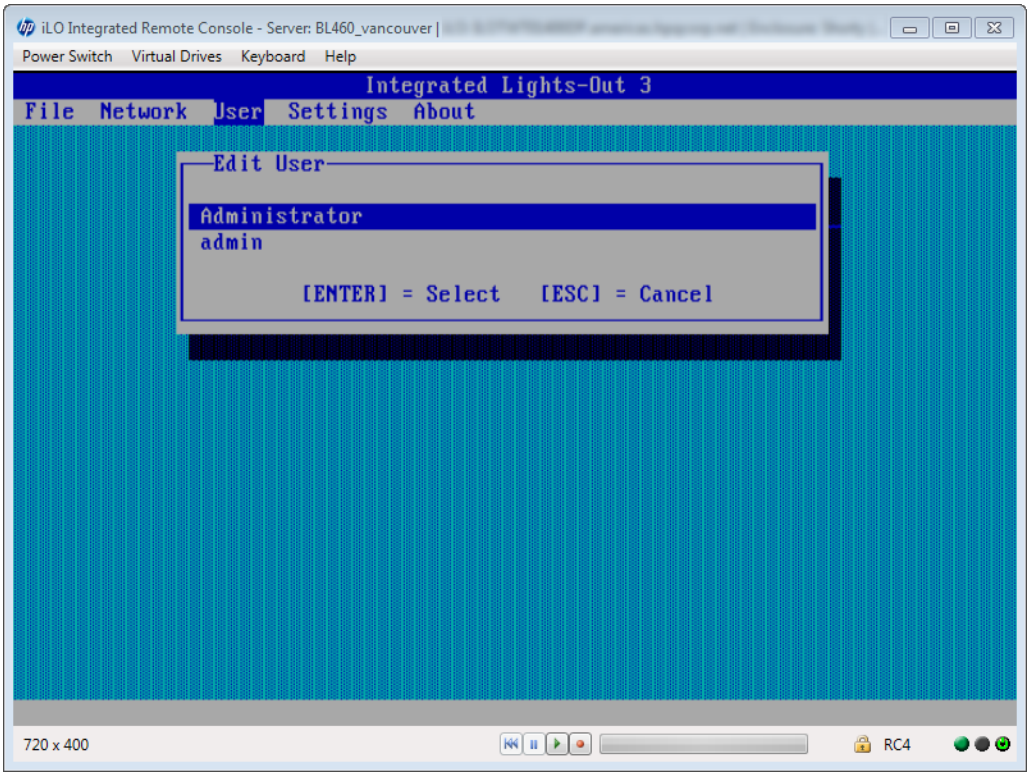
7. Press **F10** to save the new user account.
8. Repeat step 4 through step 7 until you are done creating user accounts.
9. Select **File→Exit** to exit iLO RBSU.

Editing user accounts

To edit a local iLO user account:

1. Optional: If you access the server remotely, start an iLO remote console session.
   You can use the .NET IRC or Java IRC.
2. Restart or power on the server.
3. Press **F8** in the HP ProLiant POST screen.
   The iLO RBSU screen appears.
4. Select **User→Edit**, and then press **Enter**.
   The **Edit User** screen appears, as shown in Figure 6 (page 20).

Figure 6 Editing user accounts



5. Select the user name that you want to edit, and then press **Enter**.
6. Update the user name, login name, password, or user privileges, and then press **F10** to save the changes.
7. Select **File→Exit** to exit iLO RBSU.

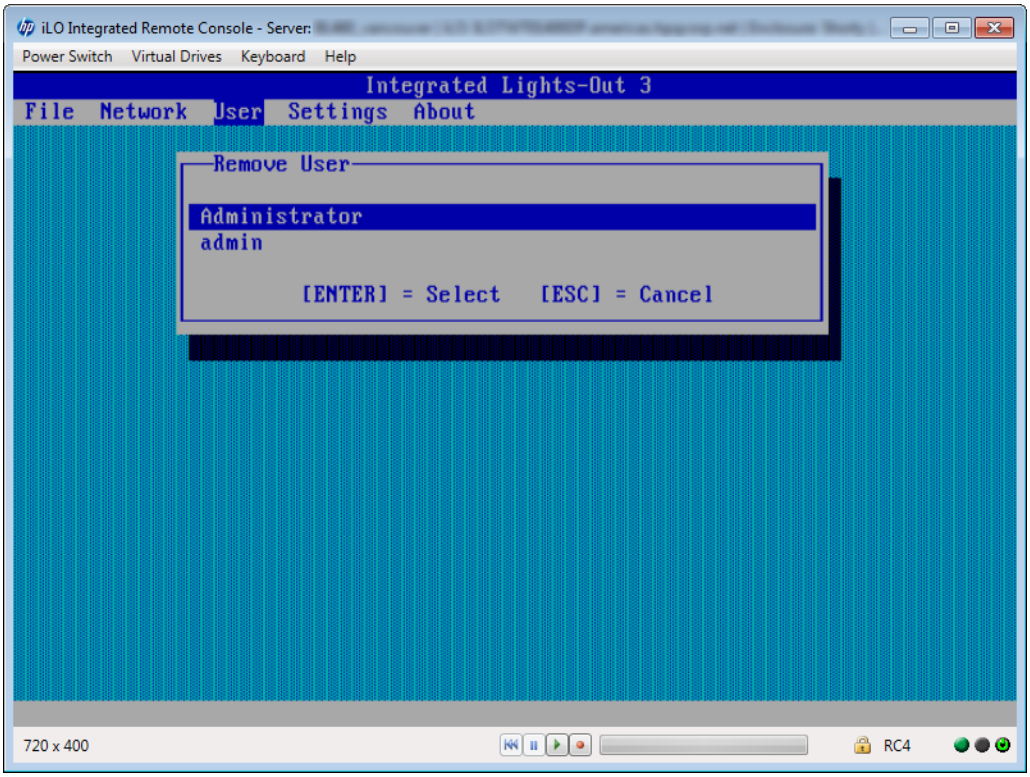
Removing user accounts

To remove a local iLO user account:

1. Optional: If you access the server remotely, start an iLO remote console session.
   You can use the .NET IRC or Java IRC.
2. Restart or power on the server.

3. Press **F8** in the HP ProLiant POST screen.
   The iLO RBSU screen appears.
4. Select **User→Remove**, and then press **Enter**.
   The **Remove User** screen appears, as shown in Figure 7 (page 21).

Figure 7 Removing user accounts



5. Select the user that you want to remove, and then press **Enter**.
   The iLO RBSU prompts you to confirm the request.
6. Press **Enter** to confirm the request.
7. Select **File→Exit** to exit iLO RBSU.

Setting up iLO by using the iLO web interface

You can use the iLO web interface to configure iLO if you can connect to iLO on the network by using a web browser. You can also use this method to reconfigure an iLO management processor.

Access iLO from a remote network client by using a supported browser and providing the default DNS name, user name, and password. For information about the DNS name and default user account credentials, see "Logging in to iLO for the first time" (page 21).

For information about the configuration procedures available in the iLO web interface, see "Configuring iLO" (page 25).

Logging in to iLO for the first time

The iLO firmware is configured with a default user name, password, and DNS name. Default user information is located on the serial number/iLO information pull tab attached to the server that contains the iLO management processor. Use these values to access iLO remotely from a network client by using a web browser.

NOTE: The serial number/iLO information pull tab is double-sided. One side shows the server serial number, and the other side shows the default iLO account information. The same information is printed on a label attached to the chassis.

The default values follow:

- **User name**—Administrator
- **Password**—A random eight-character alphanumeric string
- **DNS name**—ILO*XXXXXXXXXXXX*, where the *X*s represent the serial number of the server

If you enter an incorrect user name and password, or a login attempt fails, iLO imposes a security delay. For more information about login security, see "Login security" (page 46).

IMPORTANT: HP recommends changing the default values after you log in to iLO for the first time. For instructions, see "Managing iLO users by using the iLO web interface" (page 32).

Activating iLO licensed features

To activate iLO licensed features, install an HP iLO license. iLO licenses activate functionality such as graphical Remote Console with multi-user collaboration, video record/playback, and many more advanced features. For licensing information and installation instructions, see "iLO licensing" (page 31).

Installing the iLO drivers

iLO is an independent microprocessor running an embedded operating system. The architecture ensures that the majority of iLO functionality is available, regardless of the host operating system. The iLO drivers enable software such as HPONCFG and the HP Insight Management Agents to communicate with iLO. Your OS and system configuration determine the driver requirements.

The iLO drivers are available from the HP Service Pack for ProLiant and the HP website.

- **For Windows, Red Hat, and SLES**—Download the SPP from http://www.hp.com/go/spp/download and use it to install the iLO drivers.

  For information about using the SPP, see the SPP documentation.

- **For Windows, Red Hat, and SLES**—Download the iLO drivers from the HP Support Center:
  1. Navigate to the technical support page on the HP website: http://www.hp.com/support.
  2. Select a country or region and a language.

     The **HP Support** page opens.
  3. Click the **Drivers & Downloads** link.
  4. In the search box, enter the server model that you are using (for example, DL360).

     A list of servers is displayed.
  5. Click the link for your server.

     The HP Support Center page for the server opens.
  6. Click the link for the server operating system.
  7. Download the iLO drivers.
- **For VMware**—Download the iLO drivers from the **vibsdepot** section of the Software Delivery Repository website at http://downloads.linux.hp.com/SDR/index.html.

Follow the installation instructions provided with the downloaded software.

For OS-specific driver information, see the following:

- "Microsoft device driver support" (page 23)
- "Linux device driver support" (page 23)
- "VMware device driver support" (page 24)

Microsoft device driver support

When you are using Windows with iLO, the following drivers are available:

- **HP ProLiant iLO 3/4 Channel Interface Driver for Windows**—This driver is required for the operating system to communicate with iLO. Install this driver in all configurations.
- **HP ProLiant iLO 3/4 Management Controller Driver Package for Windows**—This package includes the following components:
  - `hpqilo3core` provides iLO Management Controller Driver support.
  - `hpqilo3service` provides the HP ProLiant Health Monitor Service and HP ProLiant System Shutdown Service.
  - `hpqilo3whea` is a helper service for Windows Hardware Error Architecture, which passes information between iLO and the operating system in the event of a hardware fault.

IMPORTANT: The Management Controller Driver Package is required to support Automatic Server Recovery and the HP Insight Management Agents or HP Insight Management WBEM Providers (if installed). For more information, see "Configuring iLO Management settings" (page 84).

Linux device driver support

When you are using Linux with iLO, the following drivers are available:

- **HP ProLiant Channel Interface Device Driver** (`hpilo`)—This driver manages agent and tool application access to iLO.
- **HP System Health Application and Command Line Utilities** (`hp-health`)—A collection of applications and tools that enables monitoring of fans, power supplies, temperature sensors, and other management events. This RPM contains the `hpasmd`, `hpasmlited`, `hpasmpld`, and `hpasmxld` daemons.

IMPORTANT: These drivers are standard for SUSE Linux Enterprise Server 11, Red Hat 5, and Red Hat 6.

For open-source Linux distributions (Ubuntu, Debian, Fedora, and others), the `hpilo` driver is part of the Linux kernel, so the driver is loaded automatically at startup.

Use the following commands to load the iLO drivers:

```
rpm -ivh hpilo-<d.vv.v-pp.Linux_version.arch>.rpm
rpm -ivh hp-health-<d.vv.v-pp.Linux_version.arch>.rpm
```

Where `<d>` is the Linux distribution and version, `<vv.v-pp>` are version numbers, and `<arch>` is the architecture (i386 or x86_64).

Use the following commands to remove the iLO drivers:

```
rpm -e hpilo
rpm -e hp-health
```

VMware device driver support

When you are using VMware with iLO, the following driver is available:

HP ProLiant Channel Interface Device Driver (`hpilo`)—This driver manages agent, WBEM provider, and tool application access to iLO. It is included in the customized HP VMware images. For raw VMware images, the driver must be installed manually.

3 Configuring iLO

Typically, an advanced or administrative user who manages users and configures global and network settings configures iLO. This guide provides information about configuring iLO by using the iLO web interface and iLO RBSU.

TIP: You can also perform many iLO configuration tasks by using XML configuration and control scripts or SMASH CLP. For information about using these methods, see the *HP iLO 3 Scripting and Command Line Guide*, *HP Scripting Toolkit for Linux User Guide*, and *HP Scripting Toolkit for Windows User Guide*.

Updating firmware

Firmware updates enhance iLO functionality with new features, improvements, and security updates. You can download the latest firmware from the following website: http://www.hp.com/support/ilo3.

Users who have the Configure iLO Settings privilege or host operating system Administrator/root privileges can update iLO firmware. If the iLO Security Override Switch is set, any out-of-band user can update the firmware.

Due to the security enhancements in iLO 3 1.50 and later, the firmware image file is larger than previous releases. To accommodate the larger firmware image file, you must have iLO 3 1.20 or later installed to upgrade to iLO 3 1.50 or later. Upgrading from earlier firmware versions is not supported.

To downgrade from iLO 3 1.50 or later to an earlier firmware version, you must disable FIPS Mode. For instructions, see "Using encryption" (page 58).

You can update the iLO firmware by using an online or offline method. For more information, see "Updating firmware by using an online method" (page 25) or "Updating firmware by using an offline method" (page 26)

Updating firmware by using an online method

When you use an online method to update the firmware, no server reboot is required. You can update the firmware and reset iLO without affecting the availability of the server host operating system. The online update method can be performed in-band or out-of-band.

Performing an in-band firmware update

When you use this method to update the iLO firmware, the iLO firmware is sent to iLO directly from the server host operating system. The HP ProLiant Channel Interface Driver is required for host-based iLO firmware updates. During a host-based firmware update, the iLO firmware does not verify login credentials or user privileges because the host-based utilities require a root login (Linux and VMware) or Administrator login (Windows).

You can use the following in-band firmware update methods:

- **iLO Online ROM Flash Component**—Use an executable file to update iLO while the server is operating. The executable file contains the installer and the firmware package. You can download an iLO Online ROM Flash Component from the following HP website: http://www.hp.com/support/ilo3.
- **HPONCFG**—Use the HP Lights-Out Online Configuration Utility to configure iLO by using XML scripts. Download the iLO firmware image and the `Update_Firmware.xml` sample script. Edit the sample script with your setup details, and then run the script.

  Sample scripts are available at http://www.hp.com/support/ilo3. For more information about scripting, see the *HP iLO 3 Scripting and Command Line Guide*.

For instructions about obtaining the iLO firmware image, see "Obtaining the iLO firmware image file" (page 26).

Performing an out-of-band firmware update

When you use this method to update the iLO firmware, you use a network connection to communicate with iLO directly.

You can use the following out-of-band firmware update methods:

- **iLO web interface**—Download the iLO Online ROM Flash Component and install it by using the iLO web interface. For instructions, see "Updating the iLO firmware by using a browser" (page 27).
- **HPQLOCFG**—Use the HP Lights-Out Configuration Utility to configure iLO by using XML scripts. Download the iLO firmware image and the `Update_Firmware.xml` sample script. Edit the sample script with your setup details, and then run the script.

  Sample scripts are available at http://www.hp.com/support/ilo3. For more information about scripting, see the *HP iLO 3 Scripting and Command Line Guide*.

  For instructions about obtaining the iLO firmware image, see "Obtaining the iLO firmware image file" (page 26).
- **HPLOMIG** (also called HP Directories Support for Management Processors)—Download the HP Directories Support for Management Processors executable file to access the directory support components. One of the components, HPLOMIG, can be used to discover multiple iLO processors and update their firmware in one step. You do not need to use directory integration to take advantage of this feature. For more information, see "Upgrading firmware on management processors" (page 200).
- **SMASH CLP**—Access SMASH CLP through the SSH port, and use standard commands to view firmware information and update the firmware.

  For more information about SMASH CLP, see the *HP iLO 3 Scripting and Command Line Guide*.

  NOTE: The SMASH CLP method for updating firmware is not supported for upgrading to iLO 3 1.50 or later.

Updating firmware by using an offline method

When you use an offline method to update the firmware, you must reboot the server by using an offline utility. Examples of offline firmware updates include the following:

- **HP Service Pack for ProLiant**—Use the HP Service Pack for ProLiant to install the firmware update. For more information, see the following website: http://www.hp.com/go/spp.
- **Windows or Linux Scripting Toolkit**—Use the Scripting Toolkit to configure several settings within the server and update firmware. This method is useful for deploying to multiple servers. For instructions, see the *HP Scripting Toolkit for Linux User Guide* or *HP Scripting Toolkit for Windows User Guide*.

Obtaining the iLO firmware image file

The `.bin` file from the iLO Online ROM Flash Component is required for some of the methods you can use to update the iLO firmware.

To download the iLO Online ROM Flash Component file, and then extract the `.bin` file:

1. Navigate to the technical support page on the HP website: http://www.hp.com/support.
2. Select a country or region and a language.

   The **HP Support** page opens.

3. Click the **Drivers & Downloads** link.
4. In the search box, enter the server model that you are using (for example, DL360).

   A list of servers is displayed.
5. Click the link for your server.

   The HP Support Center page for the server opens.
6. Click the link for your server operating system.
7. Follow the onscreen instructions to download the iLO Online ROM Flash Component file.
8. Double-click the downloaded file, and then click the **Extract** button.
9. Select a location for the extracted files, and then click **OK**.

   The firmware image is a file similar to `ilo3_<yyy>.bin`, where `<yyy>` represents the firmware version.

Updating the iLO firmware by using a browser

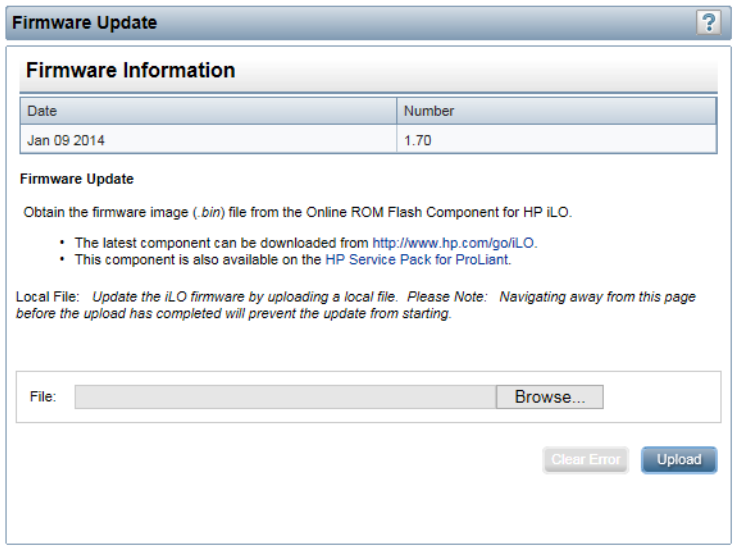
You can update the iLO firmware from any network client by using a supported browser. For a list of supported browsers, see "Using the iLO web interface" (page 92).

To update the iLO firmware:

1. Obtain the firmware image file. For instructions, see "Obtaining the iLO firmware image file" (page 26).
2. Navigate to the **Administration→iLO Firmware** page.

   The **Firmware Update** page opens, as shown in Figure 8 (page 27).

Figure 8 Firmware Update page



3. Click **Browse** (Internet Explorer or Firefox) or **Choose File** (Chrome), and then specify the location of the firmware image file in the **File** box.
4. Click **Upload** to start the update process.

   The firmware update will not start if you navigate away from the **Firmware Update** page before the upload is complete.

   The iLO firmware receives, validates, and then flashes the firmware image. After the firmware flashes and resets, iLO logs you out and the browser reconnects.

IMPORTANT: Do not interrupt a firmware update. If a firmware update is interrupted or fails, attempt it again immediately. Do not reset iLO before reattempting the update.

5. To start working with the updated firmware, clear your browser cache, and then log in to iLO.

If an error occurs during a firmware update, see "Unable to upgrade iLO firmware" (page 228).

If an iLO firmware update is corrupted or canceled, and iLO is corrupted, see "iLO network Failed Flash Recovery" (page 229).

Using language packs

Language packs enable you to easily switch the iLO web interface from English to a supported language of your choice. Language packs currently provide translations for the iLO web interface, .NET IRC, and Java IRC.

Consider the following when using language packs:

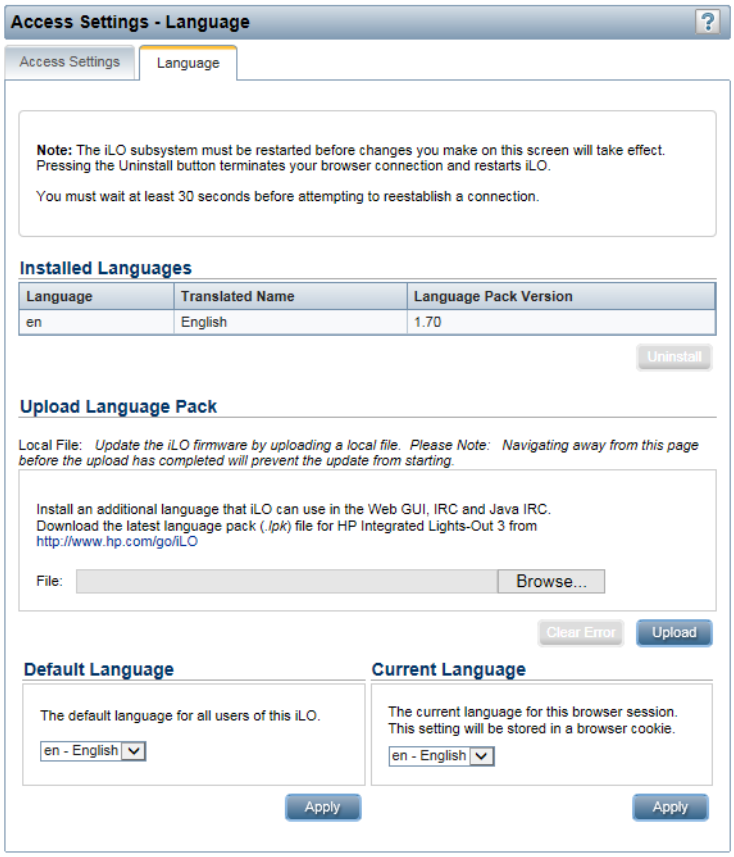
- You must have the Configure iLO Settings privilege to install a language pack.
- You can install one additional language pack at a time. Uploading a new language pack replaces the currently installed language pack, regardless of the language pack version.
- The language pack firmware is independent of the iLO firmware. Setting iLO to the factory default settings does not remove an installed language pack.
- The Java IRC and .NET IRC use the language of the current iLO session.
- For localization support with the Java IRC on Windows systems, you must select the correct language in the **Regional and Language Options** Control Panel.
- For localization support with the Java IRC on Linux systems, make sure that the fonts for the specified language are installed and available to the JRE.
- If an installed language pack does not include the translation for a text string, the text is displayed in English.
- When you update the iLO firmware, HP recommends downloading the latest language pack to ensure that the language pack contents match the iLO web interface.

  iLO 3 firmware version 1.50 or later requires version 1.50 or later of the iLO language pack.
- iLO uses the following process to determine the language of your session:
  1. If you previously logged in to the iLO web interface on the same computer using the same browser, and you have not cleared the cookies, the language setting of the last session with that iLO processor is used.
  2. If there is no cookie, the current browser language is used if it is supported by iLO and the required language pack is installed. The supported languages are English (en), Japanese (ja), and Simplified Chinese (zh).
  3. **Internet Explorer only**: If the browser language is not supported, the OS language is used if the language is supported by iLO, and the required language pack is installed.
  4. If there is no cookie, and the browser or OS language is not supported, iLO uses the configured default language. For more information, see "Configuring the default language settings" (page 30).

Installing a language pack

1. Navigate to the iLO software download website: http://www.hp.com/support/ilo3.
2. Download the language pack to your local computer.
3. Navigate to the **Administration→Access Settings→Language** page, as shown in Figure 9 (page 29).

Figure 9 Access Settings – Language page



4. Click **Browse** (Internet Explorer or Firefox) or **Choose File** (Chrome) in the **Upload Language Pack** section.
5. Select the downloaded language pack, and then click **Open**.

   The following message appears:

   ```
   Only one language pack is supported at a time. If a language pack is already installed, it will be replaced with this upload. iLO will automatically reboot after installing the new language pack. Are you sure you want to install now?
   ```

6. Click **OK** to continue.

   If you have a previously installed language pack, this language pack will replace it.
7. Click **Upload**.

   iLO will automatically reboot after installing a language pack. This will end your browser connection with iLO.

   Wait at least 30 seconds before you attempt to re-establish a connection.

Selecting a language pack

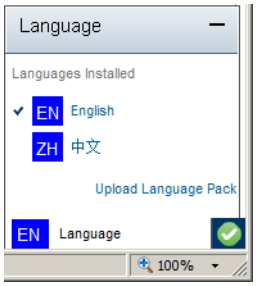
After you have installed a language pack, you can select it in the following ways:

- From the login page, as shown in Figure 10 (page 30).

Figure 10 Login page Language menu

- From the toolbar located on the bottom right side of the iLO web interface, as shown in Figure 11 (page 30).

Figure 11 Toolbar Language menu



- From the **Administration→Access Settings→Language** page. For instructions, see "Configuring the current language settings" (page 30).

Configuring the default language settings

To set the default language for the users of this instance of the iLO firmware:

1. Navigate to the **Administration→Access Settings→Language** page, as shown in Figure 9 (page 29).
2. Select a value in the **Default Language** menu.

   The available languages are English and any other language for which a language pack is installed.
3. Click **Apply**.

Configuring the current language settings

To set the current language of this browser session:

1. Navigate to the **Administration→Access Settings→Language** page, as shown in Figure 9 (page 29).
2. Select a value in the **Current Language** menu.

   The available languages are English and any other language for which a language pack is installed.
3. Click **Apply**.

Uninstalling a language pack

1. Navigate to the **Administration→Access Settings→Language** page, as shown in Figure 9 (page 29).
2. Click the **Uninstall** button in the **Installed Languages** section.

   The following message appears:

   ```
   Applying new settings requires an iLO reset.
   Would you like to apply the new settings and reset iLO now?
   ```

3. Click **OK** to continue.

   iLO resets and closes your browser connection.

   Wait at least 30 seconds before you attempt to re-establish a connection.

iLO licensing

HP iLO standard features are included in every HP ProLiant server to simplify server setup, engage health monitoring, monitor power and thermal control, and promote remote administration.

HP iLO Advanced and HP iLO Advanced for BladeSystem licenses activate functionality such as graphical Remote Console with multiuser collaboration, video record/playback, and many more advanced features.

Unlocking iLO licensed features has never been easier. Simply choose and install the license that best suits your company's infrastructure.

iLO Advanced—Enables the full set of iLO features.

- iLO Advanced Single Server License
- iLO Advanced Electronic License
- iLO Advanced Flexible Quantity License
- iLO Advanced Volume License

For details on purchasing licenses, see the following website: http://www.hp.com/go/ilo/licensing.

For a list of the features that are included with each license, see "iLO license options" (page 238).

Consider the following about iLO licenses:

- iLO licenses are versionless, meaning, regardless of the version of iLO you have enabled (iLO 2, iLO 3, or iLO 4), an iLO license can be applied. For features that are specific to the version of iLO on your ProLiant server, see "iLO license options" (page 238).
- If you purchase an iLO license with any Insight Control software suite, HP provides the Technical Support and Update Service. For more information, see "Support and other resources" (page 235).
- If you purchase an iLO license as a one-time activation of licensed features, you must purchase future functional upgrades.
- One iLO license is required for each server on which the product is installed and used. Licenses are not transferable. You cannot license an HP ProLiant SL/ML/DL server by using a BladeSystem license.
- HP will continue to provide maintenance releases with fixes, as well as iLO standard feature enhancements, at no extra charge.

Free iLO 60-day evaluation license

A free iLO evaluation license is available for download from the following HP website: http://www.hp.com/go/tryinsightcontrol .

When using an evaluation license, note the following:

- The evaluation license activates and enables access to iLO licensed features.
- The evaluation license key is a 10-seat key, meaning it can be used on 10 different servers.
- When the evaluation period has expired, your iLO system will return to the standard functionality.

- Only one evaluation license can be installed for each iLO system. The iLO firmware will not accept the reapplication of an evaluation license.
- The evaluation license expires 60 days after the installation date. HP will notify you by email when your license is about to expire.

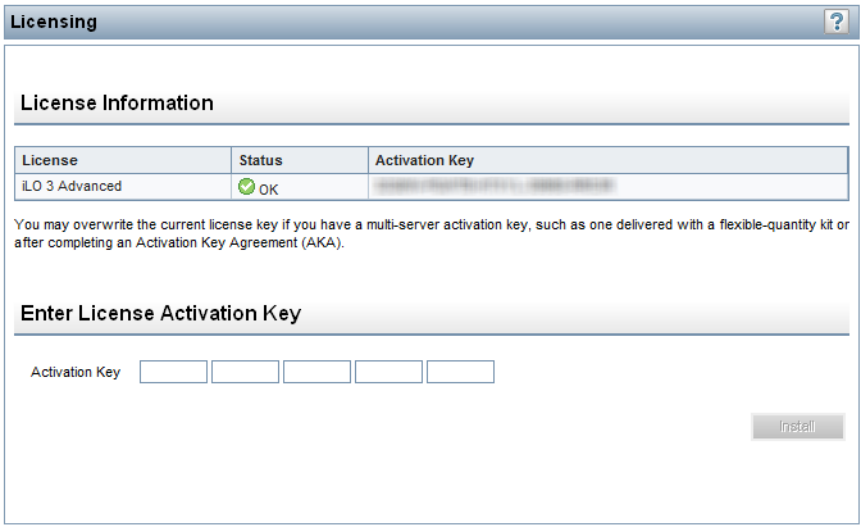
Installing an iLO license by using a browser

You must have the Configure iLO Settings privilege to install a license.

1. Navigate to the **Administration→Licensing** page in the iLO web interface.

   The **Licensing** page opens, as shown in Figure 12 (page 32).

Figure 12 Licensing page



2. Review the license agreement provided with your HP License Pack option kit.
3. Enter the license key in the **Activation Key** boxes.

   Press the **Tab** key or click inside a box to move between boxes. The cursor advances automatically when you enter the license key in the **Activation Key** boxes.
4. Click **Install**.

   The EULA confirmation opens. The EULA details are available in the HP License Pack option kit.
5. Click **OK**.

   The license key is now enabled.

For tips on troubleshooting license installation, see "Troubleshooting license installation" (page 218).

Managing iLO users by using the iLO web interface

The iLO firmware enables you to manage user accounts stored locally in the secure iLO memory and directory group accounts. Use MMC or ConsoleOne to manage directory-based user accounts.

iLO supports up to 12 users with customizable access rights, login names, and advanced password encryption. Privileges control individual user settings, and can be customized to meet user access requirements.

To support more than 12 users, you must have an iLO license, which enables integration with an unlimited number of directory-based user accounts. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.

The following privileges are required for user and directory group administration:

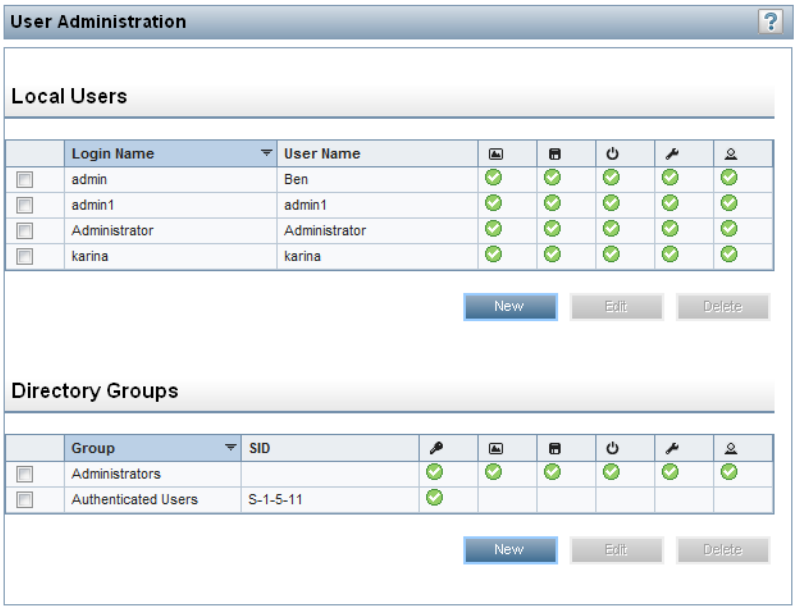
- **Administer User Accounts**—Required for adding, modifying, and deleting users. If you do not have this privilege, you can view your own settings and change your password.
- **Configure iLO Settings**—Required for adding, modifying, and deleting directory groups. If you do not have this privilege, you can view directory groups.

NOTE: You can also manage users with the iLO RBSU. For more information, see "Managing iLO users by using iLO RBSU" (page 18).

Viewing local user accounts

To view local users, navigate to the **Administration→User Administration** page, as shown in Figure 13 (page 33).

Figure 13 User Administration page



The **Local Users** table shows the login names, user names, and assigned privileges of each configured user. Move the cursor over an icon to see the privilege name. The available privileges follow:

- **Remote Console Access**—Enables a user to remotely access the host system Remote Console, including video, keyboard, and mouse control.
- **Virtual Media**—Enables a user to use the Virtual Media feature on the host system.
- **Virtual Power and Reset**—Enables a user to power-cycle or reset the host system. These activities interrupt the system availability. A user with this privilege can diagnose the system by using the **Generate NMI to System** button.
- **Configure iLO Settings**—Enables a user to configure most iLO settings, including security settings, and to remotely update the iLO firmware. This privilege does not enable local user account administration.

  After iLO is configured, revoking this privilege from all users prevents reconfiguration using the web interface, HPQLOCFG, or the CLI. Users who have access to iLO RBSU and HPONCFG

can still reconfigure iLO. Only a user who has the Administer User Accounts privilege can enable or disable this privilege.

- **Administer User Accounts**—Enables a user to add, edit, and delete local iLO user accounts. A user with this privilege can change privileges for all users. If you do not have this privilege, you can view your own settings and change your own password.

Viewing directory groups

To view directory groups, navigate to the **Administration→User Administration** page, as shown in Figure 13 (page 33).

The **Directory Groups** table shows the group DN, group SID, and the assigned privileges for the configured groups. Move the cursor over an icon to see the privilege name. The available privileges follow:

- **Login Privilege**—Enables members of a group to log in to iLO.
- **Remote Console Access**—Enables users to remotely access the host system Remote Console, including video, keyboard, and mouse control.
- **Virtual Media**—Enables users to use the Virtual Media feature on the host system.
- **Virtual Power and Reset**—Enables users to power-cycle or reset the host system. These activities interrupt the system availability. Users with this privilege can diagnose the system by using the **Generate NMI to System** button.
- **Configure iLO Settings**—Enables users to configure most iLO settings, including security settings, and to remotely update iLO firmware.

  After iLO is configured, revoking this privilege from all users prevents reconfiguration using the web interface, HPQLOCFG, or the CLI. Users who have access to iLO RBSU and HPONCFG can still reconfigure iLO. Only a user who has the Administer User Accounts privilege can enable or disable this privilege.
- **Administer User Accounts**—Enables users to add, edit, and delete local iLO user accounts.

Adding or editing local user accounts

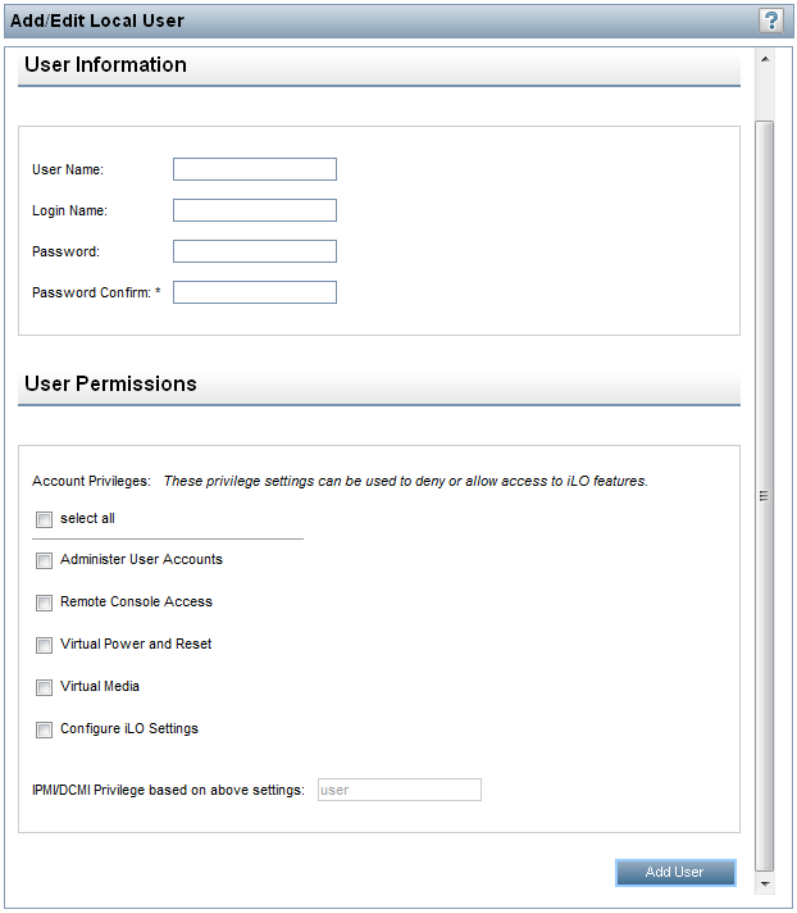
Users who have the Administer User Accounts privilege can add or edit iLO users.

To add or edit a local user:

1. Navigate to the **Administration→User Administration** page, as shown in Figure 13 (page 33).
2. Do one of the following:
   - Click **New** in the **Local Users** section.
   - Select a user in the **Local Users** section, and then click **Edit**.

   The **Add/Edit Local User** page opens, as shown in Figure 14 (page 35).

Figure 14 Add/Edit Local User page



3. Provide the following details in the **User Information** section:
   - **User Name** appears in the user list on the **User Administration** page. It does not have to be the same as the **Login Name**. The maximum length for a user name is 39 characters. The user name must use printable characters. Assigning descriptive user names can help you to easily identify the owner of each login name.
   - **Login Name** is the name you use when logging in to iLO. It appears in the user list on the **User Administration** page, on the **iLO Overview** page, and in iLO logs. The **Login Name** does not have to be the same as the **User Name**. The maximum length for a login name is 39 characters. The login name must use printable characters.
   - **Password** and **Password Confirm** set and confirm the password that is used for logging in to iLO. The minimum length for a password is set on the **Access Settings** page (Figure 16). The maximum length for a password is 39 characters. Enter the password twice for verification.

     For more information about passwords, see "Password guidelines" (page 36).
4. Select from the following privileges.
   - **Remote Console Access**
   - **Virtual Media**
   - **Virtual Power and Reset**
   - **Configure iLO Settings**
   - **Administer User Accounts**

TIP: Click the **select all** check box to select all of the available user privileges.

For more information about each privilege, see "Viewing local user accounts" (page 33).

5. Do one of the following:
   - Click **Add User** to save the new user.
   - Click **Update User** to save the user account changes.

Password guidelines

HP recommends that you follow these password guidelines:

- Passwords should:
  - Never be written down or recorded
  - Never be shared with others
  - Not be words found in a dictionary
  - Not be obvious words, such as the company name, product name, user name, or login name
- Passwords should have at least three of the following characteristics:
  - One numeric character
  - One special character
  - One lowercase character
  - One uppercase character

Depending on the **Minimum Password Length** setting on the **Access Settings** page, the password can have a minimum of zero characters (no password) and a maximum of 39 characters. The default **Minimum Password Length** is eight characters.

IMPORTANT: HP does not recommend setting the **Minimum Password Length** to fewer than eight characters unless you have a physically secure management network that does not extend outside the secure data center. For information about setting the **Minimum Password Length**, see "Configuring access options" (page 40).

IPMI/DCMI users

The iLO firmware follows the IPMI 2.0 specification. When you are adding IPMI/DCMI users, the login name must be a maximum of 16 characters, and the password must be a maximum of 20 characters.

When you select iLO user privileges, the equivalent IPMI/DCMI user privilege is displayed in the **IPMI/DCMI Privilege based on above settings** box.

- **User**—A user has read-only access. A user cannot configure or write to iLO, or perform system actions.

  For IPMI User privileges: Disable all privileges. Any combination of privileges that does not meet the Operator level is an IPMI User.

- **Operator**—An operator can perform system actions, but cannot configure iLO or manage user accounts.

  For IPMI Operator privileges: Enable Remote Console Access, Virtual Power and Reset, and Virtual Media. Any combination of privileges greater than Operator that does not meet the Administrator level is an IPMI Operator.

- **Administrator**—An administrator has read and write access to all features.

  For IPMI Administrator privileges: Enable all privileges.

Administering directory groups

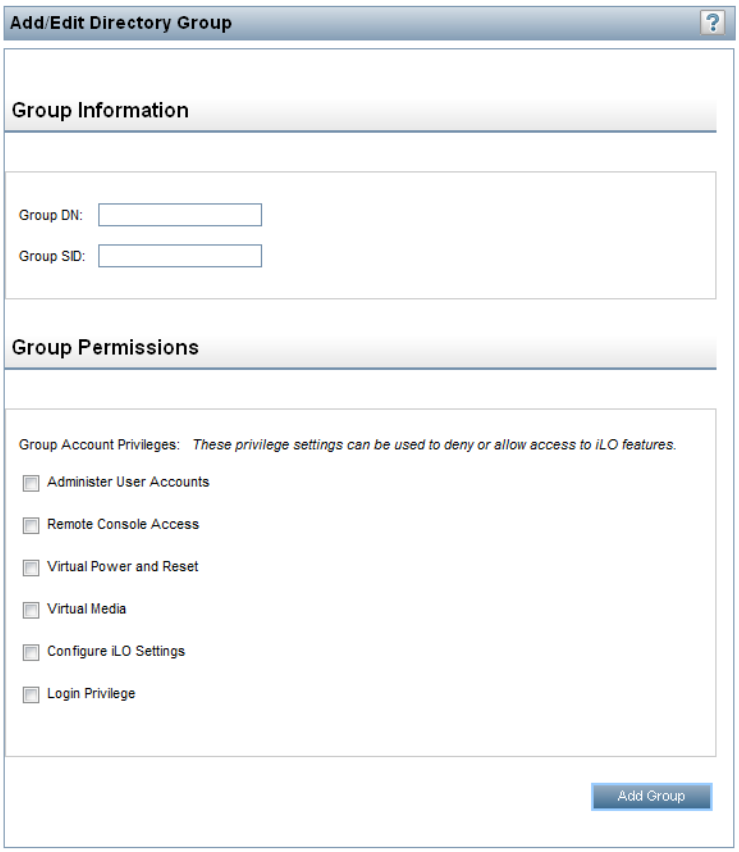
iLO enables you to view iLO groups and modify settings for those groups. You must have the Configure iLO Settings privilege to add or edit directory groups. Use the **Add/Edit Directory Group** page to add or edit iLO directory groups.

To add or edit a directory group:

1. Navigate to the **Administration→User Administration** page, as shown in Figure 13 (page 33).
2. Do one of the following:
   - Click **New** in the **Directory Groups** section.
   - Select a group in the **Directory Groups** section, and then click **Edit**.

   The **Add/Edit Directory Group** page opens, as shown in Figure 15 (page 38).

Figure 15 Add/Edit Directory Group page



3. Provide the following details in the **Group Information** section:
   - **Group DN** (Security Group DN)—DN of a group in the directory. Members of this group are granted the privileges set for the group. The specified group must exist in the directory, and users who need access to iLO must be members of this group. Enter a DN from the directory (for example, CN=Group1, OU=Managed Groups, DC=domain, DC=extension).

     Shortened DNs are also supported (for example, Group1). The shortened DN is not a unique match. Any group named Group1 is displayed. HP recommends using the fully qualified DN.
   - **Group SID** (Security ID)—Microsoft Security ID is used for Kerberos and LDAP group authorization. This is required for Kerberos. The format is S-1-5-2039349.
4. Select from the following privileges when you are adding or editing a group account:
   - **Login Privilege**
   - **Remote Console Access**
   - **Virtual Media**
   - **Virtual Power and Reset**
   - **Configure iLO Settings**
   - **Administer User Accounts**

   For more information about each privilege, see "Viewing directory groups" (page 34).
5. Do one of the following:
   - Click **Add Group** to save the new directory group.
   - Click **Update Group** to save the directory group changes.

Deleting a user account or a directory group

The privilege required for this procedure depends on the user account type.

- To delete a local user account, the Administer User Accounts privilege is required.
- To delete a directory group, the Configure iLO Settings privilege is required.

To delete an existing user account or directory group:

1. Navigate to the **Administration→User Administration** page, as shown in Figure 13 (page 33).
2. Select the check box next to the user or group that you want to delete.
3. Click **Delete**.

   A pop-up window opens with one of the following messages:

   - Local user: `Are you sure you want to delete the selected user(s)? Warning: Always leave at least one administrator.`
   - Directory group: `Are you sure you want to delete the selected group(s)?`
4. Click **OK**.

Configuring iLO access settings

You can modify iLO access settings, including service, IPMI/DCMI, and access options. The values that you enter on the **Access Settings** page apply to all iLO users. You must have the Configure iLO Settings privilege to modify access settings.

The default configuration is suitable for most operating environments. The values that you can modify on the **Access Settings** page allow complete customization of the iLO external access methods for specialized environments.

Configuring service settings

The **Service** section shows the SSH Access setting and the TCP/IP port values.

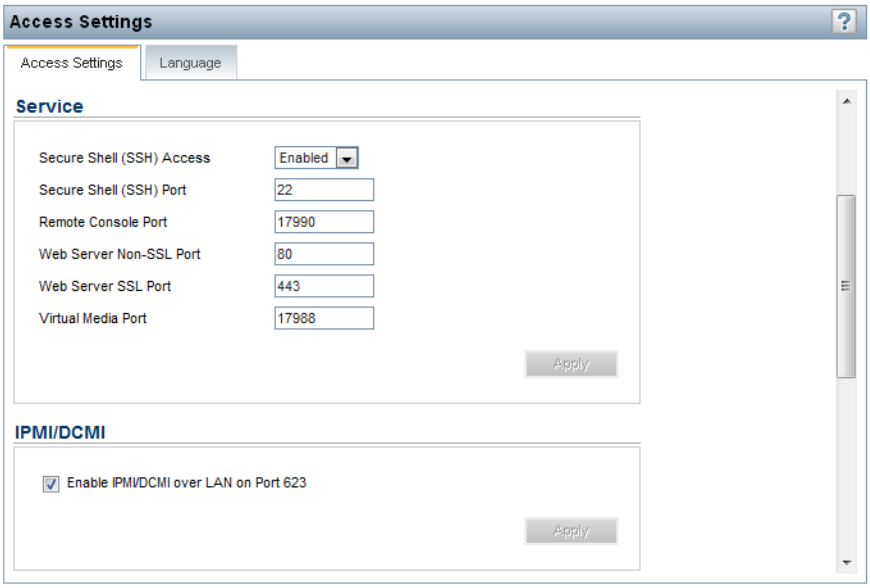
The TCP/IP ports used by iLO are configurable, which enables compliance with any site requirements or security initiatives for port settings. These settings do not affect the host system.

Changing these settings usually requires configuration of the web browser used for standard and SSL communication. When these settings are changed, iLO initiates a reset to activate the changes.

To configure **Service** settings:

1. Navigate to the **Administration→Access Settings** page, as shown in Figure 16 (page 40)

Figure 16 Access Settings page



2. Update the following settings as needed:

Table 1 Service settings

Service setting	Default value
Secure Shell (SSH) Access	Enables you to specify whether the SSH feature on iLO is enabled or disabled. SSH provides encrypted access to the iLO CLP. The default is **Enabled**.
Secure Shell (SSH) Port	**22**
Remote Console Port	**17990**
Web Server Non-SSL Port (HTTP)	**80**
Web Server SSL Port (HTTPS)	**443**
Virtual Media Port	**17988**

3. Click **Apply** to end your browser connection and restart iLO.
   Wait at least 30 seconds before you attempt to re-establish a connection.

Configuring IPMI/DCMI settings

iLO enables you to send industry-standard IPMI and DCMI commands over the LAN. The IPMI/DCMI port is set to 623 and is not configurable.

To enable or disable IPMI/DCMI, select or clear the **Enable IPMI/DCMI over LAN on Port 623** check box, and then click **Apply**.

- **Enabled** (default)—Enables you to send IPMI/DCMI commands over the LAN by using a client-side application.
- **Disabled**—Disables IPMI/DCMI over the LAN. Server-side IPMI/DCMI applications are still functional when IPMI/DCMI over LAN is disabled.

Configuring access options

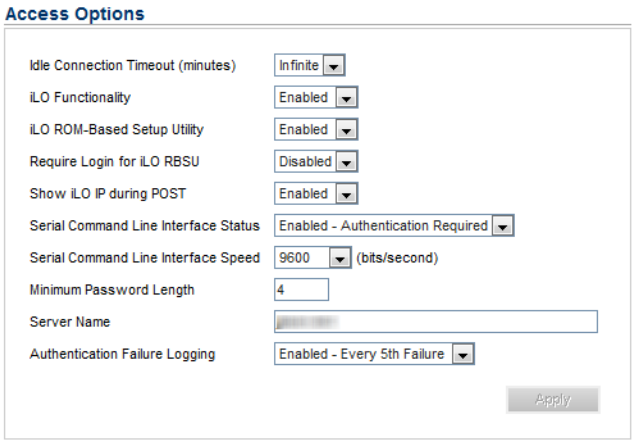
The **Access Options** section enables you to modify settings that affect all iLO users.

NOTE: You can configure some of these settings by using iLO RBSU. For instructions, see "Using the iLO RBSU" (page 87).

To view or modify iLO access options:

1. Navigate to the **Administration→Access Settings** page.
2. Click the **Access Settings** tab and scroll to the **Access Options** section of the **Access Settings** page, as shown in Figure 17 (page 41).

Figure 17 Access Options



3. Update the following settings as needed:

Table 2 Access options

Option	Default value	Description
Idle Connection Timeout (minutes)	**30**	This setting specifies how long a user can be inactive, in minutes, before the iLO web interface and Remote Console session end automatically. The following settings are valid: **15**, **30**, **60**, or **120** minutes, or **Infinite**. Inactive users are not logged out when this option is set to **Infinite**. Failure to log out of iLO by either browsing to a different site or closing the browser also results in an idle connection. The iLO firmware supports a finite number of iLO connections. Misuse of the **Infinite** timeout option might make iLO inaccessible to other users. Idle connections are recycled after they time out. This setting applies to local and directory users. Directory server timeouts might preempt the iLO setting. Changes to the setting might not take effect immediately in current user sessions, but will be enforced immediately in all new sessions.
iLO Functionality	**Enabled**	The iLO network and communications with operating system drivers are terminated when iLO functionality is disabled. If iLO functionality is disabled (including the iLO Diagnostic Port), you must use the server Security Override Switch to enable iLO. See the server documentation to locate the Security Override Switch, and then set it to **Override**. Power up the server, and then use the iLO RBSU to set **iLO Functionality** to **Enabled**. **NOTE:** The iLO functionality cannot be disabled on blade servers.

Table 2 Access options *(continued)*

Option	Default value	Description
iLO ROM-Based Setup Utility	**Enabled**	This setting enables or disables iLO RBSU. The iLO Option ROM prompts you to press **F8** to start iLO RBSU, but if iLO is disabled or iLO RBSU is disabled, this prompt is not displayed.
Require Login for iLO RBSU	**Disabled**	This setting determines whether a user-credential prompt is displayed when a user accesses iLO RBSU. If this setting is **Enabled**, a login dialog box opens when you access the iLO RBSU.
Show iLO IP during POST	**Enabled**	This setting enables the display of the iLO network IP address during host server POST.
Serial Command Line Interface Status	**Enabled-Authentication Required**	This setting enables you to change the login model of the CLI feature through the serial port. The following settings are valid: • **Enabled-Authentication Required**—Enables access to the iLO CLP from a terminal connected to the host serial port. Valid iLO user credentials are required. • **Enabled-No Authentication**—Enables access to the iLO CLP from a terminal connected to the host serial port. iLO user credentials are not required. • **Disabled**—Disables access to the iLO CLP from the host serial port. Use this option if you are planning to use physical serial devices.
Serial Command Line Interface Speed	**9600**	This setting enables you to change the speed of the serial port for the CLI feature. The following speeds (in bits per second) are valid: **9600**, **19200**, **57600**, and **115200**. The serial port configuration must be set to no parity, 8 data bits, and 1 stop bit (N/8/1) for correct operation.
Minimum Password Length	**8**	This setting specifies the minimum number of characters allowed when a user password is set or changed. The character length must be a value from 0 to 39.
Server Name	—	This setting enables you to specify the host server name. You can assign this value manually, but it might be overwritten by the host software when the operating system loads. You can enter a server name that is up to 49 bytes. To force the browser to refresh, save this setting, and then press **F5**.
Authentication Failure Logging	**Enabled-Every 3rd Failure**	This setting enables you to configure logging criteria for failed authentications. All login types are supported; each login type works independently. The following are valid settings: • **Enabled-Every Failure**—A failed login log entry is recorded after every failed login attempt. • **Enabled-Every 2nd Failure**—A failed login log entry is recorded after every second failed login attempt. • **Enabled-Every 3rd Failure**—A failed login log entry is recorded after every third failed login attempt. • **Enabled-Every 5th Failure**—A failed login log entry is recorded after every fifth failed login attempt. • **Disabled**—No failed login log entry is recorded. For information about using this setting with SSH clients, see "Logging in to iLO by using an SSH client" (page 43).

4. Click **Apply** to end your browser connection and restart iLO.
   Wait at least 30 seconds before you attempt to re-establish a connection.

Logging in to iLO by using an SSH client

When a user logs in to iLO by using an SSH client, the number of login name and password prompts displayed by iLO matches the value of the **Authentication Failure Logging** option (3 if it is disabled). The number of prompts might also be affected by your SSH client configuration. SSH clients also implement delays after login failure.

For example, to generate an SSH authentication failure log with the default value (**Enabled-Every 3rd Failure**), assuming that the SSH client is configured with the number of password prompts set to 3, three consecutive login failures occur as follows:

1. Run the SSH client and log in with an incorrect login name and password.

   You receive three password prompts. After the third incorrect password, the connection ends and the first login failure is recorded. The SSH login failure counter is set to 1.
2. Run the SSH client and log in with an incorrect login name and password.

   You receive three password prompts. After the third incorrect password, the connection ends and the second login failure is recorded. The SSH login failure counter is set to 2.
3. Run the SSH client and log in with an incorrect login name and password.

   You receive three password prompts. After the third incorrect password, the connection ends and the third login failure is recorded. The SSH login failure counter is set to 3.

The iLO firmware records an SSH failed login log entry, and sets the SSH login failure counter to 0.

Configuring iLO security

iLO provides the following security features:

- User-defined TCP/IP ports. For more information, see "Configuring iLO access settings" (page 39).
- User actions logged in the iLO Event Log. For more information, see "Using the iLO Event Log" (page 106).
- Progressive delays for failed login attempts. For more information, see "Login security" (page 46).
- Support for X.509 CA signed certificates. For more information, see "Administering SSL certificates" (page 48).
- Support for securing iLO RBSU. For more information, see "iLO RBSU security" (page 44).
- Encrypted communication that uses SSL certificate administration. For more information, see "Administering SSL certificates" (page 48).
- Support for optional LDAP-based directory services. For more information, see "Directory services" (page 160).

Some of these options are licensed features. For more information, see "iLO licensing" (page 31).

General security guidelines

General security guidelines for iLO follow:

- For maximum security, configure iLO on a separate management network. For more information, see "Connecting iLO to the network" (page 16).
- Do not connect iLO directly to the Internet.
- Use a browser that has a 128-bit cipher strength.

iLO RBSU security

iLO RBSU enables you to view and modify the iLO configuration. You can configure iLO RBSU access settings by using iLO RBSU, a web browser, RIBCL scripts, or the iLO Security Override Switch.

- For information about using a web browser to configure iLO RBSU access settings, see "Configuring access options" (page 40).
- For information about using iLO RBSU to configure iLO RBSU access settings, see "Using the iLO RBSU" (page 87).
- For information about using RIBCL scripts to configure iLO RBSU, see the *HP iLO 3 Scripting and Command Line Guide*.
- For information about using the iLO Security Override Switch to access iLO RBSU , see "iLO Security Override Switch administration" (page 44).

iLO RBSU has the following security levels:

- **Login Not Required** (default)

  Anyone who has access to the host during POST can enter iLO RBSU to view and modify configuration settings. This is an acceptable setting if host access is controlled. If host access is not controlled, any user can make changes by using the active configuration menus.

- **Login Required** (more secure)

  If iLO RBSU login is required, the active configuration menus are controlled by the authenticated user access rights.

- **Disabled** (most secure)

  If iLO RBSU is disabled, user access is prohibited. This prevents modification by using the iLO RBSU .

To change the login requirement:

- Use the iLO web interface to edit the **Require Login for iLO RBSU** setting. For instructions, see "Configuring access options" (page 40).
- Use the iLO RBSU to edit the **Require iLO 3 RBSU Login** setting. For instructions, see "Using the iLO RBSU" (page 87).

To enable or disable access to iLO RBSU:

- Use the iLO web interface to edit the **iLO ROM-Based Setup Utility** setting. For instructions, see "Configuring access options" (page 40).
- Use the iLO RBSU to edit the **iLO 3 ROM-Based Setup Utility** setting. For instructions, see "Using the iLO RBSU" (page 87).

iLO Security Override Switch administration

The iLO Security Override Switch grants the administrator full access to the iLO processor. This access might be necessary for any of the following conditions:

- iLO has been disabled and must be re-enabled.
- All user accounts that have the Administer User Accounts privilege are locked out.
- An invalid configuration prevents iLO from being displayed on the network, and iLO RBSU is disabled.
- The boot block must be flashed.
- The iLO NIC is turned off, and running iLO RBSU to turn it back on is not possible or convenient.
- Only one user name is configured, and the password is forgotten.

Ramifications of setting the iLO Security Override Switch include the following:

- All security authorization verifications are disabled when the switch is set.
- iLO RBSU runs if the host server is reset.
- iLO is not disabled and might be displayed on the network as configured.
- iLO, if disabled when the switch is set, does not log out the user and complete the disable process until the power is cycled on the server.
- The boot block is exposed for programming.
- A warning message is displayed on iLO web interface pages, indicating that the switch is currently in use.
- An iLO log entry records the use of the switch.

When iLO boots after you set or clear the iLO Security Override Switch, an SNMP alert is sent if an SNMP Alert Destination is configured.

Setting the iLO Security Override Switch enables you to flash the iLO boot block. HP does not anticipate that you will need to update the boot block. However, if an update is required, you must be physically present at the server to reprogram the boot block and reset iLO. The boot block is exposed until iLO is reset. For maximum security, HP recommends disconnecting iLO from the network until the reset is complete. You must open the server enclosure to access the iLO Security Override Switch.

To set the iLO Security Override Switch:

1. Power off the server.
2. Set the switch.
3. Power on the server.

Reverse this procedure to clear the iLO Security Override Switch.

Depending on the server, the iLO Security Override Switch might be a single jumper or a specific switch position on a DIP switch panel. For information about accessing the iLO Security Override Switch, see the server documentation or use the diagrams on the server access panel.

TPM support

A TPM is a computer chip that securely stores artifacts used to authenticate the platform. These artifacts can include passwords, certificates, or encryption keys. You can also use a TPM to store platform measurements to make sure that the platform remains trustworthy.

On a supported system, iLO decodes the TPM record and passes the configuration status to iLO, the CLP, and the XML interface. The **iLO Overview** page displays the following TPM status information:

- **Not Supported**—A TPM is not supported.
- **Not Present**—A TPM is not installed.
- **Present**—This indicates one of the following statuses:
  - A TPM is installed but is disabled.
  - A TPM is installed and enabled.
  - A TPM is installed and enabled, and Expansion ROM measuring is enabled. If Expansion ROM measuring is enabled, the **Update Firmware** page displays a legal warning message when you click **Upload**.

User accounts and access

iLO supports the configuration of up to 12 local user accounts. Each account can be managed through the following features:

- Privileges
- Login security

You can configure iLO to use a directory to authenticate and authorize its users. This configuration enables an unlimited number of users and easily scales to the number of iLO devices in an enterprise. The directory also provides a central point of administration for iLO devices and users, and the directory can enforce a stronger password policy. iLO enables you to use local users, directory users, or both.

The following directory configuration options are available:

- A directory extended with HP schema
- The directory default schema

For more information about using directory authentication, see "Directory services" (page 160).

User privileges

iLO allows you to control user account access to iLO features through the use of privileges. When a user attempts to use a feature, iLO verifies that the user has the proper privilege to use that feature.

For information about the available user account and directory group privileges, see "Managing iLO users by using the iLO web interface" (page 32).

Login security

iLO provides several login security features. After an initial failed login attempt, iLO imposes a delay of ten seconds. Each subsequent failed attempt increases the delay by ten seconds. An information page is displayed during each delay; this continues until a valid login occurs. This feature helps to prevent dictionary attacks against the browser login port.

iLO saves a detailed log entry for failed login attempts. You can configure the Authentication Failure Logging frequency on the **Administration→Access Settings** page. For more information, see "Configuring access options" (page 40).

Administering SSH keys

The **Secure Shell Key** page displays the hash of the SSH public key associated with each user. Each user can have only one key assigned. Use this page to view, add, or delete SSH keys.

You must have the Administer User Accounts privilege to add and delete SSH keys.

About SSH keys

When you add an SSH key to iLO, you paste the SSH key file into iLO as described in "Authorizing a new SSH key" (page 47). The file must contain the user-generated public key. The iLO firmware associates each key with the selected local user account. If a user is removed after an SSH key is authorized for that user, the SSH key is removed.

A sample SSH key file follows:

```
ssh-dss AAAAB3......wHM Administrator
```

In this sample, `ssh-dss AAAAB3.....wHM` is the public key, and `Administrator` is a local iLO user account.

Note the following when working with SSH keys:

- Any SSH connection authenticated through the corresponding private key is authenticated as the owner of the key and has the same privileges.
- The iLO firmware provides storage to accommodate SSH keys that have a length of 639 bytes or less. If the key is larger than 639 bytes, the authorization might fail. If this occurs, use the SSH client software to generate a shorter key.
- If you use the iLO web interface to enter the public key, you select the user associated with the public key. If you use the CLI to enter the public key, the public key is linked to the user name that you entered to log in to iLO. If you use HPQLOCFG to enter the public key, you append the iLO user name to the public key data. The public key is stored with that user name.

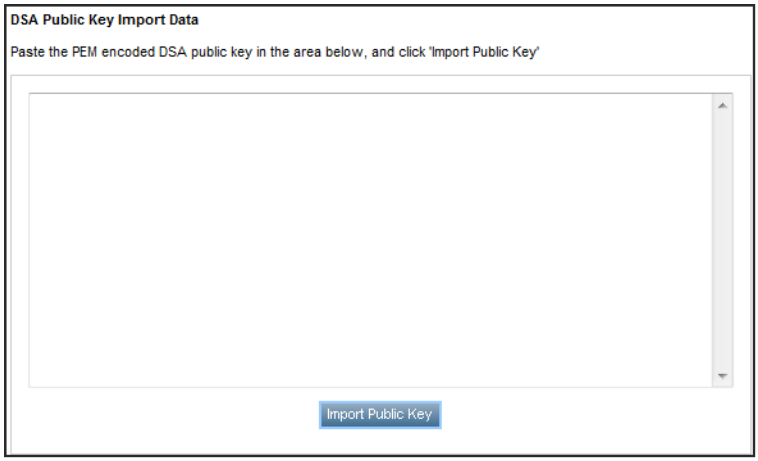
Authorizing a new SSH key

1. Generate a 1,024-bit DSA SSH key by using `ssh-keygen`, `puttygen.exe`, or another SSH key utility.
2. Create the `key.pub` file.
3. Navigate to the **Administration→Security** page.
4. Click the **Secure Shell Key** tab, as shown in Figure 18 (page 47).

Figure 18 Security–Secure Shell Key page

5. Select the check box to the left of the user to which you want to add an SSH key.
6. Click **Authorize New Key**.
7. Copy and paste the public key into the **DSA Public Key Import Data** box as shown in Figure 19 (page 48).

Figure 19 DSA Public Key Import Data box



The key must be a 1,024-bit DSA key.

8. Click **Import Public Key**.

Deleting SSH keys

1. Navigate to the **Administration→Security** page.
2. Click the **Secure Shell Key** tab, as shown in Figure 18 (page 47).
3. Select the check box to the left of the user for which you want to delete an SSH key.
4. Click **Delete Selected Key(s)**.

   The selected SSH key is removed from iLO. When an SSH key is deleted from iLO, an SSH client cannot authenticate to iLO by using the corresponding private key.

Authorizing SSH keys from an HP SIM server

The `mxagentconfig` utility enables you to authorize SSH keys from an HP SIM server.

- SSH must be enabled on iLO before you use `mxagentconfig` to authorize a key.
- The user name and password entered in `mxagentconfig` must correspond to an iLO user who has the Configure iLO Settings privilege. The user can be a directory user or a local user.
- The key is authorized on iLO and corresponds to the user name specified in the `mxagentconfig` command.

For more information about `mxagentconfig`, see the *HP iLO 3 Scripting and Command Line Guide*.

Administering SSL certificates

SSL is a standard for encrypting data so that it cannot be viewed or modified while in transit on the network. SSL uses a key to encrypt and decrypt the data. The longer the key, the better the encryption.

A certificate is a public document that describes the server. It contains the name of the server and the server's public key. Because only the server has the corresponding private key, this is how the server is authenticated.

A certificate must be signed to be valid. If it is signed by a CA, and that CA is trusted, all certificates signed by the CA are also trusted. A self-signed certificate is one in which the owner of the certificate acts as its own CA. Self-signed certificates are the default for HP management products, though they do support certificates signed by certifying authorities.

The iLO firmware enables you to create a certificate request, import a certificate, and view information associated with a stored certificate. Certificate information is encoded in the certificate by the CA and is extracted by iLO.

By default, iLO creates a self-signed certificate for use in SSL connections. This certificate enables iLO to work without additional configuration steps. Importing a trusted certificate can enhance the iLO security features. Users who have the Configure iLO Settings privilege can customize and import a trusted certificate.

Viewing SSL certificate information

To view certificate information, navigate to the **Administration→Security→SSL Certificate** page. The following certificate details are displayed:

- **Issued To**—The entity to which the certificate was issued
- **Issued By**—The CA that issued the certificate
- **Valid From**—The first date that the certificate is valid
- **Valid Until**—The date that the certificate expires
- **Serial Number**—The serial number that the CA assigned to the certificate

Obtaining and importing an SSL certificate

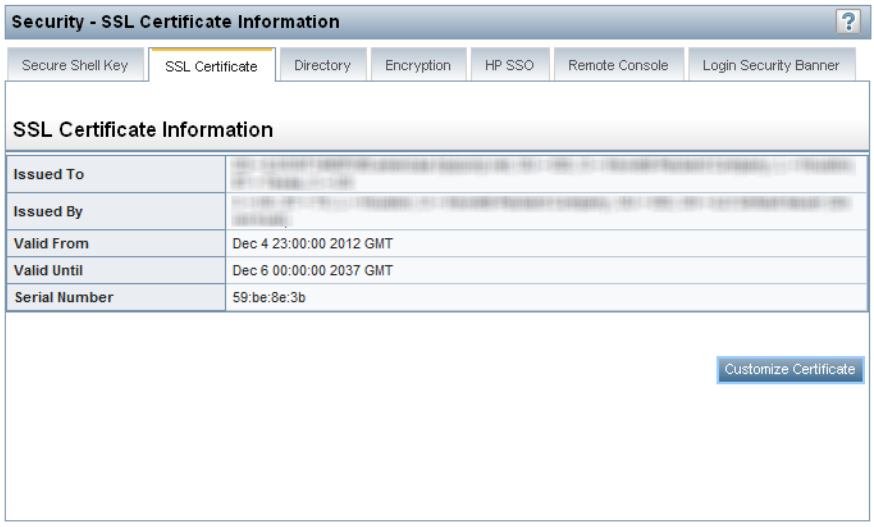
Users who have the Configure iLO Settings privilege can customize and import a trusted certificate.

A certificate works only with the keys generated with its corresponding CSR. If iLO is reset to factory defaults, or another CSR is generated before the certificate that corresponds to the previous CSR is imported, the certificate does not work. In that case, a new CSR must be generated and used to obtain a new certificate from the CA.

To obtain and import a certificate:

1. Navigate to the **Administration→Security→SSL Certificate** page, as shown in Figure 20 (page 49).

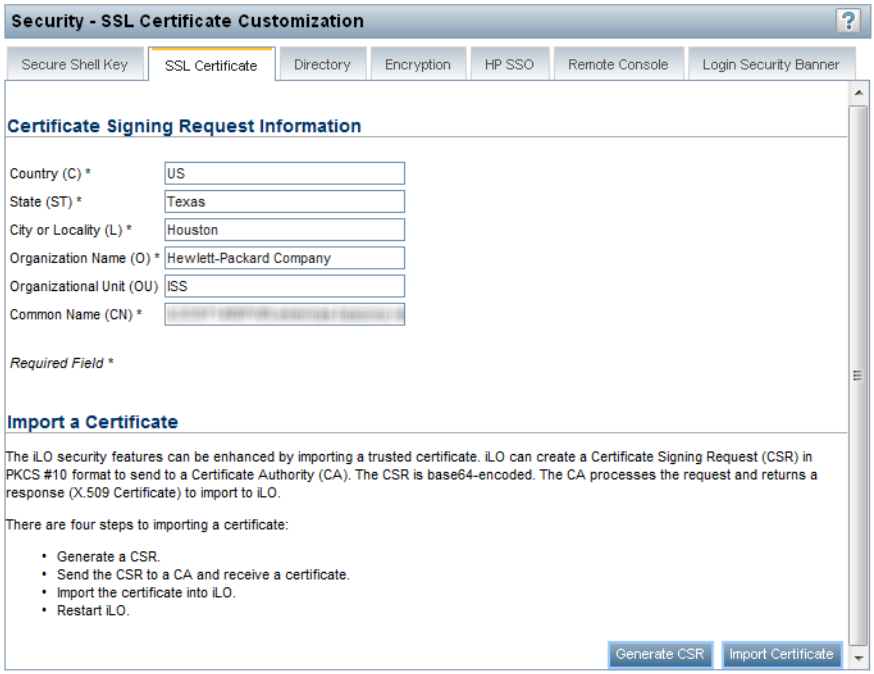
Figure 20 Security–SSL Certificate Information page



2. Click **Customize Certificate**.

   The **SSL Certificate Customization** page opens, as shown in Figure 21 (page 50).

Figure 21 Security–SSL Certificate Customization page



3. Enter the following information in the **Certificate Signing Request Information** section. The required boxes are marked with an asterisk (*) in the iLO web interface.
   - **Country (C)**—The two-character country code that identifies the country where the company or organization that owns this iLO subsystem is located
   - **State (ST)**—The state where the company or organization that owns this iLO subsystem is located
   - **City or Locality (L)**—The city or locality where the company or organization that owns this iLO subsystem is located
   - **Organization Name (O)**—The name of the company or organization that owns this iLO subsystem
   - **Organizational Unit (OU)**—(Optional) The unit within the company or organization that owns this iLO subsystem
   - **Common Name (CN)**—The FQDN of this iLO subsystem
4. Click **Generate CSR**.

   The following message appears:

   ```
   The iLO subsystem is currently generating a Certificate Signing
   Request (CSR). This may take 10 minutes or more. In order to view
   the CSR, wait 10 minutes or more, and then click the Generate CSR
   button again.
   ```
5. After 10 minutes or more, click the **Generate CSR** button again.

   A new window displays the CSR.

   The CSR contains a public and private key pair that validates communications between the client browser and iLO. iLO supports key sizes up to 2,048 bits. The generated CSR is held in memory until a new CSR is generated, iLO is reset, or a certificate is imported.
6. Select and copy the CSR text.
7. Open a browser window and navigate to a third-party CA.

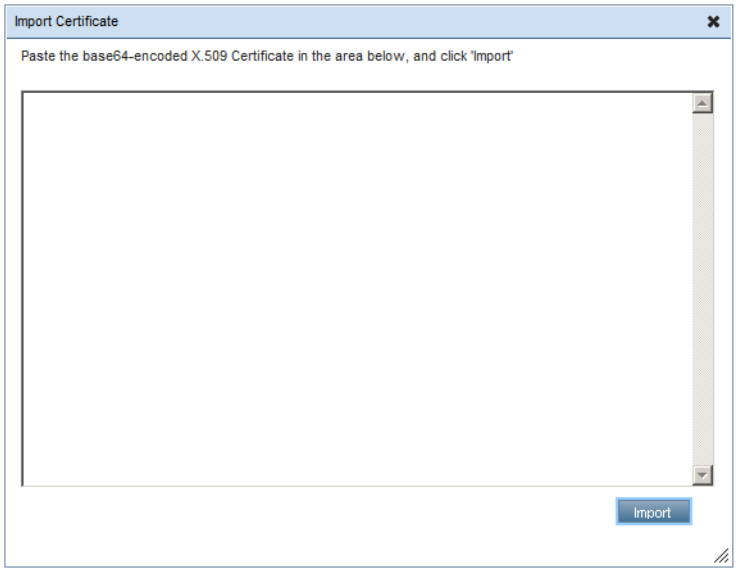
8. Follow the onscreen instructions and submit the CSR to the CA.

   The CA will generate a certificate in the PKCS #10 format.

9. After you obtain the certificate, make sure that:
   - The CN matches the iLO FQDN. This is listed as the **iLO Hostname** on the **Information→Overview** page.
   - The certificate is generated as a Base64-encoded X.509 certificate, and is in the RAW format.
   - The first and last lines are included in the certificate.
10. Return to the **SSL Certificate Customization** page (Figure 21) in the iLO user interface.
11. Click the **Import Certificate** button.

    The **Import Certificate** window opens, as shown in Figure 22 (page 51).

Figure 22 Import Certificate window



12. Paste the certificate into the text box, and then click the **Import** button.

    iLO supports DER-encoded SSL certificates that are up to 3 KB in size (including the 609 or 1,187 bytes used by the private key, for 1,024-bit and 2,048-bit certificates, respectively).

13. Restart iLO.

Configuring directory settings

The iLO firmware connects to Microsoft Active Directory, Novell e-Directory, and other LDAP 3.0-compliant directory services for user authentication and authorization. You can configure iLO to authenticate and authorize users by using the HP Extended Schema directory integration or the schema-free directory integration. The HP Extended Schema works only with Microsoft Windows. The iLO firmware connects to directory services by using SSL connections to the directory server LDAP port. The default secure LDAP port is 636.

For more information about using directory authentication with iLO, see "Directory services" (page 160).

Locally stored user accounts (listed on the **User Administration** page) can be active when iLO directory support is enabled. This enables both local-based and directory-based user access. Typically, you can delete local user accounts (with the possible exception of an emergency access account) after iLO is configured to access the directory service. You can also disable access to these accounts when directory support is enabled.

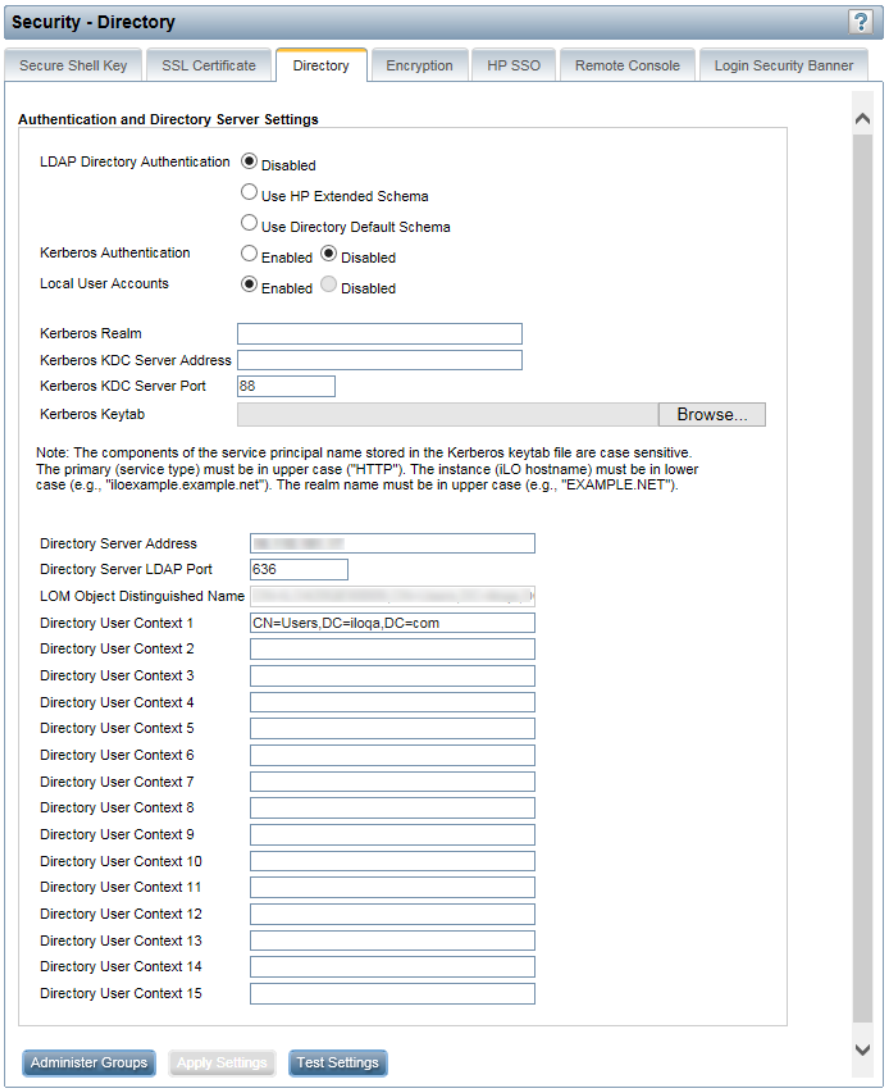
You must have the Configure iLO Settings privilege to change directory settings.

This feature and many others are part of an iLO licensing package. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.

Configuring authentication and directory server settings

1. Navigate to the **Administration→Security→Directory** page, as shown in Figure 23 (page 52).

Figure 23 Security - Directory page



2. Configure the following options:

- **LDAP Directory Authentication**—Enables or disables directory authentication. If directory authentication is enabled and configured correctly, users can log in by using directory credentials.

  Choose from the following options:

  - **Disabled**—User credentials are not validated by using a directory.
  - **Use HP Extended Schema**—Selects directory authentication and authorization by using directory objects created with the HP Extended Schema. Select this option when the directory has been extended with the HP Extended Schema.
  - **Use Directory Default Schema**—Selects directory authentication and authorization by using user accounts in the directory. Select this option when the directory is not

extended with the HP Extended Schema. User accounts and group memberships are used to authenticate and authorize users. After you enter and save the directory network information, click **Administer Groups**, and then enter one or more valid directory DNs and privileges to grant users access to iLO.

- **Kerberos Authentication**—Enables Kerberos login. If Kerberos login is enabled and configured correctly, the **HP Zero Sign In** button appears on the login page.
- **Local User Accounts**—Enables or disables local user account access.
  - **Enabled**—A user can log in by using locally stored user credentials. HP recommends enabling this option and configuring a user account with administrator privileges. This account can be used if iLO cannot communicate with the directory server.
  - **Disabled**—User access is limited to valid directory credentials.

  Access through local user accounts is enabled when directory support is disabled or an iLO license is revoked. You cannot disable local user access when you are logged in through a local user account.
- **Kerberos Realm**—The name of the Kerberos realm in which the iLO processor is operating. This string can be up to 128 characters. A realm name is usually the DNS name converted to uppercase. Realm names are case sensitive.
- **Kerberos KDC Server Address**—The IP address or DNS name of the KDC server. This string can be up to 128 characters. Each realm must have at least one KDC that contains an authentication server and a ticket grant server. These servers can be combined.
- **Kerberos KDC Server Port**—The TCP or UDP port number on which the KDC is listening. The default KDC port is 88.
- **Kerberos Keytab**—A binary file that contains pairs of service principal names and encrypted passwords. In the Windows environment, the keytab file is generated by the `ktpass` utility. Click **Browse** (Internet Explorer or Firefox) or **Choose File** (Chrome), and then follow the onscreen instructions to select a file.

IMPORTANT: The components of the service principal name stored in the Kerberos keytab file are case sensitive. The primary (service type) must be in uppercase letters, for example, (`HTTP`). The instance (iLO host name) must be in lowercase letters, for example, `iloexample.example.net`. The realm name must be in uppercase, for example, `EXAMPLE.NET`.

3. Enter the directory server settings.

   iLO directory server settings enable you to identify the directory server address and LDAP port.

   - **Directory Server Address**—Specifies the network DNS name or IP address of the directory server. The directory server address can be up to 127 characters.

   IMPORTANT: HP recommends using DNS round-robin when you are defining the directory server.

   - **Directory Server LDAP Port**—Specifies the port number for the secure LDAP service on the server. The default value is 636. You can specify a different value if your directory service is configured to use a different port.

- **LOM Object Distinguished Name**—Specifies where this iLO instance is listed in the directory tree (for example, `cn=iLO Mail Server,ou=Management Devices,o=hp`). This option is available when **Use HP Extended Schema** is selected.

  User search contexts are not applied to the LOM object DN when iLO accesses the directory server.

- **Directory User Contexts**—These boxes enable you to specify common directory subcontexts so that users do not need to enter their full DNs at login. Directory user contexts can be up to 128 characters.

  You can identify the objects listed in a directory by using unique DNs. However, DNs can be long, and users might not know their DNs or might have accounts in different directory contexts. iLO attempts to contact the directory service by DN, and then applies the search contexts in order until successful.

  - **Example 1**—If you enter the search context `ou=engineering,o=hp`, you can log in as `user` instead of logging in as `cn=user,ou=engineering,o=hp`.
  - **Example 2**—If a system is managed by Information Management, Services, and Training, search contexts such as the following enable users in any of these organizations to log in by using their common names:

    ```
    Directory User Context 1:ou=IM,o=hp
    Directory User Context 2:ou=Services,o=hp
    Directory User Context 3:ou=Training,o=hp
    ```

    If a user exists in both the `IM` organizational unit and the `Training` organizational unit, login is first attempted as `cn=user,ou=IM,o=hp`.

  - **Example 3 (Active Directory only)**—Microsoft Active Directory allows an alternate user credential format. A user can log in as `user@domain.example.com`, in which case a search context of `@domain.example.com` allows the user to log in as `user`. Only a successful login attempt can test search contexts in this format.

4. Click **Apply Settings**.
5. To test the communication between the directory server and iLO, click **Test Settings**.

   For more information, see "Running directory tests" (page 54).
6. Optional: Click **Administer Groups** to navigate to the **User Administration** page.

   For information about group administration, see "Administering directory groups" (page 37).

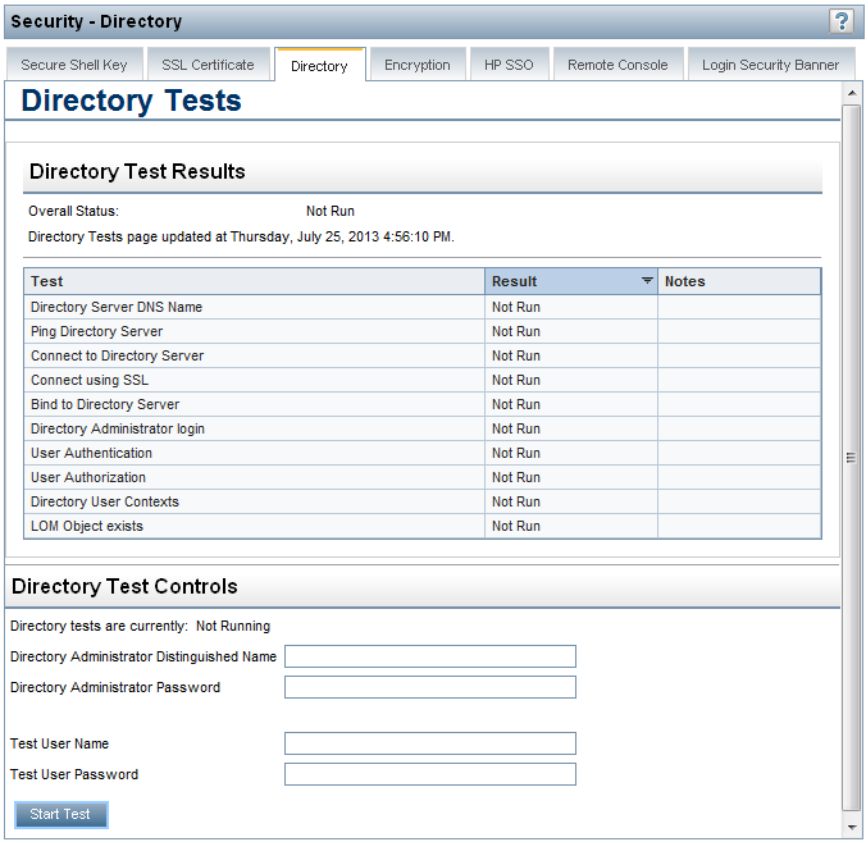
Running directory tests

Directory tests enable you to validate the configured directory settings. The directory test results are reset when directory settings are saved, or when the directory tests are started.

To validate the configured directory settings:

1. Click **Test Settings** on the **Security→Directory** page.
   The **Directory Tests** page opens, as shown in Figure 24 (page 55).

Figure 24 Directory Tests page



This page displays the results of a series of simple tests designed to validate the current directory settings. Also, it includes a test log that shows test results and any detected issues. After your directory settings are configured correctly, you do not need to rerun these tests. The **Directory Tests** page does not require that you be logged in as a directory user.

2. In the **Directory Test Controls** section, enter the DN and password of a directory administrator.
   - **Directory Administrator Distinguished Name**—Searches the directory for iLO objects, roles, and search contexts. This user must have rights to read the directory.
   - **Directory Administrator Password**—Authenticates the directory administrator.

   HP recommends that you use the same credentials that you used when creating the iLO objects in the directory. These credentials are not stored by iLO; they are used to verify the iLO object and user search contexts.
3. In the **Directory Test Controls** section, enter a test user name and password.
   - **Test User Name**—Tests login and access rights to iLO. The name does not have to be fully distinguished because user search contexts can be applied. This user must be associated with a role for this iLO.
   - **Test User Password**—Authenticates the test user.

   Typically, this account is used to access the iLO processor being tested. It can be the directory administrator account, but the tests cannot verify user authentication with a superuser account. These credentials are not stored by iLO.

4. Click **Start Test**.

   Several tests begin in the background, starting with a network ping of the directory user by establishing an SSL connection to the server and evaluating user privileges.

While the tests are running, the page refreshes periodically. You can stop the tests or manually refresh the page at any time.

Viewing directory test results

The **Directory Test Results** section shows the directory test status with the date and time of the last update.

- **Overall Status**—Summarizes the results of the tests.
  - **Not Run**—No tests were run.
  - **Inconclusive**—No results were reported.
  - **Passed**—No failures were reported.
  - **Problem Detected**—A problem was reported.
  - **Failed**—A specific subtest failed. Check the onscreen log to identify the problem.
  - **Warning**—One or more of the directory tests reported a **Warning** status.
- **Test**—The name of each test.

  Table 3 (page 56) provides details about each directory test.

Table 3 Directory tests

Test	Description
Directory Server DNS Name	If the directory server is defined in FQDN format (`directory.company.com`), iLO resolves the name from FQDN format to IP format, and queries the configured DNS server. If the test is successful, iLO obtained an IP address for the configured directory server. If iLO cannot obtain an IP address for the directory server, this test and all subsequent tests fail. If the directory server is configured with an IP address, iLO skips this test. If a failure occurs: **1.** Verify that the DNS server configured in iLO is correct. **2.** Verify that the directory server FQDN is correct. **3.** As a troubleshooting tool, use an IP address instead of the FQDN. **4.** If the problem persists, check the DNS server records and network routing.
Ping Directory Server	iLO initiates a ping to the configured directory server. The test is successful if iLO receives the ping response; it is unsuccessful if the directory server does not reply to iLO. If the test fails, iLO will continue with the subsequent tests. If a failure occurs: **1.** Check to see if a firewall is active on the directory server. **2.** Check for network routing issues.
Connect to Directory Server	iLO attempts to negotiate an LDAP connection with the directory server. If the test is successful, iLO was able to initiate the connection. If the test fails, iLO was not able to initiate an LDAP connection with the specified directory server. Subsequent tests will stop. If a failure occurs:

Table 3 Directory tests *(continued)*

Test	Description
	1. Verify that the configured directory server is the correct host. 2. Verify that iLO has a clear communication path to the directory server through port 636 (consider any routers or firewalls between iLO and the directory server). 3. Verify that any local firewall on the directory server is enabled to allow communications through port 636.
Connect using SSL	iLO initiates SSL handshake and negotiation and LDAP communications with the directory server through port 636. If the test is successful, the SSL handshake and negotiation between iLO and the directory server were successful. If a failure occurs, the directory server is not enabled for SSL negotiations. If you are using Microsoft Active Directory, verify that Active Directory Certificate Services (Windows Server 2008) are installed.
Bind to Directory Server	This test binds the connection with the user name specified in the test boxes. If no user is specified, iLO will do an anonymous bind. If the test is successful, the directory server accepted the binding. If a failure occurs: 1. Verify that the directory server allows anonymous binding. 2. If you entered a user name in the test boxes, verify that the credentials are correct. 3. If you verified that the user name is correct, try using other user-name formats; for example, `user@domain.com`, `DOMAIN\username`, `username` (called Display Name in Active Directory), or `userlogin`. 4. Verify that the specified user is allowed to log in and is enabled.
Directory Administrator Login	If **Directory Administrator Distinguished Name** and **Directory Administrator Password** were specified, iLO uses these values to log in to the directory server as an administrator. These boxes are optional.
User Authentication	iLO authenticates to the directory server with the specified user name and password. If the test is successful, the supplied user credentials are correct. If the test fails, the user name and/or password is incorrect. If a failure occurs: 1. If you verified that the user name is correct, try using other user-name formats; for example, `user@domain.com`, `DOMAIN\username`, `username` (called Display Name in Active Directory), or `userlogin`. 2. Verify that the specified user is allowed to log in and is enabled. 3. Check to see if the specified user name is restricted by logon hours or IP-based logging.
User Authorization	This test verifies that the specified user name is part of the specified directory group, and is part of the directory search context specified during directory services configuration. If a failure occurs: 1. Verify that the specified user name is part of the specified directory group. 2. Check to see if the specified user name is restricted by logon hours or IP-based logging.
Directory User Contexts	If **Directory Administrator Distinguished Name** was specified, iLO tries to search the specified context. If the test is successful, iLO found the context by using the administrator credentials to search for the container in the directory. Contexts that begin with "@" can be tested only by user login. A failure indicates that the container could not be located.
LOM Object Exists	This test searches for the iLO object in the directory server by using the **LOM Object Distinguished Name** configured on the **Security→Directory** page.

Table 3 Directory tests *(continued)*

Test	Description
	NOTE: You can enter a **LOM Object Distinguished Name** on the **Security→Directory** page only when **Use HP Extended Schema** is selected. This test is run even if **LDAP Directory Authentication** is disabled. If the tests is successful, iLO found the object that represents itself. If a failure occurs: 1. Verify that the LDAP FQDN of the LOM object is correct. 2. Try to update the HP Extended Schema and snap-ins in the directory server by updating the HP Directories Support for ProLiant Management Processors software.

- **Result**—Reports status for a specific directory setting or an operation that uses one or more directory settings. These results are generated when a sequence of tests is run. The results stop when the tests run to completion, when a test failure prevents further progress, or when the tests are stopped. Test results follow:
  - **Passed**—The test ran successfully. If more than one directory server was tested, all servers that ran this test were successful.
  - **Not Run**—The test was not run.
  - **Failed**—The test was unsuccessful on one or more of the directory servers. Directory support might not be available on those servers.
  - **Warning**—The test ran and reported a warning condition, for example, a certificate error. Check the **Notes** column for suggested actions to correct the warning condition.
- **Notes**—Indicates the results of various phases of the directory tests. The data is updated with failure details and information that is not readily available, like the directory server certificate subject and which roles were evaluated successfully.

Using the directory test controls

The **Directory Test Controls** section enables you to view the current state of the directory tests, adjust the test parameters, start and stop the tests, and refresh the page contents.

- **In Progress**—Indicates that directory tests are currently being performed in the background. Click the **Stop Test** button to cancel the current tests, or click the **Refresh** button to update the contents of the page with the latest results. Using the **Stop Test** button might not stop the tests immediately.
- **Not Running**—Indicates that directory tests are current, and that you can supply new parameters to run the tests again. Use the **Start Test** button to start the tests and use the current test control values. Directory tests cannot be started after they are already in progress.
- **Stopping**—Indicates that directory tests have not yet reached a point where they can stop. You cannot restart tests until the status changes to **Not Running**. Use the **Refresh** button to determine whether the tests are complete.

For information about the parameters you can enter, see "Running directory tests" (page 54).

Using encryption

iLO provides enhanced security for remote management in distributed IT environments. SSL encryption protects web browser data. SSL encryption of HTTP data ensures that the data is secure as it is transmitted across the network. iLO supports the following cipher strengths:

- 256-bit AES with RSA, DHE, and a SHA1 MAC
- 256-bit AES with RSA, and a SHA1 MAC

- 128-bit AES with RSA, DHE, and a SHA1 MAC
- 128-bit AES with RSA, and a SHA1 MAC
- 168-bit 3DES with RSA, and a SHA1 MAC
- 168-bit 3DES with RSA, DHE, and a SHA1 MAC

iLO also provides enhanced encryption through the SSH port for secure CLP transactions. iLO supports AES128-CBC and 3DESCBC cipher strengths through the SSH port.

If enabled, iLO enforces the use of these enhanced ciphers (both AES and 3DES) over the secure channels, including secure HTTP transmissions through the browser, SSH port, and XML port. When AES/3DES encryption is enabled, you must use a cipher strength equal to or greater than AES/3DES to connect to iLO through these secure channels. The AES/3DES encryption enforcement setting does not affect communications and connections over less-secure channels.

By default, Remote Console data uses 128-bit RC4 bidirectional encryption. The HPQLOCFG utility uses 128-bit RC4 with 160-bit SHA1 and 2048-bit RSAKeyX encryption to securely send RIBCL scripts to iLO over the network.

Version 1.50 and later of the iLO 3 firmware supports FIPS Mode.

NOTE: The term *FIPS Mode* is used in this document and in iLO to describe the feature, not its validation status.

- FIPS is a set of standards mandated for use by United States government agencies and contractors.
- FIPS Mode in iLO 3 1.50 and later is intended to meet the requirements of FIPS 140-2 level 1. This version or any other version of the iLO firmware might have this feature but might or might not be FIPS validated. The FIPS validation process is lengthy, so not all iLO firmware versions will be validated. For information about the current FIPS status of this or any other version of the iLO firmware, see the following document: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140InProcess.pdf.

Viewing encryption enforcement settings

Navigate to the **Administration→Security→Encryption** page, as shown in Figure 25 (page 59).

Figure 25 Security–Encryption Settings page

The **Encryption Settings** page displays the current encryption settings for iLO.

- **Current Negotiated Cipher**—The cipher in use for the current browser session. After you log in to iLO through the browser, the browser and iLO negotiate a cipher setting to use during the session.
- **Encryption Enforcement Settings**—The current encryption settings for iLO:
  - **FIPS Mode**—Indicates whether FIPS Mode is enabled or disabled for this iLO system.
  - **Enforce AES/3DES Encryption**—Indicates whether AES/3DES encryption is enforced for this iLO.

    When enabled, iLO accepts only those connections through the browser and SSH interface that meet the minimum cipher strength. A cipher strength of at least AES or 3DES must be used to connect to iLO when this setting is enabled.

Modifying the AES/DES encryption setting

You must have the Configure iLO Settings privilege to change the encryption settings.

To modify the AES/DES encryption setting:

1. Navigate to the **Administration→Security→Encryption** page, as shown in Figure 25 (page 59).
2. Change the **Enforce AES/3DES Encryption** setting to **Enabled** or **Disabled**.
3. Click **Apply** to end your browser connection and restart iLO.

   Wait at least 30 seconds before you attempt to re-establish a connection.

   When changing the **Enforce AES/3DES Encryption** setting to **Enabled**, close all open browsers after clicking **Apply**. Any browsers that remain open might continue to use a non-AES/3DES cipher.

Connecting to iLO by using AES or 3DES encryption

After you enable the **Enforce AES/3DES Encryption** setting, iLO requires that you connect through secure channels (web browser, SSH connection, or XML channel) by using a cipher strength of at least AES or 3DES.

- **Web browser**—You must configure the browser with a cipher strength of at least AES or 3DES. If the browser is not using AES or 3DES ciphers, iLO displays an error message. The error text varies depending on the installed browser.

  Different browsers use different methods for selecting a negotiated cipher. For more information, see your browser documentation. You must log out of iLO through the current browser before changing the browser cipher setting. Any changes made to the browser cipher setting while you are logged in to iLO might enable the browser to continue using a non-AES/3DES cipher.
- **SSH connection**—For instructions on setting the cipher strength, see the SSH utility documentation.
- **XML channel**—HPQLOCFG uses a secure 3DES cipher by default. For example, HPQLOCFG displays the following cipher strength in the XML output:

```
Connecting to Server...
Negotiated cipher: 128-bit Rc4 with 160-bit SHA1 and 2048-bit RsaKeyx
```

Enabling FIPS Mode

You must have the Configure iLO Settings privilege to change the encryption settings.

To enable FIPS Mode for iLO:

1. Optional: Capture the current iLO configuration by using HPONCFG.

   For more information, see the *HP iLO 3 Scripting and Command Line Guide*.

2. Verify that a trusted certificate is installed.

   Using iLO in FIPS Mode with the default self-signed certificate is not FIPS compliant. For instructions, see "Obtaining and importing an SSL certificate" (page 49).

IMPORTANT: Some interfaces to iLO, such as supported versions of IPMI and SNMP, are not FIPS compliant and cannot be made FIPS compliant. For information about the iLO firmware versions that are FIPS validated, see the following document: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140-1val.zip

3. Power off the server.
4. Navigate to the **Administration→Security→Encryption** page, as shown in Figure 25 (page 59).
5. Set FIPS Mode to **Enabled**.

CAUTION: Enabling FIPS Mode resets iLO to the factory default settings, and clears all user and license data.

6. Click **Apply**.

   iLO reboots in FIPS Mode. Wait at least 90 seconds before attempting to re-establish a connection.

7. Optional: Restore the iLO configuration by using HPONCFG.

   For more information, see the *HP iLO 3 Scripting and Command Line Guide*.

TIP: You can use the Login Security Banner feature to notify iLO users that a system is using FIPS Mode. For more information, see "Configuring the Login Security Banner" (page 67).

You can also use XML configuration and control scripts to enable FIPS mode. For more information, see the *HP iLO 3 Scripting and Command Line Guide*.

Disabling FIPS Mode

If you want to disable FIPS Mode for iLO (for example, if a server is decommissioned), you must set iLO to the factory default settings. You can perform this task by using RIBCL scripts or iLO RBSU.

For instructions, see "Resetting iLO to the factory default settings by using iLO RBSU" (page 230) or the *HP iLO 3 Scripting and Command Line Guide*.

When you disable FIPS Mode, all potentially sensitive data is erased, including all logs and settings.

Configuring iLO for HP SSO

HP SSO enables you to browse directly from an HP SSO-compliant application (such as HP SIM) to iLO, bypassing an intermediate login step. To use SSO, you must have a supported version of an HP SSO-compliant application, and you must configure the iLO processor to trust the SSO-compliant application.

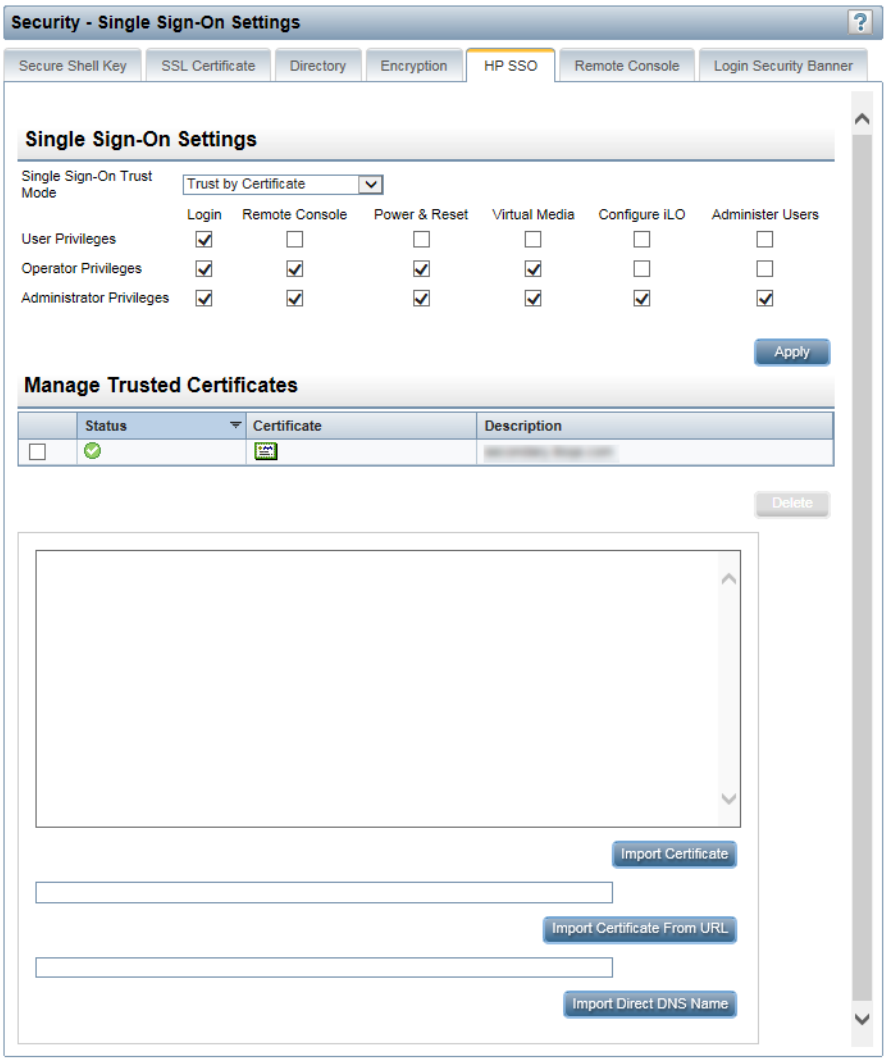
This feature and many others are part of an iLO licensing package. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.

Some HP SSO-compliant applications automatically import trust certificates when they connect to iLO. For applications that do not do this automatically, use the HP SSO page to configure the SSO settings through the iLO web interface. You must have the Configure iLO Settings privilege to change these settings.

Configuring iLO for HP SSO

1. Navigate to the **Administration→Security→HP SSO** page, as shown in Figure 26 (page 62).

Figure 26 Security–Single Sign-On Settings page



2. Make sure you have an iLO license key installed.
3. Enable Single Sign-On Trust Mode by selecting **Trust by Certificate**, **Trust by Name**, or **Trust All**.

   The iLO firmware supports configurable trust modes, which enables you to meet your security requirements. The trust mode affects how iLO responds to HP SSO requests. If you enable support for HP SSO, HP recommends using the **Trust by Certificate** mode. The available modes follow:

   - **Trust None (SSO disabled)** (default)—Rejects all SSO connection requests
   - **Trust by Certificate** (most secure)—Enables SSO connections from an HP SSO-compliant application by matching a certificate previously imported to iLO
   - **Trust by Name**—Enables SSO connections from an HP SSO-compliant application by matching an IP address or DNS name imported directly, or an IP address or DNS name included in a certificate imported to iLO
   - **Trust All** (least secure)—Accepts any SSO connection initiated from any HP SSO-compliant application.

4. Configure iLO privileges for each role in the **Single Sign-On Settings** section.

   When you log in to an HP SSO-compliant application, you are authorized based on your HP SSO-compliant application role assignment. The role assignment is passed to iLO when SSO is attempted. For more information about each privilege, see "Managing iLO users by using the iLO web interface" (page 32).

   SSO attempts to receive only the privileges assigned in this section. iLO directory settings do not apply. Default privilege assignments are as follows:

   - **User**—Login only
   - **Operator**—Login, Remote Console, Power and Reset, and Virtual Media
   - **Administrator**—Login, Remote Console, Power and Reset, Virtual Media, Configure iLO, and Administer Users

5. Click **Apply** to save the SSO settings.
6. If you selected **Trust by Certificate** or **Trust by Name**, add the trusted certificate or DNS name to iLO.

   For more information about adding certificates and DNS names, see "Adding trusted certificates" (page 64).

   The certificate repository can hold five typical certificates. However, if typical certificates are not issued, certificate sizes might vary. When all of the allocated storage is used, no more imports are accepted.
7. After you configure SSO in iLO, log in to an HP SSO-compliant application and browse to iLO. For example, log in to HP SIM, navigate to the **System** page for the iLO processor, and then click the iLO link in the **More Information** section.

   NOTE: Although a system might be registered as a trusted server, SSO might be refused because of the current trust mode or certificate status. For example, if an HP SIM server name is registered, and the trust mode is **Trust by Certificate**, but the certificate is not imported, SSO is not allowed from that server. Likewise, if an HP SIM server certificate is imported, but the certificate has expired, SSO is not allowed from that server. The list of trusted servers is not used when SSO is disabled. iLO does not enforce SSO server certificate revocation.

Viewing trusted certificates

The Manage Trusted Certificates table on the **Single Sign-On Settings** page displays the status of the trusted certificates configured to use SSO with the current iLO management processor.

- **Status**—The status of the record (if any are installed).

Table 4 HP trusted certificate status

Icon	Description
	The record is valid.
	There is a problem with the trust settings or the iLO license. Possible reasons follow: ○ This record contains a DNS name, and the trust mode is set to **Trust by Certificate** (only certificates are valid). ○ **Trust None (SSO disabled)** is selected. ○ A valid license key is not installed.
	The record is not valid. Possible reasons follow: ○ An out-of-date certificate is stored in this record. Check the certificate details for more information. ○ The iLO clock is not set or is set incorrectly. ○ The iLO clock must be in the **Valid from** and **Valid until** range.

- **Certificate**—Indicates that the record contains a stored certificate. Move the cursor over the icon to view the certificate details, including subject, issuer, and dates.
- **Description**—The server name (or certificate subject).

Adding trusted certificates

iLO users who have the Configure iLO Settings privilege can install trusted certificates or add direct DNS names.

The Base64-encoded X.509 certificate data resembles the following:

```
-----BEGIN CERTIFICATE-----
. . . several lines of encoded data . . .
-----END CERTIFICATE-----
```

To add trusted HP SSO records by using the iLO web interface:

1. Navigate to the **Administration→Security→HP SSO** page, as shown in Figure 26 (page 62).
2. Use one of the following methods to add a trusted certificate:
   - To directly import a trusted certificate, copy the Base64-encoded certificate X.509 data, paste it into the text box above the **Import Certificate** button, and then click the button.
   - To indirectly import a trusted certificate, type the DNS name or IP address in the text box above the **Import Certificate from URL** button, and then click the button. iLO contacts the HP SSO-compliant application over the network, retrieves the certificate, and then saves it.
   - To import the direct DNS name, enter the DNS name in the text box above the **Import Direct DNS Name** button, and then click the button.

For information about how to extract an HP SIM certificate, see "Extracting the HP SIM server certificate" (page 65).

For information about how to extract certificates from other HP SSO-compliant applications, see your HP SSO-compliant application documentation.

Extracting the HP SIM server certificate

You can use the following methods to extract HP SIM certificates.

- Enter one of the following links in a web browser:
  - For HP SIM versions earlier than 7.0:

    `http://<HP SIM name or network address>:280/GetCertificate`

    `https://<HP SIM name or network address>:50000/GetCertificate`

  - For HP SIM 7.0 or later:

    `http://<HP SIM name or network address>:280/GetCertificate?certtype=sso`

    `https://<HP SIM name or network address>:50000/GetCertificate?certtype=sso`

    NOTE: All request parameters are case-sensitive. If you capitalize the lowercase **`certtype`** parameter, the parameter will not be read, and HP SIM will return the default HP SIM server certificate instead of a trust certificate.

- Export the certificate from HP SIM:
  - For HP SIM versions earlier than 7.0:

    Select **Options**→**Security**→**Certificates**→**Server Certificate**.

  - For HP SIM 7.0 or later:

    Select **Options**→**Security**→**HP Systems Insight Manager Server Certificate**, and then click **Export**.

- Use the HP SIM command-line tools. For example, using the alias `tomcat` for the HP SIM certificate, enter **`mxcert -l tomcat`**.

For more information, see the HP SIM documentation.

Removing trusted certificates

1. Navigate to the **Administration**→**Security**→**HP SSO** page, as shown in Figure 26 (page 62).
2. Select one or more records in the **Manage Trusted Certificates** table.
3. Click **Delete**.

   The following message appears:

   `Are you sure you want to remove the selected certificates?`
4. Click **Yes**.

Configuring Remote Console security settings

Use the Remote Console security settings to control the Remote Console Computer Lock settings and the Integrated Remote Console Trust setting. You must have the Configure iLO Settings privilege to change these settings.

Configuring Remote Console Computer Lock settings

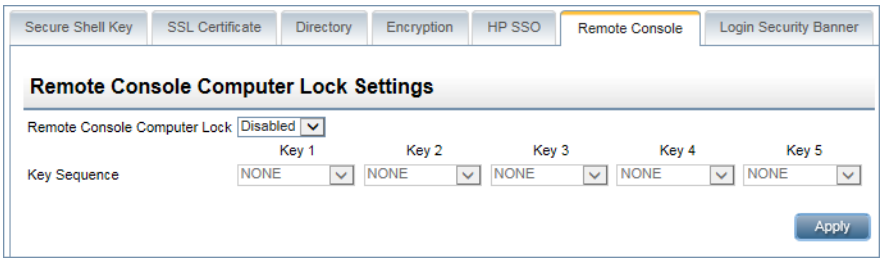
Remote Console Computer Lock enhances the security of an iLO-managed server by automatically locking an operating system or logging out a user when a Remote Console session ends or the network link to iLO is lost. This feature is standard and does not require an additional license. As a result, if you open a .NET IRC or Java IRC window and this feature is already configured, the operating system will be locked when you close the window, even if an iLO license is not installed.

The Remote Console Computer Lock feature is set to **Disabled** by default.

To change the Remote Console Computer Lock settings:

1. Navigate to the **Administration→Security→Remote Console** page, as shown in Figure 27 (page 66).

Figure 27 Remote Console Computer Lock Settings



2. Modify the Remote Console Computer Lock settings as required:
   - **Windows**—Use this option to configure iLO to lock a managed server running a Windows operating system. The server automatically displays the **Computer Locked** dialog box when a Remote Console session ends or the iLO network link is lost.
   - **Custom**—Use this option to configure iLO to use a custom key sequence to lock a managed server or log out a user on that server. You can select up to five keys from the list. The selected key sequence is sent automatically to the server operating system when a Remote Console session ends or the iLO network link is lost.
   - **Disabled** (default)—Use this option to disable the Remote Console Computer Lock feature. Terminating a Remote Console session or losing an iLO network link will not lock the operating system on the managed server.

   You can create a Remote Console Computer Lock key sequence by using the keys listed in Table 5 (page 66):

Table 5 Remote Console Computer Lock keys

ESC	**SCRL LCK**	**1**	**g**
L_ALT	**SYS RQ**	**2**	**h**
R_ALT	**F1**	**3**	**i**
L_SHIFT	**F2**	**4**	**j**
R_SHIFT	**F3**	**5**	**k**
L_CTRL	**F4**	**6**	**l**
R_CTRL	**F5**	**7**	**m**
L_GUI	**F6**	**8**	**n**
R_GUI	**F7**	**9**	**o**
INS	**F8**	**;**	**p**
DEL	**F9**	**=**	**q**
HOME	**F10**	**[**	**r**
END	**F11**	****	**s**
PG_UP	**F12**	**]**	**t**
PG_DN	**" " (space)**	**'**	**u**
ENTER	**'**	**a**	**v**
TAB	**,**	**b**	**w**

Table 5 Remote Console Computer Lock keys *(continued)*

BREAK	**-**	**c**	**x**
BACKSPACE	**.**	**d**	**y**
NUM PLUS	**/**	**e**	**z**
NUM MINUS	**0**	**f**	

3. Click **Apply** to save the changes.

Configuring the Integrated Remote Console Trust setting (.NET IRC)

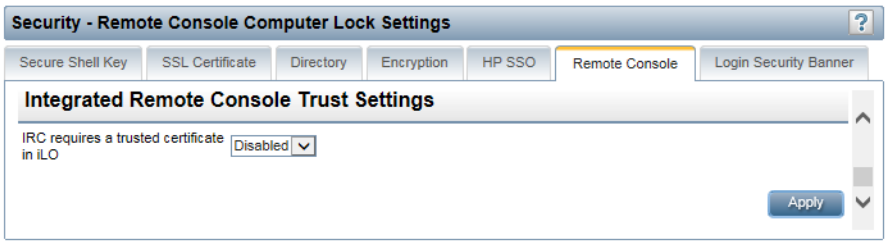
The .NET IRC is launched through Microsoft ClickOnce, which is part of the Microsoft .NET Framework. ClickOnce requires that any application installed from an SSL connection be from a trusted source. If a browser is not configured to trust an iLO processor, and the Integrated Remote Console Trust setting is set to **Enabled**, ClickOnce displays the following error message:

```
Cannot Start Application – Application download did not succeed...
```

To specify whether all clients that browse to this iLO require a trusted iLO certificate to run the .NET IRC:

1. Navigate to the **Administration→Security→Remote Console** page, as shown in Figure 28 (page 67).

Figure 28 Remote Console Trust Settings



2. Select one of the following in the **Integrated Remote Console Trust Setting** section:
   - **Enabled**—The .NET IRC is installed and runs only if this iLO certificate and the issuer certificate have been imported and are trusted.
   - **Disabled** (default)—When you launch the .NET IRC, the browser installs the application from a non-SSL connection. SSL is still used after the .NET IRC starts to exchange encryption keys.
3. Click **Apply**.

Configuring the Login Security Banner

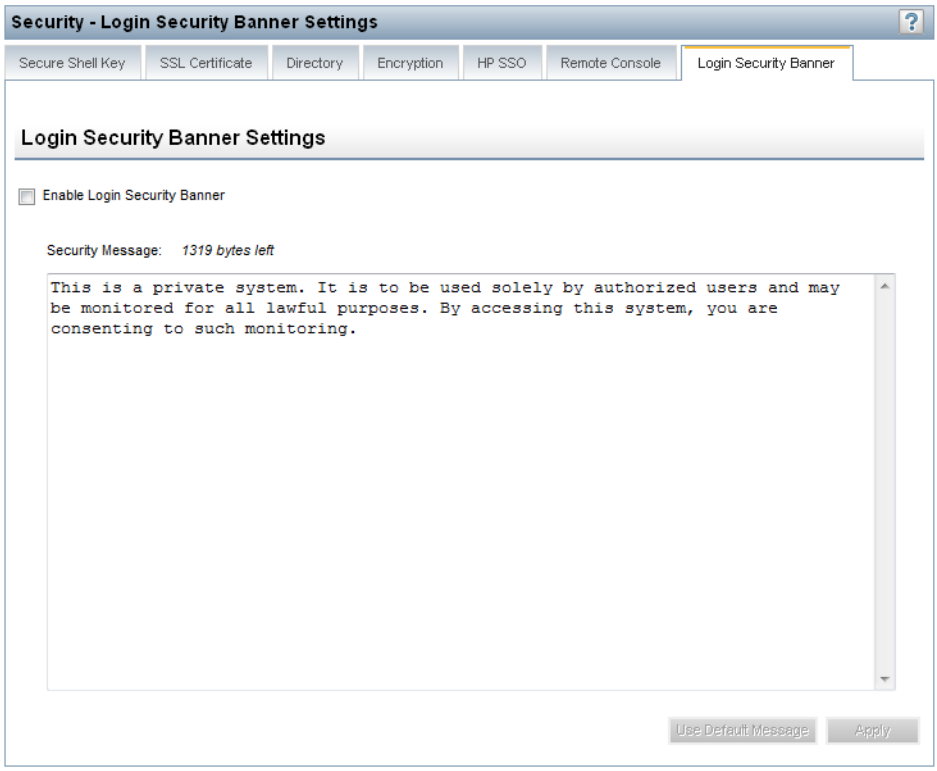
The Login Security Banner feature allows you to configure the security banner displayed on the iLO login page. For example, you could enter a message indicating that an iLO system uses FIPS Mode.

You must have the Configure iLO Settings privilege to make changes on the Login Security Banner page.

To enable the Login Security Banner:

1. Navigate to the **Administration→Security→Login Security Banner** page, as shown in Figure 29 (page 68).

Figure 29 Security–Login Security Banner Settings page



2. Select the **Enable Login Security Banner** check box.

   iLO uses the following default text for the Login Security Banner:

   ```
   This is a private system. It is to be used solely by authorized
   users and may be monitored for all lawful purposes. By accessing
   this system, you are consenting to such monitoring.
   ```

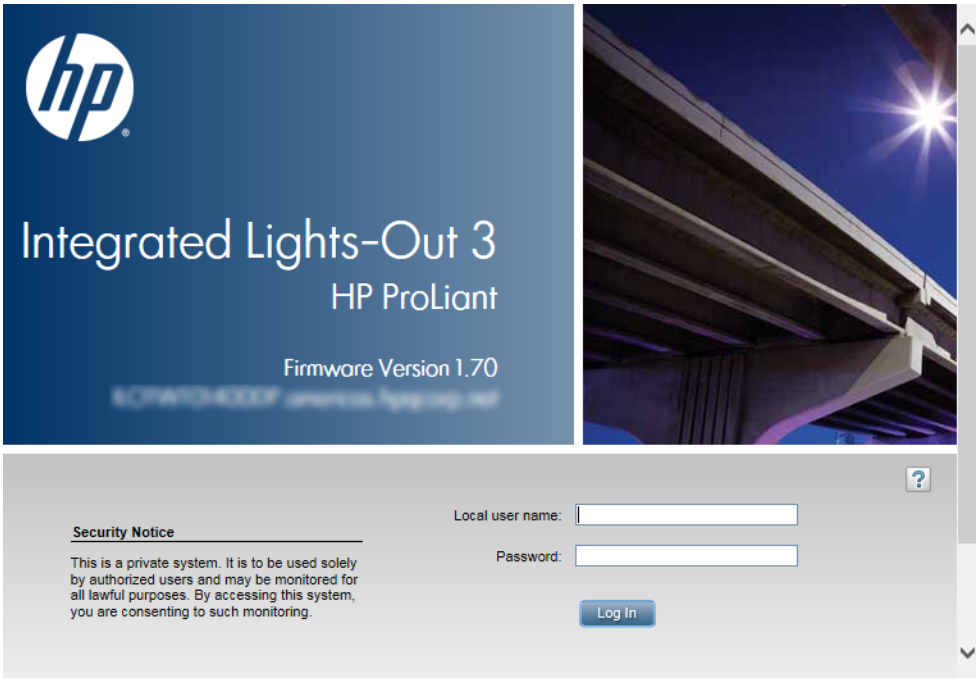
3. Optional: To customize the security message, enter a custom message in the **Security Message** text box.

   The byte counter above the text box indicates the remaining number of bytes allowed for the message. The maximum is 1,500 bytes.

TIP: Click **Use Default Message** to restore the default text for the Login Security Banner.

4. Click **Apply**.
   The security message is displayed at the next login, as shown in Figure 30 (page 69).

Figure 30 Security message example



Configuring iLO network settings

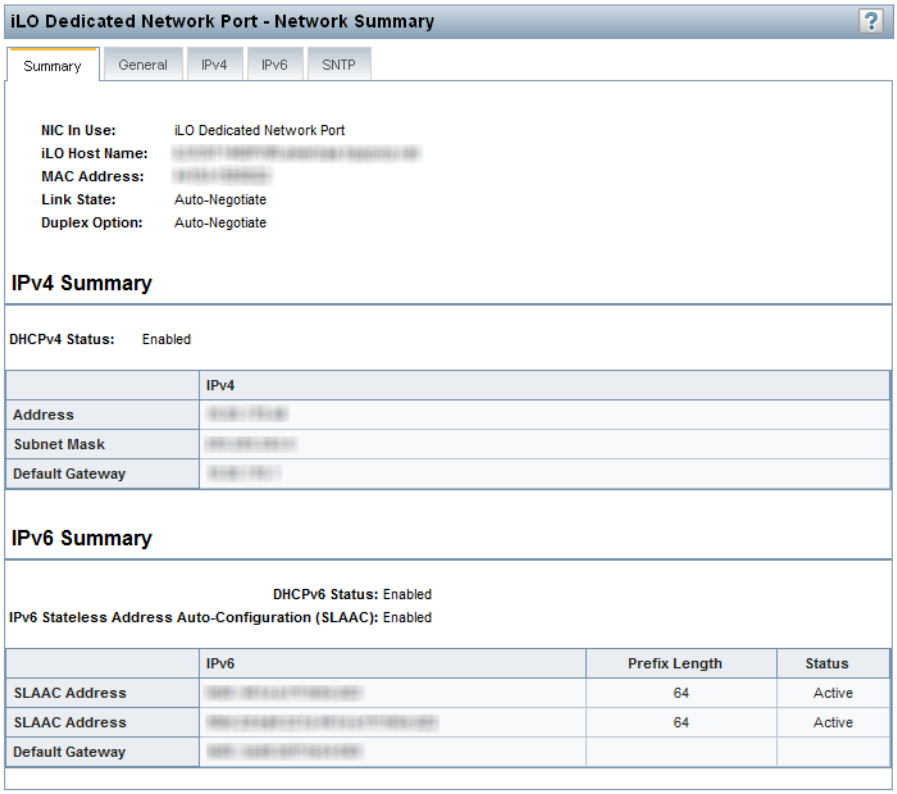
Use the tabs on the **Network** page to view and configure the iLO network settings.

You must have the Configure iLO Settings privilege to view and change these settings.

Viewing network settings

To view a summary of the configured network settings, select **Network→iLO Dedicated Network Port** or **Network→Shared Network Port** to navigate to the **Network Summary** page. See Figure 31 (page 70).

Figure 31 Network Summary page (iLO Dedicated Network Port)



The iLO Shared Network Port and the iLO Dedicated Network Port cannot operate simultaneously. If you enable the iLO Dedicated Network Port, you will disable the iLO Shared Network Port. If you enable the iLO Shared Network Port, you will disable the iLO Dedicated Network Port.

The **Network Summary** page for the inactive port displays the message `iLO is not configured to use this NIC.`

The summary information follows:

- **NIC in Use**—The name of the selected iLO network interface (iLO Dedicated Network Port or Shared Network Port).
- **iLO Host Name**—The fully qualified network name assigned to the iLO subsystem. By default, the iLO host name is **ILO** followed by the system serial number and the current domain name. This value is used for the iLO network name and must be unique.
- **MAC Address**—The MAC address of the selected iLO network interface.
- **Link State**—The current link speed of the selected iLO network interface. The default value is Auto-Negotiate.
- **Duplex Option**—The current link duplex selection for the selected iLO network interface. The default value is Auto-Negotiate.

You can configure the iLO host name and NIC settings on the **Network General Settings** page. For instructions, see "Configuring general network settings" (page 72).

IPv6 is supported by iLO 3 1.50 and later in the iLO Dedicated Network Port configuration. The IPv6 protocol was introduced by the IETF in response to the ongoing depletion of the IPv4 address pool. In IPv6, addresses are increased to 128 bits in length, to avoid an address shortage problem. iLO supports the simultaneous use of both protocols through a dual-stack implementation. All previously available iLO features are still supported in IPv4.

NOTE: IPv6 is not supported in the Shared Network Port configuration.

The following features support the use of IPv6:

- IPv6 Static Address Assignment
- IPv6 SLAAC Address Assignment
- IPv6 Static Route Assignment
- Integrated Remote Console
- OA Single Sign-On
- Web Server
- SSH Server
- SNTP Client
- DDNS Client
- DHCPv6 Address Assignment
- DHCPv6 DNS and NTP Configuration
- RIBCL over an IPv6 connection
- HP SIM SSO
- WinDBG Support
- HPQLOCFG and HPLOMIG over an IPv6 connection
- Scriptable Virtual Media
- CLI/RIBCL key import over an IPv6 connection

IPv6 support for the iLO scripting interfaces requires the following versions of the iLO utilities:

- HPQLOCFG 1.0 or later
- HP Lights-Out XML Scripting Sample bundle 4.2.0 or later
- HPONCFG 4.2.0 or later
- LOCFG.PL 4.20 or later
- HPLOMIG 4.20 or later

The **IPv4 Summary** section displays the following information:

- **DHCPv4 Status**—Indicates whether DHCP is enabled for IPv4.
- **Address**—The IPv4 address currently in use. If the value is `0.0.0.0`, the IPv4 address is not configured.
- **Subnet Mask**—The subnet mask of the IPv4 address currently in use. If the value is `0.0.0.0`, no address is configured.
- **Default Gateway**—The default gateway address in use for the IPv4 protocol. If the value is `0.0.0.0`, the gateway is not configured.

The **IPv6 Summary** section displays the following information:

- **DHCPv6 Status**—Indicates whether DHCP is enabled for IPv6. The following values are possible:
  - **Enabled**—Stateless and Stateful DHCPv6 are enabled.
  - **Enabled (Stateless)**—Only Stateless DHCPv6 is enabled.
  - **Disabled**—DHCPv6 is disabled.
- **IPv6 Stateless Address Auto-Configuration (SLAAC)**—Indicates whether SLAAC is enabled for IPv6. When SLAAC is disabled, the SLAAC link-local address for iLO is still configured because it is required.

- **Address list**—This table shows the currently configured IPv6 addresses for iLO. It provides the following information:
  - **Source**—Indicates whether the address is a static or SLAAC address.
  - **IPv6**—The IPv6 address.
  - **Prefix Length**—The address prefix length.
  - **Status**—The address status: **Active** (the address is in use by iLO), **Pending** (Duplicate Address Detection is in progress for this address), or **Failed** (Duplicate Address Detection failed and the address is not in use by iLO).
- **Default Gateway**—The default IPv6 gateway address that is currently in use. For IPv6, iLO keeps a list of possible default gateway addresses. The addresses in this list originate from router advertisement messages and the IPv6 **Static Default Gateway** setting.

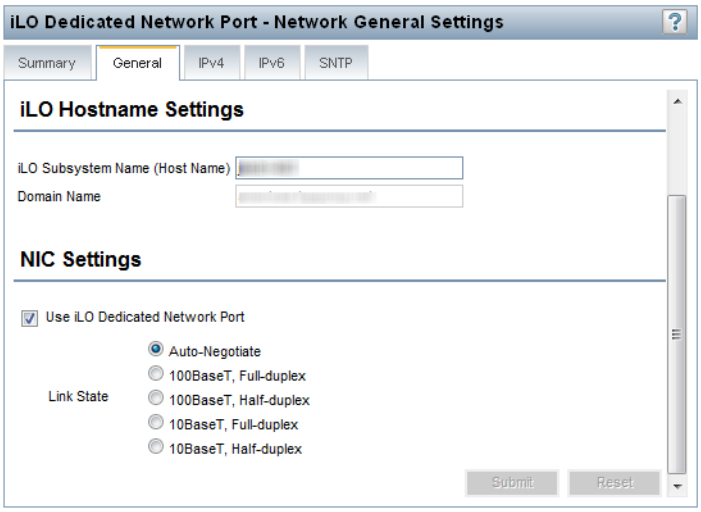
  The **Static Default Gateway** setting is configured on the IPv6 page. For more information, see "Configuring IPv6 settings" (page 76).

Configuring general network settings

Use the iLO Dedicated Network Port or Shared Network Port **Network General Settings** page to configure general network settings. You must have the Configure iLO Settings privilege to make changes on this page.

1. Navigate to the **Network→iLO Dedicated Network Port** or **Network→Shared Network Port** page.
2. Click the **General** tab, as shown in Figure 32 (page 72).

Figure 32 Network General Settings page (iLO Dedicated Network Port)



3. Enter the following information in the **iLO Hostname Settings** section:
   - **iLO Subsystem Name (Host Name)**—The DNS name of the iLO subsystem (for example, `ilo` instead of `ilo.example.com`). This name can be used only if DHCP and DNS are configured to connect to the iLO subsystem name instead of the IP address.

     iLO subsystem-name limitations follow:

     - **Name service limitations**—The subsystem name is used as part of the DNS name.
       - DNS allows alphanumeric characters and hyphens.
       - Name service limitations also apply to the **Domain Name**.
     - **Namespace issues**—To avoid these issues:
       - Do not use the underscore character.
       - Limit subsystem names to 15 characters.
       - Verify that you can ping iLO by IP address and by DNS/WINS name.
       - Verify that NSLOOKUP resolves the iLO network address correctly and that no namespace conflicts exist.
       - If you are using both DNS and WINS, verify that they resolve the iLO network address correctly.
       - Flush the DNS name if you make any namespace changes.
   - **Domain Name**—The iLO domain name. If DHCP is not used, enter a domain name.
4. Enter the following information in the **NIC Settings** section:
   - Select the **Use iLO Dedicated Network Port** or **Use Shared Network Port** check box to enable or disable the iLO Dedicated Network Port or Shared Network Port.
     - **Use iLO Dedicated Network Port**—Uses a NIC with a jack on the back of the server. The NIC handles iLO traffic only.
     - **Shared Network Port – LOM**—Uses a NIC that is built into the server. The NIC handles server network traffic and can, if iLO is configured to do so, handle iLO traffic at the same time.
     - **Shared Network Port Enabled Standup NIC**—An optional NIC that plugs into a PCI slot on the server and requires a special cable to connect it to the server motherboard. The NIC handles server network traffic and can, if iLO is configured to do so, handle iLO traffic at the same time.

     On systems that have more than one Shared Network Port option, select the check box, and then select a Shared Network Port option.
   - Select a **Link State** (iLO Dedicated Network Port only).

     The link setting controls the speed and duplex settings of the iLO network transceiver.

     NOTE: This setting is not available on blade servers.

     The available settings follow:
     - **Auto-Negotiate** (default)—Enables iLO to negotiate the highest supported link speed and duplex settings when connected to the network
     - **100BaseT, Full-duplex**—Forces a 100 Mb connection using full duplex
     - **100BaseT, Half-duplex**—Forces a 100 Mb connection using half duplex

- **10BaseT, Full-duplex**—Forces a 10 Mb connection using full duplex
- **10BaseT, Half-duplex**—Forces a 10 Mb connection using half duplex

If the Shared Network Port is enabled, you cannot modify the link state or duplex option. In Shared Network Port configurations, link settings must be managed in the operating system.

- Select or clear the **Enable VLAN** check box to enable or disable VLAN (Shared Network Port only).

  When the Shared Network Port is active and VLAN is enabled, the iLO Shared Network Port becomes part of a VLAN. All network devices with different VLAN tags will appear to be on separate LANs, even if they are physically connected to the same LAN.

- If you enabled VLAN, enter a **VLAN Tag** (Shared Network Port only). All network devices that you want to communicate with each other must have the same VLAN tag. The VLAN tag can be any number between 1 and 4094.

5. Click **Submit** to save the changes.
6. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart iLO.

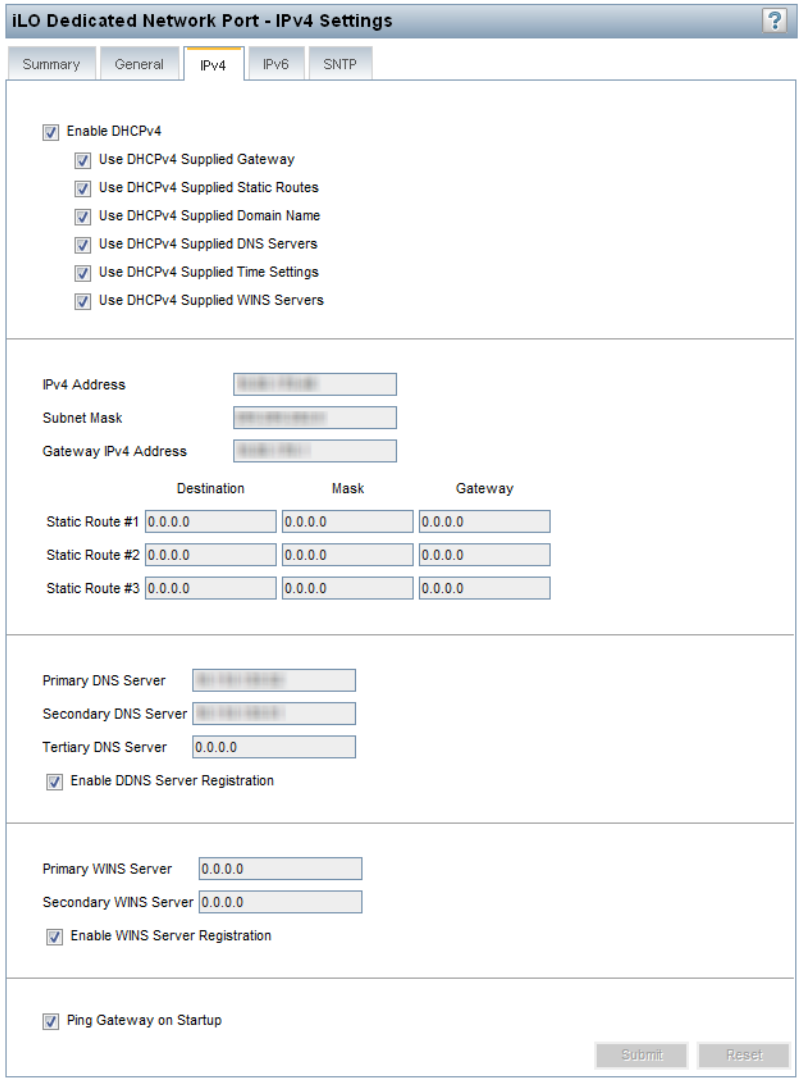
   Wait at least 30 seconds before you attempt to re-establish a connection.

Configuring IPv4 settings

Use the iLO Dedicated Network Port or Shared Network Port **IPv4 Settings** page to configure IPv4 settings for iLO. You must have the Configure iLO Settings privilege to make changes on this page.

1. Navigate to the **Network→iLO Dedicated Network Port** or **Network→Shared Network Port** page.
2. Click the **IPv4** tab, as shown in Figure 33 (page 75).

Figure 33 IPv4 Settings page (iLO Dedicated Network Port)



3. Configure the following settings:
   - **Enable DHCPv4**—Enables iLO to obtain its IP address (and many other settings) from a DHCP server.
     - **Use DHCPv4 Supplied Gateway**—Specifies whether iLO uses the DHCP server-supplied gateway. If DHCP is not used, enter a gateway address in the **Gateway IPv4 Address** box.
     - **Use DHCPv4 Supplied Static Routes**—Specifies whether iLO uses the DHCP server-supplied static routes. If not, enter the static route destination, mask, and gateway addresses in the **Static Route #1**, **Static Route #2**, and **Static Route #3** boxes.
     - **Use DHCPv4 Supplied Domain Name**—Specifies whether iLO uses the DHCP server-supplied domain name. If DHCP is not used, enter a domain name in the **Domain Name** box on the **Network General Settings** page. For more information, see "Configuring general network settings" (page 72).
     - **Use DHCPv4 Supplied DNS Servers**—Specifies whether iLO uses the DHCP server-supplied DNS server list. If not, enter the DNS server addresses in the **Primary DNS Server**, **Secondary DNS Server**, and **Tertiary DNS Server** boxes.

- **Use DHCPv4 Supplied Time Settings**—Specifies whether iLO uses the DHCPv4-supplied NTP service locations.
- **Use DHCPv4 Supplied WINS Servers**—Specifies whether iLO uses the DHCP server-supplied WINS server list. If not, enter the WINS server addresses in the **Primary WINS Server** and **Secondary WINS Server** boxes.

- **IPv4 Address**—The iLO IP address. If DHCP is used, the iLO IP address is supplied automatically. If DHCP is not used, enter a static IP address.
- **Subnet Mask**—The subnet mask of the iLO IP network. If DHCP is used, the subnet mask is supplied automatically. If DHCP is not used, enter a subnet mask for the network.
- **Gateway IPv4 Address**—The iLO gateway IP address. If DHCP is used, the iLO gateway IP address is supplied automatically. If DHCP is not used, enter the iLO gateway IP address.
- **Static Route #1**, **Static Route #2**, and **Static Route #3**—The iLO static route destination, mask, and gateway addresses. If **Use DHCPv4 Supplied Static Routes** is used, these values are supplied automatically. If not, enter the static route values.
- **DNS server information**—Enter the following information:
  - **Primary DNS Server**—If **Use DHCPv4 Supplied DNS Servers** is enabled, this value is supplied automatically. If not, enter the Primary DNS Server address.
  - **Secondary DNS Server**—If **Use DHCPv4 Supplied DNS Servers** is enabled, this value is supplied automatically. If not, enter the Secondary DNS Server address.
  - **Tertiary DNS Server**—If **Use DHCPv4 Supplied DNS Servers** is enabled, this value is supplied automatically. If not, enter the Tertiary DNS Server address.
  - **Enable DDNS Server Registration**—Select or clear this check box to specify whether iLO registers its IPv4 address and name with a DNS server.
- **WINS server information**—Enter the following information:
  - **Primary WINS Server**—If **Use DHCPv4 Supplied WINS Servers** is enabled, this value is supplied automatically. If not, enter the Primary WINS Server address.
  - **Secondary WINS Server**—If **Use DHCPv4 Supplied WINS Servers** is enabled, this value is supplied automatically. If not, enter the Secondary WINS Server address.
  - **Enable WINS Server Registration**—Specifies whether iLO registers its name with a WINS server.
- **Ping Gateway on Startup**—Causes iLO to send four ICMP echo request packets to the gateway when iLO initializes. This ensures that the ARP cache entry for iLO is up-to-date on the router responsible for routing packets to and from iLO.

4. Click **Submit** to save the changes you made on the **IPv4 Settings** page.
5. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart iLO.

   Wait at least 30 seconds before you attempt to re-establish a connection.

Configuring IPv6 settings

Use the iLO Dedicated Network Port **IPv6 Settings** page to configure IPv6 settings for iLO. You must have the Configure iLO Settings privilege to make changes on this page.

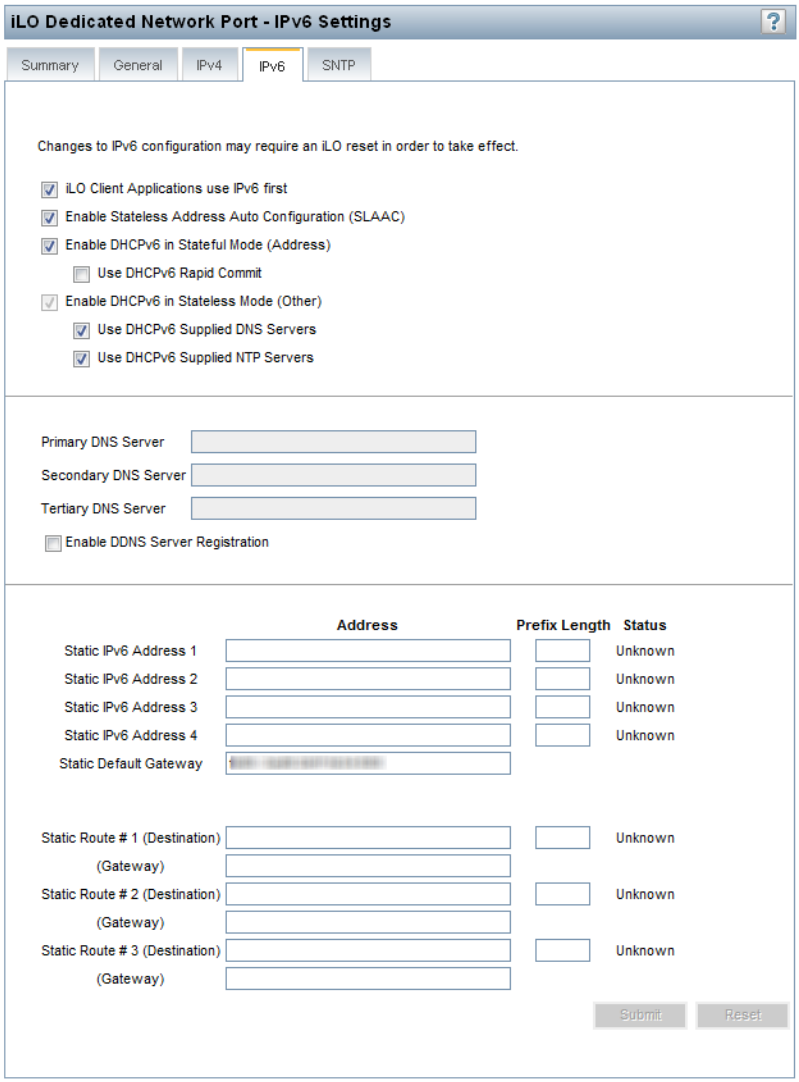
When using IPv6, note the following:

- IPv6 is not supported in the Shared Network Port configuration.
- If you downgrade the iLO firmware from version 1.6x or later to version 1.5x, the IPv6 settings will be reset to the default values.

To configure the IPv6 settings:

1. Navigate to the **Network→iLO Dedicated Network Port** page.
2. Click the **IPv6** tab, as shown in Figure 34 (page 77).

Figure 34 IPv6 Settings page (iLO Dedicated Network Port)



3. Configure the following settings:
   - **iLO Client Applications use IPv6 first**—When both IPv4 and IPv6 service addresses are configured for iLO client applications, this option specifies which protocol iLO tries first when accessing a client application. This setting also applies to lists of addresses received from the name resolver when using FQDNs to configure NTP.
     - Select this check box if you want iLO to use IPv6 first.
     - Clear this check box if you want iLO to use IPv4 first.

If communication fails using the first protocol, iLO automatically tries the second protocol.

- **Enable Stateless Address Auto Configuration (SLAAC)**—Select this check box to enable iLO to create IPv6 addresses for itself from router advertisement messages.

  NOTE: iLO will create its own link-local address even when this option is not selected.

- **Enable DHCPv6 in Stateful Mode (Address)**—Select this check box to allow iLO to request and configure IPv6 addresses provided by a DHCPv6 server.
  - **Use DHCPv6 Rapid Commit**—Select this check box to instruct iLO to use the Rapid Commit messaging mode with the DHCPv6 server. This mode reduces DHCPv6 network traffic, but might cause problems if it is used in networks where more than one DHCPv6 server can respond and provide addresses.
- **Enable DHCPv6 in Stateless Mode (Other)**—Select this check box to enable iLO to request settings for NTP and DNS service location from the DHCPv6 server.
  - **Use DHCPv6 Supplied DNS Servers**—Select this check box to use IPv6 addresses provided by the DHCPv6 server for DNS server locations. This setting can be enabled in addition to the IPv4 DNS server location options.
  - **Use DHCPv6 Supplied NTP Servers**—Select this check box to use IPv6 addresses provided by the DHCPv6 server for NTP server locations. This setting can be enabled in addition to the IPv4 NTP server location options.

  NOTE: When **Enable DHCPv6 in Stateful Mode (Address)** is selected, **Enable DHCPv6 in Stateless Mode (Other)** is always selected by default, because it is implicit in the DHCPv6 Stateful messages required between iLO and the DHCPv6 server.

- **Primary DNS Server**, **Secondary DNS Server**, and **Tertiary DNS Server**—Enter the IPv6 addresses for the DNS service.

  When DNS server locations are configured in both IPv4 and IPv6, both sources are used, with preference given according to the **iLO Client Applications use IPv6 first** configuration option, primary sources, then secondary, and then tertiary.
- **Enable DDNS Server Registration**—Specify whether iLO registers its IPv6 address and name with a DNS server.
- **Static IPv6 Address 1**, **Static IPv6 Address 2**, **Static IPv6 Address 3**, and **Static IPv6 Address 4**—Enter up to four static IPv6 addresses and prefix lengths for iLO. Do not enter link-local addresses.
- **Static Default Gateway**—Enter a default IPv6 gateway address for cases in which no router advertisement messages are present in the network.
- **Static Route #1**, **Static Route #2**, and **Static Route #3**—Enter static IPv6 route destination prefix and gateway address pairs. You must specify the prefix length for the destination. Link-local addresses are not allowed for the destination, but are allowed for the gateway.

4. Click **Submit** to save the changes you made on the **IPv6 Settings** page.
5. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart iLO.

   Wait at least 30 seconds before you attempt to re-establish a connection.

Configuring SNTP settings

SNTP allows iLO to synchronize its clock with an external time source. Configuring SNTP is optional because the iLO date and time can also be synchronized from the following sources:

- System ROM (during POST only)
- Insight Management Agents (in the OS)
- Onboard Administrator (blade servers only)

To use iLO SNTP, you must have at least one NTP server available on your management network.

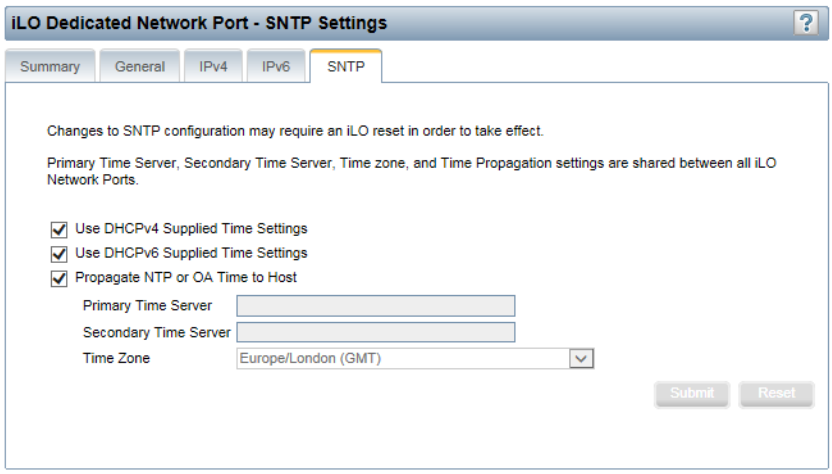
Primary and secondary NTP server addresses can be configured manually or via DHCP servers. If the primary server address cannot be contacted, the secondary address is used. You must have the Configure iLO Settings privilege to change these settings.

NOTE: IPv6 is not supported in the Shared Network Port configuration.

To configure the SNTP settings:

1. Navigate to the **Network→iLO Dedicated Network Port** or **Network→Shared Network Port** page.
2. Click the **SNTP** tab, as shown in Figure 35 (page 79).

Figure 35 SNTP Settings page (iLO Dedicated Network Port)



3. Do one of the following:
   - Select the **Use DHCPv4 Supplied Time Settings** check box, the **Use DHCPv6 Supplied Time Settings** check box, or both check boxes to use DHCP-provided NTP server addresses.

     Note the following configuration prerequisites:

     - To configure a DHCPv4-provided NTP service configuration, you must first enable DHCPv4 on the **IPv4** tab.
     - To configure a DHCPv6-provided NTP service configuration, DHCPv6 Stateless Mode must be enabled on the **IPv6** tab.

     When you use DHCP servers to provide NTP server addresses, the **iLO Client Applications use IPv6 first** setting controls the selection of the primary and secondary NTP values. When **iLO Client Applications use IPv6 first** is selected on the **IPv6** tab, a DHCPv6-provided NTP service address (if available) is used for the primary time server and a DHCPv4-provided address (if available) is used for the secondary time server.

     To change the protocol-based priority behavior to use DHCPv4 first, clear the **iLO Client Applications use IPv6 first** check box.

If a DHCPv6 address is not available for the primary or secondary address, a DHCPv4 address (if available) is used.

- Enter NTP server addresses in the **Primary Time Server** and **Secondary Time Server** boxes. You can enter the server addresses by using the server FQDN, IPv4 address, or IPv6 address.

4. If you selected only **Use DHCPv6 Supplied Time Settings**, or if you entered a primary and secondary time server, select the server time zone from the **Time Zone** list.

   This setting determines how iLO adjusts UTC time to obtain the local time, and how it adjusts for Daylight Savings Time (Summer Time). In order for the entries in the iLO Event Log and IML to display the correct local time, you must specify the time zone in which the server is located.

   If you want iLO to use the time the SNTP server provides, without adjustment, configure iLO to use a time zone that does not apply an adjustment to UTC time. In addition, that time zone must not apply a Daylight Savings Time (Summer Time) adjustment. There are several time zones that fit this requirement. One example is the Atlantic/Reykjavik time zone, which is neither east or west of the Prime Meridian, and in which the time does not change in the spring or fall. If you select the Atlantic/Reykjavik time zone, iLO web pages and log entries will display the exact time provided by the SNTP server.

   NOTE: Configure the NTP servers to use Coordinated Universal Time (GMT).

5. Configure the NTP time propagation setting by selecting or clearing the **Propagate NTP Time to Host** check box (ML, DL, and SL servers) or the **Propagate NTP or OA Time to Host** check box (BL servers).

   These settings are enabled by default, and they determine whether the server time is synchronized with the iLO time during the first POST after AC power is applied, a blade is inserted, or iLO is reset to the default settings.

   For BladeSystems only: When **Propagate NTP or OA Time to Host** is enabled, and NTP is not configured or functional, the server time is synchronized with the OA time.

6. Click **Submit** to save the changes you made on the **SNTP Settings** page.
7. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart iLO.

   Wait at least 30 seconds before you attempt to re-establish a connection.

TIP: If you notice that iLO Event Log entries have an incorrect date or time, make sure that the NTP server addresses and time zone are correct. The iLO Event Log includes entries that indicate success or failure when contacting the NTP server(s).

Configuring and using the iLO Shared Network Port

The iLO Shared Network Port feature enables you to choose between the Shared Network Port LOM, Shared Network Port Enabled Standup NIC, and the iLO Dedicated Network Port for server management. When you enable the iLO Shared Network Port, regular network traffic and iLO network traffic pass through the selected Shared Network Port NIC.

If you install a Shared Network Port Enabled Standup NIC, the Shared Network Port LOM is no longer available to send and receive iLO network traffic. That traffic will go through the iLO Dedicated Network Port or the Shared Network Port Enabled Standup NIC, depending on the iLO configuration.

If you install a Shared Network Port Enabled Standup NIC, you do not need to change the iLO configuration to use that NIC. The first time that the server is plugged in with a correctly installed Shared Network Port Enabled Standup NIC, iLO will detect the NIC and automatically begin using

it. If you later decide to switch back to the iLO Dedicated Network Port, you can do this using any of the standard iLO interfaces.

On servers that do not have an iLO Dedicated Network Port, the standard hardware configuration provides iLO network connectivity only through the iLO Shared Network Port connection. The iLO firmware automatically defaults to the Shared Network Port.

The iLO Shared Network Port uses the network port labeled NIC 1 on the rear panel of the server when **Shared Network Port – LOM** is selected, and the network port labeled 1 on the Shared Network Port Enabled Standup NIC adapter if **Shared Network Port Enabled Standup NIC** is selected. NIC numbering in the operating system can be different from system numbering. The iLO Shared Network Port does not incur an iLO performance penalty. Peak iLO traffic is less than 2 Mb/s (on a NIC capable of 1 GB/s or 10 GB/s speeds), and iLO traffic volume is low unless the Virtual Media or Remote Console feature is in use.

When using the iLO Shared Network Port, observe the following:

- The iLO Shared Network Port is supported on all nonblade servers.
- You can use the iLO Shared Network Port and the iLO Dedicated Network Port only for iLO server management.
- The iLO Shared Network Port is not an availability feature. Its purpose is to allow managed network port consolidation.
- Due to server auxiliary-power budget limitations, some 1Gb/s copper network adapters used for iLO Shared Network Port functionality might run at 10/100 speed when the server is powered off. To avoid this issue, HP recommends configuring the switch the iLO Shared Network Port is connected to for autonegotiation.

  If you want to configure the iLO switch for a speed of 1Gb/s, be aware that some copper iLO Shared Network Port adapters might lose connectivity when the server is powered off. Connectivity will return when the server is powered back on.
- The iLO Shared Network Port and iLO Dedicated Network Port cannot operate simultaneously. If you enable the iLO Dedicated Network Port, you will disable the iLO Shared Network Port. If you enable the iLO Shared Network Port, you will disable the iLO Dedicated Network Port.
- Disabling the iLO Shared Network Port does not completely disable the system NIC—network traffic still passes through the NIC. When the iLO Shared Network Port is disabled, any traffic going to or originating from iLO will not pass through the iLO Shared Network Port because that port is no longer shared with iLO.
- Using the iLO Shared Network Port can create a single failure point. If the port fails or is unplugged, both the host and iLO become unavailable to the network.

Enabling the iLO Shared Network Port feature

The iLO Shared Network Port feature is disabled by default on servers that are shipped with a Dedicated iLO Management NIC. You can enable it by using the following methods:

- **iLO RBSU**—For more information, see "Enabling the iLO Shared Network Port feature through iLO RBSU" (page 82).
- **iLO web interface**—For more information, see "Enabling the iLO Shared Network Port feature through the iLO web interface" (page 82).
- **XML configuration and control scripts**—For more information, see the *HP iLO 3 Scripting and Command Line Guide*.
- **SMASH CLP**—For more information, see the *HP iLO 3 Scripting and Command Line Guide*.

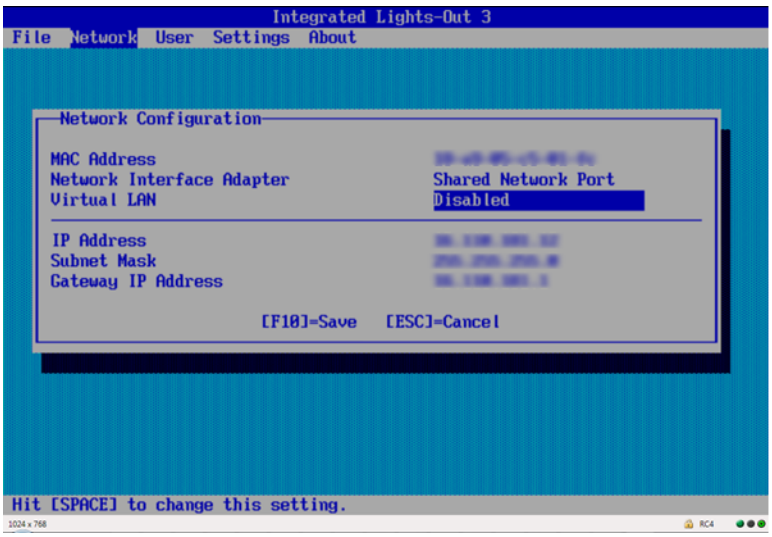
Enabling the iLO Shared Network Port feature through iLO RBSU

1. Connect the Shared Network Port LOM or Shared Network Port Enabled Standup NIC port 1 to a LAN.
2. Optional: If you will access the server remotely, start an iLO remote console session.

   You can use the .NET IRC or Java IRC.
3. Restart or power on the server.
4. Press **F8** in the HP ProLiant POST screen.
5. Select **Network→NIC and TCP/IP**, and then press **Enter**.
6. On the **Network Configuration** menu, press the spacebar to toggle the **Network Interface Adapter** setting to **Shared Network Port**, as shown in Figure 36 (page 82).

   NOTE: The Shared Network Port option is available only on supported servers.

Figure 36 iLO RBSU Network Configuration window



7. Press **F10** to save the configuration.
8. Select **File→Exit**, and then press **Enter**.

After iLO resets, the Shared Network Port feature is active. Any network traffic going to or originating from iLO is directed through the Shared Network Port LOM or Shared Network Port Enabled Standup NIC port 1.

Enabling the iLO Shared Network Port feature through the iLO web interface

1. Connect the Shared Network Port LOM or Shared Network Port Enabled Standup NIC port 1 to a LAN.
2. Log in to the iLO web interface.
3. Navigate to the **Network→Shared Network Port** page.
4. Click the **General** tab.
5. Depending on your configuration, select the **Shared Network Port Enabled Standup NIC** or **Use Shared Network Port** check box.

   NOTE: The Shared Network Port option is available only on supported servers.
6. To use a VLAN, select the **Enable VLAN** check box.

   VLAN is only available for the Shared Network Port. When the Shared Network Port is activated and VLAN is enabled, the iLO Shared Network Port becomes part of a VLAN. All network

devices with different VLAN tags will appear to be on separate LANs, even if they are physically connected to the same LAN.

7. If you enabled VLAN, enter a **VLAN tag** (Shared Network Port only). All network devices that you want to communicate with each other must have the same VLAN tag. The VLAN tag can be any number between 1 and 4,094.
8. Click **Apply**.

   Your changes are applied to the iLO network configuration, your browser connection ends, and iLO restarts. You must wait at least 30 seconds before you attempt to re-establish a connection.

After iLO resets, the Shared Network Port feature is active. Any network traffic going to or originating from iLO is directed through the Shared Network Port LOM or Shared Network Port Enabled Standup NIC port 1.

Re-enabling the iLO Dedicated Network Port

Only the Shared Network Port or the iLO Dedicated Network Port is active for server management. They cannot be enabled at the same time. If you enabled the Shared Network Port, use one of the following methods if you want to re-enable the iLO Dedicated Network Port:

- **iLO RBSU** (on servers that support iLO RBSU)—For more information, see "Enabling the iLO Dedicated Network Port through iLO RBSU" (page 83).
- **iLO web interface**—For more information, see "Enabling the iLO Dedicated Network Port through the web interface" (page 83).
- **XML scripting**—For more information, see the *HP iLO 3 Scripting and Command Line Guide*.
- **SMASH CLP**—For more information, see the *HP iLO 3 Scripting and Command Line Guide*.

Enabling the iLO Dedicated Network Port through iLO RBSU

1. Connect the iLO Dedicated Network Port to a LAN from which the server is managed.
2. Optional: If you access the server remotely, start an iLO remote console session.

   You can use the .NET IRC or Java IRC.
3. Restart or power on the server.
4. Press **F8** in the HP ProLiant POST screen.
5. Select **Network→NIC and TCP/IP**, and then press **Enter**.
6. On the **Network Configuration** menu, press the spacebar to toggle the **Network Interface Adapter** setting to **On**.
7. Press **F10** to save the configuration.
8. Select **File→Exit**, and then press **Enter**.

   After iLO resets, the iLO Dedicated Network Port is active.

Enabling the iLO Dedicated Network Port through the web interface

1. Connect the iLO Dedicated Network Port to a LAN from which the server is managed.
2. Log in to the iLO web interface.
3. Navigate to the **Network→iLO Dedicated Network Port** page.
4. Click the **General** tab.
5. Select the **Use iLO Dedicated Network Port** check box.
6. Select a **Link State**.

   For more information, see "Configuring general network settings" (page 72).

7. Click **Apply**.

   Your changes are applied to the iLO network configuration, your browser connection ends, and iLO restarts. You must wait at least 30 seconds before you attempt to re-establish a connection.

Configuring iLO Management settings

The **Administration→Management** page allows you to configure the iLO settings for SNMP alerts and Insight Manager integration.

You must have the Configure iLO Settings privilege to change these settings.

Depending on your configuration, you might need to install additional software. See "Installing the Insight Management Agents" (page 84).

Installing the Insight Management Agents

The Insight Management Agents are available from the HP Service Pack for ProLiant and the HP website. For instructions about using the HP Service Pack for ProLiant to install the Insight Management Agents, see the Service Pack for ProLiant documentation.

To download the Insight Management Agents from the HP website:

1. Navigate to the technical support page on the HP website: http://www.hp.com/support.
2. Select a country or region and a language.

   The **HP Support** page opens.
3. Click the **Drivers & Downloads** link.

   In the search box, enter the server model that you are using (for example, DL360p).

   A list of servers is displayed.
4. Click the link for your server.

   The HP Support Center page for the server opens.
5. Click the link for the server operating system.
6. Download the software.
7. Follow the installation instructions provided with the downloaded software.

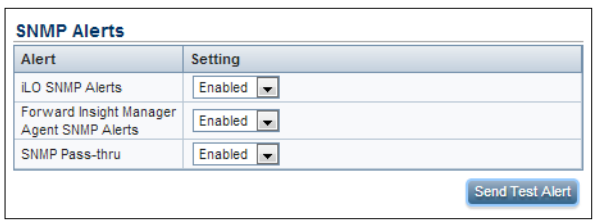
Configuring SNMP alerts

You can enable or disable iLO SNMP alerts, forwarding of Insight Management Agent SNMP alerts, and SNMP Pass-thru.

To configure SNMP alerts:

1. Navigate to the **Administration→Management** page.
2. Click the **SNMP Settings** tab and scroll to the **SNMP Alerts** section, as shown in Figure 37).

Figure 37 Editing the SNMP alerts



3. Enable or disable the following alert types:
   - **iLO SNMP Alerts**—Alert conditions that iLO detects independently of the host operating system can be sent to specified SNMP alert destinations, such as HP SIM.
   - **Forward Insight Manager Agent SNMP Alerts**—Alert conditions detected by the host management agents can be forwarded to SNMP alert destinations through iLO. These alerts are generated by the Insight Management Agents, which are available for each supported operating system. Insight Management Agents must be installed on the host server to receive these alerts.
   - **SNMP Pass-thru**—Use SNMP agents running on the host operating system to manage the server. SNMP requests sent by the client to iLO over the network are passed to the host operating system. The responses are then passed to iLO and returned to the client over the network. Alerts are not affected by this setting.
4. Optional: Click **Send Test Alert** to generate a test alert and send it to the TCP/IP addresses in the **SNMP Alert Destination(s)** boxes.

   Test alerts include an Insight Management SNMP trap, and are used to verify the network connectivity of iLO in HP SIM. Only users with the Configure iLO Settings privilege can send test alerts.

   After the alert is generated, a confirmation dialog box opens. Check the HP SIM console for receipt of the alert.
5. Click **Apply** to save the configuration.

SNMP traps

You can generate the following SNMP traps with iLO 3:

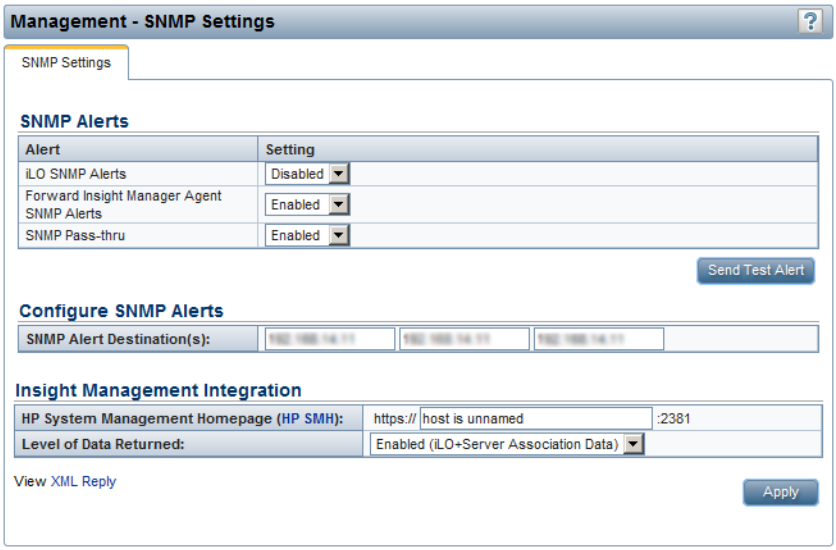
- ALERT_TEST is used to verify that the SNMP configuration, client SNMP console, and network are operating correctly. You can use the iLO web interface to generate this alert to verify receipt of the alert at the SNMP console. You can also generate this alert using the iLO Option ROM to verify SNMP configuration settings.
- ALERT_SERVER_POWER occurs when the iLO management processor detects an unexpected transition of the host system power, either from ON to OFF, or OFF to ON. Transitions of the host system power are unexpected when the change takes place because of events unknown to the management processor. This alert is not generated when the system is powered up or down using the iLO web interface, CLI, RIBCL or other management feature. If the server is powered down because of the operating system, physical power button presses, or other methods, the alert is generated and sent.
- ALERT_SERVER_RESET occurs when the iLO management processor is used to perform a cold boot or warm boot of the host system. This alert is also sent when the iLO management processor detects the host system is in reset because of events unknown to the management processor. Certain operating system behavior or actions can cause this type of event to be detected, and the alert transmitted.
- ALERT_SELFTEST_FAILURE is an SNMP alert transmitted when iLO detects an error in any of the monitored internal components. If an error is detected an SNMP alert is transmitted.
- ALERT_THRESHOLD_BREACH alert is transmitted when the iLO management processor detects host system power to be above a user configurable power threshold, over a user configurable period of time.

Configuring SNMP alert destinations

iLO 3 supports up to three IP addresses to receive SNMP alerts.

1. Navigate to the **Administration→Management** page, as shown in Figure 38 (page 86).

Figure 38 iLO Management – SNMP Settings page



2. Enter the SNMP Alert Destinations in the **Configure SNMP Alerts** section. You can provide the IP addresses of up to three remote management systems to receive SNMP alerts from iLO.

NOTE: Typically, you enter the HP SIM server console IP address in this section.

3. Click **Apply**.

Configuring Insight Management integration

1. Navigate to the **Administration→Management** page.
2. Configure the **HP System Management Homepage (HP SMH)**.

   This value sets the browser destination of the **Insight Agent** link on iLO pages.

   Enter the IP address or DNS name of the host server. The protocol (`https://`) and port number (`:2381`) are added automatically to the IP address or DNS name to allow access from iLO. If the URL is set through another method (for example, HPQLOCFG), click the browser refresh button to display the updated URL.
3. Select the **Level of Data Returned**.

   This setting controls the content of an anonymous discovery message received by iLO. The information returned is used for HP SIM HTTP identification requests. The following options are available:

   - **Enabled (iLO+Server Association Data)** (default)—Enables HP SIM to associate the management processor with the host server, and provides sufficient data to enable integration with HP SIM.
   - **Disabled (No Response to Request)**—Prevents iLO from responding to HP SIM requests.
4. Optional: Click **View XML Reply** to view the response that is returned to HP SIM when it requests iLO management processor identification using the provided address.
5. Click **Apply** to save the changes.

For more information about the Insight Management Agents, navigate to the **Information→Insight Agent** page.

Using the iLO RBSU

Accessing the iLO RBSU

You can access the iLO RBSU from the physical system console, or by using an iLO remote console session.

To access iLO RBSU:

1. Optional: If you access the server remotely, start an iLO remote console session.

   You can use the .NET IRC or Java IRC.
2. Restart or power on the server.
3. Press **F8** in the HP ProLiant POST screen.

   The iLO RBSU screen appears.
4. Select an option, and then press **Enter**.

   You can use iLO RBSU to perform the following tasks:

   - "Configuring NIC and TCP/IP settings" (page 87)
   - "Configuring DNS/DHCP settings" (page 88)
   - "Configuring global settings by using iLO RBSU" (page 89)
   - "Configuring serial CLI options by using iLO RBSU" (page 90)
   - "Resetting iLO to the factory default settings by using iLO RBSU" (page 230)
   - "Managing iLO users by using iLO RBSU" (page 18)

Configuring NIC and TCP/IP settings

You can use the iLO RBSU **Network** menu to configure basic iLO network options, including NIC and TCP/IP settings.

To configure NIC and TCP/IP settings:

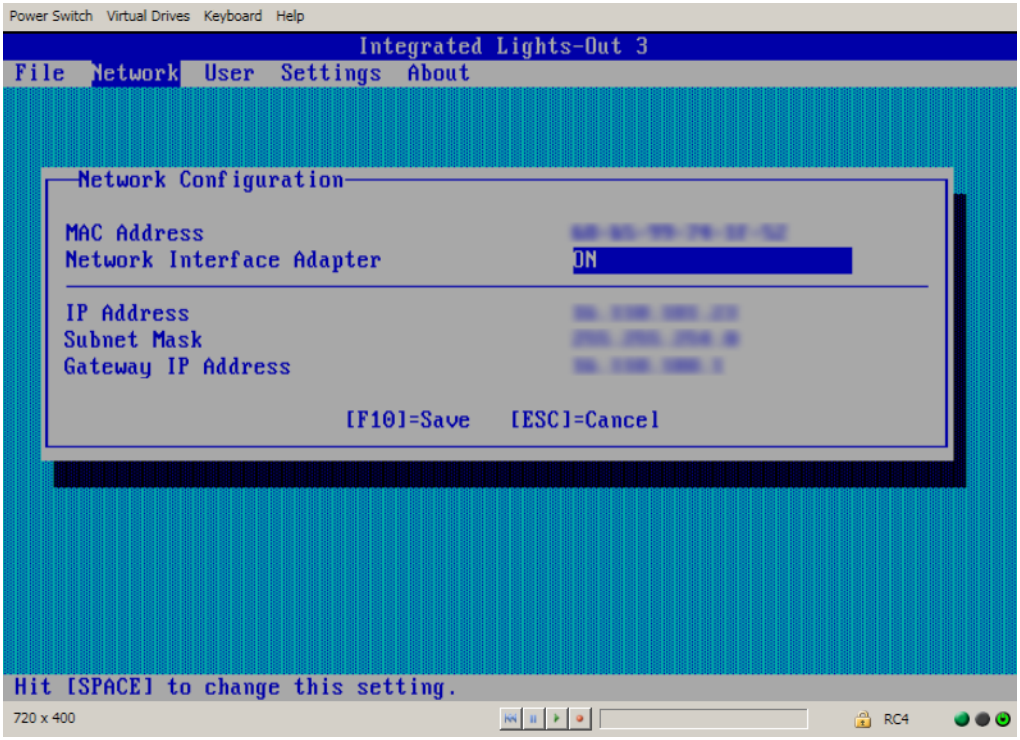
1. Optional: If you access the server remotely, start an iLO remote console session.

   You can use the .NET IRC or Java IRC.
2. Restart or power on the server.
3. Press **F8** in the HP ProLiant POST screen.

   The iLO RBSU screen appears.
4. Select **Network→NIC and TCP/IP**.

   The **Network Configuration** screen appears, as shown in Figure 39 (page 88).

Figure 39 Network Configuration screen



5. View or update the following values, as needed:
   - **MAC Address** (read-only)—The MAC address of the selected iLO network interface.
   - **Network Interface Adapter**—Specifies the iLO network interface adapter to use. Select **ON** or **OFF** to enable or disable the iLO Dedicated Network Port. Select **Shared Network Port** to use the Shared Network Port.

     The Shared Network Port option is available only on supported servers.
   - **Transceiver Speed Autoselect** (iLO Dedicated Network port only)—Enables iLO to negotiate the highest supported link speed and duplex settings when connected to the network.
   - **IP Address**—The iLO IP address. If DHCP is used, the iLO IP address is supplied automatically. If DHCP is not used, enter a static IP address.
   - **Subnet Mask**—The subnet mask of the iLO IP network. If DHCP is used, the subnet mask is supplied automatically. If DHCP is not used, enter a subnet mask for the network.
   - **Gateway IP Address**—The iLO gateway IP address. If DHCP is used, the iLO gateway IP address is supplied automatically. If DHCP is not used, enter the iLO gateway IP address.
6. Press **F10** to save your changes.
7. Select **File→Exit** to exit iLO RBSU.

Configuring DNS/DHCP settings

You can use the iLO RBSU **Network** menu to configure basic iLO network options, including DNS and DHCP settings.

To configure DNS and DHCP settings:

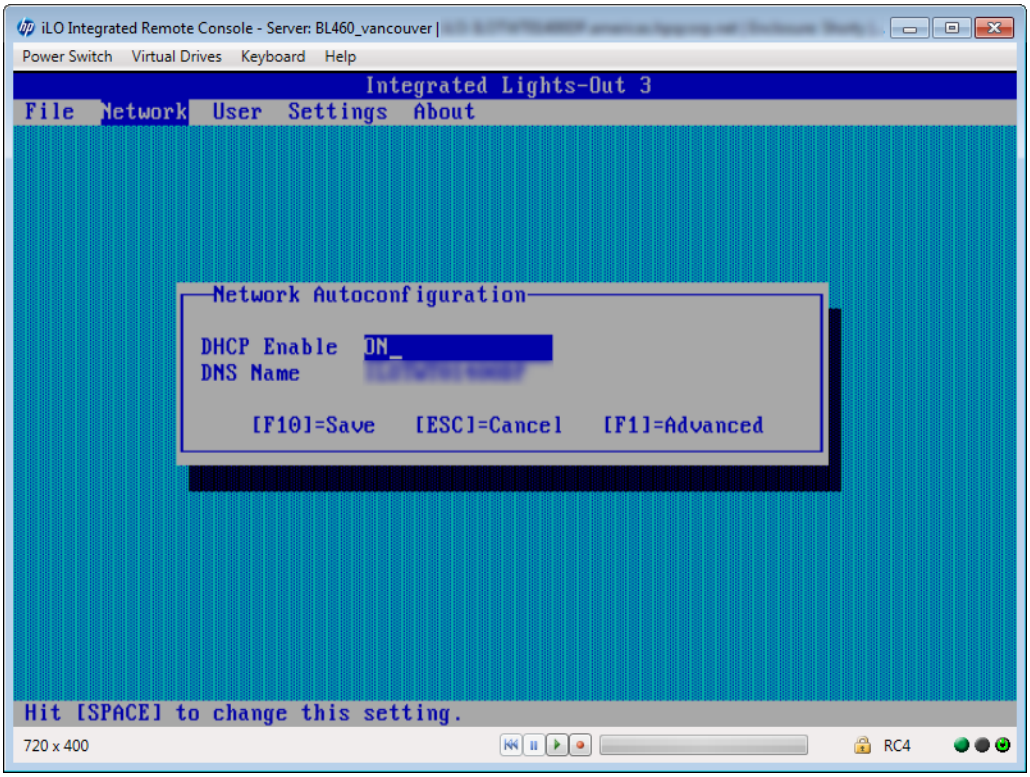
1. Optional: If you access the server remotely, start an iLO remote console session.

   You can use the .NET IRC or Java IRC.
2. Restart or power on the server.
3. Press **F8** in the HP ProLiant POST screen.

   The iLO RBSU screen appears.

4. Select **Network→DNS/DHCP**.
   The **Network Autoconfiguration** screen appears, as shown in Figure 40 (page 89).

Figure 40 Network Autoconfiguration screen

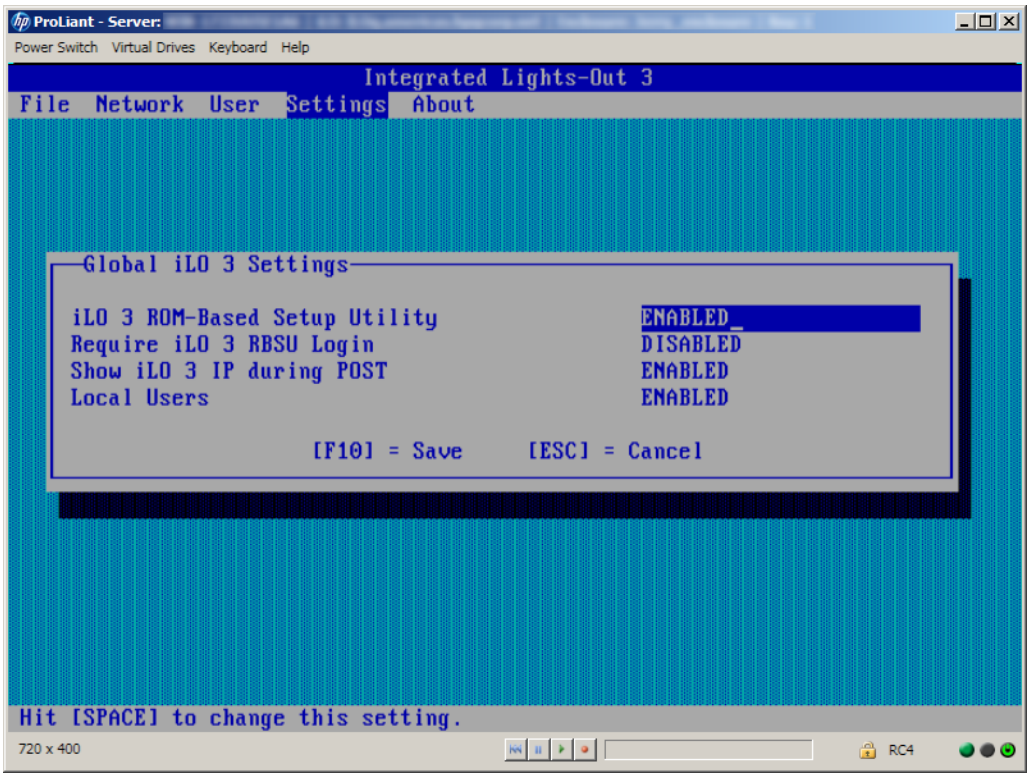


5. View or update the following values, as needed:
   - **DHCP Enable**—Configures iLO to obtain its IP address (and many other settings) from a DHCP server.
   - **DNS Name**—The DNS name of the iLO subsystem (for example, `ilo` instead of `ilo.example.com`).
     This name can be used only if DHCP and DNS are configured to connect to the iLO subsystem name instead of the IP address.
6. Press **F10** to save your changes.
7. Select **File→Exit** to exit iLO RBSU.

Configuring global settings by using iLO RBSU

1. Optional: If you will access the server remotely, start an iLO remote console session.
   You can use the .NET IRC or Java IRC.
2. Restart or power on the server.
3. Press **F8** during POST to enter iLO RBSU.
4. Select **Settings→Configure**, and then press **Enter**.
   The **Global iLO 3 Settings** menu opens, as shown in Figure 41 (page 90).

Figure 41 Global iLO 3 Settings window



5. For each option that you want to change, select the option, and press the **spacebar** to toggle the setting to **ENABLED** or **DISABLED**. You can change the following settings:
   - **iLO 3 ROM-Based Setup Utility**
   - **Require iLO 3 RBSU Login**
   - **iLO 3 ROM-Based Setup Utility**
   - **Local Users**

   For more information about the first four options in the list, see Table 2 (page 41).

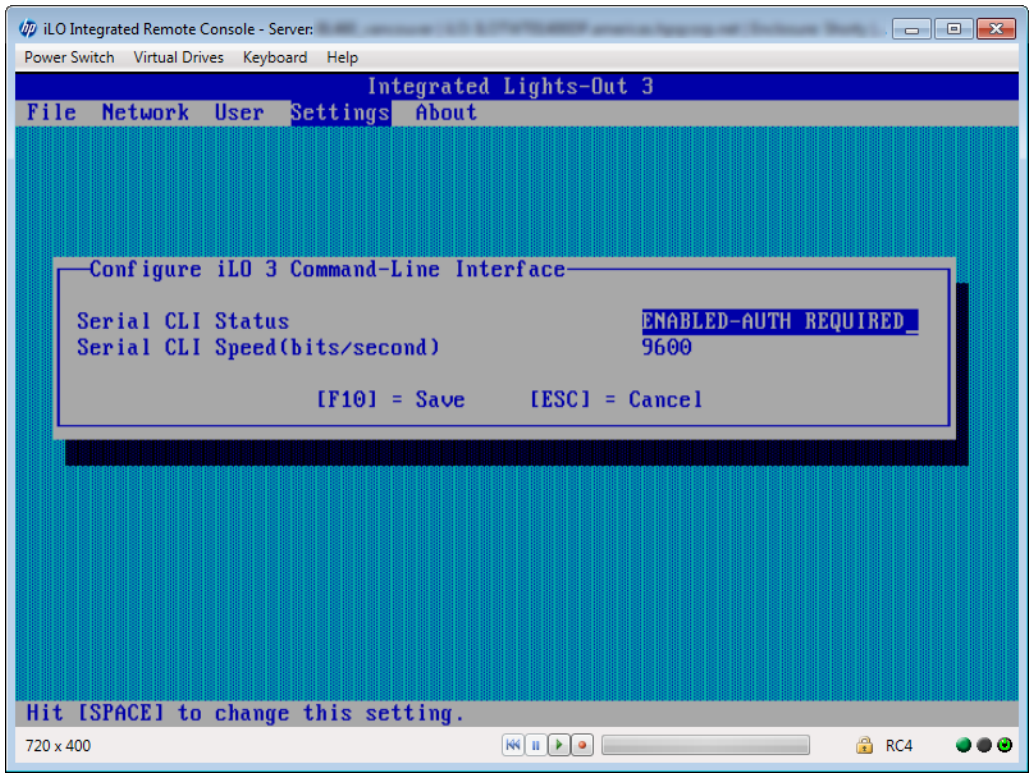
   For more information about the last option in the list, see "Configuring authentication and directory server settings" (page 52).
6. Press **F10** to save the settings.
7. Select **File→Exit** to close iLO RBSU.

Configuring serial CLI options by using iLO RBSU

1. Optional: If you access the server remotely, start an iLO remote console session.

   You can use the .NET IRC or Java IRC.
2. Restart or power on the server.
3. Press **F8** in the HP ProLiant POST screen.
4. Select **Settings→CLI**, and then press **Enter**.
5. The **Configure iLO Command-Line Interface** menu opens, as shown in Figure 42 (page 91).

Figure 42 iLO RBSU Configure iLO Command-Line Interface window



6. For each option that you want to change, select the option, and press the **spacebar** to toggle through the available settings. You can change the following settings:
   - **Serial CLI Status**
   - **Serial CLI Speed (bits/second)**

   For more information about these options, see Table 2 (page 41).
7. Press **F10** to save the settings.
8. Select **File→Exit** to close iLO RBSU.

4 Using iLO

The main iLO features for a nonadministrative user are located in the **Information**, **Remote Console**, **Virtual Media**, **Power Management**, and **BL c-Class** sections of the navigation pane. This guide provides information about using iLO with the iLO web interface.

TIP: You can also perform many iLO tasks by using XML configuration and control scripts or SMASH CLP. For information about using these methods, see the *HP iLO 3 Scripting and Command Line Guide, HP Scripting Toolkit for Linux User Guide*, and *HP Scripting Toolkit for Windows User Guide*.

Using the iLO web interface

You can use the iLO web interface to access iLO. You can also use a Remote Console, scripting, or the CLP.

For Technical Support information, see the *HP iLO 3 User Guide*.

Browser support

The iLO web interface requires a browser that supports JavaScript. For a list of supported browsers, see Table 6 (page 92).

Table 6 Supported browsers

iLO version	Internet Explorer	Firefox	Chrome
iLO 3 1.50	7, 8, 9	ESR 10	Chrome (latest version)
iLO 3 1.55	7, 8, 9	ESR 10	Chrome (latest version)
iLO 3 1.57	7, 8, 9	ESR 10	Chrome (latest version)
iLO 3 1.61	8, 9, 10	ESR 17	Chrome (latest version)
iLO 3 1.70	8, 10	ESR 24	Chrome (latest version)

If you receive a notice that your browser does not have the required functionality, verify that your browser settings meet the following requirements, or contact your administrator.

The following settings must be enabled:

- **JavaScript**—The iLO web interface uses client-side JavaScript extensively.
- **Cookies**—Cookies must be enabled for certain features to function correctly.
- **Pop-up windows**—Pop-up windows must be enabled for certain features to function correctly. Verify that pop-up blockers are disabled.

Logging in to iLO

You must access the iLO web interface through HTTPS (HTTP exchanged over an SSL encrypted session).

To log in to iLO:

1. Enter `https://<iLO host name or IP address>`.

   The iLO login page opens.

   If iLO is configured to use the Login Security Banner feature, a security message is displayed on the login page.

   For information about configuring the Login Security Banner, see "Configuring the Login Security Banner" (page 67).

2. Enter an HP iLO user name and password, and then click **Log In**.

Login problems might occur for the following reasons:

- You have recently upgraded the iLO firmware. You might need to clear your browser cache before attempting to log in again.
- You are not entering the login information correctly.
  - Passwords are case sensitive.
  - User names are not case sensitive. Uppercase and lowercase characters are treated the same (for example, Administrator is treated as the same user as administrator).
- The account you are entering is not a valid iLO account.
- The account you are entering has been deleted, disabled, or locked out.
- The password for the account must be changed.
- You are attempting to sign in from an IP address that is not valid for the specified account.

  Contact the administrator if you continue to have problems.

If iLO is configured for Kerberos network authentication, the **HP Zero Sign In** button is displayed below the **Log In** button. Clicking the **HP Zero Sign In** button logs the user in to iLO without requiring the user to enter a user name and password. If the Kerberos login fails, the user can log in by using a user name and password.

A failed Kerberos login might be due to one of the following reasons:

- The client does not have a ticket or has an invalid ticket. Press **Ctrl+Alt+Del** to lock the client PC and get a new ticket.
- The browser is not configured correctly. The browser might display a dialog box requesting credentials.
- The Kerberos realm that the client PC is logged in to does not match the Kerberos realm for which iLO is configured.
- The computer account in Active Directory for iLO does not exist or is disabled.
- The user logged in to the client PC is not a member of a universal or global directory group authorized to access iLO.
- The key in the Kerberos keytab stored in iLO does not match the key in Active Directory.
- The KDC server address for which iLO is configured is incorrect.
- The date and time do not match between the client PC, the KDC server, and iLO. To log in to Kerberos successfully, ensure that the date and time of the following are set to within 5 minutes of one another:
  - The iLO server
  - The client running the web browser
  - The servers performing the authentication
- The DNS server is not working correctly. iLO requires a functioning DNS server for Kerberos support.

Handling an unknown authority

If the message `Website Certified by an Unknown Authority` is displayed, take the following action:

1. View the certificate to ensure that you are browsing to the correct management server (not an imposter).
   - Verify that the **Issued To** name is your management server. Perform any other steps you feel necessary to verify the identity of the management server.
   - If you are not sure that this is the correct management server, do not proceed. You might be browsing to an imposter and giving your sign-in credentials to that imposter when you sign in. Contact the administrator. Exit the certificate window, and then click **No** or **Cancel** to cancel the connection.
2. After verifying the items in Step 1, you have the following options:
   - Accept the certificate temporarily for this session.
   - Accept the certificate permanently.
   - Stop now and import the certificate into your browser from a file provided by your administrator.

Using the iLO controls

When you log in to the iLO web interface, the controls at the bottom of the browser window are available from any iLO page.

- **POWER**—Use this menu to access the iLO Virtual Power features.
- **UID**—Use this button to turn the UID on and off.
- **Language**—Use this menu to select a language or to navigate to the **Access Settings**→**Language** page, where you can install a language pack and configure other language-related settings.
- **Health icon**—Use this icon to view the overall health status for the server fans, temperature sensors, and other monitored subsystems. Click the icon to view the status of the monitored components. Select a component to view more information about the component status.

Language pack support

If a language pack is currently installed in iLO, a language menu is available on the login screen for you to select the language for the iLO session. This selection is saved in a browser cookie for future use.

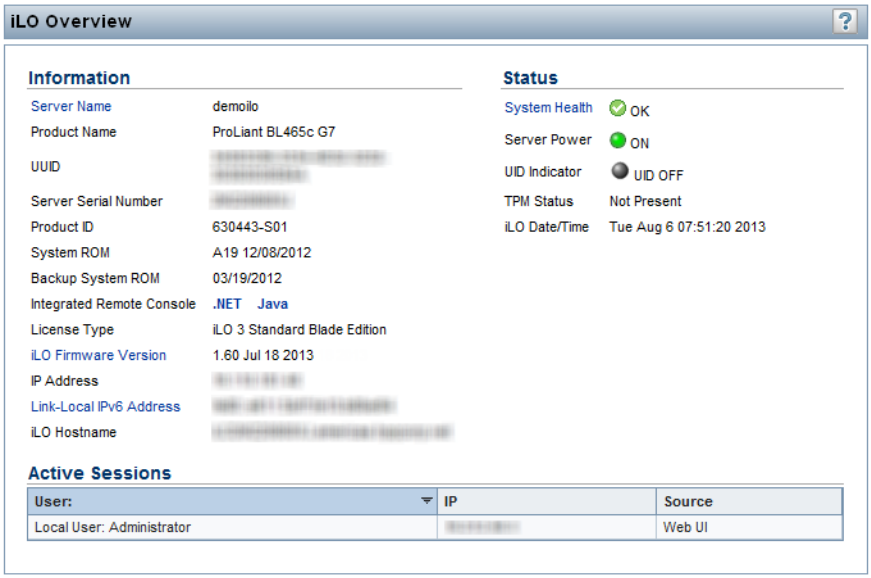
Viewing iLO overview information

The **iLO Overview** page displays high-level details about the server and iLO subsystem, as well as links to commonly used features.

Viewing system information

To view iLO overview information, navigate to the **Information**→**Overview** page, as shown in Figure 43 (page 95).

Figure 43 iLO Overview page



The **Information** section displays the following information:

- **Server Name**—The server name defined by the host operating system. Click the **Server Name** link to navigate to the **Administration→Access Settings** page.
- **Product Name**—The product with which this iLO processor is integrated.
- **UUID**—The universally unique identifier that software (for example, HP SIM) uses to uniquely identify this host. This value is assigned when the system is manufactured.
- **UUID (Logical)**—The system UUID that is presented to host applications. This value is displayed only when it has been set by other HP software, such as HP Virtual Connect Manager. This value might affect operating system and application licensing. The **UUID (Logical)** value is set as part of the logical server profile that is assigned to the system. If the logical server profile is removed, the system **UUID** value reverts from the **UUID (Logical)** value to the **UUID** value. If no **UUID (Logical)** value is set, this item is not displayed on the **iLO Overview** page.
- **Server Serial Number**—The server serial number, which is assigned when the system is manufactured. You can change this value by using the system RBSU during POST.
- **Serial Number (Logical)**—The system serial number that is presented to host applications. This value is displayed only when it has been set by other HP software, such as HP Virtual Connect Manager. This value might affect operating system and application licensing. The **Serial Number (Logical)** value is set as part of the logical server profile that is assigned to the system. If the logical server profile is removed, the serial number value reverts from the **Serial Number (Logical)** value to the **Server Serial Number** value. If no **Serial Number (Logical)** value is set, this item is not displayed on the **iLO Overview** page.
- **Product ID**—This value distinguishes between different systems with similar serial numbers. The product ID is assigned when the system is manufactured. You can change this value by using the system RBSU during POST.
- **System ROM**—The family and version of the active system ROM.
- **Backup System ROM**—The date of the backup system ROM. The backup system ROM is used if a system ROM update fails or is rolled back. This value is displayed only if the system supports a backup system ROM. For information about using the backup system ROM, see "Using iLO diagnostics" (page 112).
- **Integrated Remote Console**—Provides links to start the .NET IRC or Java IRC application for remote, out-of-band communication with the server console. For information about Remote Console requirements and features, see "Using the Integrated Remote Console" (page 114).

- **License Type**—The level of licensed iLO functionality.
- **iLO Firmware Version**—The version and date of the installed iLO firmware. Click the **iLO Firmware Version** link to navigate to the **Administration→iLO Firmware** page. For more information about firmware, see "Updating firmware" (page 25).
- **IP Address**—The network IP address of the iLO subsystem.
- **Link-Local IPv6 Address**—The SLAAC link-local address for iLO, followed by the address prefix length. Click the **Link-Local IPv6 Address** link to navigate to the **Network Summary** page.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. By default, the iLO host name is **ILO**, followed by the system serial number and the current domain name. This value is used for the network name and must be unique. You can change this name on the **Network General Settings** page for the **iLO Dedicated Network Port** or **Shared Network Port**.

Viewing status information

To view general status information, navigate to the **Information→Overview** page, as shown in Figure 43 (page 95).

The **Status** section displays the following information:

- **System Health**—The server health indicator. This value summarizes the condition of the monitored subsystems, including overall status and redundancy (ability to handle a failure). Click the **System Health** link to navigate to the **System Information→Health Summary** page. For more information about viewing system health information, see "Viewing health summary information" (page 97).
- **Server Power**—The server power state (**ON** or **OFF**).
- **UID Indicator**—The state of the UID. The UID helps you identify and locate a system, especially in high-density rack environments. The possible states are **UID ON**, **UID OFF**, and **UID BLINK**.

  You can change the UID state to **UID ON** or **UID OFF** by using the UID buttons on the server chassis or the UID control at the bottom of the browser window.

△ **CAUTION:** The UID blinks automatically to indicate that a critical operation is underway on the host, such as Remote Console access or a firmware update. Do not remove power from a server when the UID is blinking.

  When the UID is blinking, the **UID Indicator** displays the status **UID BLINK**. When the UID stops blinking, the status reverts to the previous value (**UID ON** or **UID OFF**). If a new state is selected while the UID is blinking, that state takes effect when the UID stops blinking.

- **TPM Status**—The current status of the TPM. If the host system or system ROM does not support TPM, the value **Not Supported** is displayed.
- **iLO Date/Time**—The internal clock of the iLO subsystem. The iLO clock can be synchronized automatically with the network.

Viewing the active iLO sessions

To view the active iLO sessions, navigate to the **Information→Overview** page, as shown in Figure 43 (page 95).

The **Active Sessions** section displays the following information for all users logged in to iLO:

- Login name
- IP address
- Source (for example, iLO web interface, Remote Console, or SSH)

Viewing iLO system information

The iLO **System Information** page displays the health of the monitored subsystems and devices.

The **System Information** page includes the following embedded health tabs: **Summary**, **Fans**, **Temperatures**, **Power**, **Processors**, **Memory**, **NIC Information**, and **Drives**.

Viewing health summary information

The **Health Summary** page displays the status of monitored subsystems and devices. Depending on the server type, the information on this page varies.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

To view health summary information, navigate to the **Information→System Information** page, and then click the **Summary** tab to view the list of monitored subsystems and devices, as shown in Figure 44 (page 97).

Redundancy information is available for the following items in the list:

- **Fan Redundancy**
- **Power Supply Redundancy**

Summarized status information is available for the following items in the list:

- **Fans**
- **Power Supplies**
- **Drives**
- **Temperatures**
- **VRMs**

Figure 44 System Information – Health Summary page

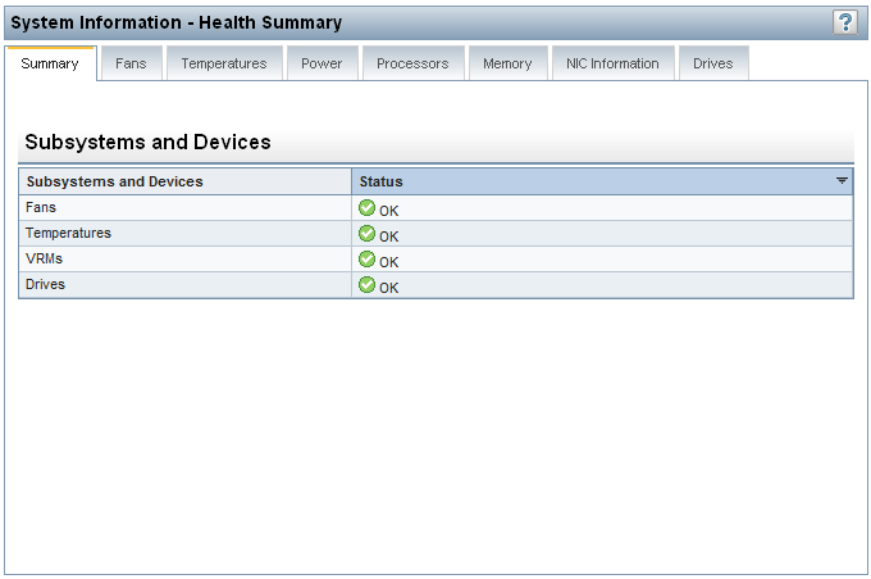


Table 7 (page 97) lists the displayed health status values.

Table 7 Health status values

Value	Description
Redundant	There is a backup component for the device or subsystem.
OK	The device or subsystem is working correctly.

Table 7 Health status values *(continued)*

Value	Description
Not Redundant	There is no backup component for the device or subsystem.
Failed Redundant	The device or subsystem is in a nonoperational state.
Failed	One or more components of the device or subsystem are nonoperational.
Other	Navigate to the **System Information** page of the component that is reporting this status for more information.

Viewing fan information

The iLO firmware, in conjunction with the hardware, controls the operation and speed of the fans. Fans provide essential cooling of components to ensure reliability and continued operation. The fans react to the temperatures monitored throughout the system to provide sufficient cooling with minimal noise.

Fan operation policies might differ from server to server based on fan configuration and cooling demands. Fan control takes into account the internal temperature of the system, increasing the fan speed to provide more cooling, and decreasing the fan speed if cooling is sufficient. In the event of a fan failure, some fan operation policies might increase the speed of the other fans, record the event in the IML, or turn LED indicators on.

Monitoring the fan subsystem includes the sufficient, redundant, and nonredundant fan configurations. If one or more fans fail, the server still provides sufficient cooling to continue operation.

In nonredundant configurations, or redundant configurations where multiple fan failures occur, the system might be incapable of providing sufficient cooling to protect the system from damage and to ensure data integrity. In this case, in addition to the cooling policies, the system might start a graceful shutdown of the operating system and server.

To view fan information, navigate to the **Information→System Information** page, and then click the **Fans** tab.

The information displayed on this page varies depending on the server type.

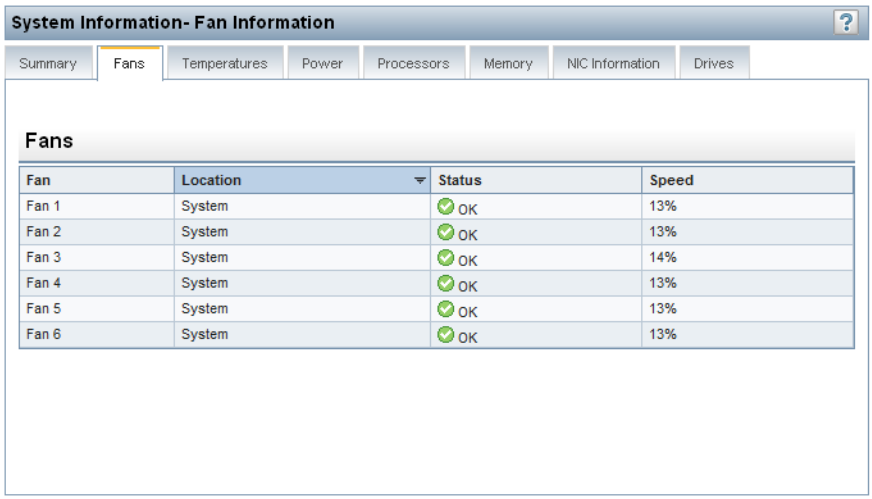
If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

The following information is displayed:

- **Rack servers**—The following information is displayed for each fan in the server chassis:
  - Location
  - Status
  - Speed

  Figure 45 (page 99) shows the **Fan Information** page for a rack server.

Figure 45 System Information – Fan Information page for rack servers



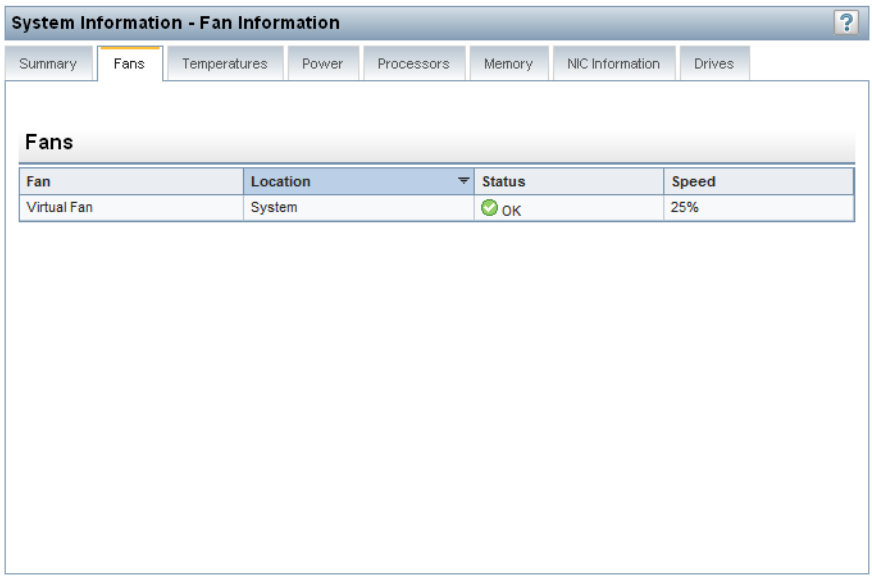
- **Blade servers**—ProLiant c-Class server blades use the enclosure fans to provide cooling because they do not have internal fans. The enclosure fans are called "virtual fans" on this page. The virtual-fan reading represents the cooling amount that a server blade is requesting from the enclosure. The server blade calculates the amount of cooling required by examining various temperature sensors and calculating an appropriate fan speed. The enclosure uses information from all of the installed server and nonserver blades to adjust the fans to provide the appropriate enclosure cooling.

  The following information is displayed for virtual fans:

  - Location
  - Status
  - Speed

  Figure 46 (page 99) shows the **Fan Information** page for a blade server.

Figure 46 System Information – Fan Information page for blade servers



Viewing temperature information

The **Temperature Information** page displays the location, status, temperature, and threshold settings of temperature sensors in the server chassis.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

The temperature is monitored to maintain the sensor location temperature below the caution threshold. If one or more sensors exceed this threshold, iLO implements a recovery policy to prevent damage to server components.

- If the temperature exceeds the caution threshold, the fan speed is increased to maximum.
- If the temperature exceeds the caution threshold for 60 seconds, a graceful server shutdown is attempted.
- If the temperature exceeds the critical threshold, the server is shut down immediately to prevent permanent damage.

Monitoring policies differ depending on the server requirements. Policies usually include increasing fan speeds to maximum cooling, logging temperature events in the IML, providing a visual indication of events by using LED indicators, and starting a graceful shutdown of the operating system to avoid data corruption.

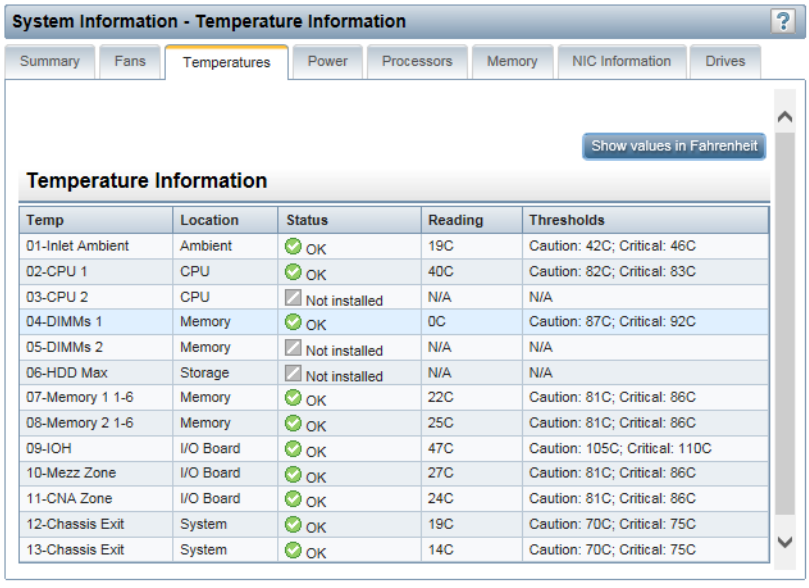
Additional policies are implemented after an excessive temperature condition is corrected, including returning the fan speed to normal, recording the event in the IML, turning off the LED indicators, and canceling shutdowns in progress (if applicable).

Viewing temperature sensor data

To view temperature sensor data, navigate to the **Information→System Information** page, and then click the **Temperatures** tab, as shown in Figure 47 (page 100).

When temperatures are displayed in Celsius, click the **Show values in Fahrenheit** button to change the display to Fahrenheit. When temperatures are displayed in Fahrenheit, click the **Show values in Celsius** button to change the display to Celsius.

Figure 47 Viewing temperature sensor data



The **Temperature Information** page table displays the following information:

- **Temp**—The ID of the temperature sensor.
- **Location**—The area where the temperature is being measured.

  In this column, **Memory** refers to the following:

  - Temperature sensors located on physical memory DIMMs.
  - Temperature sensors located close to the memory DIMMs, but not located on the DIMMs. These sensors are located further down the airflow cooling path, near the DIMMs, to provide additional temperature information.
- **Status**—The temperature status. Depending on the server configuration, some sensors show a status of **Not installed**.
- **Reading**—The temperature recorded by the listed temperature sensor. If a temperature sensor is not installed, the **Reading** column shows the value **N/A**.
- **Thresholds**—The temperature thresholds for the warning for overheating conditions. The two threshold values are **Caution** and **Critical**. If a temperature sensor is not installed, the **Thresholds** column shows the value **N/A**.
  - **Caution**—The server is designed to maintain a temperature below the caution threshold while operating. If a failure prevents the server from maintaining this temperature, the server increases the fan speed and initiates a graceful operating system shutdown. This ensures both data integrity and system safety.
  - **Critical**—If temperatures are uncontrollable or rise quickly, the critical temperature threshold prevents system failure by physically shutting down the system before the high temperature causes an electronic component failure.

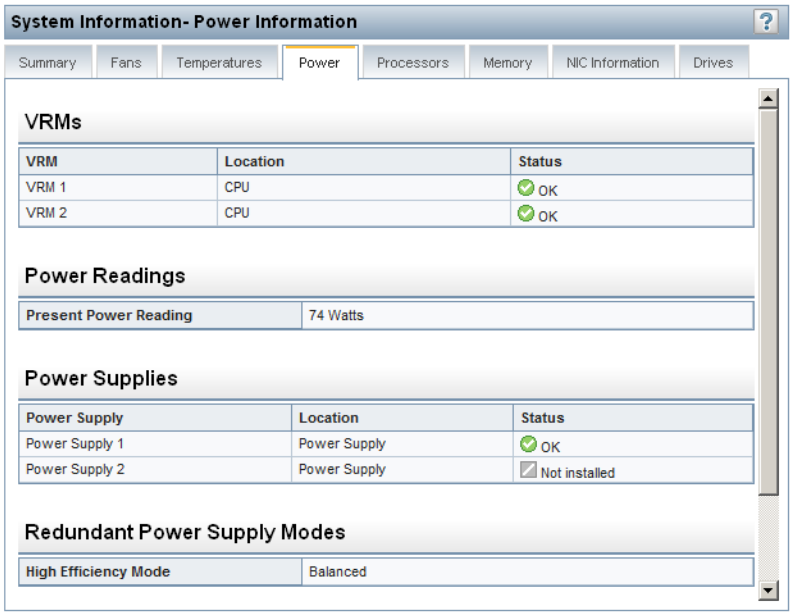
Viewing power information

iLO monitors the power supplies in the server to ensure the longest available uptime of the server and operating system. Power supplies might be affected by brownouts and other electrical conditions, or AC cords might be unplugged accidentally. These conditions result in a loss of redundancy if redundant power supplies are configured, or result in a loss of operation if redundant power supplies are not in use. If a power supply failure is detected (hardware failure) or the AC power cord is disconnected, events are recorded in the IML and LED indicators are used.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

To view power information, navigate to the **Information**→**System Information** page, and then click the **Power** tab, as shown in Figure 48 (page 102).

Figure 48 System Information – Power Information page



The information displayed on this page varies depending on the server type.

- **Rack servers**—The page displays **VRMs**, **Power Readings**, **Power Supplies**, **Redundant Power Supply Modes**, and **Power Microcontroller**.
- **Blade servers**—The page displays **VRMs**, **Power Readings** and **Power Microcontroller**.

Depending on the server type, this page displays the following information:

- **VRMs**—Voltage regulators, either modular (VRMs) or integrated devices (VRDs), are used and monitored in some systems.

  In some servers, VRMs are required for each processor in the system. They adjust the power to suit the needs of the supported processor. A VRM can be replaced if it fails. A failed VRM prevents the processor from being supported. The VRM name, location, and status are displayed.
- **Present Power Reading**—The most recent power reading from the server.
- **Power Supplies**—The name, location, and status of the installed power supplies.
  - **OK**—Indicates that the power supply is installed and operational.
  - **Not Installed**—Indicates that the power supply is not installed. Power is not redundant.
  - **Failed**—Indicates that the power supply is not functioning. Ensure that the power cord is plugged in.
  - **Mismatched Supply Types**—Indicates that multiple types of power supplies are installed and that this power supply is not in use. If mismatched power supply types are installed, only one type is used. For correct operation at the power subsystem, ensure that the power supplies are the same type, wattage, and part number.
- **Redundant Power Supply Modes**—Identifies the redundant power supply mode that will be used if redundant power supplies are configured.

  High Efficiency Mode improves the power efficiency of the system by placing the secondary power supplies in standby mode. When the secondary power supplies are in standby mode, primary power provides all DC power to the system. The power supplies are more efficient (more DC output watts for each watt of AC input) at higher output levels, and the overall power efficiency improves.

High Efficiency Mode does not affect power redundancy. If the primary power supplies fail, then the secondary power supplies immediately begin supplying DC power to the system, preventing any downtime. You can configure redundant power supply modes only through the system RBSU. You cannot modify these settings through iLO. For more information, see the *HP ROM-Based Setup Utility User Guide*.

The available redundant power supply modes are:

- **Balanced Mode**—Shares the power delivery equally between all installed power supplies.
- **High Efficiency Mode (Auto)**—Delivers full power to one of the power supplies and places the other power supplies on standby at a lower power-usage level. A semi-random distribution is achieved, because the Auto option chooses between the odd or even power supply based on the server serial number.
- **High Efficiency Mode (Even Supply Standby)**—Delivers full power to the odd-numbered power supplies, and places the even-numbered power supplies on standby at a lower power-usage level.
- **High Efficiency Mode (Odd Supply Standby)**—Delivers full power to the even-numbered power supplies, and places the odd-numbered power supplies on standby at a lower power-usage level.

- **Power Microcontroller**—Displays the firmware version of the power microcontroller. The server must be powered on in order for iLO to determine the power microcontroller firmware version.

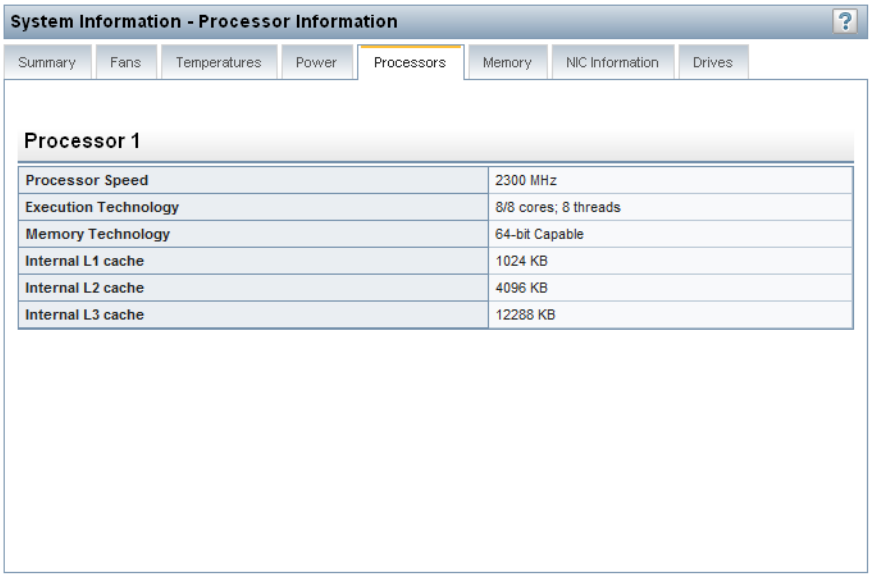
Viewing processor information

The **Processor Information** page displays the available processor slots, the type of processor installed in each slot, and a summary of the processor subsystem.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

To view the **Processor Information** page, navigate to the **Information→System Information** page, and then click the **Processors** tab, as shown in Figure 49 (page 103).

Figure 49 System Information – Processor Information page



The following information is displayed:

- **Processor Speed**—The speed of the processor
- **Execution Technology**—Information about the processor cores and threads
- **Memory Technology**—The processor memory capabilities
- **Internal L1 cache**—The L1 cache size
- **Internal L2 cache**—The L2 cache size
- **Internal L3 cache**—The L3 cache size

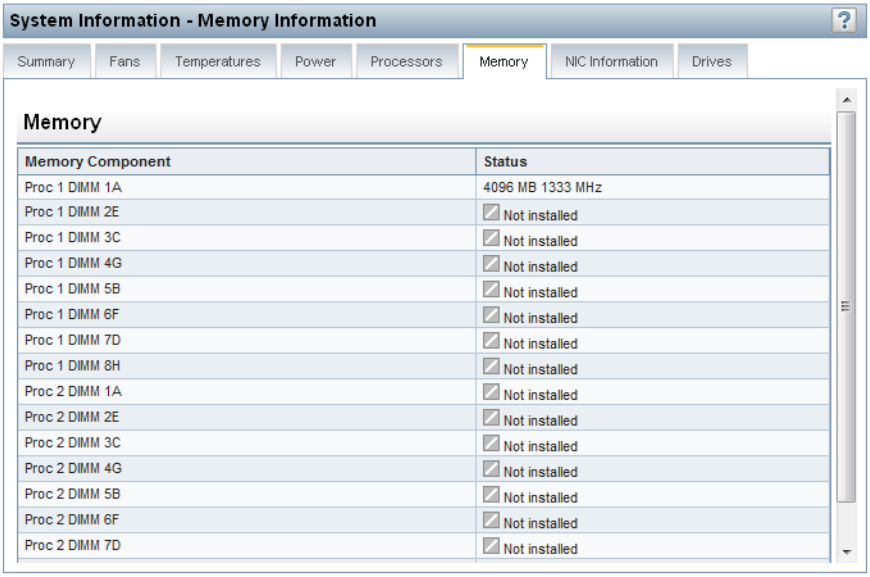
Viewing memory information

The **Memory Information** page displays a list of the memory modules in the host that are installed and operational at POST. In some systems with large memory module populations, all module positions might not be listed.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

To view memory information, navigate to the **Information→System Information** page, and then click the **Memory** tab, as shown in Figure 50 (page 104).

Figure 50 System Information – Memory Information page



The following information is displayed:

- **Memory Component**—The memory module location.
- **Status**—The memory size and frequency. If a module is not installed, the value **Not installed** is displayed.

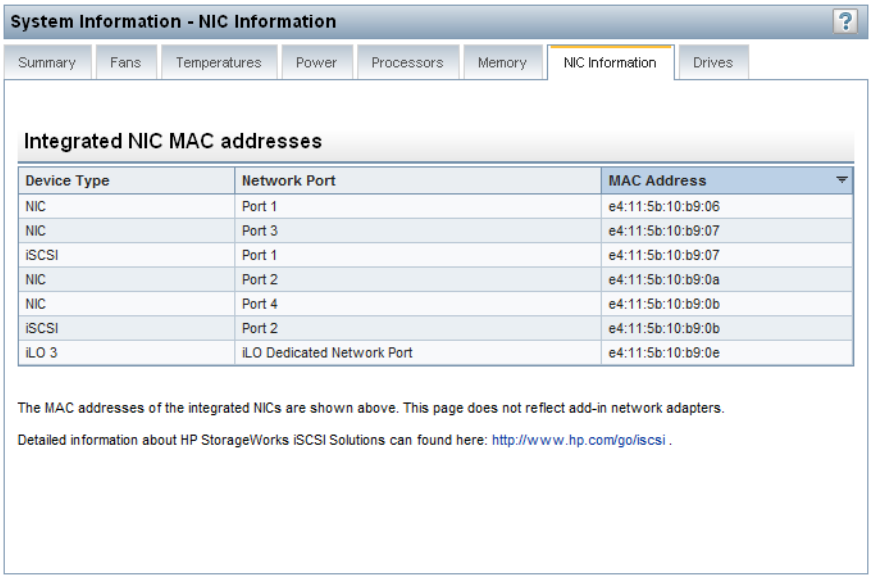
Viewing network information

The **NIC Information** page displays read-only information about the integrated NICs.

If the server is powered off, the system health information on this page is current as of the last power off. Health information is updated only when the server is powered on and POST is complete.

To view NIC information, navigate to the **Information→System Information** page, and then click the **NIC Information** tab, as shown in Figure 51 (page 105).

Figure 51 System Information – NIC Information page



The following information is displayed:

- **Device Type**—The device type is one of the following:
  - **iLO 3**—This device type is assigned to the iLO Dedicated Network Port or iLO Shared Network Port. Users who have the Configure iLO Settings privilege can configure the iLO NIC settings on the **General** tab of the **Network→iLO Dedicated Network Port** or **Network→Shared Network Port** page.
  - **NIC**—This device type indicates NIC or LAN adapter components embedded in the server or added after manufacturing. Because system NICs are directly available to the server host operating system, the iLO firmware cannot directly obtain current IP addresses (or other configuration settings) for these devices.
  - **iSCSI**—iSCSI implements the SCSI protocol for interacting with storage devices over a TCP/IP network. This reduces the cost and complexity of having shared network storage. If this table shows iSCSI in the Device Type column, then the listed network port supports iSCSI. If the same port also lists the NIC Device Type, then this is a multifunction network adapter that combines Ethernet and iSCSI capabilities in a single NIC interface, including support for TCP/IP offload engine and iSCSI acceleration.

    Using the iSCSI protocol, HP ProLiant servers can connect to any valid iSCSI target in the IP network and map to a logical drive. The iSCSI initiator on ProLiant servers sees a logical SCSI block device, regardless of whether the volume on the target is a physical disk, an array, or a SAN volume. Several HP product families incorporate iSCSI target support as one of the primary means for servers to access their storage resources. You can find detailed information about HP iSCSI Solutions at http://www.hp.com/go/iscsi.
- **Network Port**—The configured network port name.
- **MAC Address**—The port MAC address.

This page shows the system NIC and iSCSI port and MAC Addresses.

NOTE: This page does not display add-in network adapters.

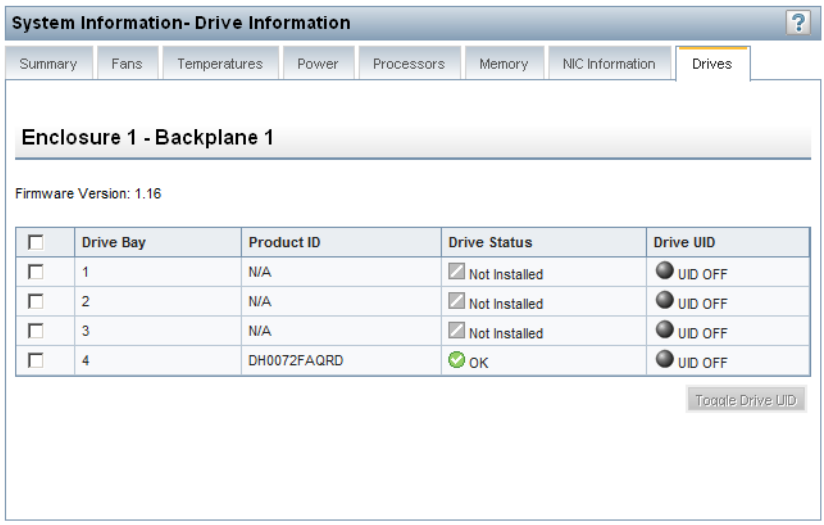
Viewing drive information

The **Drive Information** page displays information about each hard drive installed in the server.

NOTE: Drive information is available only on systems that have supported hardware.

To view drive information, navigate to the **Information→System Information** page, and then click the **Drives** tab. See Figure 52 (page 106).

Figure 52 System Information – Drive Information page



The following information is displayed:

- Firmware version
- Drive bay number
- Product ID
- Drive status
- Drive UID status

The UID lights can be toggled to help physically identify the drives. To toggle the UID light of a drive, select the check box to the left of the Drive Bay number, and then click **Toggle Drive UID**.

Using the iLO Event Log

The iLO Event Log provides a record of significant events detected by iLO. Logged events include major server events such as a server power outage or a server reset, and iLO events such as unauthorized login attempts. Other logged events include successful or unsuccessful browser and Remote Console logins, virtual power and power-cycle events, clearing the log, and some configuration changes, such as creating or deleting a user.

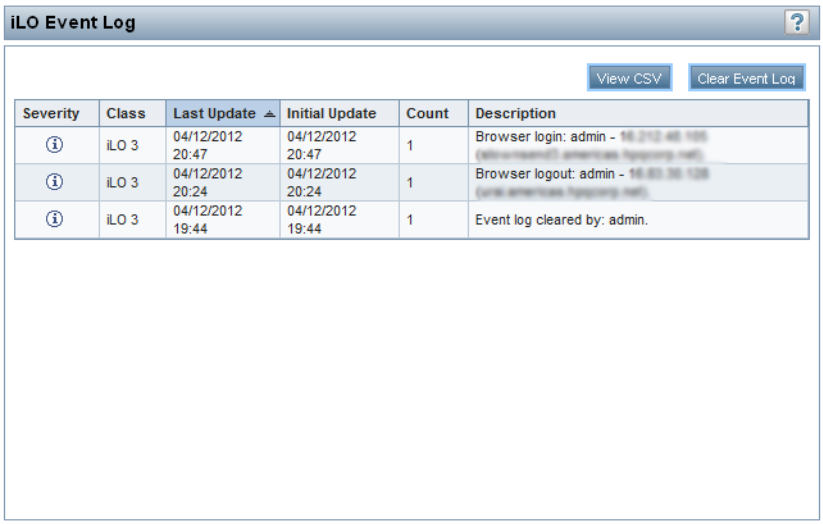
iLO provides secure password encryption, tracking all login attempts and maintaining a record of all login failures. The **Authentication Failure Logging** setting allows you to configure logging criteria for failed authentications. The Event Log captures the client name for each logged entry to improve auditing capabilities in DHCP environments, and records the account name, computer name, and IP address.

Earlier versions of iLO firmware might not support events logged by later versions of iLO firmware. If an unsupported firmware version logs an event, the event is listed as `UNKNOWN EVENT TYPE`. You can clear the event log to eliminate these entries, or update the firmware to the latest supported version.

Viewing the iLO Event Log

To view the iLO Event Log, navigate to the **Information→iLO Event Log** page, as shown in Figure 53 (page 107).

Figure 53 iLO Event Log page



The iLO Event Log displays the following information:

- **Severity**—The importance of the detected event.

  Possible values follow:

  - **Informational**—The event provides background information.
  - **Caution**—The event is significant but does not indicate performance degradation.
  - **Critical**—The event indicates a service loss or imminent service loss. Immediate attention is needed.

- **Class**—The component or subsystem that identified the logged event.
- **Last Update**—The date and time, as reported by the server clock, when the latest event of this type occurred. This value is based on the date and time stored by iLO.

  The iLO date and time can be synchronized through the following:

  - System ROM (during POST)
  - Insight Management Agents (in the OS)
  - SNTP setting in iLO
  - SNTP setting in OA (blade servers only)

  If iLO did not recognize the date and time when an event was updated, `[NOT SET]` is displayed.

- **Initial Update**—The date and time, as reported by the server clock, when the first event of this type occurred. This value is based on the date and time stored by iLO.

  If iLO did not recognize the date and time when the event was first created, `[NOT SET]` is displayed.

- **Count**—The number of times this event has occurred (if supported).

  In general, serious events generate an event log entry each time they occur. They are not consolidated into one event log entry.

When less important events are repeated, they are consolidated into one event log entry, and the **Count** and **Last Update** values are updated. Each event type has a specific time interval that determines whether repeated events are consolidated or a new event is logged.

- **Description**—The description identifies the component and detailed characteristics of the recorded event.

  If the iLO firmware is rolled back to an earlier version, the description `UNKNOWN EVENT TYPE` might be displayed for events recorded by the newer firmware. You can resolve this issue by updating the firmware to the latest supported version, or by clearing the event log.

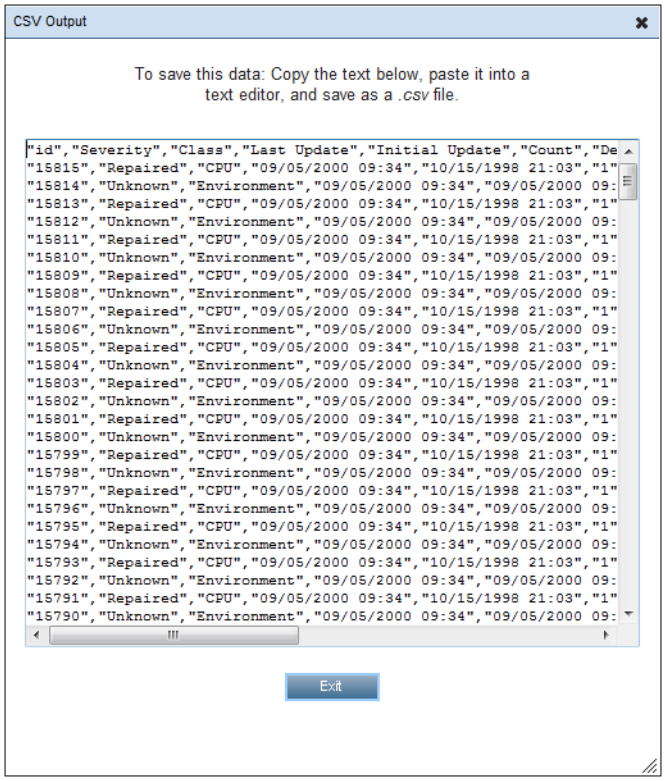
Saving the iLO Event Log

To save the iLO Event Log as a CSV file:

1. Click the **View CSV** button.

   The iLO Event Log is displayed in a format that you can copy and paste into a text editor, as shown in Figure 54 (page 108).

Figure 54 CSV Output window



2. Copy the text displayed in the **CSV Output** window, and save it in a text editor as a `*.csv` file.
3. Click **Exit** to close the window.

Clearing the iLO Event Log

Users with the Configure iLO Settings privilege can clear the iLO Event Log of all previously logged information.

To clear the iLO Event Log:

1. Click **Clear Event Log**.

   The following message appears:

   `Are you sure you want to clear the iLO Event Log?`

2. Click **OK**.

   The following event is recorded:

   ```
   Event log cleared by <user name>.
   ```

Using the Integrated Management Log

The IML provides a record of historical events that have occurred on the server. Events are generated by the system ROM and by services such as the iLO health driver. Logged events include all server-specific events recorded by the system health driver, including operating system information and ROM-based POST codes.

Entries in the IML can help you diagnose issues or identify potential issues. Preventative action might help to avoid disruption of service. iLO manages the IML, which you can access through a supported browser, even when the server is off. The ability to view the log when the server is off can be helpful when troubleshooting remote host server issues.

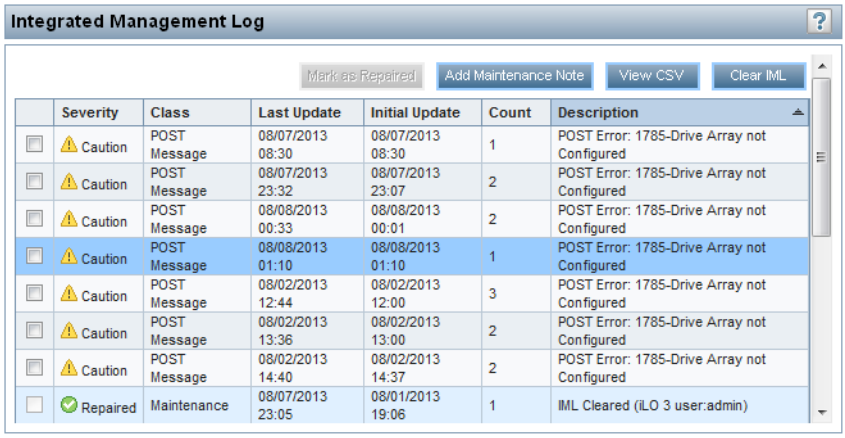
Examples of the types of information that the iLO processor records in the IML follow:

- Fan inserted
- Fan removed
- Fan failure
- Fan degraded
- Fan repaired
- Fan redundancy lost
- Fans redundant
- Power supply inserted
- Power supply removed
- Power supply failure
- Power supplies redundancy lost
- Power supplies redundant
- Temperature over threshold
- Temperature normal
- Automatic shutdown started
- Automatic shutdown canceled
- Drive failure

Viewing the IML

To view the IML, navigate to the **Information→Integrated Management Log** page, as shown in Figure 55 (page 110).

Figure 55 Integrated Management Log page



The log displays the following information:

- **Severity**—The importance of the detected event.

  Possible values follow:

  - **Informational**—The event provides background information.
  - **Caution**—The event is significant but does not indicate performance degradation.
  - **Critical**—The event indicates a service loss or an imminent service loss. Immediate attention is needed.
  - **Repaired**—An event has undergone corrective action.
- **Class**—Identifies the component or subsystem that identified the logged event.
- **Last Update**—The date and time, as reported by the server clock, when the latest event of this type occurred. This value is based on the date and time stored by iLO.

  The iLO date and time can be synchronized through the following:

  - System ROM (during POST only)
  - Insight Management Agents (in the OS)
  - NTP server (configured in iLO)
  - Onboard Administrator (blade servers only)

  If iLO did not recognize the date and time when an event was updated, `[NOT SET]` is displayed.
- **Initial Update**—The date and time, as reported by the server clock, when the first event of this type occurred. This value is based on the date and time stored by iLO.

  If iLO did not recognize the date and time when the event was first created, `[NOT SET]` is displayed.
- **Count**—The number of times this event has occurred (if supported).

  In general, serious events generate an event log entry each time they occur. They are not consolidated into one event log entry.

When less important events are repeated, they are consolidated into one event log entry, and the **Count** and **Last Update** values are updated. Each event type has a specific time interval that determines whether repeated events are consolidated or a new event is logged.

- **Description**—The description identifies the component and detailed characteristics of the recorded event.

  If the iLO firmware is rolled back, the description `UNKNOWN EVENT TYPE` might be displayed for events recorded by the newer firmware. You can resolve this issue by updating the firmware to the latest supported version, or by clearing the log.

Marking a log entry as repaired

Use this feature to change the status of an IML log entry from **Critical** or **Caution** to **Repaired**. You must have the Configure iLO Settings privilege to use this feature.

When a **Critical** or **Caution** event is reported in the IML log:

1. Investigate and repair the issue.
2. Navigate to the **Information**→**Integrated Management Log** page.
3. Select the log entry.
4. Click **Mark as Repaired**.

   The iLO web interface refreshes, and the selected log entry status changes to **Repaired**.

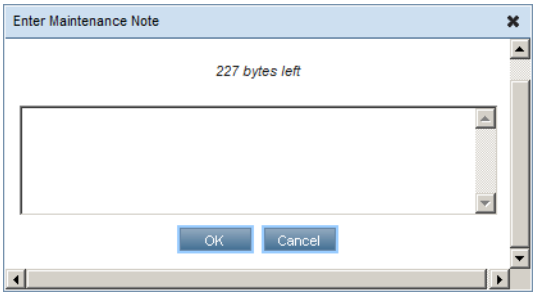
Adding a maintenance note to the IML

Use the maintenance note feature to create a log entry that logs information about maintenance activities such as component upgrades, system backups, periodic system maintenance, or software installations. You must have the Configure iLO Settings privilege to use this feature.

1. Navigate to the **Information**→**Integrated Management Log** page.
2. Click **Add Maintenance Note**.

   The **Enter Maintenance Note** window opens, as shown in Figure 56 (page 111).

Figure 56 Enter Maintenance Note window



3. Enter the text that you want to add as a log entry, and then click **OK**.

   You can enter up to 227 bytes of text. You cannot submit a maintenance note without entering some text.

   An **Informational** log entry with the class **Maintenance** is added to the IML.

Saving the IML

To save the IML as a CSV file:

1. Click the **View CSV** button.

   The IML is displayed in a format that you can copy and paste into a text editor.

2. Copy the text displayed in the **CSV Output** window, and save it in a text editor as a `*.csv` file.

3. Click **Exit** to close the window.

Clearing the IML

To clear the IML of all previously logged information:

1. Click **Clear IML**.

   The following message appears:

   ```
   Are you sure you want to clear the Integrated Management Log?
   ```

2. To confirm that you want to clear the IML, click **OK**.

   The following event is recorded:

   ```
   IML Cleared by <user name>.
   ```

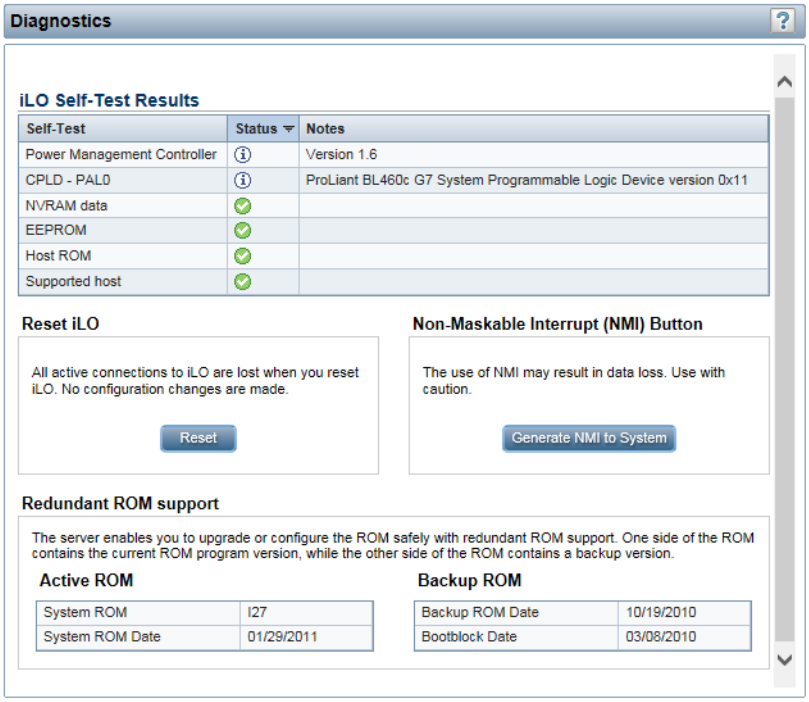
You can also clear the IML from the server HP System Management Homepage.

Using iLO diagnostics

The **Diagnostics** page displays iLO self-test results and allows you to reset iLO or generate an NMI to the system.

To view iLO diagnostics information, navigate to the **Information**→**Diagnostics** page, as shown in Figure 57 (page 112).

Figure 57 Diagnostics page



The **Diagnostics** page contains the following sections:

- **iLO Self-Test Results**—This section displays the results of internal iLO diagnostics.
  - The status of each self-test is listed in the **Status** column. Move the cursor over the status icons to view a tooltip description. If a status has not been reported for a test, the test is not listed.
  - The tests that are run are system dependent. Not all tests are run on all systems. View the list on the **Diagnostics** page to verify which tests are performed on your system.
  - A test might include additional information in the **Notes** column. This column show the versions of other system programmable logic, such as the System Board PAL or the Power Management Controller.
- **Reset iLO**—This section contains the **Reset** button, which enables you to reboot the iLO processor. Using **Reset** does not make any configuration changes, but ends all active connections to iLO. If a firmware file upload is in progress, it is terminated. If a firmware flash is in progress, you cannot reset iLO until the process is finished. You must have the Configure iLO Settings privilege to use this feature.
- **Non-Maskable Interrupt (NMI) button**—This section contains the **Generate NMI to System** button, which enables you to stop the operating system for debugging. The Virtual Power and Reset privilege is required to generate an NMI.

△ **CAUTION:** Generating an NMI as a diagnostic and debugging tool is used primarily when the operating system is no longer available. NMI is not used during normal operation of the server. Generating an NMI does not gracefully shut down the operating system, but causes the operating system to crash, resulting in lost service and data. Use the **Generate NMI to System** button only in extreme cases in which the operating system is not functioning properly and an experienced support organization has recommended that you proceed with an NMI.

Note the following:

- Use the Debug feature if a software application hangs the system. Use the **Generate NMI to System** button to engage the operating system debugger.
- Initiate the dump of an unresponsive host if you want to capture the server context.

- **Redundant ROM Support**—You can safely upgrade or configure the server ROM with redundant ROM support.
  - The **Active ROM** table shows the current version and the release date of the system ROM on the local machine.
  - The **Backup ROM** table shows the release date of the backup ROM and the release date of the backup ROM bootblock. The backup ROM is typically the previously installed version.

Resetting iLO through the web interface

If iLO is slow to respond, you might need to perform a reset.

1. Navigate to the **Information**→**Diagnostics** page in the iLO web interface.
2. Click **Reset**.

   Clicking **Reset iLO** does not make any configuration changes, but it ends all active connections to iLO. You must have the Configure iLO Settings privilege to use this feature.

For other reset methods, see "Resetting iLO" (page 230).

Using the HP Insight Management Agents

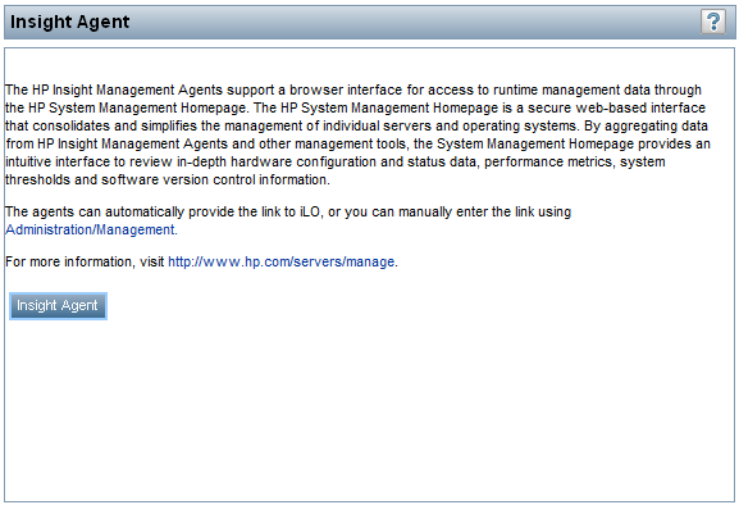
The HP Insight Management Agents support a browser interface for access to run-time management data through the HP System Management Homepage. The HP System Management Homepage is a secure web-based interface that consolidates and simplifies the management of individual servers and operating systems. By aggregating data from HP Insight Management Agents and other management tools, the HP System Management Homepage provides an intuitive interface to review in-depth hardware configuration and status data, performance metrics, system thresholds, and software version control information.

The agents can automatically provide the link to iLO, or you can manually enter the link on the **Administration→Management** page. For more information, see http://www.hp.com/servers/manage.

To open the HP System Management Homepage:

1. Navigate to the **Information→Insight Agent** page, as shown in Figure 58 (page 114).

Figure 58 Insight Agent page



2. Click the **Insight Agent** button to open the HP System Management Homepage.

Using the Integrated Remote Console

The iLO Integrated Remote Console is a graphical remote console that turns a supported browser into a virtual desktop, allowing full control over the display, keyboard, and mouse of the host server. Using the Remote Console also provides access to the remote file system and network drives.

With Integrated Remote Console access, you can observe POST boot messages as the remote host server restarts, and initiate ROM-based setup routines to configure the remote host server hardware. When you are installing operating systems remotely, the Integrated Remote Console (if licensed) enables you to view and control the host server monitor throughout the installation process.

iLO provides the following Integrated Remote Console access options:

- **.NET IRC**—Provides access to the system KVM, allowing control of Virtual Power and Virtual Media from a single console through a supported browser on a Windows client. In addition to the standard features, the .NET IRC supports Console Capture, Shared Console, Virtual Folder, and Scripted Media.
- **Java IRC**—Provides access to the system KVM, allowing control of Virtual Power and Virtual Media from a Java-based console. In addition to the standard features, the Java IRC includes the iLO disk image tool and Scripted Media.
- **Standalone IRC (HPLOCONS)**—Provides full iLO Integrated Remote Console functionality directly from your Windows desktop, without going through the iLO web interface. HPLOCONS has

the same functionality and requirements as the .NET IRC application that is launched from the iLO web interface. Download HPLOCONS from the HP website: http://www.hp.com/go/ilo.

- **iLO Mobile Application for iOS and Android devices**—Provides Integrated Remote Console access from your supported mobile phone or tablet. For more information, see http://www.hp.com/go/ilo/mobileapp.

For a list of supported browsers, see the "Browser support" (page 92).

.NET IRC requirements

This section lists the requirements for using the .NET IRC.

Microsoft .NET Framework

The .NET IRC requires one of the following versions of the Microsoft .NET Framework. You can use Windows Update to install the .NET Framework.

- .NET Framework 3.5 Full (SP1 recommended)
- .NET Framework 4.0 Full
- .NET Framework 4.5

The .NET Framework versions 3.5 and 4.0 have two deployment options: Full and Client Profile. The Client Profile is a subset of the Full framework. The .NET IRC is supported with the Full framework only; the Client Profile is not supported. Version 4.5 of the .NET Framework does not have the Client Profile option.

For Internet Explorer users only: The **.NET Framework Detection** table on the **iLO Integrated Remote Console** page lists the compatible .NET versions and indicates whether the installed version is compatible with the .NET IRC. If the installed version is compatible, the status **OK** is listed in the **Status** column.

Microsoft ClickOnce

The .NET IRC is launched using Microsoft ClickOnce, which is part of the .NET Framework. ClickOnce requires that any application installed from an SSL connection be from a trusted source. If a browser is not configured to trust an iLO system, and the **IRC requires a trusted certificate in iLO** setting is set to **Enabled**, ClickOnce displays the following error message:

```
Cannot Start Application - Application download did not succeed...
```

For more information, see "Configuring the Integrated Remote Console Trust setting (.NET IRC)" (page 67).

Note the following ClickOnce requirements:

- Mozilla Firefox requires an add-on to launch a ClickOnce application. You can launch the .NET IRC from a supported version of Firefox by using a ClickOnce add-on such as the Microsoft .NET Framework Assistant. You can download the .NET Framework Assistant from http://addons.mozilla.org/.
- Google Chrome requires an extension to launch a ClickOnce application. You can launch the .NET IRC from a supported version of Chrome by using the ClickOnce plug-in for the Chrome browser. You can download this extension from http://code.google.com/p/clickonceforchrome/.

Java IRC requirements

The Java IRC requires a supported version of the Java software.

To view the Java requirements or to download the Java software, navigate to the **Remote Console→Java** page, and then click the **Java** tab, as shown in Figure 59 (page 116).

Figure 59 Remote Console – Java page

Click the **Download** button to navigate to the following website and download the Java software: http://www.java.com/en/.

Recommended client settings

Ideally, the remote server display resolution is the same or lower than that of the client computer. Higher resolutions transmit more information, reducing the overall performance.

Use the following client and browser settings to optimize performance:

- **Display properties**
  - Select an option greater than 256 colors.
  - Select a screen resolution higher than that of the remote server.
  - Linux X Display properties—Set the font size to **12** on the **X Preferences** screen.
- **Mouse properties**
  - Set the mouse pointer speed to the middle setting.
  - Set the mouse pointer acceleration to low or disable it.

Recommended server settings

For all servers, note the following:

- To optimize performance, set the server display properties to use a plain background (no wallpaper pattern), and set the server mouse properties to disable pointer trails.
- To display the entire host server screen in the client Java IRC window, select a server display resolution that is less than or equal to that of the client.

For Red Hat Linux and SUSE Linux servers only, note the following: To optimize performance, set the value for server mouse properties pointer acceleration to **1x**. For KDE, access the **Control Center**, select **Peripherals/Mouse**, and then click the **Advanced** tab.

Configuring the Java IRC keyboard layout for Linux systems

1. Configure the client PC to use the required keyboard layout.
2. Configure the host server to use the required keyboard layout.

Starting the Remote Console

Users with the Remote Console privilege can use the .NET IRC and the Java IRC.

An iLO license must be installed to use this feature after the OS is started. Select **Administration→Licensing** to determine whether a license is installed. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.

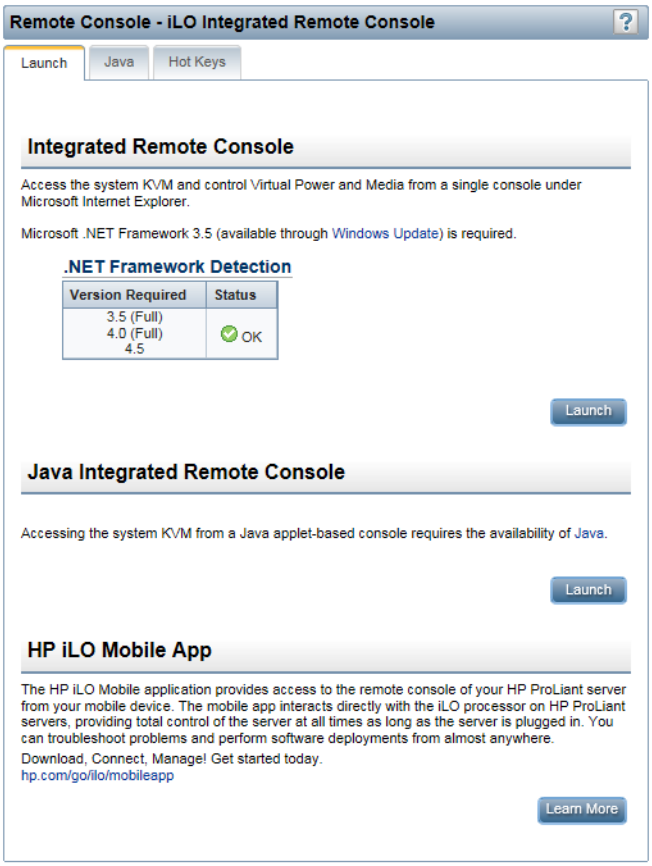
When using the Remote Console, note the following:

- The Java IRC is a signed Java applet. If you do not accept the Java IRC applet certificate, the Java IRC will not work. If you did not accept the certificate and you want to use the Java IRC:
  1. Click the **Clear** button in the **Java Console** window.
  2. Click the **Close** button to close the **Java Console** window.
  3. Reset iLO.
  4. Clear the browser cache.
  5. Close the browser and open a new browser window.
  6. Log in to iLO, start the Java IRC, and then accept the certificate.
- The Java IRC experiences a slight delay when the Java applet first loads in your browser.
- The Java IRC is a Java applet-based console that you launch from the iLO web interface. When you close the iLO web interface window, the Remote Console connection is also closed, and you will lose access to any Virtual Media devices that were connected through the Java IRC.
- The .NET IRC and Java IRC are suitable for high-latency (modem) connections.
- Do not run the .NET IRC or Java IRC from the host operating system on the server that contains the iLO management processor.
- HP recommends that users who log in to a server through the .NET IRC or Java IRC log out before closing the .NET IRC or Java IRC.
- Pop-up blockers prevent the .NET IRC or Java IRC from running, so you must disable them before starting a .NET IRC or Java IRC session. In some cases, you can **Ctrl+click** the .NET IRC or Java IRC **Launch** button to bypass the pop-up blocker and launch the .NET IRC or Java IRC.
- The UID blinks when a .NET IRC or Java IRC session is active.
- When you are finished using the Remote Console, exit the .NET IRC or Java IRC by closing the window or clicking the **Close** button.

To start the Remote Console:

1. Navigate to the **Remote Console** page, and then click the **Launch** tab, as shown in Figure 60 (page 118).

Figure 60 Remote Console – iLO Integrated Remote Console page



2. Verify that your system meets the requirements for using the .NET IRC or Java IRC.
3. Click the **Launch** button for the Remote Console that you want to use.

   If you attempt to open the Remote Console while it is in use, a warning message indicates that another user is using it. To view the Remote Console session that is in progress, follow the instructions in "Using Shared Remote Console (.NET IRC only)" (page 119). To take control of the session, follow the instructions in "Acquiring the Remote Console" (page 118).

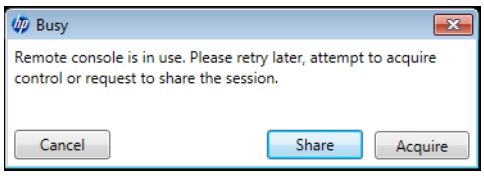
Acquiring the Remote Console

If another user is working in the Remote Console, you can acquire it from that user.

1. Start the .NET IRC or Java IRC.

   The system notifies you that another user is working in the Remote Console, as shown in Figure 61 (page 118).

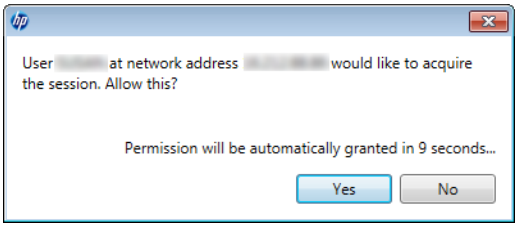
Figure 61 Acquiring the Remote Console



2. Click the **Acquire** button.

   The other user is prompted to approve or deny permission to acquire the Remote Console, as shown in Figure 62 (page 119).

Figure 62 Granting or denying permission to acquire the Remote Console



If there is no response in 10 seconds, permission is granted.

Using the Remote Console power switch

To use the power switch, select one of the following options from the power switch menu:

- **Momentary Press**—The same as pressing the physical power button. If a server is powered off, a momentary press will turn the server power on.

  Some operating systems might be configured to initiate a graceful shutdown after a momentary press, or to ignore this event. HP recommends using system commands to complete a graceful operating system shutdown before you attempt to shut down by using the Virtual Power button.

- **Press and Hold**—The same as pressing the physical power button for 5 seconds and then releasing it.

  The server is powered off as a result of this operation. Using this option might circumvent the graceful shutdown features of the operating system.

  This option provides the ACPI functionality that some operating systems implement. These operating systems behave differently depending on a short press or long press.

- **Cold Boot**—Immediately removes power from the server. Processors, memory, and I/O resources lose main power. The server will restart after approximately 6 seconds. Using this option circumvents the graceful shutdown features of the operating system.
- **Reset**—Forces the server to warm-boot: CPUs and I/O resources are reset. Using this option circumvents the graceful shutdown features of the operating system.

NOTE: The **Press and Hold**, **Reset**, and **Cold Boot** options are not available when the server is powered down.

Using iLO Virtual Media from the Remote Console

For instructions on using the Virtual Media feature from the Remote Console, see "Using iLO Virtual Media from the Remote Console" (page 137).

Using Shared Remote Console (.NET IRC only)

Shared Remote Console allows the connection of multiple sessions on the same server. This feature can be used for activities such as training and troubleshooting.

This feature and many others are part of an iLO licensing package. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.

The first user to initiate a Remote Console session connects to the server normally and is designated as the session leader. Any subsequent user who requests Remote Console access initiates an access request for a satellite client connection. A dialog box for each access request opens on the session leader's desktop, identifying the requester's user name and DNS name (if available) or IP address.

The session leader can grant or deny access. If there is no response, permission is denied automatically.

Shared Remote Console does not support passing the session leader designation to another user, or reconnecting a user after a failure. You must restart the Remote Console session to allow user access after a failure.

During a Shared Remote Console session, the session leader has access to all Remote Console features, whereas all other users can access only the keyboard and mouse. Satellite clients cannot control Virtual Power or Virtual Media.

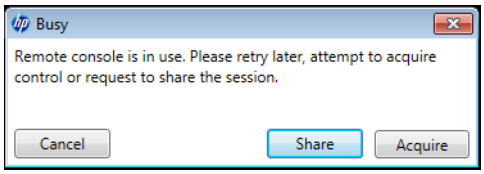
iLO encrypts Shared Remote Console sessions by authenticating the client first, and then the session leader determines whether to allow new connections.

To join a Shared Remote Console session:

1. Navigate to the **Remote Console→Remote Console** page.
2. Click **Launch** to start the .NET IRC.

   A message notifies you that the .NET IRC is already in use, as shown in Figure 63 (page 120).

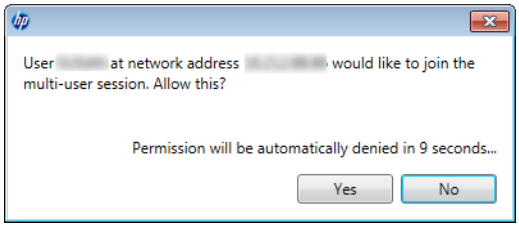
Figure 63 Remote Console Busy dialog box



3. Click **Share**.

   A message notifies the session leader that you are requesting to join the .NET IRC session, as shown in Figure 64 (page 120).

Figure 64 Shared Remote Console request



If the session leader clicks **Yes**, you are granted access to the .NET IRC session with access to the keyboard and mouse.

Using Console Capture (.NET IRC only)

Console Capture allows you to record and play back video streams of events such as startup, ASR events, and sensed operating system faults. The Server Startup and Server Prefailure sequences are captured automatically by iLO. You can manually start and stop the recording of console video.

This feature and many others are part of an iLO licensing package. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.

When you are using Console Capture, note the following:

- Console Capture is supported with the .NET IRC; it is not supported with the Java IRC.
- Console Capture is available only through the .NET IRC. It cannot be accessed through XML scripting or the CLP.
- The Server Startup and Server Prefailure sequences are not captured automatically during firmware upgrades or while the Remote Console is in use.

- Server Startup and Server Prefailure sequences are saved automatically in iLO memory. They will be lost during firmware upgrades, iLO reset, and power loss. You can save the captured video to your local drive by using the .NET IRC.
- The Server Startup file starts capturing when server startup is detected, and stops when it runs out of space. This file is overwritten each time the server starts.
- The Server Prefailure file starts capturing when the Server Startup file is full, and stops when iLO detects an ASR event. The Server Prefailure file is locked when iLO detects an ASR event. The file is unlocked and can be overwritten after it is downloaded through the .NET IRC.
- The Console Capture control buttons are located on the bottom of the .NET IRC session window. Table 8 (page 121) explains the playback controls used for viewing a captured video.

Table 8 Playback controls

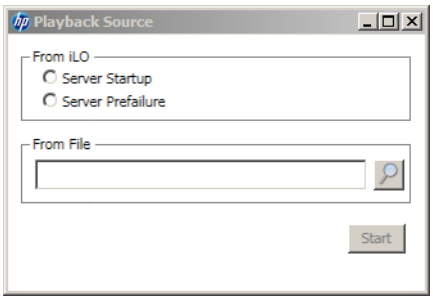
Control	Name	Function
	Skip to Start	Restarts playback from the beginning of the file
	Pause	Pauses the playback
	Play	Starts playback if the currently selected file is not playing or is paused
	Record	Records your .NET IRC session
	Progress Bar	Shows the progress of the video session

Viewing Server Startup and Server Prefailure sequences

1. Start the .NET IRC.
2. Press the **Play** button.

   The **Playback Source** dialog box opens, as shown in Figure 65 (page 121).

Figure 65 Playback Source dialog box



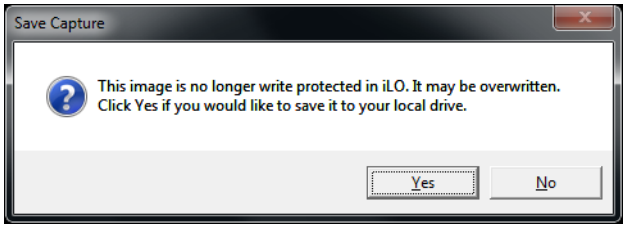
3. Select **Server Startup** or **Server Prefailure**.
4. Click **Start**.

Saving Server Startup and Server Prefailure video files

1. Start the .NET IRC
2. Press the **Play** button.
3. Select **Server Startup** or **Server Prefailure**.
4. Click **Start**.

5. Press the **Play** button again to stop playback.
   The **Save Capture** dialog box opens, as shown in Figure 66 (page 122).

Figure 66 Save Capture dialog box



6. Click **Yes**, and then follow the onscreen instructions to save the file.

Capturing video files

You can use Console Capture to manually capture video files of sequences other than Server Startup and Server Prefailure.

1. Start the .NET IRC.
2. Click the **Record** button.
3. The **Save Video** dialog box opens.
4. Enter a file name and save location, and then click **Save**.
5. When you are finished recording, press the **Record** button again to stop recording.

Viewing saved video files

1. Start the .NET IRC.
2. Press the **Play** button.
   The **Playback Source** dialog box opens, as shown in Figure 65 (page 121).
3. Click the magnifying glass icon next to the **From File** box.
4. Navigate to a video file, and then click **Open**.
   Video files captured in the Remote Console have the file type `.ilo`.
5. Click **Start**.

Using Remote Console hot keys

The **Program Remote Console Hot Keys** page allows you to define up to six hot keys to use during Remote Console sessions. Each hot key represents a combination of up to five keys that are sent to the host server when the hot key is pressed. Hot keys are active during Remote Console sessions that use .NET IRC, Java IRC, and the text-based Remote Console.

If a hot key is not set—for example, **Ctrl+V** is set to **NONE**, **NONE**, **NONE**, **NONE**, **NONE**—this hot key is disabled. The server operating system will interpret **Ctrl+V** as it usually does (paste, in this example). If you set the **Ctrl+V** hot key to use another combination of keys, the server operating system will use the key combination set in iLO (losing the paste functionality).

Example 1: If you want to send **Alt+F4** to the remote server, but pressing that key combination closes your browser, you can configure the hot key **Ctrl+X** to send the **Alt+F4** key combination to the remote server. After you configure the hot key, press **Ctrl+X** in the Remote Console window whenever you want to use **Alt+F4** on the remote server.

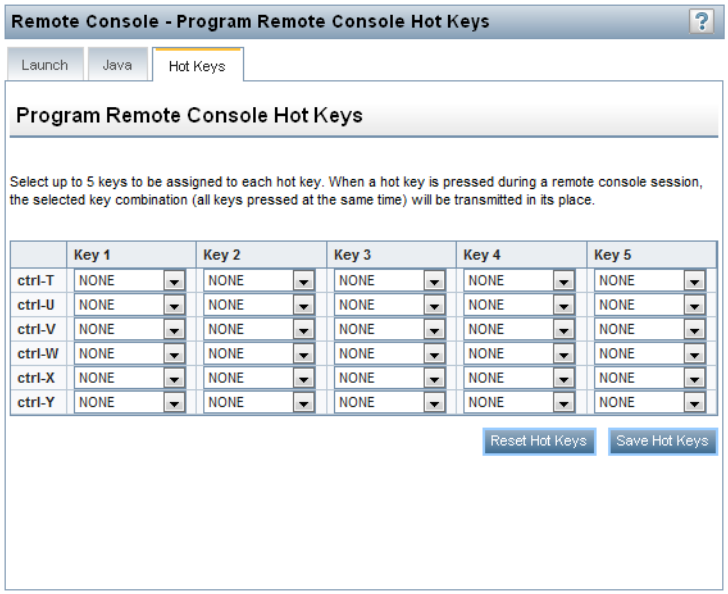
Example 2: If you want to create a hot key to send the international **AltGR** key to the remote server, use **R_ALT** in the key list.

Creating a hot key

You must have the Configure iLO Settings privilege to create hot keys.

1. Navigate to the **Remote Console→Hot Keys** page, as shown in Figure 67 (page 123).

Figure 67 Remote Console – Hot Keys page



2. For each hot key that you want to define, select the key combination to send to the remote server.

   To configure hot keys to generate key sequences from international keyboards, select the key on a U.S. keyboard that is in the same position as the desired key on the international keyboard. Table 9 (page 123) lists the available keys.

Table 9 Keys for configuring hot keys

ESC	SCRL LCK	1	g
L_ALT	SYS RQ	2	h
R_ALT	F1	3	I
L_SHIFT	F2	4	j
R_SHIFT	F3	5	k
L_CTRL	F4	6	l
R_CTRL	F5	7	m
L_GUI	F6	8	n
R_GUI	F7	9	o
INS	F8	;	p
DEL	F9	=	q
HOME	F10	[	r
END	F11	\	s
PG UP	F12	]	t
PG DN	SPACE	`	u
ENTER	'	a	v
TAB	,	b	w
BREAK	-	c	x

Table 9 Keys for configuring hot keys *(continued)*

BACKSPACE	.	d	y
NUM PLUS	/	e	z
NUM MINUS	0	f	

3. Click **Save Hot Keys**.
   The following message appears:
   ```
   Remote Console Hot Keys settings successful.
   ```

Resetting hot keys

Resetting the hot keys clears all current hot-key assignments.

1. Navigate to the **Remote Console→Hot Keys** page, as shown in Figure 67 (page 123).
2. Click **Reset Hot Keys**.
3. The following message appears:
   ```
   Are you sure you want to reset all hot keys?
   ```
4. Click **OK**.
   The following message appears:
   ```
   Remote Console Hot Keys reset successful.
   ```

Using the text-based Remote Console

iLO supports a true text-based Remote Console. Video information is obtained from the server, and the contents of the video memory are sent to the iLO management processor, compressed, encrypted, and forwarded to the management client application. iLO uses a screen-frame buffer that sends the characters (including screen positioning information) to text-based client applications. This method ensures compatibility with standard text-based clients, good performance, and simplicity. However, you cannot display non-ASCII or graphical information, and screen positioning information (displayed characters) might be sent out of order.

iLO uses the video adapter DVO port to access video memory directly. This method increases iLO performance significantly. However, the digital video stream does not contain useful text data. This data cannot be rendered by a text-based client application such as SSH.

There are two text-based console options, as described in the following sections:

- "Using the iLO Virtual Serial Port" (page 124)
- "Using the Text-based Remote Console (Textcons)" (page 129)

Using the iLO Virtual Serial Port

You can access a text-based console from iLO using a standard license and the iLO Virtual Serial Port.

The iLO Virtual Serial Port is one type of iLO text-based remote console. The iLO Virtual Serial Port gives you a bidirectional data flow with a server serial port. Using the remote console, you can operate as if a physical serial connection exists on the remote server serial port.

The iLO Virtual Serial Port is displayed as a text-based console, but the information is rendered through graphical video data. iLO displays this information through an SSH client when the server is in a pre-operating-system state, enabling a nonlicensed iLO to observe and interact with the server during POST activities.

By using the iLO Virtual Serial Port, the remote user can perform operations such as the following:

- Interact with the server POST sequence and the operating system boot sequence.

IMPORTANT: To start iLO RBSU during a Virtual Serial Port session, enter the key combination **ESC+8**.

- Establish a login session with the operating system, interact with the operating system; and execute and interact with applications on the operating system.
- For an iLO running Linux in a graphical format, you can configure `getty()` on the server serial port, and then use the iLO Virtual Serial Port to view a login session to the Linux operating system. For more information, see "Configuring the iLO Virtual Serial Port for Linux" (page 128).
- Use the EMS Console through the iLO Virtual Serial Port. EMS is useful for debugging Windows boot issues and kernel-level issues. For more information, see "Configuring the iLO Virtual Serial Port for the Windows EMS Console" (page 129).

Configuring the iLO Virtual Serial Port in the host system RBSU

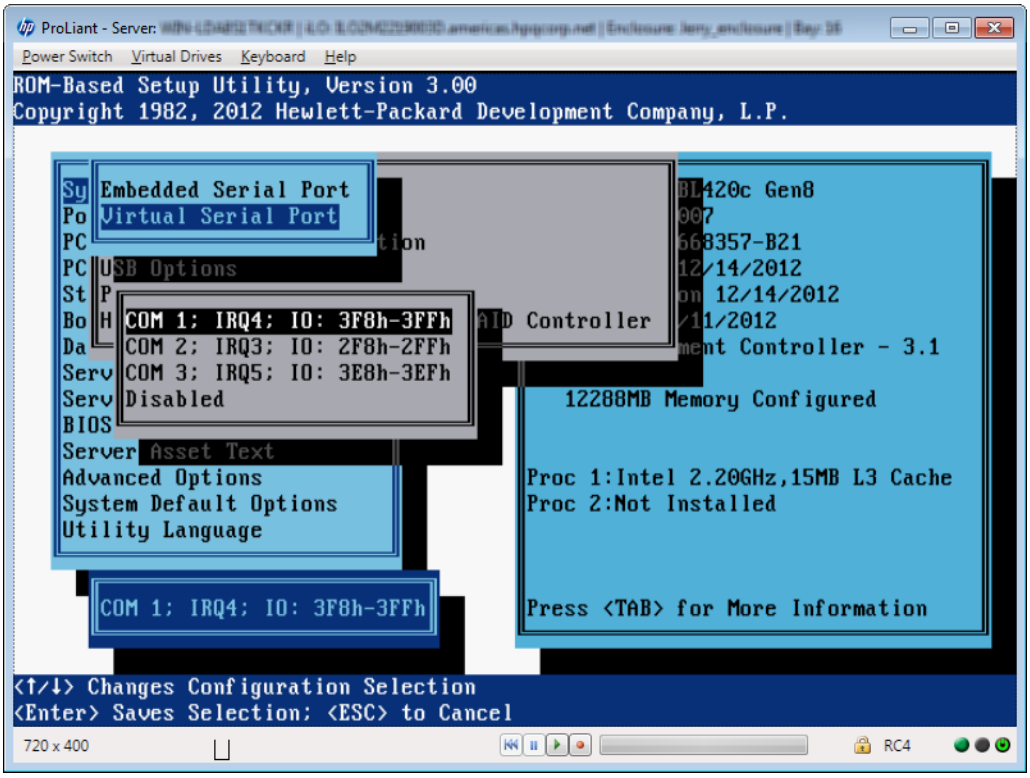
The following procedure describes the settings you must configure before you can use the iLO Virtual Serial Port. This procedure is required for both Windows and Linux systems.

1. Optional: If you access the server remotely, start an iLO remote console session.

   You can use the .NET IRC or Java IRC.
2. Restart or power on the server.
3. Press **F9** in the HP ProLiant POST screen.

   The System RBSU screen appears.
4. Select **System Options**, and then press **Enter**.
5. Select **Serial Port Options**, and then press **Enter**.
6. Select **Virtual Serial Port**, and then press **Enter**.
7. Select the COM port you want to use, and then press **Enter**, as shown in Figure 68 (page 125).

Figure 68 Configuring the Virtual Serial Port COM port (system RBSU)



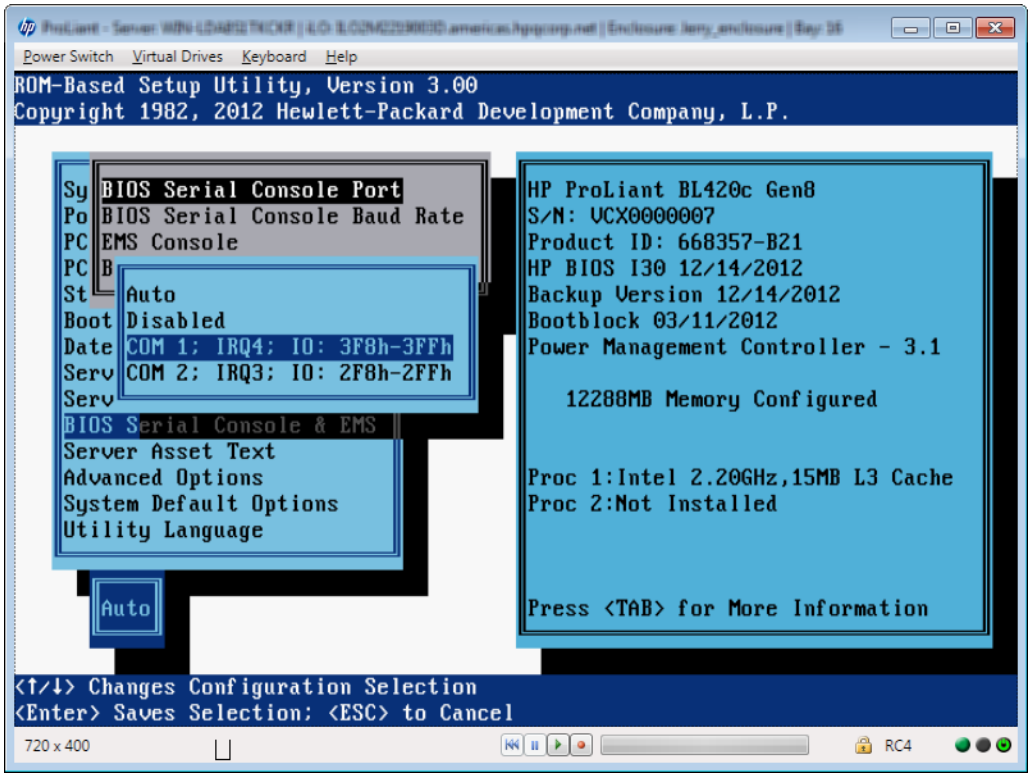
8. Press **ESC** twice to return to the main menu.

9. Select **BIOS Serial Console & EMS**, and then press **Enter**.

NOTE: EMS is for Windows only.

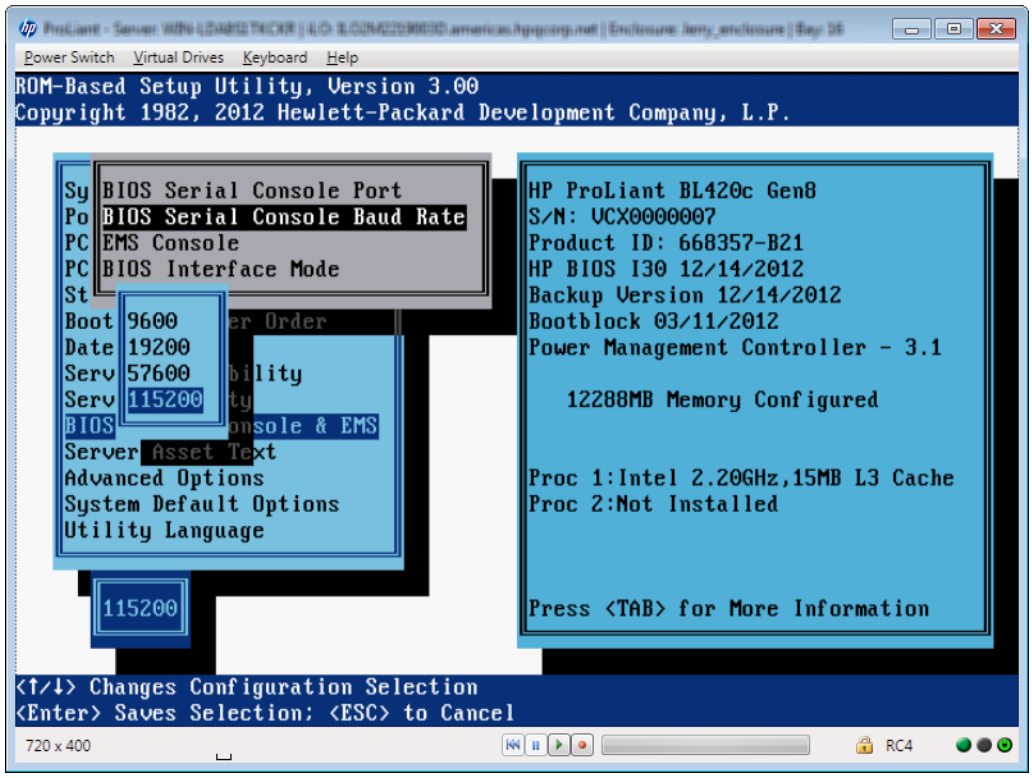
10. Select **BIOS Serial Console Port**, and then press **Enter**.
11. Select the COM port that matches the value selected in step 7, and then press **Enter**, as shown in Figure 69 (page 126).

Figure 69 Configuring the BIOS Serial Console Port



12. Select **BIOS Serial Console Baud Rate**, and then press **Enter**.
13. Select **115200**, and then press **Enter**, as shown in Figure 70 (page 127).

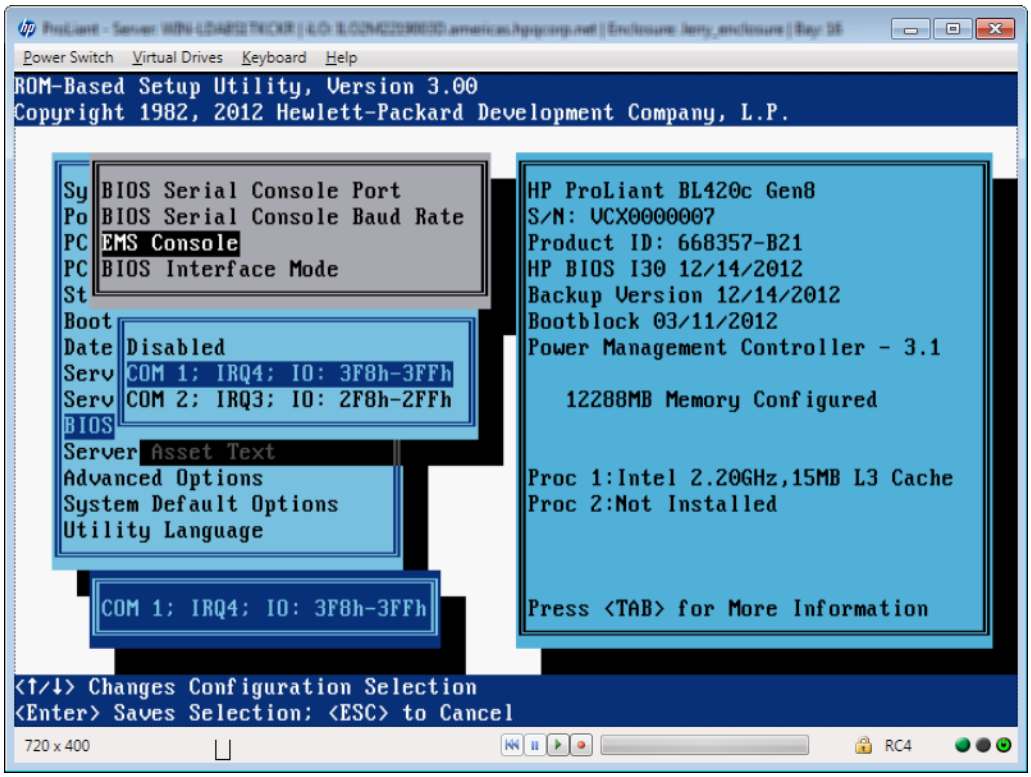
Figure 70 Configuring the BIOS Serial Console Baud Rate



NOTE: The current implementation of the iLO Virtual Serial Port does not use a physical UART, so the **BIOS Serial Console Baud Rate** value will have no effect on the actual speed the iLO Virtual Serial Port will use to send and receive data from the system.

14. Select **EMS Console**, and then press **Enter**.
15. Select the COM port that matches the value selected in step 7, and then press **Enter**, as shown in Figure 71 (page 128).

Figure 71 Configuring the EMS Console



16. Exit the system RBSU.

Configuring the iLO Virtual Serial Port for Linux

You can manage Linux servers remotely using console redirection. To configure Linux to use console redirection, you must configure the Linux boot loader (GRUB). The boot-loader application loads from the bootable device when the server system ROM finishes POST. Define the serial interface (ttyS0) as the default interface so that if no input arrives from the local keyboard within 10 seconds (the default timeout value), the system will redirect output to the serial interface (iLO Virtual Serial Port).

NOTE: ttyS0 and unit 0 are for com1 and ttyS1 and unit 1 are for com2.

The following configuration example uses Red Hat Linux and com1:

```
serial -unit=0 -speed=115200
terminal -timeout=10 serial console
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
title Red Hat Linux (2. 6.18-164.e15)
root (hd0,2)
9
kernel /vmlinux-2.6.18-164.e15 ro root=/dev/sda9 console=tty0 console=ttyS0,115200
initrd /initrd-2.6.18-164.e15.img
```

If com2 was selected, the configuration example would be as follows:

```
serial -unit=1 -speed=115200
terminal -timeout=10 serial console
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
title Red Hat Linux (2. 6.18-164.e15)
root (hd0,2)
9
kernel /vmlinux-2.6.18-164.e15 ro root=/dev/sda9 console=tty0 console=ttyS1,115200
initrd /initrd-2.6.18-164.e15.img
```

After Linux is fully booted, a login console can be redirected to the serial port.

- If configured, the `/dev/ttyS0` and `/dev/ttyS1` devices enable you to obtain serial TTY sessions through the iLO Virtual Serial Port. To begin a shell session on a configured serial port, add the following line to the `/etc/inittab` file to start the login process automatically during system boot.

  The following example initiates the login console on `/dev/ttyS0`:

  ```
  S0:2345:respawn:/sbin/agetty 115200 ttyS0 vt100
  ```

  The following example initiates the login console on `dev/ttys1`:

  ```
  S1:2345:respawn:/sbin/agetty 115200 ttyS1 vt100
  ```

- Use SSH to connect to iLO, and then use the iLO CLP command `start /system1/oemhp_vsp1` to view a login session to the Linux operating system.

Configuring the iLO Virtual Serial Port for the Windows EMS Console

iLO enables you to use the Windows EMS Console over the network through a web browser. EMS enables you to perform emergency management services when video, device drivers, or other operating system features prevent normal operation and normal corrective actions from being performed.

When using the Windows EMS Console with iLO, note the following:

- You must configure the Windows EMS console within the operating system before you can use the iLO Virtual Serial Port. For information about how to enable the EMS console, see your operating system documentation. If the EMS console is not enabled in the operating system, iLO displays an error message when you try to access the iLO Virtual Serial Port.
- The Windows EMS serial port must be enabled through the host system RBSU. The configuration allows you to enable or disable the EMS port, and select the COM port. iLO automatically detects whether the EMS port is enabled or disabled, and detects the selection of the COM port. For more information about enabling the Windows EMS serial port, see "Configuring the iLO Virtual Serial Port in the host system RBSU" (page 125) .
- You can use the Windows EMS Console and the iLO Remote Console at the same time.
- To display the `SAC>` prompt, you might have to press **Enter** after connecting through the iLO Virtual Serial Port.

To configure Windows for use with the iLO Virtual Serial Port:

1. Open a command window.
2. Enter the following command to edit the boot configuration data:

   ```
   bcdedit /ems on
   ```

3. Enter the following command to configure the EMSPORT and EMSBAUDRATE values:

   ```
   bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
   ```

   NOTE: EMSPORT:1 is COM1, and EMSPORT:2 is COM2.

   Enter **`bcdedit /?`** for syntax help.

4. Reboot the operating system.

Using the Text-based Remote Console (Textcons)

You can access the Text-based Remote Console (Textcons) using a licensed iLO system and SSH. When you use SSH, the data stream, including authentication credentials, is protected by the encryption method that the SSH client and iLO use.

NOTE: For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.

For more information about the security of the communication methods used by iLO, see the *Integrated Lights-Out security technology brief* on the HP website at http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00212796/c00212796.pdf.

When you use the Text-based Remote Console, the presentation of colors, characters, and screen controls depends on the client you are using, which can be any standard SSH client compatible with iLO. Features and support include the following:

- Display of text-mode screens that are 80x25 (standard color configurations), including:
  - System boot process (POST)
  - Standard option ROMs
  - Text boot loaders (LILO or GRUB)
  - Linux operating system in VGA 80x25 mode
  - DOS
  - Other text-based operating systems
- International language keyboards (if the server and client systems have a similar configuration)
- Line-drawing characters when the correct font and code page are selected in the client application

Customizing the Text-based Remote Console

You can use the `textcons` command options and arguments to customize the Text-based Remote Console display. In general, you do not need to change these options.

- **To control the sampling rate:**

  Use the `textcons speed` option to indicate, in ms, the time between each sampling period. A sampling period is when the iLO firmware examines screen changes and updates the Text-based Remote Console. Adjusting the speed can alleviate unnecessary traffic on long or slow network links, reduce bandwidth use, and reduce iLO CPU time. HP recommends that you specify a value between 1 and 5,000 (1 ms to 5 seconds). For example:

  ```
  textcons speed 500
  ```

- **To control smoothing:**

  iLO attempts to transmit data only when it changes and becomes stable on the screen. If a line of the text screen is changing faster than iLO can sample the change, the line is not transmitted until it becomes stable.

  When a Text-based Remote Console session is active, the data is displayed rapidly and is essentially indecipherable. If the data is transmitted by iLO across the network, it consumes bandwidth. The default behavior is smoothing (`delay 0`), which transmits data only when the changes become stable on the screen. You can control or disable smoothing by using the delay option. For example:

  ```
  textcons speed 500 delay 10
  ```

- **To configure character mapping:**

  In the ASCII character set, CONTROL characters (ASCII characters less than 32) are not printable and are not displayed. These characters can be used to represent items such as arrows, stars, or circles. Some of the characters are mapped to equivalent ASCII representations. Table 10 (page 131) lists the supported equivalents.

Table 10 Character equivalents

Character value	Description	Mapped equivalent
0x07	Small dot	·
0x0F	Sun	⊙
0x10	Right pointer	>
0x11	Left pointer	<
0x18	Up arrow	^
0x19	Down arrow	v
0x1A	Left arrow	<
0x1B	Right arrow	>
0x1E	Up pointer	^
0x1F	Down pointer	v
0xFF	Shaded block	Blank space

Using the Text-based Remote Console

1. Use SSH to connect to iLO.

   Make sure that the terminal application character encoding is set to **Western (ISO-8859-1)**.
2. Log in to iLO.
3. At the prompt, enter `textcons`.

   A message appears, indicating that the Text-based Remote Console is initiating.

To exit the Text-based Remote Console and return to the CLI session, press **Esc+Shift+9**.

Using Linux with the Text-based Remote Console

You can run the Text-based Remote Console on a Linux system that is configured to present a terminal session on the serial port. This feature enables you to use a remote logging service. You can log on to the serial port remotely and redirect output to a log file. Any system messages directed to the serial port are logged remotely.

Some keyboard combinations that Linux requires in text mode might not be passed to the Text-based Remote Console—for example, the client might intercept the **Alt+Tab** keyboard combination.

Using iLO Virtual Media

iLO Virtual Media provides an iLO Virtual Floppy/USB key and Virtual CD/DVD-ROM , which can be used to boot a remote host server from standard media anywhere on the network. Virtual Media devices are available when the host system is booting. Virtual Media devices connect to the host server by using USB technology.

When you are using Virtual Media, note the following:

- An iLO license key is required to use some forms of Virtual Media. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.
- You must have the Virtual Media privilege to use this feature.
- Only one of each type of media can be connected at a time.
- In an operating system, an iLO Virtual Floppy/USB key or Virtual CD/DVD-ROM behaves like any other drive. When you are using iLO for the first time, the host operating system might prompt you to complete a New Hardware Found wizard.

- When virtual devices are connected, they are available to the host server until you disconnect them. When you are finished using a Virtual Media device and you disconnect it, you might receive a warning message from the host operating system regarding unsafe removal of a device. You can avoid this warning by using the operating system feature to stop the device before disconnecting it.
- The iLO Virtual Floppy/USB key or Virtual CD/DVD-ROM is available at server boot time for supported operating systems. Booting from an iLO Virtual Floppy/USB key or Virtual CD/DVD-ROM enables you to perform tasks such as deploying an operating system from network drives and performing disaster recovery of failed operating systems.
- If the host server operating system supports USB mass storage devices or secure digital devices, the iLO Virtual Floppy/USB key is available after the host server operating system loads.
  - You can use the iLO Virtual Floppy/USB key when the host server operating system is running to upgrade device drivers, create an emergency repair disk, and perform other tasks.
  - Having the iLO Virtual Floppy/USB key available when the server is running can be useful if you must diagnose and repair the NIC driver.
  - The iLO Virtual Floppy/USB key can be the physical floppy disk, USB key, or secure digital drive on which the web browser is running, or an image file stored on your local hard drive or network drive.
  - For optimal performance, HP recommends using image files stored on the hard drive of your client PC or on a network drive accessible through a high-speed network link.
- If the host server operating system supports USB mass storage devices, the iLO Virtual CD/DVD-ROM is available after the host server operating system loads.
  - You can use the iLO Virtual CD/DVD-ROM when the host server operating system is running to upgrade device drivers, install software, and perform other tasks.
  - Having the iLO Virtual CD/DVD-ROM available when the server is running can be useful if you must diagnose and repair the NIC driver.
  - The iLO Virtual CD/DVD-ROM can be the physical CD/DVD-ROM drive on which the web browser is running, or an image file stored on your local hard drive or network drive.
  - For optimal performance, HP recommends using image files stored on the hard drive of your client PC or on a network drive accessible through a high-speed network link.
- You can use the .NET IRC to mount a Virtual Folder to access and copy files between a client and a managed server.
- Before you use the iLO Virtual Media feature, review the operating system considerations in "Virtual Media operating system information" (page 133).
- You can also access the Virtual Media feature using the .NET IRC or Java IRC, XML configuration and control scripts, or the SMASH CLP.
- If the Virtual Floppy/USB key or Virtual CD/DVD-ROM capability is enabled, you cannot typically access the floppy drive or CD/DVD-ROM drive from the client operating system.

△ **CAUTION:** To prevent file and data corruption, do not access the local media when you are using it as iLO Virtual Media.

Virtual Media operating system information

This section describes the operating system requirements to consider when you are using the iLO Virtual Media features.

Operating system USB requirement

To use Virtual Media devices, your operating system must support USB devices, including USB mass storage devices. For more information, see your operating system documentation.

During system boot, the ROM BIOS provides USB support until the operating system loads. Because MS-DOS uses the BIOS to communicate with storage devices, utility diskettes that boot DOS will also function with Virtual Media.

Using Virtual Media with Windows 7

By default, Windows 7 powers off the iLO virtual hub when no Virtual Media devices are enabled or connected during boot. To change this setting, use the following procedure:

1. Open **Device Manager**.
2. Select **View→Devices by connection**.
3. Expand **Standard Universal PCI to USB Host Controller** to display the USB devices, including the Generic USB Hub.

   The Generic USB Hub option is the iLO virtual USB hub controller.
4. Right-click **Generic USB Hub** and select **Properties**.
5. Click the **Power Management** tab.
6. Clear the **Allow the computer to turn off this device to save power** check box.

Operating system considerations: Virtual Floppy/USB key

- **Boot process and DOS sessions**—During the boot process and DOS sessions, the virtual floppy device appears as a standard BIOS floppy drive (drive A). If a physically attached floppy drive exists, it is unavailable at this time. You cannot use a physical local floppy drive and a virtual floppy drive simultaneously.
- **Windows Server 2008 or later and Windows Server 2003**—Virtual Floppy/USB key drives appear automatically after Windows recognizes the USB device. Use the virtual device as you would use a locally attached device.

  To use a Virtual Floppy as a driver diskette during a Windows installation, disable the integrated diskette drive in the host RBSU, which forces the virtual floppy disk to appear as drive A.

  To use a virtual USB key as a driver diskette during a Windows installation, change the boot order of the USB key drive. HP recommends placing the USB key drive first in the boot order.
- **Windows Vista**—Virtual Media does not work correctly on Windows Vista if you are using Internet Explorer 7 with Protected Mode enabled. If you attempt to use Virtual Media with Protected Mode enabled, various error messages appear. To use Virtual Media, select **Tools→Internet Options→Security**, clear **Enable Protected Mode**, and then click **Apply**. After you disable Protected Mode, close all open browser instances and restart the browser.
- **Red Hat and SUSE Linux**—Linux supports the use of USB diskette and key drives.

Changing diskettes

When you are using a Virtual Floppy/USB key on a client machine with a physical USB disk drive, disk-change operations are not recognized. For example, if a directory listing is obtained from a floppy disk, and then the disk is changed, a subsequent directory listing shows the directory listing for the first disk. If disk changes are necessary when you are using a Virtual Floppy/USB key, make sure that the client machine contains a non-USB disk drive.

Operating system considerations: Virtual CD/DVD-ROM

- **MS-DOS**—The Virtual CD/DVD-ROM is not supported in MS-DOS.
- **Windows Server 2008 and Windows Server 2003**—The Virtual CD/DVD-ROM appears automatically after Windows recognizes the mounting of the device. Use it as you would use a locally attached CD/DVD-ROM device.
- **Linux**—The requirements for Red Hat Linux and SLES follow:
  - **Red Hat Linux**

    On servers that have a locally attached IDE CD/DVD-ROM, the Virtual CD/DVD-ROM device is accessible at `/dev/cdrom1`. However, on servers that do not have a locally attached CD/DVD-ROM, such as BL c-Class blade systems, the Virtual CD/DVD-ROM is the first CD/DVD-ROM accessible at `/dev/cdrom`.

    You can mount the Virtual CD/DVD-ROM as a normal CD/DVD-ROM device by using the following command:

    ```
    mount /mnt/cdrom1
    ```

  - **SLES**

    The Virtual CD/DVD-ROM can be found at `/dev/scd0`, unless a USB-connected local CD/DVD-ROM is present. In that case, the Virtual CD/DVD-ROM uses `/dev/scd1`.

    You can mount the Virtual CD/DVD-ROM as a normal CD/DVD-ROM device by using the following command:

    ```
    mount /dev/scd0 /media/cdrom11
    ```

  For instructions, see "Mounting a USB Virtual Media CD/DVD-ROM on Linux systems" (page 134).

Mounting a USB Virtual Media CD/DVD-ROM on Linux systems

1. Log in to iLO through the web interface.
2. Start the .NET IRC or Java IRC.
3. Select the **Virtual Drives** menu.
4. Select the CD/DVD-ROM to use.
5. Mount the drive by using the following commands:

   For Red Hat Linux:

   ```
   mount /dev/cdrom1 /mnt/cdrom1
   ```

   For SLES:

   ```
   mount /dev/scd0 /media/cdrom1
   ```

Operating system considerations: Virtual Folder

- **Boot process and DOS sessions**—The Virtual Folder device appears as a standard BIOS floppy drive (drive A). If a physically attached floppy drive exists, it is unavailable at this time. You cannot use a physical local floppy drive and the Virtual Folder simultaneously.
- **Windows**—A Virtual Folder appears automatically after Windows recognizes the mounting of the virtual USB device. You can use the folder the same way that you use a locally attached device. Virtual Folders are nonbootable. Attempting to boot from the Virtual Folder might prevent the server from starting.
- **Red Hat and SLES**—Linux supports the use of the Virtual Folder feature, which uses a FAT 16 file system format.

Using iLO Virtual Media from the iLO web interface

The Virtual Media page allows you to perform the following tasks:

- View or change the Virtual Media port.

  You can also change the port on the **Administration→Access Settings** page.
- View or eject local media, including locally stored image files, floppy disks, USB keys, CDs/DVD-ROMs, and virtual folders.
- View, connect, eject, or boot from scripted media. Scripted media refers to connecting images hosted on a web server by using a URL. iLO will accept URLs in HTTP or HTTPS format. FTP is not supported.

Viewing and modifying the Virtual Media port

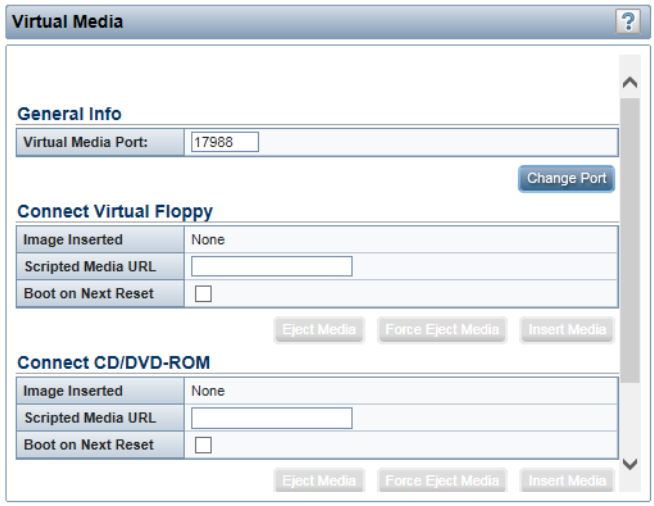
The Virtual Media port is the port that iLO uses to listen for incoming local Virtual Media connections. The default value is 17988.

You must have the Configure iLO Settings privilege to change the Virtual Media port.

To change the Virtual Media port:

1. Navigate to the **Virtual Media→Virtual Media** page, as shown in Figure 72 (page 135).

Figure 72 Virtual Media page



2. Enter a new port number in the **Virtual Media Port** box.
3. Click **Change Port**.

   The system prompts you to reset iLO.
4. Click **OK**.

Viewing and ejecting local media

When local Virtual Media is connected, the details are listed in the following sections:

- **Virtual Floppy/USB Key/Virtual Folder Status**
  - **Image Inserted**—The Virtual Media type that is connected. **Local media** is displayed when local media is connected.
  - **Connected**—Indicates whether a Virtual Media device is connected.
- **Virtual CD/DVD-ROM Status**
  - **Image Inserted**—The Virtual Media type that is connected. **Local media** is displayed when local media is connected.
  - **Connected**—Indicates whether a Virtual Media device is connected.

To eject local Virtual Media devices, click the **Force Eject Media** button in the **Virtual Floppy/USB Key/Virtual Folder Status** section or **Virtual CD/DVD-ROM Status** section.

NOTE: For blade servers without an iLO license that grants full Virtual Media privileges, you cannot use the **Force Eject Media** option with a virtual media image that was mounted via URL. In this case, the connection is most likely the HP BladeSystem Onboard Administrator DVD Drive. This connection must be disconnected through the Onboard Administrator. An iLO reset will also close the connection.

Connecting scripted media

You can connect scripted media from the Virtual Media page. Use the .NET IRC or Java IRC, RIBCL/XML, or the iLO CLI to connect other types of Virtual Media. Scripted media supports only 1.44 MB floppy images (`.img`) and CD/DVD-ROM images (`.iso`). The image must be located on a web server on the same network as iLO.

To connect scripted media:

1. Navigate to the **Virtual Media**→**Virtual Media** page, as shown in Figure 72 (page 135).
2. Enter the URL for the scripted media in the **Scripted Media URL** box in the **Connect Virtual Floppy** section (`.img` files) or the **Connect CD/DVD-ROM** section (`.iso` files).
3. Select the **Boot on Next Reset** check box if the server should boot to this image only on the next server reboot.

   The image will be ejected automatically on the second server reboot so that the server does not boot to this image twice.

   If this check box is not selected, the image will remain connected until it is manually ejected, and the server will boot to it on all subsequent server resets, if the system boot options are configured accordingly.
4. Click **Insert Media**.
5. Optional: To boot to the connected image now, click **Server Reset** to initiate a server reset.

Viewing and ejecting scripted media

When scripted Virtual Media is connected, the following details are listed in the **Virtual Floppy/Virtual Folder Status** section and **Virtual CD/DVD-ROM Status** section:

- **Image Inserted**—The Virtual Media type that is connected. **Scripted media** is displayed when scripted media is connected.
- **Connected**—Indicates whether a Virtual Media device is connected.
- **Image URL**—The URL that points to the connected scripted media.

To eject scripted media devices, click the **Eject Media** button in the **Virtual Floppy/Virtual Folder Status** section or **Virtual CD/DVD-ROM Status** section.

Using iLO Virtual Media from the Remote Console

You can access Virtual Media on a host server by using the .NET IRC or Java IRC, the iLO web interface, XML configuration and control scripts, and the CLP. This section describes how to use the iLO Virtual Media feature with the .NET IRC or Java IRC.

Using a Virtual Drive

The Virtual Drive feature supports the use of a physical floppy disk or CD/DVD-ROM, a USB key drive, an image file, and an image file through a URL.

Using a physical drive on a client PC

1. Start the .NET IRC or Java IRC.
2. Click the **Virtual Drives** menu, and then select the drive letter of a floppy disk, CD/DVD-ROM, or USB key drive on your client PC.

   The virtual drive activity LED changes to reflect the current status of the floppy disk, CD/DVD-ROM, or USB key drive.

NOTE: When you are using the .NET IRC or Java IRC with Windows Vista or Windows Server 2008 or later, you must have Windows administrator rights in order to mount a physical drive.

Using an image file

1. Start the .NET IRC or Java IRC.
2. Click the **Virtual Drives** menu, and then select **Image File Removable Media** (.img files) or **Image File CD-ROM/DVD** (.iso files).

   The .NET IRC or Java IRC prompts you to select a disk image.
3. Enter the path or file name of the image file in the **File name** text box, or browse to the image file location, and then click **Open**.

   The virtual drive activity LED changes to reflect the current status of the virtual drive.

Using an image file through a URL (IIS/Apache)

You can connect scripted media by using the .NET IRC or Java IRC. Scripted media supports only 1.44 MB floppy disk images (`.img`) and CD/DVD-ROM images (`.iso`). The image must be located on a web server on the same network as iLO.

1. Start the .NET IRC or Java IRC.
2. Depending on the image type you will use, select **Virtual Drives→URL Removable Media** (`.img`) or **Virtual Drives→URL CD-ROM/DVD** (`.iso`).

   The **Image file at URL** dialog box opens.
3. Enter the URL for the image file that you want to mount as a virtual drive, and then click **Connect**.

   The virtual drive activity LED changes to reflect the current status of the virtual drive.

Using the Create Media Image feature (Java IRC only)

When you use iLO Virtual Media, performance is fastest when image files are used instead of physical disks. You can use industry-standard tools like DD to create image files or to copy data from a disk image file to a physical disk. You can also use the iLO Java IRC to perform these tasks.

Creating an iLO disk image file

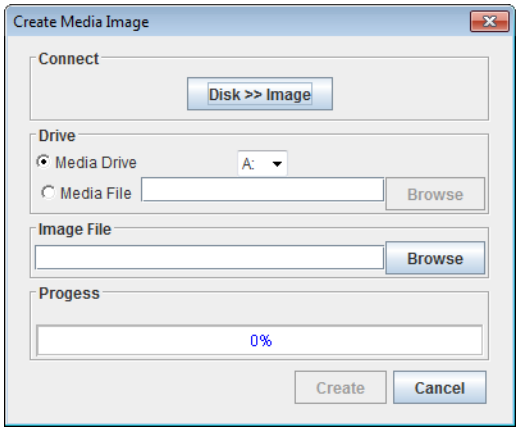
The iLO Create Media Image feature enables you to create disk image files from data in a file or on a physical disk.

To create an ISO-9660 disk image file (`.img` or `.iso`):

1. Start the Java IRC.
2. Select **Virtual Drives →Create Disk Image**.

   The Create Media Image dialog box opens as shown in Figure 73 (page 138).

Figure 73 Create Media Image dialog box



3. Verify that the **Disk>>Image** button is displayed. If the button label is **Image>>Disk**, click the button to change it to **Disk>>Image**.
4. Do one of the following:
   - If you will use a file, select the **Media File** option, and then click **Browse** and navigate to the file you want to use.
   - If you will use physical media, select the drive letter of the floppy disk, USB key, or CD-ROM in the **Media Drive** menu.
5. Enter the path and file name for the image file in the **Image File** text box.
6. Click **Create**.

   The Java IRC begins the process of creating the image file. The following message is displayed:

   ```
   Creating image file, please wait...
   ```

   When the image creation is complete, the following message is displayed:

   ```
   Image file was created successfully.
   ```

7. Click **Close** to close the **Create Media Image** dialog box.
8. Confirm that the image was created in the specified location.

Copying data from an image file to a physical disk

The iLO Create Media Image feature enables you to copy the data from a disk image file to a floppy disk or USB key. Only `.img` disk image files are supported. Copying data to a CD-ROM is not supported.

To copy disk image data to a floppy disk or USB key:

1. Start the Java IRC.
2. Select **Virtual Drives →Create Disk Image**.

   The Create Media Image dialog box opens as shown in Figure 73 (page 138).
3. Click the **Disk>>Image** button to toggle the setting to **Image>>Disk**.
4. Select the drive letter of the floppy disk or USB key in the **Media Drive** menu.

5. Enter the path and file name for the existing image file in the **Image File** text box.

   The Java IRC begins the process of copying the data from the image file to the disk. The following message is displayed:

   ```
   Creating disk, please wait...
   ```

   When the disk creation is complete, the following message is displayed:

   ```
   Disk was created successfully.
   ```

6. Click **Close** to close the Create Media Image dialog box.
7. Confirm that the files were copied to the specified location.

Using a Virtual Folder (.NET IRC only)

This feature enables you to access, browse to, and transfer files from a client to a managed server. You can mount and dismount a local or networked directory that is accessible through the client. After you create a virtual image of a folder or directory, the server connects to that image as a USB storage device, enabling you to browse to the server and transfer the files from the iLO-generated image to any location on the server.

This feature and many others are part of an iLO licensing package. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.

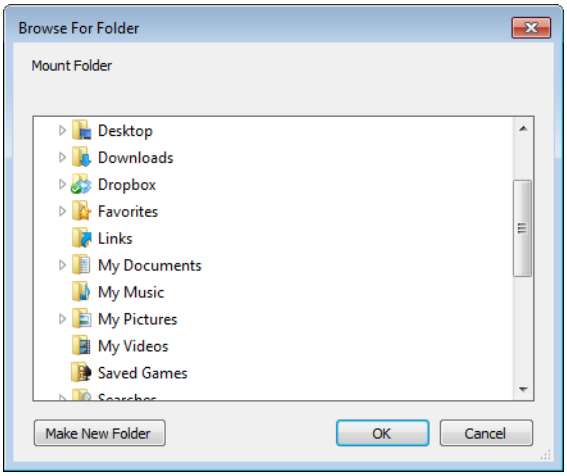
The Virtual Folder is nonbootable and read-only; the mounted folder is static. Changes to the client file are not replicated in the mounted folder.

To use a Virtual Folder:

1. Start the .NET IRC.
2. Select **Virtual Drives→Folder**.

   The **Browse For Folder** window opens, as shown in Figure 74 (page 139).

Figure 74 Browse For Folder window



3. Select the folder that you want to use, and then click **OK**.

   The Virtual Folder is mounted on the server with the name **iLO Folder**.

Setting up IIS for scripted Virtual Media

Before you set up IIS for scripted Virtual Media, verify that IIS is operational. Use IIS to set up a simple website, and then browse to the site to verify that it is working correctly.

Configuring IIS

To configure IIS to serve diskette or ISO-9660 CD images for read-only access:

1. Add a directory to your website and place your images in the directory.

2. Verify that IIS can access the MIME type for the files you are serving.

   For example, if your diskette image files use the extension `.img`, you must add a MIME type for that extension. Use the IIS Manager to access the **Properties** dialog box of your website. On the **HTTP Headers** tab, click **MIME Types** to add MIME types.

   HP recommends adding the following types:

   ```
   .img application/octet-stream
   .iso application/octet-stream
   ```

After you complete these steps, you should be able to navigate to the location of your images by using a web browser, and then download the images to a client. If you can complete this step, your web server is configured to serve read-only disk images.

Configuring IIS for read/write access

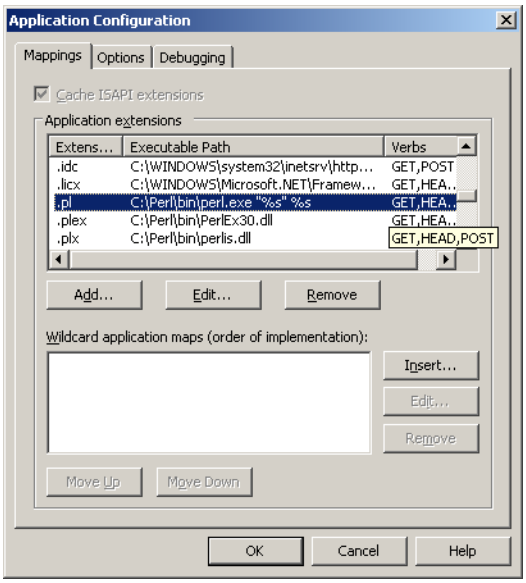
1. Install Perl (for example, ActivePerl).
2. Customize the Virtual Media helper application as needed.

   For a sample helper application, see "Sample Virtual Media helper application" (page 141).
3. Create a directory on your website for the Virtual Media helper script, and then copy the script to that directory.

   The sample script uses the directory name `cgi-bin`, but you can use any name.
4. On the **Properties** page for your directory, under **Application Settings**, click **Create** to create an application directory.

   The icon for your directory in IIS Manager changes from a folder icon to a gear icon.
5. Set the **Execute** permissions to **Scripts only.**
6. Verify that Perl is set up as a script interpreter. Click **Configuration** on the **Properties** page to view the application associations. Perl must be configured as shown in Figure 75 (page 140).

Figure 75 Perl configuration example



7. Verify that Web Service Extensions allows Perl scripts to execute. If not, click **Web Service Extensions** and set **Perl CGI Extension** to **Allowed**.
8. Verify that the prefix variable in the helper application is set correctly.

   To view a sample helper application, see "Sample Virtual Media helper application" (page 141).

Inserting Virtual Media with a helper application

When you are using a helper application with the `INSERT_VIRTUAL_MEDIA` command, the basic format of the URL is as follows:

```
protocol://user:password@servername:port/path,helper-script
```

where:

- `protocol`—Mandatory. Either HTTP or HTTPS.
- `user:password`—Optional. When present, HTTP basic authorization is used.
- `servername`—Mandatory. Either the host name or the IP address of the web server.
- `port`—Optional. A web server on a nonstandard port.
- `path`—Mandatory. The image file that is being accessed.
- `helper-script`—Optional. The location of the helper script on IIS web servers.

For detailed information about the `INSERT_VIRTUAL_MEDIA` command, see the *HP iLO 3 Scripting and Command Line Guide*.

Sample Virtual Media helper application

The following Perl script is an example of a CGI helper application that allows diskette writes on web servers that cannot perform partial writes. A helper application can be used in conjunction with the `INSERT_VIRTUAL_MEDIA` command to mount a writable disk.

When you are using the helper application, the iLO firmware posts a request to this application using the following parameters:

- The `file` parameter contains the name of the file provided in the original URL.
- The `range` parameter contains an inclusive range (in hexadecimal) that designates where to write the data.
- The `data` parameter contains a hexadecimal string that represents the data to be written.

The helper script must transform the `file` parameter into a path relative to its working directory. This might involve prefixing it with "../," or transforming an aliased URL path into the true path on the file system. The helper script requires write access to the target file. Diskette image files must have the appropriate permissions.

Example:

```
#!/usr/bin/perl

use CGI;
use Fcntl;

#
# The prefix is used to get from the current working directory to the
# location of the image file that you are trying to write
#
my ($prefix) = "c:/inetpub/wwwroot";
my ($start, $end, $len, $decode);

my $q = new CGI();            # Get CGI data

my $file =  $q->param('file');  # File to be written
my $range = $q->param('range'); # Byte range to be written
my $data =  $q->param('data');  # Data to be written

#
# Change the file name appropriately
#
$file = $prefix . "/" . $file;
```

```
#
# Decode the range
#
if ($range =~ m/([0-9A-Fa-f]+)-([0-9A-Fa-f]+)/) {
 $start = hex($1);
 $end = hex($2);
 $len = $end - $start + 1;
}

#
# Decode the data (a big hexadecimal string)
#
$decode = pack("H*", $data);

#
# Write it to the target file
#
sysopen(F, $file, O_RDWR);
binmode(F);
sysseek(F, $start, SEEK_SET);
syswrite(F, $decode, $len);
close(F);

print "Content-Length: 0\r\n";
print "\r\n";
```

Configuring Virtual Media Boot Order

The Virtual Media Boot Order feature enables you to set the server boot options. You must have the Virtual Media and Configure iLO Settings privileges to change these settings.

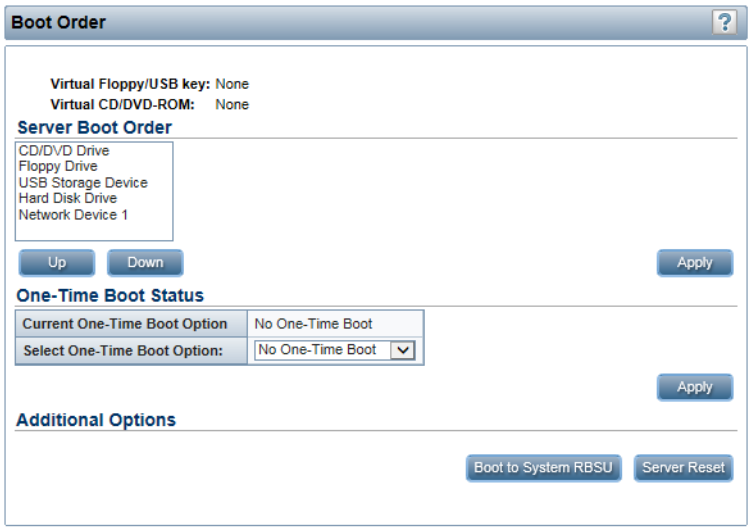
NOTE: Changes made to the boot order or one-time boot status might require a server reset. iLO will notify you when a reset is necessary.

Changing the server boot order

To change the boot order of floppy, CD/DVD-ROM, USB, hard disk, and network devices:

1. Navigate to the **Virtual Media→Boot Order** page, as shown in Figure 76 (page 142).

Figure 76 Boot Order page



2. Select a device in the **Server Boot Order** list, and click **Up** or **Down** to move it up or down in the boot order.

   You can select from the following devices:

   - **CD/DVD Drive**
   - **Floppy Drive**
   - **USB Storage Device**
   - **Hard Disk Drive**
   - **Network Device <number>**, where the server Ethernet card is Network Device 1, and additional NIC/ALOM cards are Network Device 2, Network Device 3, and so on.

3. Click **Apply**.

Changing the one-time boot status

To set the type of media to boot on the next server reset, without changing the predefined boot order:

1. Navigate to the **Virtual Media→Boot Order** page, as shown in Figure 76 (page 142).
2. Select an option from the **Select One-Time Boot Option** list.

   The following options are available:

   - **No One-Time Boot**
   - **CD/DVD Drive**
   - **Floppy Drive**
   - **USB Storage Device**
   - **Hard Disk Drive**
   - **Network Device**

3. Click **Apply**.

   The following message appears:

   `Successfully set one-time boot option.`

   The **Current One-Time Boot Option** value is updated to show the selection.

Using the additional options

Navigate to the **Virtual Media→Boot Order** page, as shown in Figure 76 (page 142).

- Click **Boot to System RBSU** to load the system RBSU on the next server reset.
- Click **Server Reset** to reboot the server. If a one-time boot option is specified, this setting takes precedence over the **Server Boot Order** value.

About server power

Brownout recovery

A brownout condition occurs when power to a running server is lost momentarily. A brownout interrupts the operating system, but does not interrupt the iLO firmware unless it lasts more than 4 seconds.

iLO detects and recovers from power brownouts. If iLO detects that a brownout has occurred, server power is restored after the power-on delay unless **Automatically Power-On Server** is disabled. After the brownout recovery, iLO firmware records a `Brown-out recovery` event in the iLO Event Log.

Graceful shutdown

The ability of the iLO processor to perform a graceful shutdown requires cooperation from the operating system. To perform a graceful shutdown, the iLO health driver must be loaded. iLO communicates with the health driver and uses the appropriate operating system method of shutting down the system safely to ensure that data integrity is preserved.

If the health driver is not loaded, the iLO processor attempts to use the operating system to perform a graceful shutdown through the power button. iLO emulates a physical power-button press (iLO momentary press) in order to prompt the operating system to shut down gracefully. The behavior of the operating system depends on its configuration and settings for a power-button press.

For more information about the iLO drivers, see "Installing the iLO drivers" (page 22).

When using Windows Server 2003 or later, the computer group policy disables a graceful system shutdown via a momentary press unless an Administrator is logged into the operating system. To change this setting and enable a graceful shutdown, do the following:

1. From a command prompt, execute the `gpedit.misc` command.
2. Set the following setting to **Enabled**: **Computer Configuration→Windows Settings→Security Settings→Local Policies→Security Options→Shutdown: Allow system to be shut down without having to log on**.

Power efficiency

iLO enables you to improve power usage by using High Efficiency Mode. HEM improves the power efficiency of the system by placing the secondary power supplies in step-down mode. When the secondary supplies are in step-down mode, the primary supplies provide all DC power to the system. The power supplies are more efficient because there are more DC output watts for each watt of AC input.

NOTE: HEM is available on nonblade servers only.

When the system draws more than 70% of the maximum power output of the primary supplies, the secondary supplies return to normal operation (that is, they exit step-down mode). When power use drops below 60% capacity of the primary supplies, the secondary supplies return to step-down mode. HEM enables you to achieve power consumption equal to the maximum power output of the primary and secondary power supplies, while maintaining improved efficiency at lower power-usage levels.

HEM does not affect power redundancy. If the primary supplies fail, the secondary supplies immediately begin supplying DC power to the system, preventing any downtime.

You must configure HEM through the system RBSU. You cannot modify these settings through iLO. For more information, see the *HP ROM-Based Setup Utility User Guide*.

The configured HEM settings are displayed on the **System Information→Server Power** page.

Using iLO Power Management

iLO Power Management enables you to view and control the power state of the server, monitor power usage, and modify power settings. The **Power Management** menu has three options: **Server Power**, **Power Meter**, and **Power Settings**.

Managing the server power

The **Virtual Power Button** section on the **Server Power** page displays the current power state of the server, as well as options for remotely controlling server power. **System Power** indicates the state of the server power when the page is first opened. The server can be **ON**, **OFF**, or **Reset**. Use the browser refresh feature to view the current server power state.

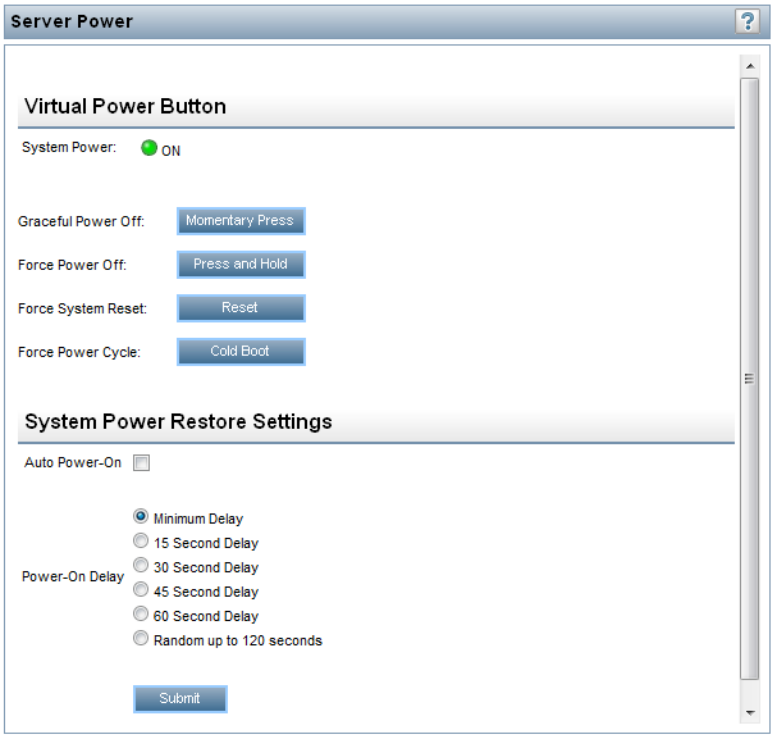
The server is rarely in the **Reset** state.

To change the server power state by using the **Virtual Power Button** options, you must have the Virtual Power and Reset privilege. Some of the power control options do not shut down the operating system gracefully. Before you use the **Virtual Power Button** options, you must use the Remote Console to initiate an operating system shutdown.

To change the server power state:

1. Navigate to the **Power Management→Server Power** page, as shown in Figure 77 (page 145).

Figure 77 Server Power page



2. Click one of the following buttons:
   - **Momentary Press**—The same as pressing the physical power button. If the server is powered off, a momentary press will turn the server power on.

     Some operating systems might be configured to initiate a graceful shutdown after a momentary press, or to ignore this event. HP recommends using system commands to complete a graceful operating system shutdown before you attempt to shut down by using the Virtual Power button.
   - **Press and Hold**—The same as pressing the physical power button for 5 seconds and then releasing it.

     The server is powered off as a result of this operation. Using this option might circumvent the graceful shutdown features of the operating system.

     This option provides the ACPI functionality that some operating systems implement. These operating systems behave differently depending on a short press or long press.
   - **Reset**—Forces the server to warm-boot: CPUs and I/O resources are reset. Using this option circumvents the graceful shutdown features of the operating system.
   - **Cold Boot**—Immediately removes power from the server. Processors, memory, and I/O resources lose main power. The server will restart after approximately 6 seconds. Using this option circumvents the graceful shutdown features of the operating system.

NOTE: The **Press and Hold**, **Reset**, and **Cold Boot** options are not available when the server is powered down.

Configuring the System Power Restore Settings

The **System Power Restore Settings** section enables you to control system behavior after power is lost. You can also configure these settings by using the system RBSU during POST. You must have the Configure iLO Settings privilege to change the System Power Restore Settings.

To change the System Power Restore Settings:

1. Navigate to the **Power Management**→**Server Power** page, as shown in Figure 77 (page 145).
2. Select or clear the **Auto Power-On** check box.

   This setting enables iLO to power on a server when power is applied, such as when the server is plugged in, or when a UPS is activated after a power outage.

   If power is unexpectedly lost while the server is powering up, the server always powers back on, even if **Auto Power-On** is disabled.
3. Select a **Power-On Delay** value.

   This setting staggers server automatic power-on in a data center. It determines the amount of time iLO delays before powering on a server after iLO startup is complete.

   The following options are available:

   - **Minimum Delay**—Power-on occurs after iLO startup is complete.
   - **15 Second Delay**—Power-on is delayed by 15 seconds.
   - **30 Second Delay**—Power-on is delayed by 30 seconds.
   - **45 Second Delay**—Power-on is delayed by 45 seconds.
   - **60 Second Delay**—Power-on is delayed by 60 seconds.
   - **Random up to 120 seconds**—The power-on delay varies and can be up to 120 seconds.
4. Click **Submit**.

Viewing server power usage

The **Power Meter** page enables you to view the server power consumption over time.

This feature and many others are part of an iLO licensing package. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.

To access power-meter graphs, navigate to the **Power Management**→**Power Meter** page, as shown in Figure 78 (page 147).

Figure 78 Power Meter page

The power-meter graphs display recent server power usage. The graph data is reset when iLO or the server is reset. The iLO firmware periodically samples peak power, average power, and power cap. The following graphs are displayed:

- **24-Hour History Graph**—This graph displays the power usage of the server over the previous 24 hours. The iLO firmware collects power usage information from the server every 5 minutes. The bar graph displays the average values in blue and the peak values in red. The graph shows **No cap set** during a host power reset.
- **20-Minute History Graph**—This graph displays the power usage of the server over the previous 20 minutes. The iLO firmware collects power usage information from the server every 10 seconds. The bar graph displays the average values in blue and the peak values in red.

TIP: Move the mouse cursor over the graph to view the power usage for a specific point in time.

When you are viewing the power-meter graphs, use the **Display Options** to control the information that is displayed. You can view minimum, average, peak, and cap power information.

Select one or more of the following check boxes, and then click **Refresh Page** to update the graphs.

- **Min (static low)**—The minimum value observed during a measurement period. Typically, the 20-minute graph measures a minimum value every 10 seconds, which matches the average value. The 24-hour graph can capture minimum values lower than the 5-minute average value.
- **Avg**—The mean power reading during the sample.
- **Peak**—The highest instantaneous power reading during the sample. iLO records this value on a subsecond basis.
- **Cap**—The configured power cap during the sample. If the power cap is not configured or is not supported, it does not appear.
  - A power cap limits average power draw for extended periods of time.
  - Power caps are not maintained during server reboots, resulting in temporary spikes during boot.
  - Power caps set for less than 50% of the difference between maximum power and idle power might become unreachable because of changes in the server. HP does not recommend configuring power caps for less than 20%. Configuring a power cap that is too low for the system configuration can affect system performance.
  - For more information about HP Insight Control power management software, see http://www.hp.com/go/dpc.

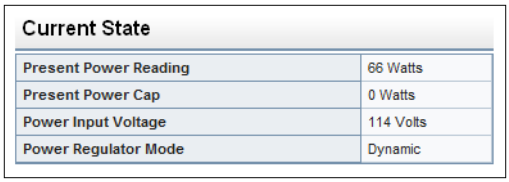
The following options are also available:

- **Power Unit**—Select a value on the **Power Unit** list to show the power readings in either watts or BTU/hr.
- **Refresh Page**—Click the **Refresh Page** button to update the history graphs.

Viewing the current power state

To view the current power state, navigate to the **Power Management**→**Power Meter** page, as shown in Figure 78 (page 147). Scroll to the **Current State** section, as shown in Figure 79 (page 148).

Figure 79 Power Meter page Current State section



The values displayed in the **Current State** table vary depending on the server type:

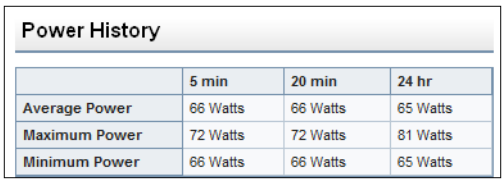
- **Present Power Reading**—The current power reading from the server. This value is displayed for all HP ProLiant server types.
- **Present Power Cap**—The configured power cap for the server. This value is 0 if the power cap is not configured. This value is displayed for HP ProLiant ML, DL, and blade servers.
- **Power Input Voltage**—The supplied input voltage for the server. This value is displayed for HP ProLiant ML and DL servers.
- **Power Regulator Mode**—The configured HP Power Regulator for ProLiant mode. This value is displayed for all HP ProLiant server types. For information about the possible settings, see "Configuring power settings" (page 149).

- **Power Supply Capacity**—The server power capacity. This value is displayed for HP ProLiant SL servers.
- **Peak Measured Power**—The highest measured power reading. This value is displayed for HP ProLiant SL servers.

Viewing the server power history

To view the server power history, navigate to the **Power Management→Power Meter** page, as shown in Figure 78 (page 147). Scroll to the **Power History** section, as shown in Figure 79 (page 148).

Figure 80 Power Meter page Power History section



The **Power History** table shows power readings from three time periods: 5 minutes, 20 minutes, and 24 hours.

- **Average Power**—The average of the power readings for the specified time period. If the server has not been running for the specified time period, the value is the average of all readings since the server booted.
- **Maximum Power**—The maximum power reading from the server for the specified time period. If the server has not been running for the specified time period, the value is the maximum of all readings since the server booted.
- **Minimum Power**—The minimum power reading from the server for the specified time period. If the server has not been running for the specified time period, the value is the minimum of all readings since the server booted.

Configuring power settings

The **Power Settings** page enables you to view and control the power management features of the server. The power management features on this page vary based on the server configuration. You must have the Configure iLO Settings privilege to change the values on this page.

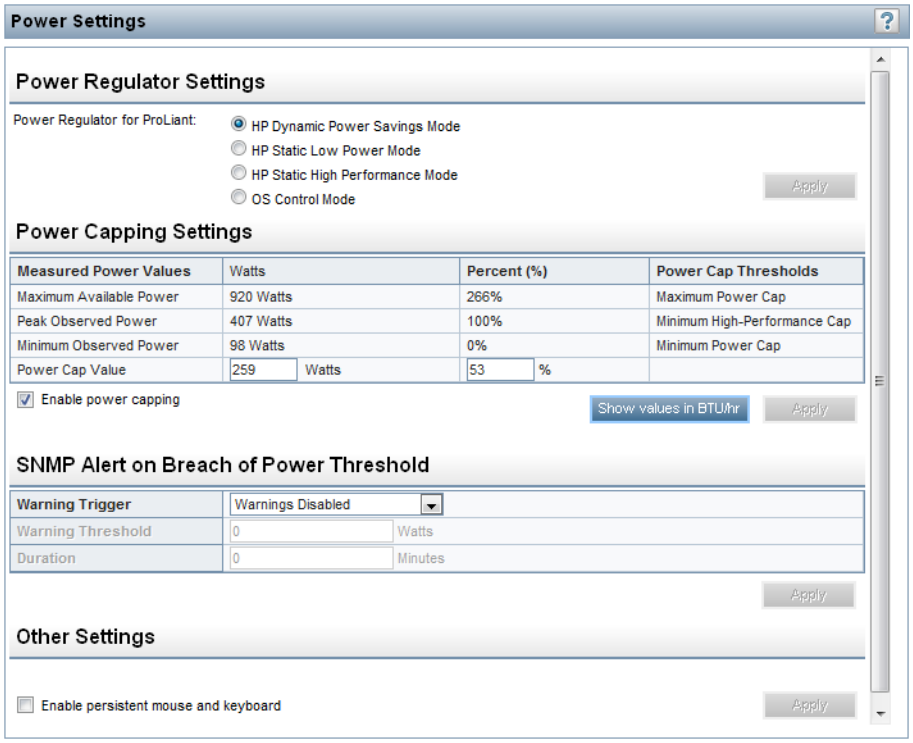
Configuring Power Regulator settings

The HP Power Regulator for ProLiant feature enables iLO to dynamically modify processor frequency and voltage levels, based on operating conditions, to provide power savings with minimal effect on performance. The **Power Settings** page allows you to view and control the **Power Regulator Mode** of the server.

To configure the Power Regulator settings:

1. Navigate to the **Power Management→Power Settings** page, as shown in Figure 81 (page 150).

Figure 81 Power Settings page



2. Select one of the following options:
   - **HP Dynamic Power Savings Mode**—Automatically varies processor speed and power usage based on processor utilization. This option allows the reduction of overall power consumption with little or no impact to performance. It does not require OS support.
   - **HP Static Low Power Mode**—Reduces processor speed and power usage. This option guarantees a lower maximum power usage for the system.
   - **HP Static High Performance Mode**—Processors will run at maximum power/performance at all times, regardless of the OS power management policy.
   - **OS Control Mode**—Processors will run at maximum power/performance at all times, unless the OS enables a power management policy.
3. Click **Apply**.

   One of the following messages appears:
   - For the **HP Dynamic Power Savings Mode**, **HP Static Low Power Mode**, and **HP Static High Performance Mode** settings: `Power Regulator Settings changed.`
   - For the **OS Control Mode** setting: `You must reboot the server to invoke this change of the Power Regulator Settings.`

   The Power Regulator settings cannot be changed while the server is in POST. If the settings do not change after you click **Apply**, the server might be in the boot process or require rebooting. Exit any ROM-based program that is running, allow POST to complete, and then try the operation again.
4. If iLO notified you that a reboot is required, reboot the server.

Configuring power capping settings

The **Power Capping Settings** section enables you to view measured power values, set a power cap, and disable power capping.

- The **Measured Power Values** section lists the following:
  - **Maximum Available Power**—The power supply capacity for a nonblade server, or the initial power-on request value for a blade server
  - **Peak Observed Power**—The maximum observed power for the server
  - **Minimum Observed Power**—The minimum observed power for the server

  During POST, the ROM runs two power tests that determine the peak and minimum observed power values.
- Power cap settings are disabled when the server is part of an Enclosure Dynamic Power Cap. These values are set and modified by using Onboard Administrator or Insight Power Manager.
- Use the **Power Cap Thresholds** as guidelines for configuring a power cap.
  - **Maximum Power Cap**—The maximum power available for the server. The server must not exceed this value.
  - **Minimum High-Performance Cap**—The maximum power that the server uses in the current configuration. A power cap set to this value does not affect server performance.
  - **Minimum Power Cap**—The minimum power that the server users. A power cap set to this value reduces the server power usage to the minimum, which results in server performance degradation.
- When a power cap is set, the average power reading of the server must be at or below the power cap value.
- You cannot use the iLO web interface to configure the power capping settings for SL servers. Use one of the following tools to configure the power capping settings for SL servers:
  - **Power Interface Control Utility**—This utility is available at the following website: http://h20000.www2.hp.com/bizsupport/TechSupport/SoftwareDescription.jsp?prodTypeId=15351&prodSeriesId=4324034&swItem=MTX-cb0c48d305d24a4dbe80e5eecc&prodNameId=5037746.
  - **HP ProLiant SL Advanced Power Manager**—For more information, see the *HP ProLiant SL Advanced Power Manager User Guide*.

To configure a power cap:

1. Navigate to the **Power Management→Power Settings** page, as shown in Figure 81 (page 150).
2. Select the **Enable power capping** check box.
3. Enter the **Power Cap Value** in watts, BTU/hr, or as a percentage.

   The percentage is the difference between the maximum and minimum power values. The power cap value cannot be set below the server minimum power value.

   When values are displayed in watts, click **Show values in BTU/hr** to change the display to BTU/hr. When values are displayed in BTU/hr, click **Show values in Watts** to change the display to watts.
4. Click **Apply**.

Configuring SNMP alert settings

The **SNMP Alert on Breach of Power Threshold** section enables the sending of an SNMP alert when power consumption exceeds a defined threshold.

To configure the SNMP alert settings:

1. Navigate to the **Power Management→Power Settings** page, as shown in Figure 81 (page 150).
2. Select a value in the **Warning Trigger** list.

   The warning trigger determines whether warnings are based on peak power consumption, average power consumption, or if they are disabled.
3. Enter a value in the **Warning Threshold** box.

   This value sets the power consumption threshold, in watts. If power consumption exceeds this value for the specified time duration, an SNMP alert is triggered.
4. Enter a value in the **Duration** box.

   This value sets the length of time, in minutes, that power consumption must remain above the warning threshold before an SNMP alert is triggered. The maximum duration is 240 minutes, and the duration must be a multiple of 5.
5. Click **Apply** to save the configuration.

Configuring the persistent mouse and keyboard

The **Other Settings** section on the **Power Settings** page allows you to enable or disable the persistent keyboard and mouse feature.

When this feature is enabled, the iLO virtual keyboard and mouse are always connected to the iLO UHCI USB controller. When this feature is disabled, the iLO virtual keyboard and mouse are connected dynamically to the iLO UHCI controller only when a Remote Console application is open and connected to iLO. Disabling the feature allows some HP servers to increase power savings by 15 watts when the server operating system is idle and no virtual USB keyboard and mouse are connected.

For example, the power savings for a 24–hour period might be 15 watts x 24 hours, or 360 watt hours (.36 kilowatt-hours).

The persistent mouse and keyboard feature is enabled by default because some operating systems cannot enumerate the USB keyboard correctly during installation.

To change the persistent mouse and keyboard setting:

1. Navigate to the **Power Management→Power Settings** page, as shown in Figure 81 (page 150).
2. Select or clear the **Enable persistent mouse and keyboard** check box.
3. Click **Apply** to save the configuration.

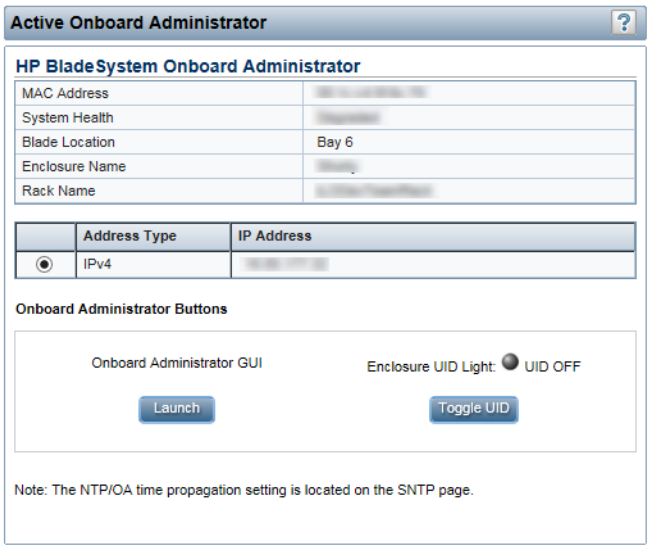
Using iLO with Onboard Administrator

OA is the enclosure management processor, subsystem, and firmware base that supports the HP BladeSystem and all managed devices in the enclosure.

Using the Active Onboard Administrator

The **BL c-Class→Active Onboard Administrator** page provides general information about the primary OA in the enclosure in which the iLO processor is located. This page is displayed only when there is an enclosure. Figure 82 (page 153) shows an example of the page.

Figure 82 Active Onboard Administrator page



This page displays the following information and options:

- **MAC Address**—The MAC address of the active OA.
- **System Health**—The health of the active OA, as reported by the OA.

  A value of **unknown** means that the OA health has not been reported to iLO.
- **Blade Location**—The location (enclosure bay) of the blade that is hosting the current iLO session.
- **Enclosure Name**—The enclosure that the active OA is managing. You can change this value through the OA.
- **Rack Name**—The rack that contains the enclosure managed by the active OA. You can change this value through the OA.

Starting the Onboard Administrator GUI

1. Navigate to the **BL c-Class→Active Onboard Administrator** page.
2. If the OA supports multiple addresses, select the address to use from the options in the **Onboard Administrator Address Selection** table.

   Depending on the configuration, the following options might be available:

   - **IPv4**
   - **IPv6 SLAAC**
   - **IPv6 Static**
   - **IPv6 DHCP**
3. Click **Launch**.

   The OA GUI opens in a new browser window.

Toggling the enclosure UID light

To change the state of the enclosure UID where iLO is located, click the **Toggle UID** button.

The UID status on this page represents the Enclosure UID status when the iLO page loaded. To update the status, refresh the page.

Enclosure bay IP addressing

The First Time Setup Wizard prompts you to set up your enclosure bay IP addressing. For more information about the wizard, see the *HP BladeSystem Onboard Administrator User Guide*.

Dynamic Power Capping for server blades

Dynamic Power Capping is an iLO feature available for c-Class server blades, and is accessed through OA. Dynamic Power Capping is available only if your system hardware platform, BIOS (ROM), and power microcontroller firmware version support this feature. If your system supports Dynamic Power Capping, iLO automatically runs in Dynamic Power Capping mode.

For information about the power setting options for c-Class server blades, see the *HP BladeSystem Onboard Administrator User Guide.*

iLO virtual fan

In c-Class blade servers, OA controls the enclosure fans (also called virtual fans). The iLO firmware cannot detect these enclosure fans. Instead, the iLO firmware monitors an ambient temperature sensor located on the blade server. This information is displayed on the iLO web interface, and is retrieved by OA periodically. OA uses the sensor information collected from all iLO processors in the enclosure to determine enclosure fan speeds.

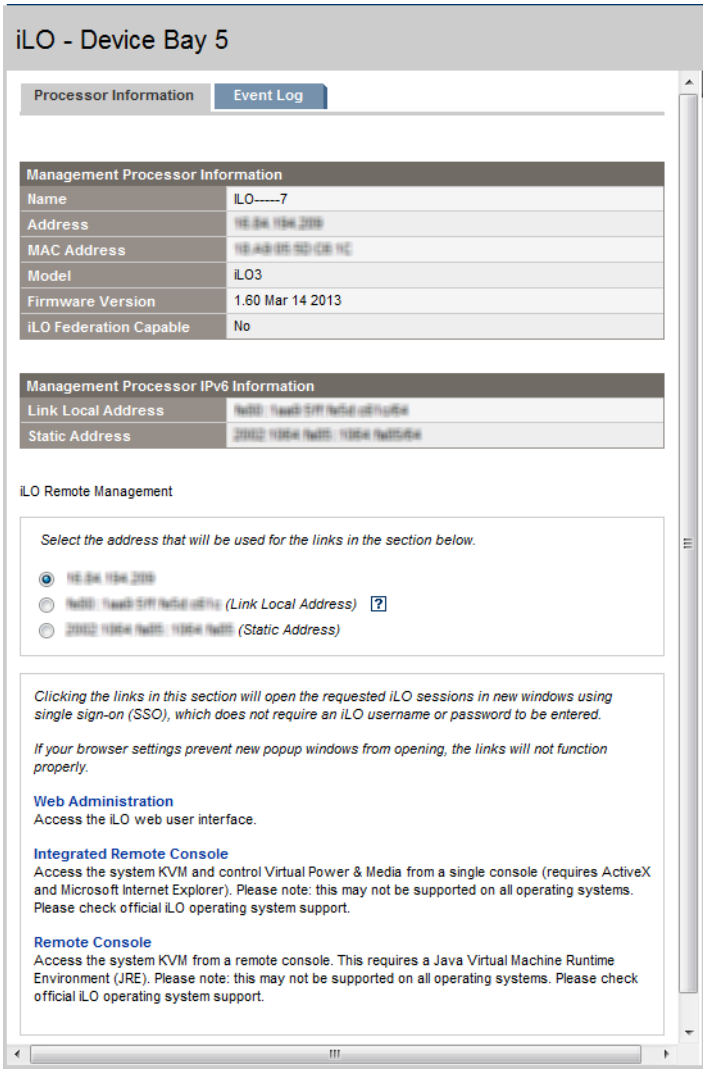
iLO option

The **iLO - Device Bay <XX>** page in OA (Figure 83) provides the following links:

- **Web Administration**—Starts the iLO web interface
- **Integrated Remote Console**—Starts the .NET IRC
- **Remote Console**—Starts the Java IRC

Clicking a link on this page opens the requested iLO session in a new window that uses SSO, which does not require an iLO user name or password. If your browser settings prevent new windows from opening, these links do not work correctly.

Figure 83 Onboard Administrator page



IPMI server management

Server management through IPMI is a standard method for controlling and monitoring the server. The iLO firmware provides server management based on the IPMI version 2.0 specification, which defines the following:

- Monitoring of system information such as fans, temperatures, and power supplies
- Recovery capabilities such as system resets and power on/off operations
- Logging capabilities for abnormal events such as over-temperature readings or fan failures
- Inventory capabilities such as identification of failed hardware components

IPMI communications depend on the BMC and the SMS. The BMC manages the interface between the SMS and the platform management hardware. The iLO firmware emulates the BMC functionality, and the SMS functionality can be provided by various industry-standard tools. For more information, see the IPMI specification on the Intel website at http://www.intel.com/design/servers/ipmi/tools.htm.

The iLO firmware provides the KCS interface, or open interface, for SMS communications. The KCS interface provides a set of I/O mapped communications registers. The default system base address for the I/O-mapped SMS interface is `0xCA2`, and it is byte aligned at this system address.

The KCS interface is accessible to the SMS software running on the local system. Examples of compatible SMS software applications follow:

- **IPMI version 2.0 Command Test Tool**—A low-level MS-DOS command-line tool that enables hex-formatted IPMI commands to be sent to an IPMI BMC that implements the KCS interface. You can download this tool from the Intel website at http://www.intel.com/design/servers/ipmi/tools.htm.
- **IPMItool**—A utility for managing and configuring devices that support the IPMI version 1.5 and version 2.0 specifications. IPMItool can be used in a Linux environment. You can download this tool from the IPMItool website at http://ipmitool.sourceforge.net/index.html.

When emulating a BMC for the IPMI interface, iLO supports all mandatory commands listed in the IPMI version 2.0 specification. The SMS should use the methods described in the specification for determining which IPMI features are enabled or disabled in the BMC (for example, using the `Get Device ID` command).

If the server operating system is running, and the iLO health driver is enabled, any IPMI traffic through the KCS interface can affect health driver performance and overall system health. Do not issue any IPMI commands through the KCS interface that might have a negative effect on health driver monitoring. This restriction includes any command that sets or changes IPMI parameters, such as `Set Watchdog Timer` and `Set BMC Global Enabled`. Any IPMI command that simply returns data is safe to use, such as `Get Device ID` and `Get Sensor Reading`.

Using iLO with HP Insight Control server deployment

HP Insight Control server deployment is integrated with iLO to enable the management of remote servers and the performance of Remote Console operations, regardless of the state of the operating system or hardware.

The deployment server enables you to use the power management features of iLO to power on, power off, or cycle power on the target server. Each time a server connects to the deployment server, the deployment server polls the target server to verify that an iLO device is installed. If installed, the server gathers information, including the DNS name, IP address, and user login name. Security is maintained by requiring the user to enter the correct password for that user name.

For more information about HP Insight Control server deployment, see the documentation on the HP Insight Control website at http://www.hp.com/go/insightcontrol.

5 Integrating HP Systems Insight Manager

The iLO firmware is integrated with HP SIM in key operating environments, providing a single management console from a standard web browser. While the operating system is running, you can establish a connection to iLO by using HP SIM.

Integration with HP SIM provides the following:

- **Support for SNMP trap delivery to an HP SIM console**—The HP SIM console can be configured to forward SNMP traps to a pager or email address.
- **Support for management processors**—All iLO devices installed in servers on the network are discovered in HP SIM as management processors.
- **Grouping of iLO management processors**—All iLO devices can be grouped logically and displayed on one page.
- **HP Management Agents**—iLO, combined with the HP Management Agents, provides remote access to system management information through the iLO web interface.
- **Support for SNMP management**—HP SIM can access Insight Management Agent information through iLO.

HP SIM features

HP SIM enables you to do the following:

- Identify iLO processors.
- Create an association between an iLO processor and its server.
- Create links between an iLO processor and its server.
- View iLO and server information and status.
- Control the amount of information displayed for iLO.

The following sections summarize these features. For detailed information, see the *HP Systems Insight Manager User Guide*.

Establishing SSO with HP SIM

1. Configure iLO for HP SIM SSO and add HP SIM trusted servers.

   For instructions, see "Configuring iLO for HP SSO" (page 61).
2. Log in to the HP SIM server that you specified in Step 1, and discover the iLO processor.

   After you complete the discovery process, SSO is enabled for iLO.

   For more information about HP SIM discovery tasks, see the *HP Systems Insight Manager User Guide*.

iLO identification and association

HP SIM can identify an iLO processor and create an association between iLO and a server. You can configure iLO to respond to HP SIM identification requests by setting the **Level of Data Returned** value on the **Administration→Management** page. For more information, see "Configuring Insight Management integration" (page 86).

Viewing iLO status in HP SIM

HP SIM identifies iLO as a management processor. HP SIM displays the management processor status on the **All Systems** page.

The iLO management processor is displayed as an icon on the same row as its host server. The color of the icon represents the status of the management processor.

For a list of device statuses, see the *HP Systems Insight Manager User Guide*.

iLO links in HP SIM

For ease of management, HP SIM creates links to the following:

- iLO and the host server from any **System(s)** list
- The server from the **System** page for iLO
- iLO from the **System** page for the server

The **System(s)** list pages display iLO, the server, and the relationship between iLO and the server.

- Click a status icon to display the iLO web interface.
- Click the iLO or server name to display the **System** page of the device.

Viewing iLO in HP SIM System(s) lists

iLO management processors can be viewed in HP SIM. A user who has full configuration rights can create and use customized system collections to group management processors. For more information, see the *HP Systems Insight Manager User Guide*.

Receiving SNMP alerts in HP SIM

You can configure iLO to forward alerts from the management agents of the host operating system and to send iLO alerts to HP SIM.

HP SIM supports full SNMP management. iLO supports SNMP trap delivery to HP SIM. You can view the event log, select the event, and view additional information about the alert.

Configuring the receipt of SNMP alerts in HP SIM:

1. To enable iLO to send SNMP traps, navigate to the **Administration→Management** page and configure the settings for SNMP, SNMP alerting, and Insight Management Integration. Enter the IP address of the HP SIM computer in the **SNMP Alert Destination(s)** box.

   For more information, see "Configuring iLO Management settings" (page 84).
2. To discover iLO in HP SIM, configure iLO as a managed device for HP SIM.

   This enables the NIC interface on iLO to function as a dedicated management port, isolating management traffic from the NIC interface for the remote host server. For instructions, see the *HP Systems Insight Manager User Guide*.

   For major events that are not cleared, iLO traps appear in **All Events**. To obtain more information about the event, click **Event Type**.

HP SIM port matching

HP SIM is configured to start an HTTP session to check for iLO at port 80. If you want to change the port number, you must change it in both iLO and HP SIM.

- To change the port in iLO, navigate to the **Administration→Access Settings** page, and then enter the new port number in the **Web Server Non-SSL Port** box.
- To change the port number in HP SIM, add the port to the `config\identification\additionalWsDisc.props` file in the HP SIM installation directory. If iLO uses the default port (80), you do not need to edit this file.

  The port entry must be on a single line with the port number first, and with all other items identical to the following example (including capitalization). This example shows the correct entry for discovering iLO at port 55000.

```
55000=iLO 3,
,true,false,com.hp.mx.core.tools.identification.mgmtproc.MgmtProcessorParser
```

Reviewing iLO license information in HP SIM

HP SIM displays the license status of the iLO management processors. You can use this information to determine how many and which iLO devices have an optional license installed.

To view license information, select **Deploy→License Manager**. To ensure that the displayed data is current, run the **Identify Systems** task for your management processors. For more information, see the *HP Systems Insight Manager User Guide*.

6 Directory services

This chapter describes how to configure iLO to use Kerberos login, schema-free directory authentication, and HP extended schema directory authentication.

Directory integration benefits

Directory integration with iLO provides the following benefits:

- **Scalability**—The directory can be leveraged to support thousands of users on thousands of iLO processors.
- **Security**—Robust user-password policies are inherited from the directory. User-password complexity, rotation frequency, and expiration are policy examples.
- **User accountability**—In some environments, users share iLO accounts, which makes it difficult to determine who performed an operation.
- **Role-based administration**—You can create roles (for example, clerical, remote control of the host, complete control) and associate users or user groups with those roles. A change to a single role applies to all users and iLO devices associated with that role.
- **Single point of administration**—You can use native administrative tools like MMC and ConsoleOne to administer iLO users.
- **Immediacy**—A single change in the directory rolls out immediately to associated iLO processors. This eliminates the need to script this process.
- **Simpler credentials**—You can use existing user accounts and passwords in the directory without having to record a new set of credentials for iLO.
- **Flexibility**—You can create a single role for a single user on a single iLO processor, a single role for multiple users on multiple iLO processors, or a combination of roles as suited to your enterprise.
- **Compatibility**—iLO directory integration supports Active Directory and eDirectory.
- **Standards**—iLO directory support is based on the LDAP 2.0 standard for secure directory access.

Choosing a directory configuration to use with iLO

Some directory configuration practices work better with iLO than others. Before you configure iLO for directories, you must decide whether to use the schema-free directory integration method or the HP extended schema directory integration method. Answer the following questions to help evaluate your directory integration requirements:

1. **Can you apply schema extensions to your directory?**
   - **No**—You are using Active Directory, and your company policy prohibits applying extensions.

     No—Directory integration does not fit your environment. Consider deploying an evaluation server to assess the benefits of directory integration.

     Use group-based schema-free directory integration. For more information, see "Schema-free directory integration" (page 166).
   - **Yes**—Proceed to question 2.

2. **Is your configuration scalable?**
   - **No**—Deploy an instance of the schema-free directory integration to evaluate whether this method meets your policy and procedural requirements. If necessary, you can deploy HP schema directory integration later. For more information, see "Schema-free directory integration" (page 166).
   - **Yes**—Use HP schema directory integration. For more information, see "Setting up HP extended schema directory integration" (page 170).

   The following questions can help you determine whether your configuration is scalable:
   - Are you likely to change the rights or privileges for a group of directory users?
   - Will you regularly script iLO changes?
   - Do you use more than five groups to control iLO privileges?

For more information, see the comprehensive list of benefits in "Directory integration benefits" (page 160). "Directory-enabled remote management" (page 190) explains how roles, groups, and security are enabled and enforced through directories.

Kerberos support

Kerberos support enables a user to log in to iLO without supplying a user name and password if the client workstation is logged in to the domain and the user is a member of a directory group for which iLO is configured. If the workstation is not logged in to the domain, the user can also log in to iLO by using the Kerberos user name and domain password. Kerberos support can be configured through the web interface, XML (RIBCL), or SSH (partial support for CLI).

Because a trust relationship between iLO and the domain is established by a system administrator before user sign-on, any form of authentication (including two-factor authentication) is supported. For instructions on configuring a user to support two-factor authentication, see the server operating system documentation.

Domain controller preparation

In a Windows Server environment, Kerberos support is part of the domain controller.

Realm names

The Kerberos realm name for a DNS domain is usually the domain name converted to uppercase. For example:

- Parent domain name: `example.net`
- Kerberos realm name: `EXAMPLE.NET`

Computer accounts

A computer account must be present and enabled in the domain directory for each iLO account. In Windows, create the user account in the **Active Directory Users and Computers** snap-in. For example:

- iLO host name: `iloname`
- Parent domain name: `example.net`
- iLO domain name (fully qualified): `iloname.example.net`

User accounts

A user account must be present and enabled in the domain directory for each user who is allowed to log in to iLO.

Generating a keytab

This section describes how to generate a keytab file for iLO in a Windows environment.

The iLO host name that you use for keytab generation must be identical to the configured iLO host name. iLO host names are case sensitive.

1. Use the `ktpass` command to generate a keytab and set the shared secret.

   The command is case sensitive and has special characters.

   ```
   ktpass -out iloname.keytab +rndPass -ptype KRB5_NT_SRV_HST -mapuser
   iloname$@example.net -princ HTTP/iloname.example.net@EXAMPLE.NET
   ```

   The output should be similar to the following:

   ```
   Targeting domain controller: domaincontroller.example.net
   Using legacy password setting method
   Successfully mapped HTTP/iloname.example.net to iloname.
   WARNING: pType and account type do not match. This might cause problems.
   Key created.
   Output keytab to iloname.
   keytab: Keytab version: 0x502
   keysize 69 HTTP/iloname.example.net@EXAMPLE.NET ptype 3
   (KRB5 _NT_SRV_HST) vno 3 etype 0x17 (RC4-HMAC) keylength 16
   (0x5a5c7c18ae23559acc2 9d95e0524bf23)
   ```

   NOTE: The `ktpass` command might display a message about not being able to set the UPN. This is acceptable because iLO is a service, not a user. You might be prompted to confirm the password change on the computer object. Click **OK** to close the window and continue creating the keytab file. Do not use the `-kvno` option of the `ktpass` command. This option causes the `knvo` in the keytab file to be out of sync with the `kvno` in Active Directory.

2. Use the `SetSPN` command to assign the Kerberos SPN to the computer object. For example:

   ```
   SetSPN -A HTTP/iloname.example.net iloname
   ```

   If the `SetSPN` command displays an error message, do the following:

   a. Use MMC with the `ADSIEdit` snap-in and find the computer object for iLO.
   b. Set the `DNSHostName` property to the iLO DNS name. For example:

      ```
      cn=iloname,ou=us,ou=clients,dc=example,dc=net
      ```

3. Use the `SetSPN -L iloname` command to display the SPNs and DN for the iLO.

   Verify that the `HTTP/iloname.example.net` service is displayed.

   NOTE: The `SetSPN` command might display a message about not being able to set the UPN. This is acceptable because iLO is a service, not a user. You might be prompted to confirm the password change on the computer object. Click **OK** to close the window and continue creating the keytab file.

Key version number

If a domain controller OS is reinstalled, the key version number sequence resets. You must regenerate and reinstall the keytab files that iLO uses for devices associated with that domain controller.

Windows Vista

To generate keytab files on Windows Vista, use Microsoft hotfix KB960830 and `ktpass.exe` version 6.0.6001.22331 or later.

Universal and global user groups (for authorization)

To set permissions in iLO, you must create a group in the domain directory. Users who log in to iLO are granted the sum of the permissions for all groups of which they are a member. Only universal and global user groups can be used to set permissions. Domain local groups are not supported.

Configuring iLO for Kerberos login

This section describes the iLO requirements for Kerberos login. You can configure iLO for Kerberos login using the iLO web interface, XML configuration and control scripts, or the CLI, CLP, or SSH interface.

Using the iLO web interface

To configure the iLO parameters by using the web interface:

1. Navigate to the **Network→iLO Dedicated Network Port or Shared Network Port→General** page to configure the **iLO Hostname** parameter in the **iLO Subsystem Name (Host Name)** box.

   The case of the iLO host name used for keytab generation must be identical to the case of the configured iLO host name.

   For more information, see "Configuring general network settings" (page 72).
2. Navigate to the **Administration→Security→Directory** page to configure the following Kerberos-specific parameters:
   - **Kerberos Authentication**
   - **Kerberos Realm**
   - **Kerberos KDC Server Address**
   - **Kerberos KDC Server Port**
   - **Kerberos Keytab**

   For more information about the Kerberos-specific parameters, see "Configuring directory settings" (page 51).
3. Navigate to the **Administration→User Administration** page to configure directory groups.

   Each Directory Group includes a DN, SID, and permissions. For Kerberos login, the SIDs of groups of which the user is a member are compared to the SIDs for directory groups for which iLO is configured. The user is granted the sum of the permissions for all groups of which the user is a member of.

   You can only use global and universal groups to set permissions. Domain local groups are not supported.

   For more information, see "Managing iLO users by using the iLO web interface" (page 32).
4. Navigate to the **Information→Overview** page to check the **Current iLO Date/Time**.

   For more information, see "Viewing iLO overview information" (page 94).
5. Navigate to the **Administration→Network→SNTP Settings** page if you want to change the date and time.

   For Kerberos authentication to function properly, the date and time must be synchronized between the iLO processor, the KDC, and the client workstation. Set the date and time in iLO with the server, or obtain the date and time from the network by enabling the SNTP Settings feature in iLO.

   For more information, see "Configuring SNTP settings" (page 79).

Using XML configuration and control scripts

The following sample scripts show how to set the iLO parameters for directories:

- `Set_Server_Name.xml` shows how to set the iLO host name.
- `Mod_Schemaless_Directory.xml` shows how to configure directory groups.
- `Mod_Network_Settings.xml` shows how to configure SNTP settings.
- `Mod_Kerberos_Config.xml` shows how to configure Kerberos-specific parameters.

NOTE: You can download sample XML scripts from http://www.hp.com/support/ilo3. For more information, see the *HP iLO 3 Scripting and Command Line Guide*.

Using the CLI, CLP, or SSH interface

To configure the iLO parameters by using the CLI, CLP, or SSH interface:

- **iLO Hostname**—You can change the iLO host name in the `Hostname` property of the `/map1/dnsendpt1` target.
- **Directory groups**—You can configure directory group names and permissions in the properties of the `/map1/oemhp_dircfg1` target. The group SIDs cannot be configured through this interface.
- **iLO Date/Time, SNTP Settings**—The current date and time and the SNTP settings cannot be displayed through this interface.
- **Kerberos-specific configuration parameters**—You can configure Kerberos parameters in the properties of the `oemhp_dircfg1`, target.

NOTE: For more information about configuring the iLO parameters by using the CLI, CLP, or SSH, see the *HP iLO 3 Scripting and Command Line Guide*.

Time requirement

To log in to Kerberos successfully, ensure that the date and time of the following are set to within 5 minutes of one another:

- The iLO server
- The client running the web browser
- The servers performing the authentication

Configuring single sign-on

Users who are allowed to log in to iLO must be members of the groups for which permissions are assigned. For Windows clients, locking and unlocking the workstation refreshes the credentials that are used to log in to iLO. Home versions of the Windows operating system do not support Kerberos login.

Internet Explorer

This section describes the procedure for enabling single sign-on with Internet Explorer. The following steps enable login if Active Directory is configured correctly for iLO, and iLO is configured correctly for Kerberos login.

NOTE: This procedure is based on Internet Explorer 7. Newer browser versions might have different steps.

1. Enable authentication in Internet Explorer:
   a. Select **Tools→Internet Options**.
   b. Click the **Advanced** tab.
   c. Scroll to the **Security** section.
   d. Verify that the **Enable Integrated Windows Authentication** option is selected.
   e. Click **OK**.
2. Add the iLO domain to the Intranet zone:
   a. Select **Tools→Internet Options**.
   b. Click the **Security** tab.
   c. Click the **Local intranet** icon.
   d. Click the **Sites** button.
   e. Click the **Advanced** button.
   f. Enter the site to add in the **Add this website to the zone** box.

      On a corporate network, `*.example.net` is sufficient.
   g. Click **Add**.
   h. Click **Close**.
   i. Click **OK** to close the **Local intranet** dialog box.
   j. Click **OK** to close the **Internet Options** dialog box.
3. Enable **Automatic logon only in Intranet zone**:
   a. Select **Tools→Internet Options**.
   b. Click the **Security** tab.
   c. Click the **Local intranet** icon.
   d. Click **Custom level**.
   e. Scroll to the **User Authentication** section.
   f. Verify that the **Automatic logon only in Intranet zone** option is selected.
   g. Click **OK** to close the **Security Settings — Local Intranet Zone** window.
   h. Click **OK** to close the **Internet Options** dialog box.
4. If any options were changed, close and restart Internet Explorer.
5. Use the FQDN to browse to iLO (for example, `iloname.example.net`).
6. Click the **HP Zero Sign In** button.

Firefox

This section describes the procedure for enabling single sign-on with Firefox. The following steps enable login if Active Directory is configured correctly for iLO, and iLO is configured correctly for Kerberos login:

1. Enter **`about:config`** in the browser location bar to open the browser configuration page.

   If the message `This might void your warranty!` appears, click the **I'll be careful, I promise!** button.
2. Enter **`network.negotiate`** in the **Filter** box.
3. Double-click `network.negotiate-auth.trusted-uris`.
4. Enter the iLO DNS domain name (for example, `example.net`), and then click **OK**.
5. Use the FQDN to browse to iLO (for example, `iloname.example.net`).
6. Click the **HP Zero Sign In** button.

Chrome

No special settings are required for the Chrome browser.

Verifying single sign-on (HP Zero Sign In) configuration

To verify that HP Zero Sign In is configured correctly:

1. Browse to the iLO login page (for example, `http://iloname.example.net`).
2. Click the **HP Zero Sign In** button.

   If a prompt for credentials appears, Kerberos authentication has failed and the system has reverted to NTLM authentication. Click **Cancel**, and then repeat the procedures in "Configuring single sign-on" (page 164).

Login by name

To verify that login by name is working properly:

1. Browse to the iLO login page (for example, `http://iloname.example.net`).
2. Enter the user name in the Kerberos SPN format (for example, `user@EXAMPLE.NET`).
3. Enter the associated domain password.

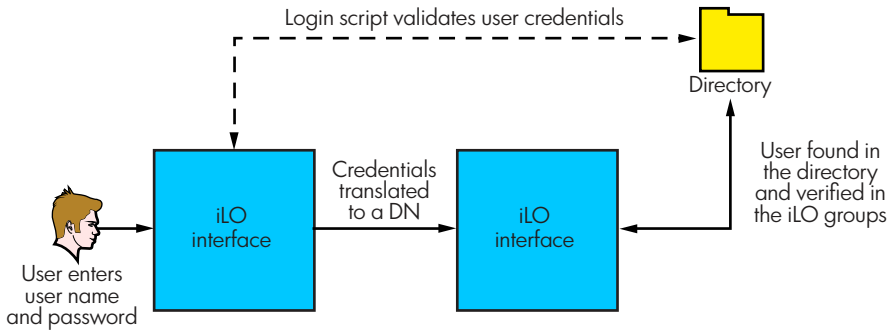
   If a prompt for credentials appears, Kerberos authentication has failed. Click **Cancel** to close the dialog box.

   Login by name might not work correctly if the computer account for iLO is part of a child domain, but the Kerberos configuration parameters (**Kerberos Realm**, **Kerberos KDC Server Address**, and **Kerberos KDC Server Port**) reference the parent domain.

Schema-free directory integration

With schema-free directory integration, users and group memberships reside in the directory, but group privileges reside in the iLO settings. iLO uses login credentials to read the user object in the directory and retrieve the user group memberships, which are compared to those stored in iLO. If the credentials and membership match, authorization is granted, as shown in Figure 84 (page 166).

Figure 84 Schema-free directory integration



Advantages of using schema-free directory integration include the following:

- You do not have to extend the directory schema.
- Minimal setup is required for users in the directory. If no setup exists, the directory uses existing users and group memberships to access iLO. For example, if you have a domain administrator named User1, you can copy the DN of the domain administrator security group to iLO and give it full privileges. User1 would then have access to iLO.

Using schema-free directory integration has the following disadvantage:

- Group privileges are administered on each iLO. However, this disadvantage has minimal impact because group privileges rarely change, and the task of changing group membership is administered in the directory and not on each iLO. HP provides tools that enable you to make changes to a large number of iLOs at the same time.

Setting up schema-free directory integration

If you want to use the schema-free directory integration method, your system must meet the prerequisites described in "Active Directory prerequisites" (page 167).

Active Directory prerequisites

SSL must be enabled at the directory level. To enable SSL, install a certificate for the domain in Active Directory. iLO communicates with the directory only over a secure SSL connection.

To validate the setup, you must have the directory DN of at least one user and the DN of a security group that the user is a member of.

Introduction to Certificate Services

Certificate Services is used to issue signed digital certificates to network hosts. The certificates are used to establish SSL connections with the host and verify the authenticity of the host.

Installing Certificate Services enables Active Directory to receive a certificate that allows iLO processors to connect to the directory service. Without a certificate, iLO cannot connect to the directory service.

Each directory service that you want iLO to connect to must be issued a certificate. If you install an Enterprise Certificate Service, Active Directory can automatically request and install certificates for all Active Directory controllers on the network.

Installing Certificate Services

Use the following procedure for Windows Server 2008:

1. Navigate to Server Manager.
2. Click **Roles** in the left pane.
3. Click **Add Roles**.
4. Select **Active Directory Certificate Services**.
5. Follow the onscreen instructions. If you are not sure what values to use, accept the default values.

Verifying Certificate Services

Because management processors communicate with Active Directory by using SSL, you must create a certificate or install Certificate Services. You must install an enterprise CA because you will issue certificates to objects in your organizational domain.

To verify that Certificate Services is installed, select **Start**→**Programs**→**Administrative Tools**→**Certification Authority**. An error message appears if Certificate Services is not installed.

For information about the OIDs supported by iLO certificates, see "OID support for certificates" (page 245).

Configuring Automatic Certificate Request

To specify that a certificate be issued to the server:

1. Select **Start**→**Run**, and then enter `mmc`.
2. Select **File**→**Add/Remove Snap-in**.
3. To add the snap-in to MMC, select **Group Policy Object**, and then click **Add**.
4. Click **Browse**, and then select the **Default Domain Policy** object. Click **OK**.

5. Click **Finish**, and then click **Close** and **OK** to close the remaining dialog boxes.
6. Expand **Computer Configuration→Windows Settings→Security Settings→Public Key**.
7. Right-click **Automatic Certificate Requests Settings**, and select **New→Automatic Certificate Request**.

   The Automatic Certificate Request Setup wizard starts.
8. Click **Next**.
9. Select the **Domain Controller** template, and click **Next**.
10. Select the listed certificate authority (it is the same CA that was defined during the Certificate Services installation). Click **Next**.
11. Click **Finish** to close the wizard.

Schema-free setup using the iLO web interface

You can set up a schema-free configuration by using the iLO web interface. Only users who have the Configure iLO Settings privilege can change these settings. Users who do not have the Configure iLO Settings privilege can only view the assigned settings.

1. Navigate to the **Administration→Security→Directory** page.
2. Select **Use Directory Default Schema** in the **Authentication and Directory Server Settings** section.

   For more information, see "Schema-free setup options" (page 169).
3. Click **Apply Settings**.
4. To test the communication between the directory server and iLO, click **Test Settings**.

Schema-free setup using scripts

To set up a schema-free directory configuration by using XML configuration and control scripts:

1. Review the *HP iLO 3 Scripting and Command Line Guide*.
2. Write and execute a script that configures iLO for schema-free directory support.

   Use the following script as a template:

```
<RIBCL VERSION="2.0">
 <LOGIN USER_LOGIN="admin" PASSWORD="admin123">
  <DIR_INFO MODE = "write">
   <MOD_DIR_CONFIG>
    <DIR_ENABLE_GRP_ACCT value = "Yes"/>

    <DIR_GRPACCT1_NAME value = "test1"/>
    <DIR_GRPACCT1_PRIV value = "3,4,5"/>
    <!--      Firmware support information for next tag:-->
    <!--      iLO 4 - All versions.-->
    <!--      iLO 3 - Version 1.20 or later only-->
    <DIR_GRPACCT1_SID value= "S-1-0"/>

<!-- alternative method for iLO 3/4 only-->
<!-- <DIR_GRPACCT INDEX="1">-->
<!-- <NAME VALUE="string"/>-->
<!-- <SID VALUE="S-1-0"/>-->
<!-- <LOGIN_PRIV VALUE="Y"/>-->
<!-- </DIR_GRPACCT>-->

   </MOD_DIR_CONFIG>
  </DIR_INFO>
 </LOGIN>
</RIBCL>
```

Schema-free setup with HP Directories Support for ProLiant Management Processors

HP recommends using HP Directories Support for ProLiant Management Processors (HPLOMIG.exe) when you are configuring multiple iLO processors for directories.

For more information, see "HP Directories Support for ProLiant Management Processors utility" (page 196).

Schema-free setup options

The schema-free setup options are the same, regardless of the method you use to configure the directory.

To review the available methods, see "Schema-free setup using the iLO web interface" (page 168), "Schema-free setup using scripts" (page 168), and "Schema-free setup with HP Directories Support for ProLiant Management Processors" (page 168).

After you enable directories and select the schema-free option, you have the following options:

Minimum login flexibility

- Enter the directory server DNS name or IP address and LDAP port. Typically, the LDAP port for an SSL connection is 636.
- Enter the DN for at least one group. This group can be a security group (for example, `CN=Administrators,CN=Builtin,DC=HP,DC=com`) or any other group as long as the intended iLO users are members of the group.

  With a minimum configuration, you can log in to iLO by using your full DN and password. You must be a member of a group that iLO recognizes.

Better login flexibility

In addition to the minimum settings, enter at least one directory user context.

At login time, the login name and user context are combined to make the user DN. For example, if the user logs in as `JOHN.SMITH`, and a user context is set up as `CN=USERS,DC=HP,DC=COM`, the DN that iLO tries is `CN=JOHN.SMITH,CN=USERS,DC=HP,DC=COM`.

Maximum login flexibility

Configure iLO with a DNS name, and not an IP address, for the directory server network address. The DNS name must be resolvable to an IP address from both iLO and the client system.

Configuring iLO with maximum login flexibility enables you to log in using your full DN and password, your name as it appears in the directory, NetBIOS format (domain/login_name), or email format (login_name@domain).

In some cases, the maximum login flexibility option might not work. For example, if the client and iLO are in different DNS domains, one of the two might not be able to resolve the directory server name to an IP address.

Schema-free nested groups

Many organizations have users and administrators arranged in groups. This arrangement of existing groups is convenient because you can associate them with one or more iLO management role objects. When iLO devices are associated with the role objects, you can use the administrator controls to access the devices associated with the role by adding or deleting members from the groups.

When using Microsoft Active Directory, you can place one group in another group to create a nested group. Role objects are considered groups and can include other groups directly. You can add the existing nested group directly to the role and assign the appropriate rights and restrictions. You can add new users to either the existing group or the role.

In previous implementations, only a schema-free user who was a direct member of the primary group was allowed to log in to iLO. In schema-free integration, users who are indirect members (a member of a group that is a nested group of the primary group) are allowed to log in to iLO.

When you are using trustee or directory rights assignments to extend role membership, users must be able to read the object that represents the iLO device. Some environments require that the trustees of a role also be read trustees of the object to successfully authenticate users.

Setting up HP extended schema directory integration

When you are using HP schema directory integration, iLO supports both Active Directory and eDirectory. However, these directory services require that the schema be extended.

Features supported by HP schema directory integration

Using the HP schema enables you to do the following:

- Authenticate users from a shared, consolidated, scalable user database.
- Control user privileges (authorization) by using the directory service.
- Use roles in the directory service for group-level administration of iLO management processors and iLO users.

A schema administrator must complete the task of extending the schema. The local user database is retained. You can decide not to use directories, to use a combination of directories and local accounts, or to use directories exclusively for authentication.

NOTE: When you are connected through the Diagnostics Port, the directory server is not available. You log in using a local account.

Advantages of using the HP extended schema include the following:

- There is more flexibility in controlling access. For example, access can be limited to a time of day or a certain range of IP addresses.
- Groups are maintained in the directory, not on each iLO.

Setting up directory services

To successfully implement directory-enabled management on any iLO management processor:

1. **Plan**

   Review the following sections:

   - Directory services. For more information, see "Directory services" (page 160).
   - Directory-enabled remote management. For more information, see "Directory-enabled remote management" (page 190).
   - Directory services schema. For more information, see "Directory services schema" (page 239).

2. **Install**
   a. Download the HP Directories Support for ProLiant Management Processors package that contains the schema installer, the management snap-in installer, and the migration utilities from http://www.hp.com/support/ilo3.
   b. Run the schema installer once to extend the schema.
   c. Run the management snap-in installer and install the appropriate snap-in for your directory service on one or more management workstations.

3. **Update**
   a. Set directory server settings and the DN of the management processor objects on the **Directory Settings** page in the iLO web interface. For more information, see "Configuring directory settings" (page 51).
   b. If you are using the schema-free integration or Kerberos Zero Sign In, configure directory groups. For more information, see "Managing iLO users by using the iLO web interface" (page 32).

4. **Manage**
   a. Create a management device object and a role object by using the snap-in.
   b. Assign rights to the role object, as necessary, and associate the role with the management device object.
   c. Add users to the role object.

   For more information about managing the directory service, see "Directory-enabled remote management" (page 190). Examples are available in "Directory services for Active Directory" (page 174) and "Directory services for eDirectory" (page 182).
5. **Handle exceptions**

   iLO migration utilities are easier to use with a single role. If you plan to create multiple roles in the directory, you might need to use directory scripting utilities, like `LDIFDE` or VBScript utilities. These utilities create complex role associations. For more information, see "Using bulk import tools" (page 196).

After the schema has been extended, you can complete the directory services setup by using HP migration utilities, which are included in the HP Directories Support for ProLiant Management Processors package.

Schema documentation

To assist with the planning and approval process, HP provides documentation about the changes made to the schema during the schema setup process. To review the changes made to your existing schema, see "Directory services schema" (page 239).

Directory services support

iLO software is designed to run with the Microsoft Active Directory Users and Computers snap-in or the Novell ConsoleOne management tools, enabling you to manage user accounts through the directory.

iLO supports the following directory services for HP schema directory integration:

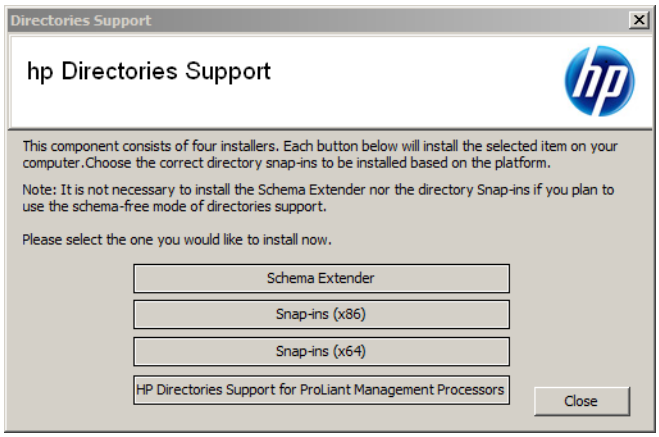
- Microsoft Active Directory
- Microsoft Windows Server 2003 Active Directory
- Microsoft Windows Server 2008 Active Directory
- Novell eDirectory

  This solution makes no distinction between eDirectory running on Linux or eDirectory running on Windows. eDirectory schema extension requires Java 1.4.0 or later for SSL authentication.

Schema required software

iLO requires specific software that extends the schema and provides snap-ins to manage the iLO network. The HP Directories Support for ProLiant Management Processors package contains the schema installer and the management snap-in installer, as shown in Figure 85 (page 172). You can download the software from http://www.hp.com/support/ilo3.

Figure 85 Installer for Schema Extender and snap-ins



You cannot run the schema installer on a domain controller that hosts Windows Server 2008 Core. For security and performance reasons, Windows Server 2008 Core does not use a GUI. To use the schema installer, you must install a GUI on the domain controller or use a domain controller that hosts an earlier version of Windows.

Schema Extender

Several `.xml` files are bundled with the Schema Extender. These files contain the schemas that are added to the directory. Typically, one of these files contains a core schema that is common to all of the supported directory services. Additional files contain product-specific schemas. The schema installer requires the .NET Framework.

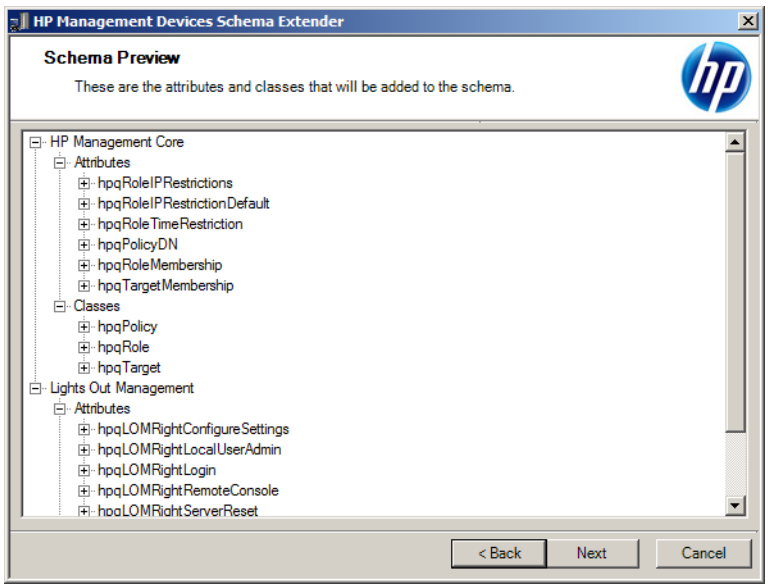
The Schema Extender installer includes three important windows:

- **Schema Preview**
- **Setup**
- **Results**

Schema Preview window

The **Schema Preview** window (Figure 86) enables the user to view the proposed extensions to the schema. The installer reads the selected schema files, parses the XML, and displays it as a tree view. It lists all details of the installed attributes and classes.

Figure 86 Schema Preview window



Setup window

You use the **Setup** window (Figure 87) to enter the appropriate information before extending the schema.

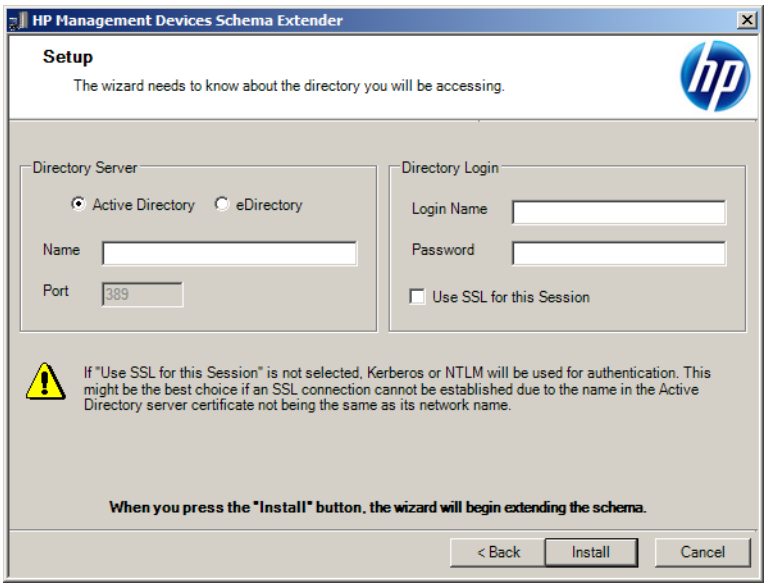
The **Directory Server** section of the **Setup** window enables you to specify whether you will use Active Directory or eDirectory, and to set the computer name and the port to be used for LDAP communications.

NOTE: When you are running the Schema Extender tool, you must use the `Administrator` login along with the domain name, for example, `Administrator@domain.com` or `domain\Administrator`.

Extending the schema for Active Directory requires that the user is an authenticated schema administrator, that the schema is not write protected, and that the directory is the FSMO role owner in the tree. The installer attempts to make the target directory server the FSMO schema master of the forest.

The **Directory Login** section of the **Setup** window enables you to enter your login name and password. These might be required to complete the schema extension. The **Use SSL for this Session** option sets the form of secure authentication to be used. If this option is selected, directory authentication through SSL is used. If this option is not selected and Active Directory is selected, Windows NT authentication is used. If this option is not selected and eDirectory is selected, the administrator authentication and the schema extension proceed by using an unencrypted (clear text) connection.

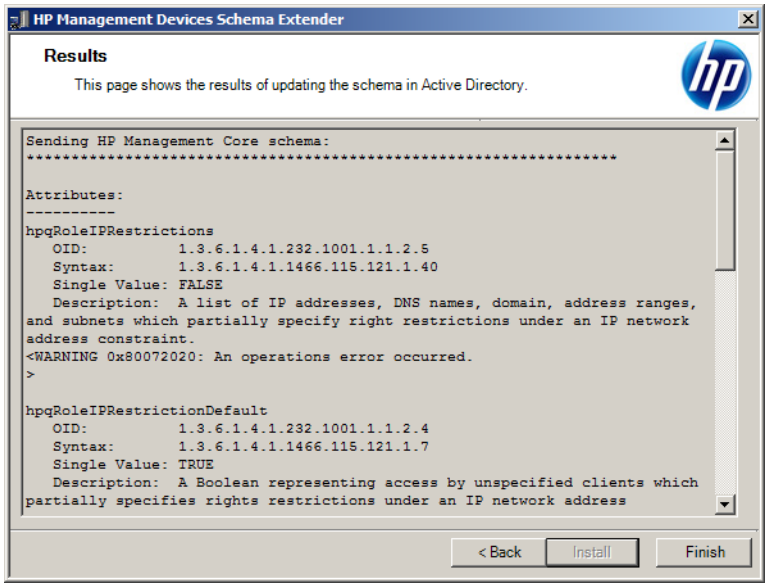
Figure 87 Setup window



Results window

The **Results** window (Figure 88) displays the results of the installation, including whether the schema could be extended and what attributes were changed.

Figure 88 Results window



Management snap-in installer

The management snap-in installer installs the snap-ins required to manage iLO objects in a Microsoft Active Directory Users and Computers directory or Novell ConsoleOne directory.

iLO snap-ins are used to perform the following tasks in creating an iLO directory:

- Creating and managing the iLO objects and role objects
- Making the associations between the iLO objects and the role objects

Directory services for Active Directory

The following sections provide installation prerequisites, preparation instructions, and a working example of directory services for Active Directory. HP provides a utility to automate much of the directory setup process. You can download HP Directories Support for ProLiant Management Processors from http://www.hp.com/support/ilo3.

Active Directory installation prerequisites

- Active Directory must have a digital certificate installed to enable iLO to connect securely over the network.
- Active Directory must have the schema extended to describe iLO object classes and properties.
- An iLO license must be installed.

  For more information about iLO licensing go to http://www.hp.com/go/ilo/licensing.

- Installing directory services for iLO requires extending the Active Directory schema. An Active Directory schema administrator must extend the schema.
- directory services for iLO uses LDAP over SSL to communicate with the directory servers. Before you install snap-ins and schema for Active Directory, read and have available the following documentation:
  - Microsoft Knowledge Base Articles

    These articles are available at http://support.microsoft.com/.
    - 321051 *Enabling LDAP over SSL with a Third-Party Certificate Authority*
    - 299687 *MS01-036: Function Exposed By Using LDAP over SSL Could Enable Passwords to Be Changed*
  - iLO requires a secure connection to communicate with the directory service. This connection requires the installation of the Microsoft CA. For more information, see the Microsoft Knowledge Base Article 321051: *How to Enable LDAP over SSL with a Third-Party Certification Authority.*

Installing Active Directory

For the schema-free configuration

1. Disable IPv6, and then install Active Directory, DNS, and the root CA to Windows Server 2008.
2. Log in to iLO and enter the directory settings and directory user contexts on the **Administration→Security→Directory** page.

   For more information, see "Configuring directory settings" (page 51).
3. Click **Apply Settings** to save the changes.
4. Click the **Administer Groups** button, and then create directory groups for the iLO users.

   For more information, see "Managing iLO users by using the iLO web interface" (page 32).
5. Navigate to the **iLO Dedicated Network Port** or **Shared Network Port General Settings** page, and then enter the environment settings in the **Domain Name** and **Primary DNS server** boxes.

   For more information, see "Configuring IPv4 settings" (page 74).

For HP extended schema

1. Disable IPv6, and then install Active Directory, DNS, and the root CA to Windows Server 2008.
2. Verify that version 2.0 or later of the .NET Framework is installed. This software is required by the iLO LDAP component.
3. Install the latest HP Directories Support for ProLiant Management Processors software from http://www.hp.com/support/ilo3.
4. Extend the schema by using the Schema Extender.

   For more information, see "Schema required software" (page 171).
5. Install the HP LDAP component snap-ins.

   For more information, see "Schema required software" (page 171).
6. Create the HP device and HP role.
7. Log in to iLO and enter the directory settings and directory user contexts on the **Administration→Security→Directory** page.

   For more information, see "Configuring directory settings" (page 51).

8. Navigate to the **iLO Dedicated Network Port** or **Shared Network Port General Settings** page, and then enter the environment settings in the **Domain Name** and **Primary DNS server** boxes.

   For more information, see "Configuring iLO network settings" (page 69).

NOTE: The LDAP component does not work with a Windows Server 2008 Core installation.

Snap-in installation and initialization for Active Directory

1. Run the snap-in installation application to install the snap-ins.
2. Configure the directory service to have the appropriate objects and relationships for iLO management.
   a. Use the management snap-ins from HP to create iLO, policy, admin, and user role objects.
   b. Use the management snap-ins from HP to build associations between the iLO object, the policy object, and the role object.
   c. Point the iLO object to the admin and user role objects. (Admin and user roles automatically point back to the iLO object.)

   For more information about iLO objects, see "Directory services objects" (page 177).

At a minimum, you must create the following:

- One role object that contains one or more users and one or more iLO objects
- One iLO object that corresponds to each iLO management processor that uses the directory

Creating and configuring directory objects for use with iLO in Active Directory

The following example describes how to set up roles and HP devices in an enterprise directory with the domain `testdomain.local`. This domain consists of two organizational units, **Roles** and **iLOs**.

TIP: For more information about using the Active Directory snap-ins, see "Active Directory snap-ins" (page 178).

Create an organizational unit that contains the iLO devices managed by the domain.

1. Use the HP-provided Active Directory Users and Computers snap-ins to create Lights-Out Management objects in the **iLOs** organizational unit for several iLO devices.
   a. Right-click the **iLOs** organizational unit in the `testdomain.local` domain, and then select **New HP Object**.

      The **Create New HP Management Object** dialog box opens.
   b. Select **Device**.
   c. Enter an appropriate name in the **Name** box.

      In this example, the DNS host name of the iLO device, `rib-email-server`, is used as the name of the Lights-Out Management object.
   d. Click **OK**.
2. Use the HP-provided Active Directory Users and Computers snap-ins to create HP role objects in the **Roles** organizational unit.
   a. Right-click the **Roles** organizational unit, and then select **New HP Object**.

      The **Create New HP Management Object** dialog box opens.
   b. Select **Role.**
   c. Enter an appropriate name in the **Name** box.

      In this example, the role contains users trusted for remote server administration and is called `remoteAdmins`.

d. Click **OK**.
e. Repeat the process, creating a role for remote server monitors called `remoteMonitors`.

3. Use the HP-provided Active Directory Users and Computers snap-ins to assign rights to the roles and associate the roles with users and devices.
   a. Right-click the `remoteAdmins` role in the **Roles** organizational unit in the `testdomain.local` domain, and then select **Properties**.

      The **remoteAdmins Properties** dialog box opens.
   b. Click the **HP Devices** tab, and then click **Add**.

      The **Select Users** dialog box opens.
   c. Enter the Lights-Out Management object created in step 2, `rib-email-server` in folder `testdomain.local/iLOs`.
   d. Click **OK** to close the dialog box, and then click **Apply** to save the list.
   e. Click the **Members** tab (Figure 90, and add users by using the **Add** button.
   f. Click **OK** to close the dialog box, and then click **Apply** to save the list.

      The devices and users are now associated.
   g. Click the **Lights Out Management** tab (Figure 94) to set the rights for the role.

      All users and groups within a role will have the rights assigned to the role on all of the iLO devices that the role manages. In this example, the users in the `remoteAdmins` role will receive full access to the iLO functionality.
   h. Select the check box next to each right, and then click **Apply**. Click **OK** to close the dialog box.
4. By using the procedure in step 3, edit the properties of the `remoteMonitors` role as follows:
   a. Add the `rib-email-server` device to the list on the **HP Devices** tab.
   b. Add users to the `remoteMonitors` role on the **Members** tab.
   c. Select the **Login** right on the **Lights Out Management** tab.

      With this right, members of the `remoteMonitors` role will be able to authenticate and view the server status.
5. To configure iLO and associate it with a Lights-Out Management object, use settings similar to the following on the **Administration→Security→Directory** page.

   ```
   LOM Object Distinguished Name =
   cn=rib-email-server,ou=ILOs,dc=testdomain,dc=local Directory User
   Context 1 = cn=Users,dc=testdomain,dc=local
   ```

Directory services objects

One of the keys to directory-based management is proper virtualization of the managed devices in the directory service. This virtualization allows the administrator to build relationships between the managed device and users or groups within the directory service. User management of iLO requires the following basic objects in the directory service:

- Lights-Out Management object
- Role object
- User objects

Each object represents a device, user, or relationship that is required for directory-based management.

After the snap-ins are installed, iLO objects and iLO roles can be created in the directory. By using the Active Directory Users and Computers tool, the user completes the following tasks:

- Creates iLO and role objects
- Adds users to the role objects
- Sets the rights and restrictions of the role objects

NOTE: After the snap-ins are installed, ConsoleOne and MMC must be restarted to show the new entries.

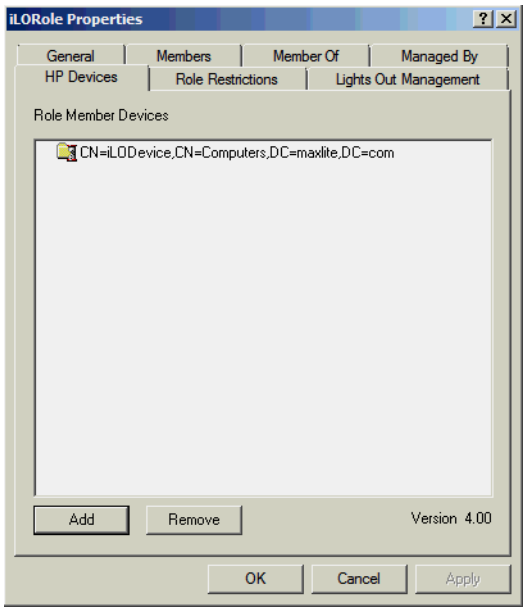
Active Directory snap-ins

The following sections discuss the additional management options available in Active Directory Users and Computers after the HP snap-ins have been installed.

HP Devices tab

The **HP Devices** tab (Figure 89) enables you to add the HP devices to be managed within a role. Clicking **Add** enables you to navigate to an HP device and add it to the list of member devices. Clicking **Remove** enables you to navigate to an HP device and remove it from the list of member devices.

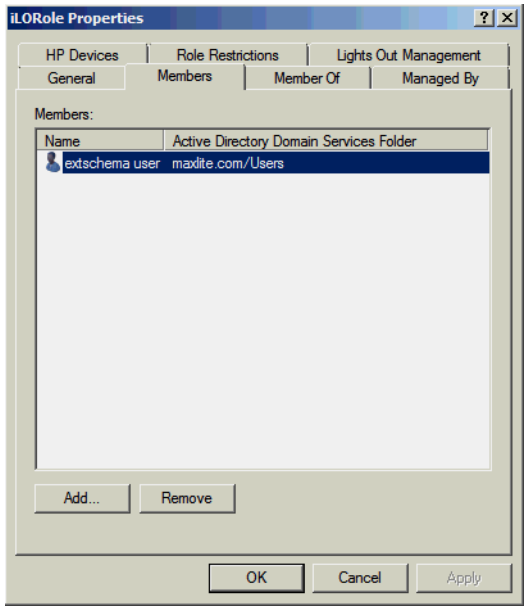
Figure 89 HP Devices tab



Members tab

After user objects are created, the **Members** tab (Figure 90) enables you to manage the users within the role. Clicking **Add** enables you to navigate to the user you want to add. Highlighting an existing user and clicking **Remove** removes the user from the list of valid members.

Figure 90 Members tab

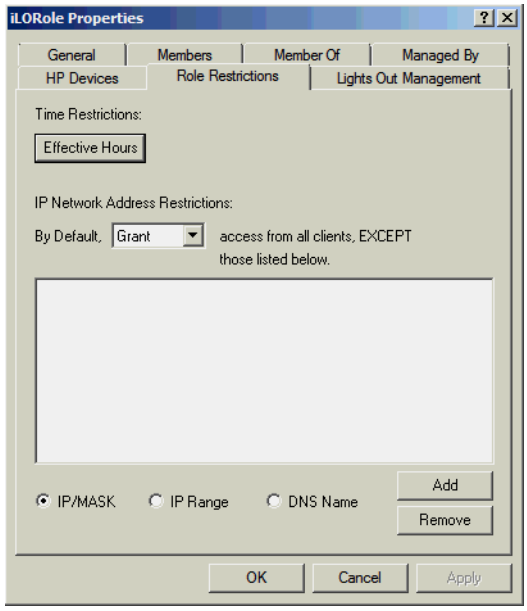


Role Restrictions tab

The **Role Restrictions** tab (Figure 91) enables you to set the following restrictions for the role:

- Time restrictions
- IP network address restrictions:
  - IP/mask
  - IP range
  - DNS name

Figure 91 Role Restrictions tab

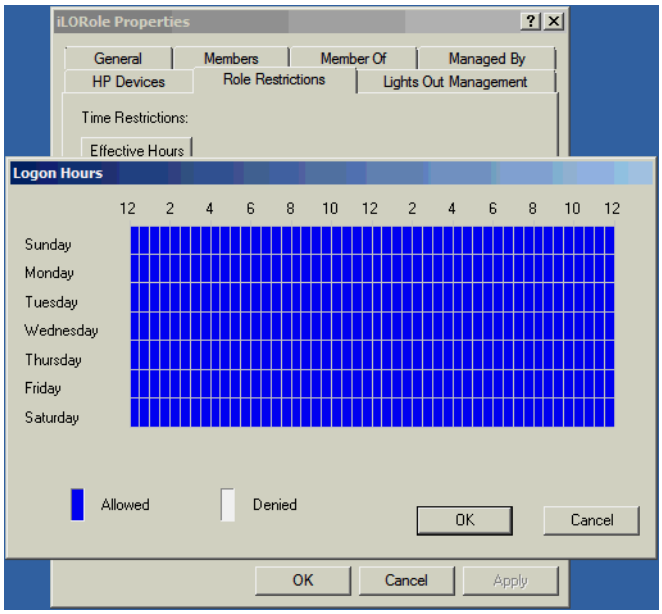


Time restrictions

You can manage the hours available for logon by members of the role by clicking **Effective Hours** on the **Role Restrictions** tab. In the **Logon Hours** dialog box (Figure 92), you can select the times available for logon for each day of the week, in half-hour increments. You can change a single

square by clicking it, or you can change a section of squares by clicking and holding the mouse button, dragging the cursor across the squares to be changed, and releasing the mouse button. The default setting is to allow access at all times.

Figure 92 Logon Hours dialog box



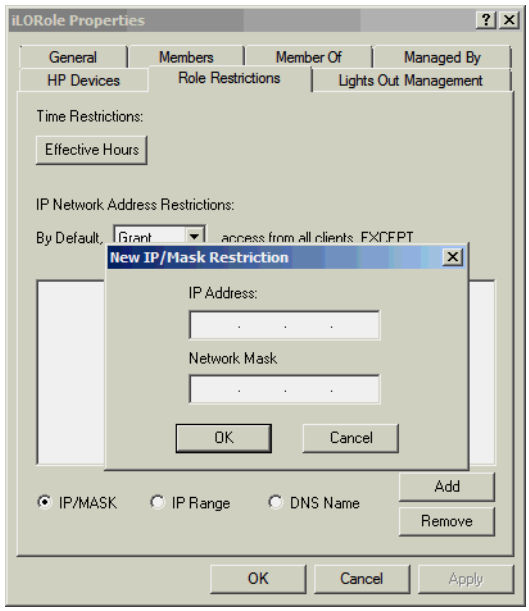
Enforced client IP address or DNS name access

Access can be granted or denied to an IP address, IP address range, or DNS name.

1. From the **By Default** list, select whether to **Grant** or **Deny** access from all addresses except the specified IP addresses, IP address ranges, and DNS names.
2. Select the type of restriction, and then click **Add**.
   - **DNS Name**—Allows you to restrict access based on a single DNS name or a subdomain, entered in the form of `host.company.com` or `*.domain.company.com`.
   - **IP/MASK**—Allows you to enter an IP address or network mask.
   - **IP Range**—Allows you to enter an IP address range.
3. In the **New IP/Mask Restriction** window (Figure 93), enter the required information, and then click **OK**.
4. Click **OK** to save the changes and close the **Properties** dialog box.

To remove any of the entries, highlight the entry in the display list and click **Remove**.

Figure 93 New IP/Mask Restriction window

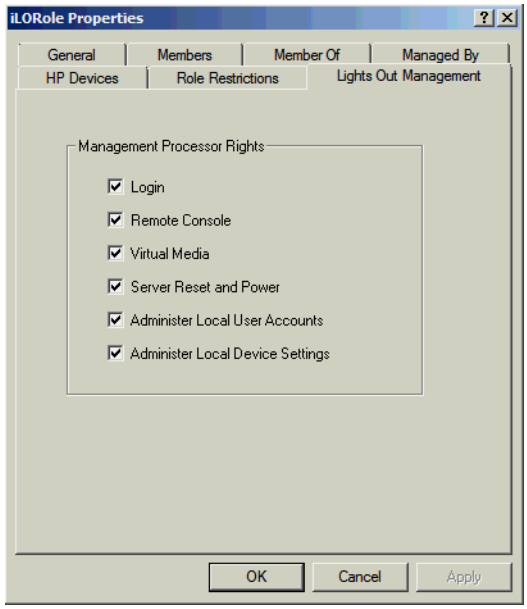


Lights Out Management tab

After you create a role, you can select rights for the role. You can make users and group objects members of the role, giving the users or group of users the rights granted by the role. Rights are managed on the **Lights Out Management** tab (Figure 94).

User rights to any iLO are calculated as the sum of all rights assigned by all roles in which the user is a member, and in which the iLO is a managed device. Using the example in "Creating and configuring directory objects for use with iLO in Active Directory" (page 176), if a user is in both the `remoteAdmins` and `remoteMonitors` roles, they will have all available rights, because the `remoteAdmins` role has all rights.

Figure 94 Lights Out Management tab



The available rights are as follows:

- **Login**—Controls whether users can log in to the associated devices.
- **Remote Console**—Enables the user to access the Remote Console.

- **Virtual Media**—Enables the user to access the iLO Virtual Media functionality.
- **Server Reset and Power**—Enables the user to access the iLO Virtual Power button to remotely reset the server or power it down.
- **Administer Local User Accounts**—Enables the user to administer accounts. Users can modify their account settings, modify other user account settings, add users, and delete users.
- **Administer Local Device Settings**—Enables the user to configure the iLO management processor settings.

Directory services for eDirectory

The following sections provide installation prerequisites, preparation instructions, and a working example of directory services for eDirectory.

eDirectory installation prerequisites

Directory services for iLO uses LDAP over SSL to communicate with the directory servers. iLO software is designed to be installed in an eDirectory version 8.6.1 (and later) tree. HP does not recommend installing this product if you have eDirectory servers with a version earlier than eDirectory 8.6.1.

Before you install snap-ins and schema extensions for eDirectory, you must read and have available the following technical documents, available from the Novell Technical Support website at http://support.novell.com.

Installing directory services for iLO requires extending the eDirectory schema. An administrator must complete the task of extending the schema. For more information, see the following Novell documents:

- TID10057565 *Unknown objects in a mixed environment*
- TID10059954 *How to test whether LDAP is working correctly*
- TID10023209 *How to configure LDAP for SSL (secure) connections*
- TID10075010 *How to test LDAP authentication*

Snap-in installation and initialization for eDirectory

The following section provides instructions for using the snap-in installation application.

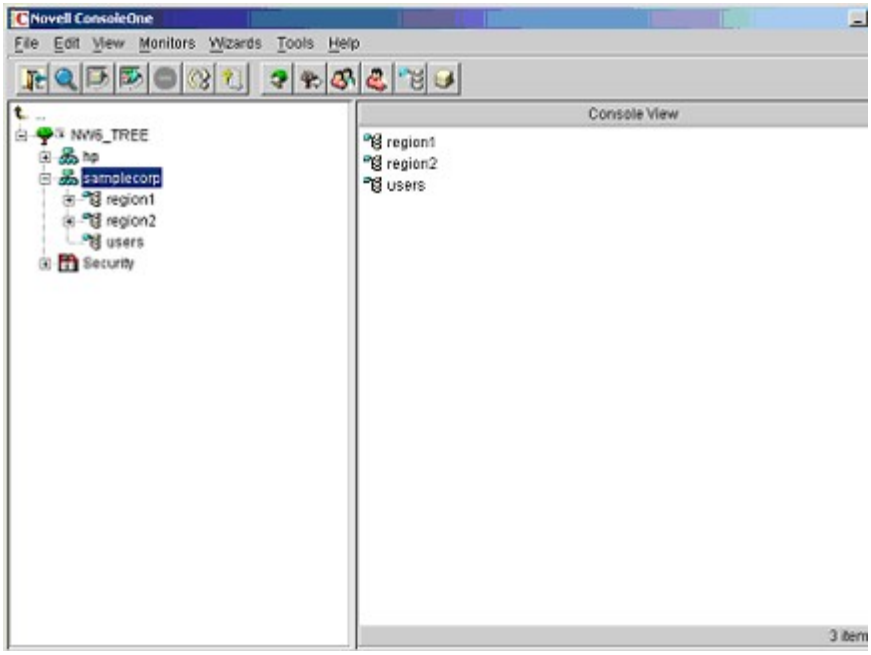
NOTE: After you install the snap-ins, you must restart ConsoleOne and MMC to show the new entries.

Example: Creating and configuring directory objects for use with iLO devices in eDirectory

This example shows how to set up roles and HP devices in a company called **samplecorp**, which consist of two regions, **region1** and **region2**.

Assume **samplecorp** has an enterprise directory as shown in Figure 95 (page 183).

Figure 95 Directory objects sample



1. Create organizational units in each region.

   Each organizational unit must contain the LOM devices and roles specific to that region.

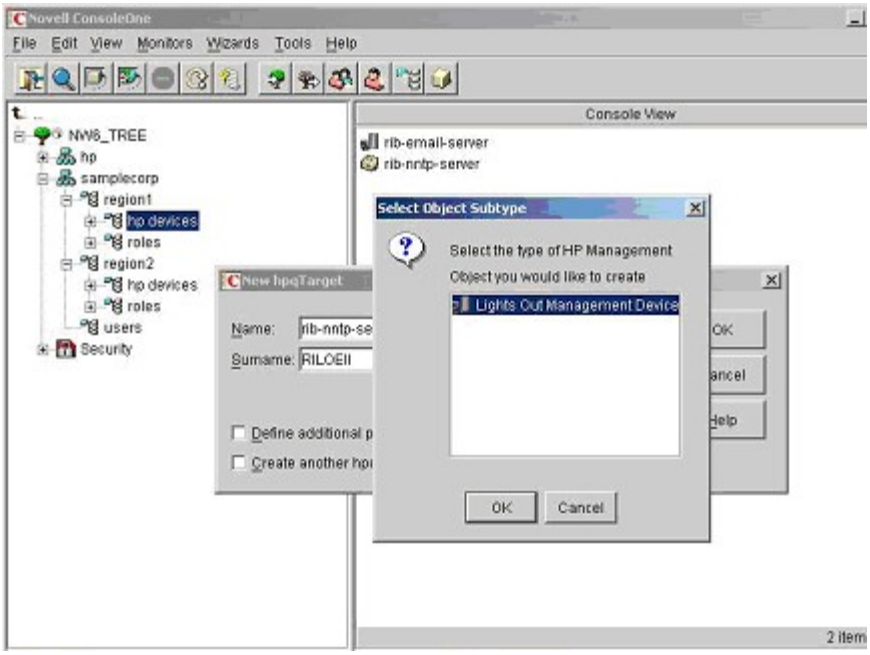
   In this example, two organizational units are created, **roles** and **hp devices**, in each organizational unit, **region1** and **region2**.

2. Create LOM objects in the **hp devices** organizational units for several iLO devices by using the HP-provided ConsoleOne snap-in tool:
   a. Right-click **hp devices** in **region1**, and then select **New→Object**.
   b. Select **hpqTarget** from the list of classes, and then click **OK**.
   c. Enter an appropriate name and surname in the **New hpqTarget** dialog box, and then click **OK**.

      In this example, the DNS host name of the iLO device, `rib-email-server`, is used as the name of the LOM object, and the surname is `RILOEII`.

      The **Select Object Subtype** dialog box opens (Figure 96).

Figure 96 Select Object Subtype window



d. Select **Lights Out Management Device**, and then click **OK**.

e. Repeat Step 2.a through Step 2.d to create the following LOM objects:

- Create **rib-nntp-server** and **rib-file-server-users1** in **hp devices** under **region1**
- Create **rib-file-server-users2** and **rib-app-server** in **hp devices** under **region2**.

3. Create HP role objects in the **roles** organizational units by using the HP-provided ConsoleOne snap-in tool:

a. Right-click the **roles** organizational unit in **region2**, and then select **New→Object**.

b. Select **hpqRole** from the list of classes, and then click **OK**.

c. Enter an appropriate name in the **New hpqRole** dialog box, and then click **OK**.

In this example, the role contains users trusted for remote server administration and is named `remoteAdmins`.

The **Select Object Subtype** dialog box opens.

d. Select **Lights Out Management Devices** from the list because this role manages the rights to Lights-Out Management devices, and then click **OK**.

e. Repeat Step 3.a through Step 3.d to create the following role objects:

- Create **remoteMonitors**, in **roles** in **region1**.
- Create **remoteAdmins** and **remoteMonitors** in **roles** in **region2**.

4. Assign rights to the roles and associate the roles with users and devices by using the HP-provided ConsoleOne snap-in tool:

a. Right-click the **remoteAdmins** role in **roles** in **region1**, and then select **Properties**.

b. Select the **HP Management→Role Managed Devices** tab (Figure 98), and then click **Add**.

The **Select Object Subtype** dialog box opens.

c. In the **Select Object Subtype** dialog box, browse to **hp devices** in **region1**. Select the three LOM objects created in Step 2.

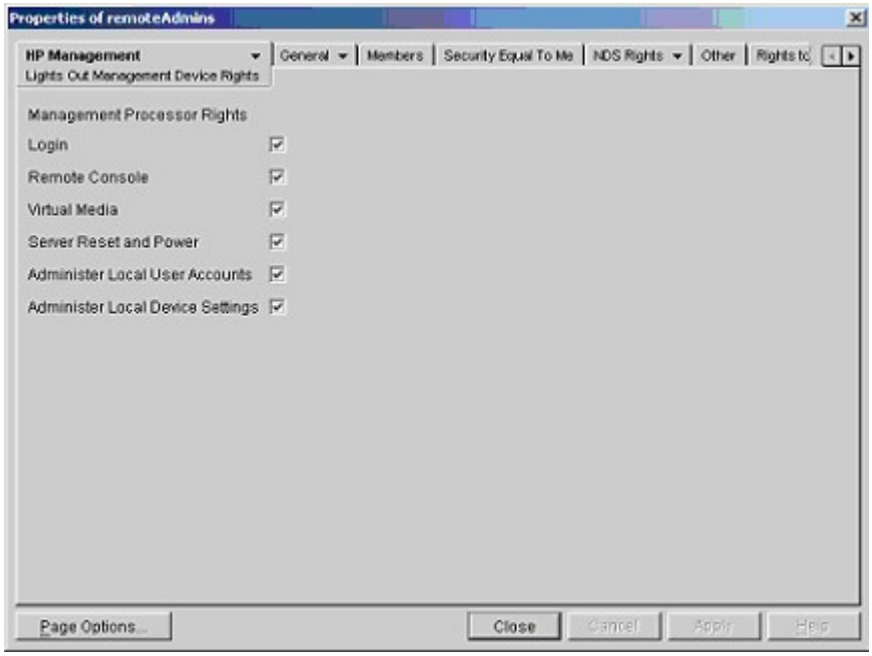
d. Click **OK**, and then click **Apply**.

e. Click the **Members** tab (Figure 99) and add users to the role by clicking the **Add** button on the **Select Objects** dialog box.

   Devices and users are now associated.

f. Select the **HP Management→Lights Out Management Device Rights** tab (Figure 97 (page 185)).

Figure 97 Properties window



g. Set the rights for the role, and then click **Apply**. Click **Close** to close the **Properties** window.

   In this example, the users in the **remoteAdmins** role receive full access to the iLO functionality.

   All users within the role have the rights assigned to the role on all iLO devices that the role manages.

5. Using the procedure in Step 4, edit the properties of the **remoteMonitors** role:
   a. Add the three LOM objects in **hp devices** in **region1** to the **Managed Devices** list on the **HP Management→Role Managed Devices** tab (Figure 98).
   b. Add users to the **remoteMonitors** role by using the **Members** tab (Figure 99).
   c. Assign the Login right to the **remoteMonitors** role by using the **HP Management→Lights Out Management Device Rights** tab.

      Members of the **remoteMonitors** role will be able to authenticate and view the server status.

6. To configure a LOM device and associate it with a LOM object used in this example, use settings similar to the following on the **Directory Settings** page.

```
LOM Object Distinguished Name = cn=rib-email-server,ou=hp
devices,ou=region1,o=samplecorp Directory User Context 1 =
ou=users,o=samplecorp
```

NOTE: Commas, not periods, are used in LDAP DNs to separate each component.

Directory services objects for eDirectory

One of the keys to directory-based management is proper virtualization of the managed devices in the directory service. This virtualization allows the administrator to build relationships between the managed device and users or groups within the directory service. User management of iLO requires the following basic objects in the directory service:

- Lights-Out Management object
- Role object
- User objects

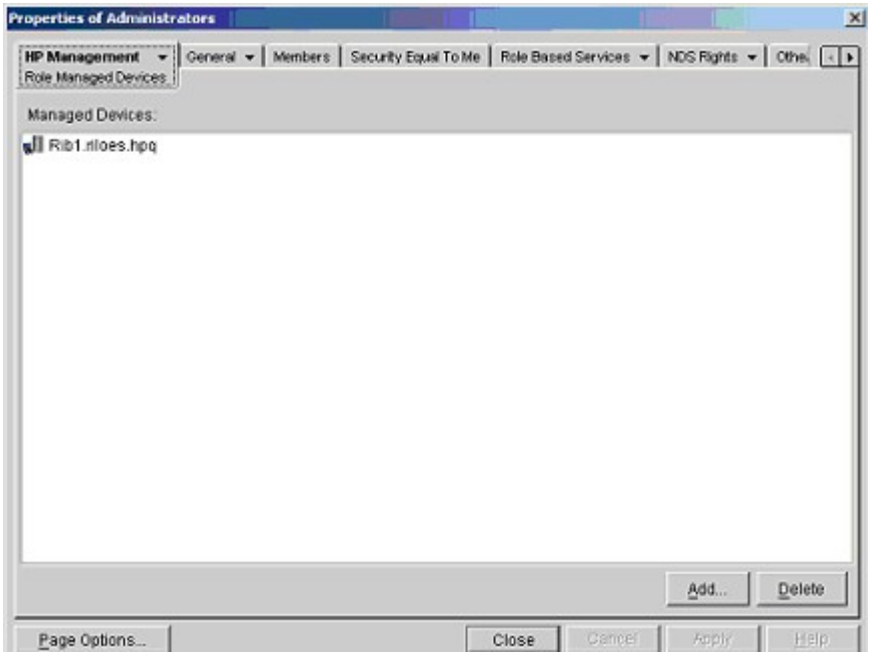
Each object represents a device, user, or relationship that is required for directory-based management.

The following sections discuss the additional management options available in the ConsoleOne snap-in tool after the HP snap-ins are installed.

Role Managed Devices

The **HP Management→Role Managed Devices** tab (Figure 98 (page 186)) is used to add HP devices to be managed within a role. Clicking **Add** allows you to browse to an HP device and add it as a managed device.

Figure 98 Role Managed Devices tab

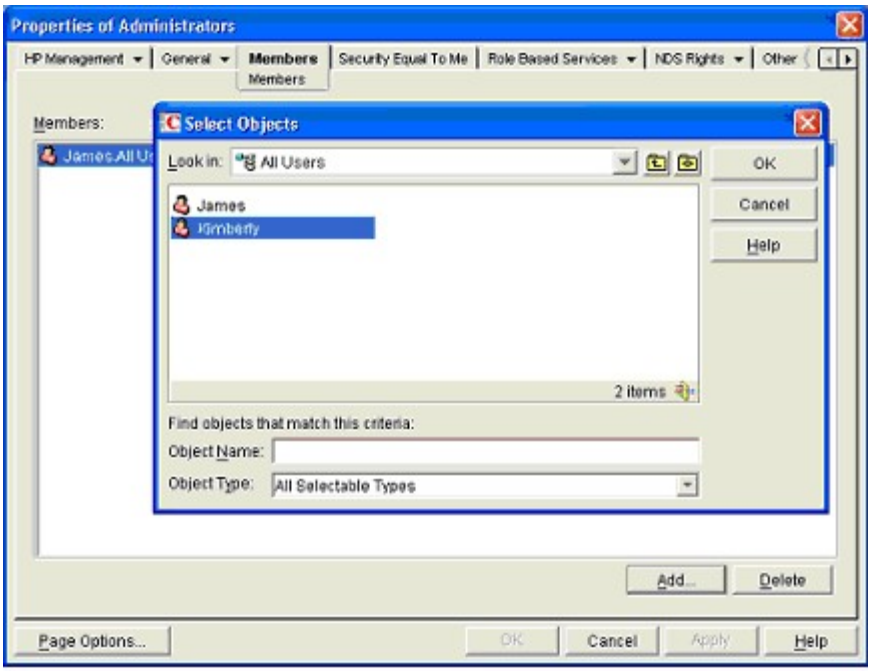


Members tab

After user objects are created, the **Members** tab allows you to manage the users within the role.

- Click **Add** to open the **Select Objects** window (Figure 99), which enables you to browse to the user that you want to add.

Figure 99 Select Objects dialog box



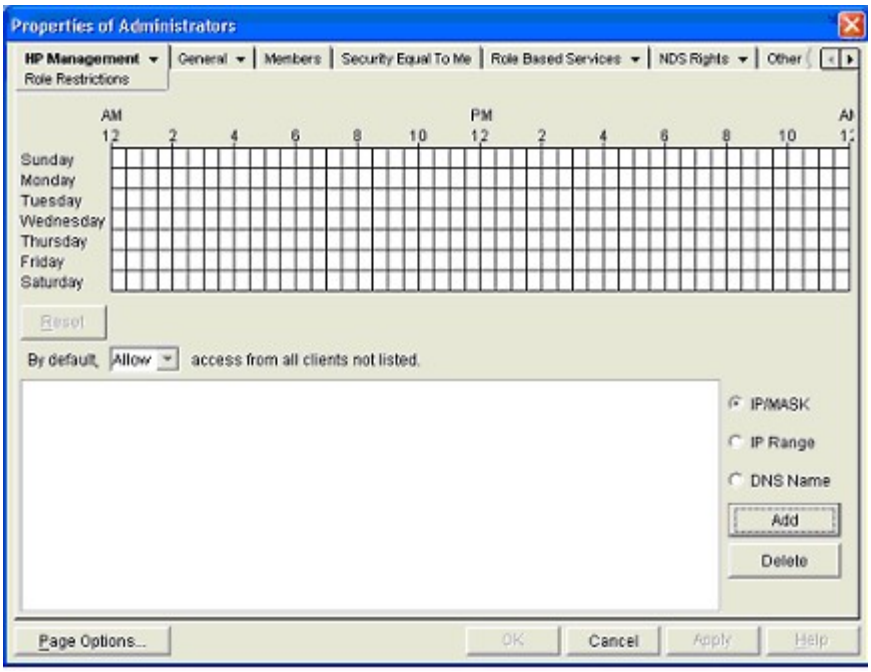
- To remove a user, select the user name, and then click **Delete**.

Role Restrictions tab

The **Role Restrictions** tab (Figure 100) allows you to set the following login restrictions for the role:

- Time restrictions
- IP network address restrictions:
  - IP/mask
  - IP range
- DNS name

Figure 100 Role Restrictions tab



Time restrictions

You can manage the hours available for logon by members of the role by using the time grid displayed on the **Role Restrictions** tab. You can select the times available for logon for each day of the week, in half-hour increments. You can change a single square by clicking it, or a section of squares by clicking and holding the mouse button, dragging the cursor across the squares to be changed, and releasing the mouse button. The default setting is to allow access at all times.

Enforced client IP address or DNS name access

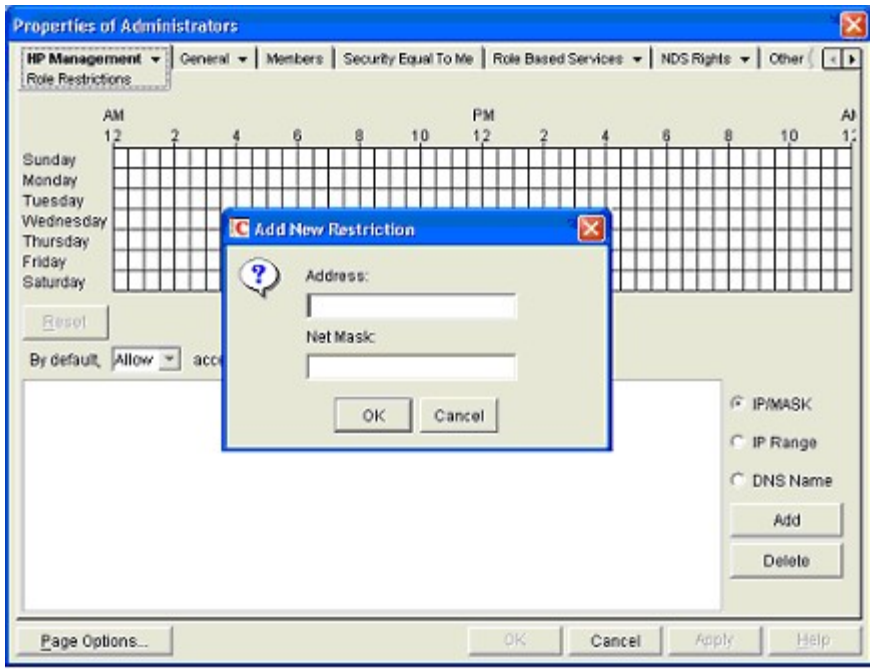
Access can be granted or denied to an IP address, IP address range, or DNS name.

1. From the **By Default** list, specify whether to **Allow** or **Deny** access from all addresses, except the specified IP addresses, IP address ranges, and DNS names.
2. Select the addresses to be added, select the type of restriction, and then click **Add**.
3. In the **Add New Restriction** dialog box, enter the information, and then click **OK**, as shown in Figure 101 (page 189).

   The **DNS Name** option allows you to restrict access based on a single DNS name or a subdomain, entered in the form of `host.company.com` or `*.domain.company.com`.
4. Click **Apply** to save the changes.

To remove any of the entries, highlight the entry in the display list and click **Delete**.

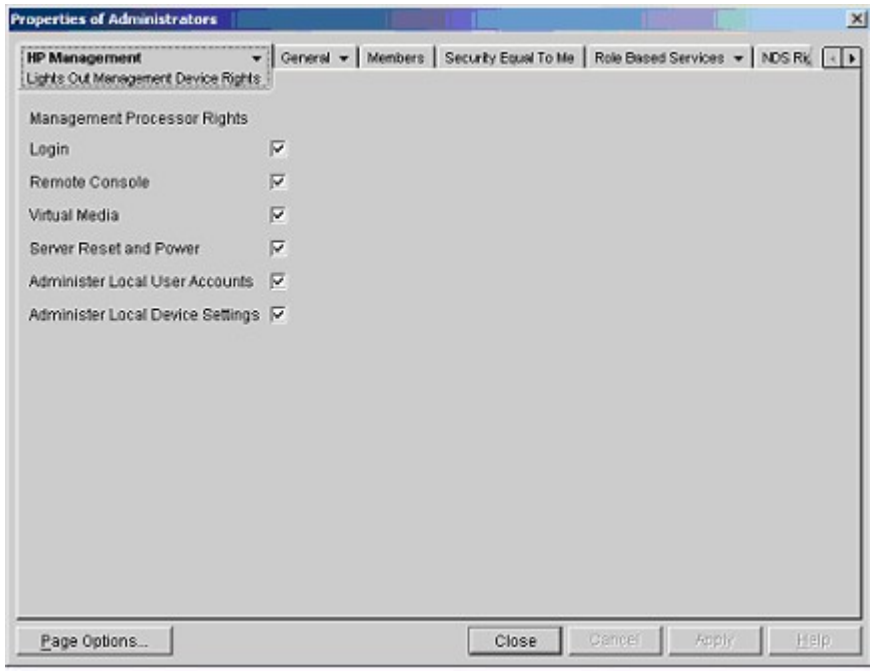
Figure 101 Add New Restriction dialog box



eDirectory Lights-Out Management

After you create a role, you can select rights for the role. You can make users and group objects members of the role, giving them the rights granted by the role. Rights are managed on the **Lights Out Management Device Rights** option of the **HP Management** tab (Figure 102).

Figure 102 Lights Out Management Device Rights tab



The available rights are as follows:

- **Login**—Controls whether users can log in to the associated devices.

  Login access can be used to create a user who is a service provider and who receives alerts from iLO but does not have login access to iLO.

- **Remote Console**—Enables the user to access the Remote Console.

- **Virtual Media**—Enables the user to access the iLO Virtual Media functionality.
- **Server Reset and Power**—Enables the user to access the iLO Virtual Power button to remotely reset the server or power it down.
- **Administer Local User Accounts**—Enables the user to administer accounts. Users can modify their account settings, modify other user account settings, add users, and delete users.
- **Administer Local Device Settings**—Enables the user to configure the iLO management processor settings.

User rights to any LOM device are calculated as the sum of all rights assigned by all roles in which the user is a member, and in which the iLO device is a managed device. Using the example in "Example: Creating and configuring directory objects for use with iLO devices in eDirectory" (page 182), if a user is in both the **remoteAdmins** and **remoteMonitors** roles, the user will have all rights, because the **remoteAdmins** role has all rights.

User login using directory services

The **Login Name** box on the iLO login page accepts directory users and local users.

The maximum length of the login name is 39 characters for local users and 256 characters for directory users.

- **Directory users**—The following formats are supported:
  - LDAP fully distinguished names

    Example: `CN=John Smith,CN=Users,DC=HP,DC=COM`, or `@HP.com`

    The short form of the login name does not notify the directory which domain you are trying to access. You must provide the domain name or use the LDAP DN of your account.
  - `DOMAIN\user name` form (Active Directory only)

    Example: `HP\jsmith`
  - `username@domain` form (Active Directory only)

    Example: `jsmith@hp.com`

    Directory users specified using the @ searchable form might be located in one of three searchable contexts, which are configured on the **Security→Directory** page.
  - Username format

    Example: John Smith

    Directory users specified using the username format might be located in one of three searchable contexts, which are configured on the **Security→Directory** page.
- **Local users**—Enter the Login Name of your iLO local user account.

Directory-enabled remote management

This section is for administrators who are familiar with directory services and the iLO product and want to use the HP schema directory integration option for iLO. You must be familiar with directory services.

Directory-enabled remote management enables you to do the following:

- **Create Lights-Out Management objects**

  You must create one LOM device object to represent each device that will use the directory service to authenticate and authorize users. For information on creating LOM device objects for Active Directory and eDirectory, see "Directory services" (page 160). In general, you can use the snap-ins that HP has provided to create objects. It is useful to give the LOM device

objects meaningful names, such as the device network address, DNS name, host server name, or serial number.

- **Configure Lights-Out management devices**

  Every LOM device that uses the directory service to authenticate and authorize users must be configured with the appropriate directory settings. For information on the specific directory settings, see "Configuring authentication and directory server settings" (page 52). In general, you can configure each device with the appropriate directory server address, LOM object DN, and any user contexts. The server address is the IP address or DNS name of a local directory server or, for more redundancy, a multihost DNS name.

Creating roles to follow organizational structure

Often, administrators in an organization are placed in a hierarchy in which subordinate administrators must assign rights independently of ranking administrators. In this case, it is useful to have one role that represents the rights assigned by higher-level administrators, and to allow subordinate administrators to create and manage their own roles.

Using existing groups

Many organizations have users and administrators arranged in groups. In many cases, it is convenient to use the existing groups and associate them with one or more Lights-Out Management role objects. When the devices are associated with the role objects, the administrator controls access to the Lights-Out devices associated with the role by adding or deleting members from the groups.

When using Microsoft Active Directory, you can place one group within another (that is, use nested groups). Role objects are considered groups and can include other groups directly. Add the existing nested group directly to the role, and assign the appropriate rights and restrictions. You can add new users to either the existing group or the role.

When you are using trustee or directory rights assignments to extend role membership, users must be able to read the LOM object that represents the LOM device. Some environments require that the trustees of a role also be read trustees of the object to successfully authenticate users.

Using multiple roles

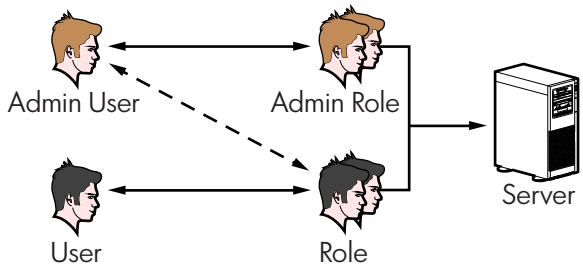
Most deployments do not require that the same user be in multiple roles managing the same device. However, these configurations are useful for building complex rights relationships. When users build multiple-role relationships, they receive all rights assigned by every applicable role. Roles can only grant rights, never revoke them. If one role grants a user a right, then the user has the right, even if the user is in another role that does not grant that right.

Typically, a directory administrator creates a base role with the minimum number of rights assigned, and then creates additional roles to add more rights. These additional rights are added under specific circumstances or to a specific subset of the base role users.

For example, an organization can have two types of users: administrators of the LOM device or host server, and users of the LOM device. In this situation, it makes sense to create two roles, one for the administrators and one for the users. Both roles include some of the same devices but grant different rights. Sometimes, it is useful to assign generic rights to the lesser role and include the LOM administrators in that role, as well as the administrative role.

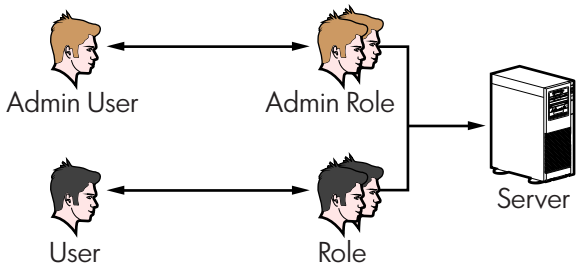
An Admin user gains the login right from the regular user role. Advanced rights are assigned through the Admin role, which assigns the advanced rights Server Reset and Remote Console (Figure 103).

Figure 103 Admin user



The Admin role assigns all Admin rights: Server Reset, Remote Console, and Login (Figure 104).

Figure 104 Admin role

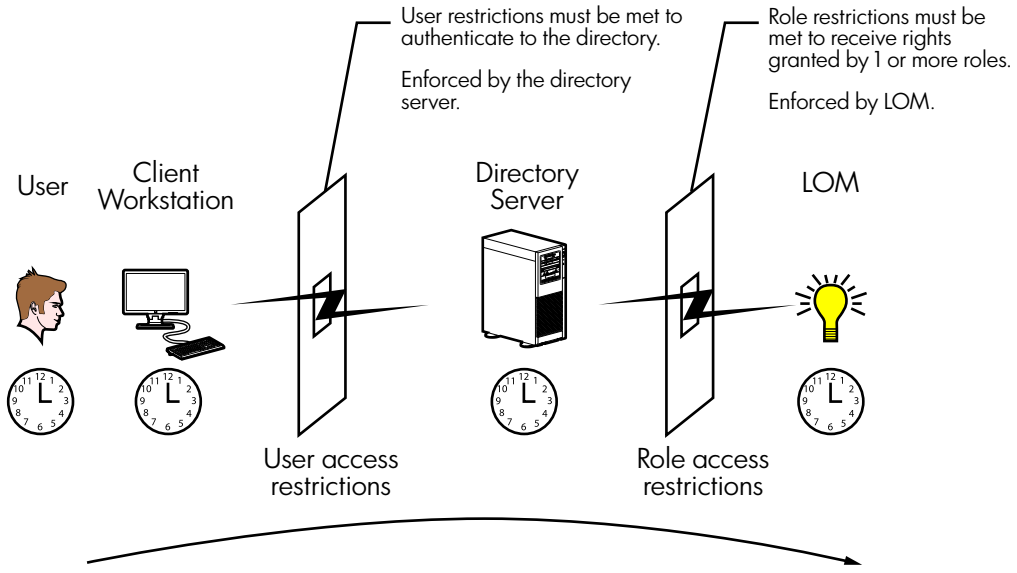


How directory login restrictions are enforced

Two sets of restrictions can limit a directory user's access to LOM devices (Figure 105).

- **User access restrictions** limit a user's access to authenticate to the directory.
- **Role access restrictions** limit an authenticated user's ability to receive LOM privileges based on rights specified in one or more roles.

Figure 105 Directory login restrictions



Restricting roles

Restrictions allow administrators to limit the scope of a role. A role grants rights only to users who satisfy the role restrictions. Using restricted roles results in users who have dynamic rights that can change based on the time of day or network address of the client.

NOTE: When directories are enabled, access to a particular iLO is based on whether the user has read access to a role object that contains the corresponding iLO object. This includes, but is not limited to, the members listed in the role object. If the role is configured to allow inheritable permissions to propagate from a parent, members of the parent that have read access privileges will also have access to iLO. To view the access control list, navigate to **Active Directory Users and Computers**, open the **Properties** page for the role object, and then click the **Security** tab. The Advanced View must be enabled in MMC in order to view the **Security** tab.

For instructions on how to create network and time restrictions for a role, see "Role Restrictions tab" (page 179) or "Role Restrictions tab" (page 187).

Role time restrictions

Administrators can place time restrictions on LOM roles. Users are granted the rights specified for the LOM devices listed in the role only if they are members of the role and meet the time restrictions for the role. LOM devices use local host time to enforce time restrictions. If the LOM device clock is not set, the role time restriction fails unless no time restrictions are specified for the role.

Role-based time restrictions can be met only if the time is set on the LOM device. The time is normally set when the host is booted. The time setting can be maintained by configuring SNTP or by running the agents in the host operating system, which allows the LOM device to compensate for leap years and minimize clock drift with respect to the host. Events, such as unexpected power loss or flashing LOM firmware, can cause the LOM device clock to not be set. Also, the host time must be correct for the LOM device to preserve time across firmware flashes.

Role address restrictions

Role address restrictions are enforced by the LOM firmware, based on the client IP network address. When the address restrictions are met for a role, the rights granted by the role apply.

Address restrictions can be difficult to manage if access is attempted across firewalls or through network proxies. Either of these mechanisms can change the apparent network address of the client, causing the address restrictions to be enforced in an unexpected manner.

User restrictions

You can restrict access using address or time restrictions.

User address restrictions

Administrators can place network address restrictions on a directory user account, which are enforced by the directory server. For information about the enforcement of address restrictions on LDAP clients, such as a user logging in to a LOM device, see the documentation for the directory service.

Network address restrictions placed on the user in the directory might not be enforced in the expected manner if the directory user logs in through a proxy server. When a user logs in to a LOM device as a directory user, the LOM device attempts authentication to the directory as that user, which means that address restrictions placed on the user account apply when the user is accessing the LOM device. However, because the user is proxied at the LOM device, the network address of the authentication attempt is that of the LOM device, not that of the client workstation.

IP address range restrictions

IP address range restrictions enable the administrator to specify network addresses that are granted or denied access. The address range is typically specified in a low-to-high range format. An address

range can be specified to grant or deny access to a single address. Addresses that fall within the low-to-high IP address range meet the IP address restriction.

IP address and subnet mask restrictions

IP address and subnet mask restrictions enable the administrator to specify a range of addresses that are granted or denied access. This format has similar capabilities as an IP address range, but might be more native to your networking environment. An IP address and subnet mask range is typically specified through a subnet address and address bit mask that identifies addresses on the same logical network.

In binary math, if the bits of a client machine address, combined with the bits of the subnet mask, match the subnet address in the restriction, the client machine meets the restriction.

DNS-based restrictions

DNS-based restrictions use the network name service to examine the logical name of the client machine by looking up machine names assigned to the client IP addresses. DNS restrictions require a functional name server. If the name service goes down or cannot be reached, DNS restrictions cannot be matched and the client machine fails to meet the restriction.

DNS-based restrictions can limit access to a specific machine name or to machines that share a common domain suffix. For example, the DNS restriction **www.example.com** matches hosts that are assigned the domain name **www.example.com**. However, the DNS restriction ***.example.com** matches any machine that originates from the **example** company.

DNS restrictions can cause ambiguity because a host can be multi-homed. DNS restrictions do not necessarily match one to one with a single system.

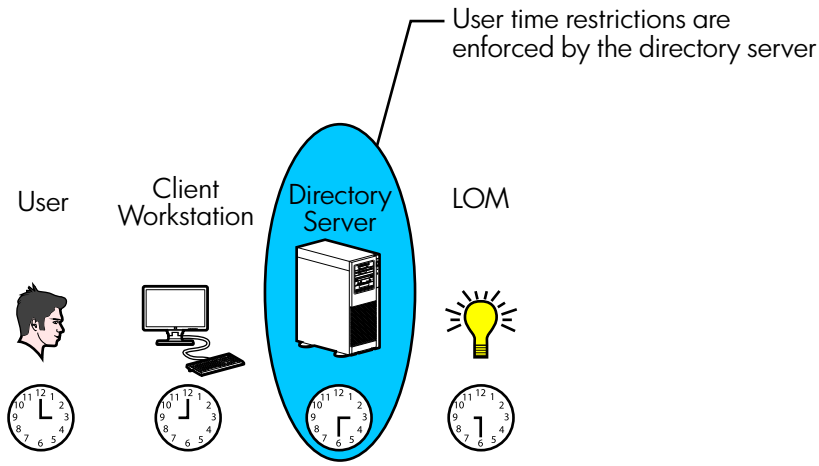
Using DNS-based restrictions can create security complications. Name service protocols are not secure. Any individual who has malicious intent and access to the network can place a rogue DNS service on the network and create a fake address restriction criterion. When implementing DNS-based address restrictions, be sure to take organizational security policies into consideration.

User time restrictions

Administrators can place a time restriction on directory user accounts (Figure 106). Time restrictions limit the ability of the user to log in (authenticate) to the directory. Typically, time restrictions are enforced using the time at the directory server. If the directory server is located in a different time zone, or if a replica in a different time zone is accessed, time-zone information from the managed object can be used to adjust for relative time.

The directory server evaluates user time restrictions, but the determination can be complicated by time-zone changes or the authentication mechanism.

Figure 106 User time restrictions



Creating multiple restrictions and roles

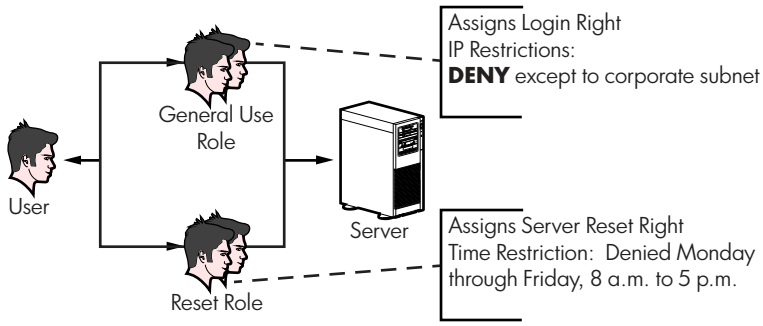
The most useful application of multiple roles is restricting one or more roles so that rights do not apply in all situations. Other roles provide different rights under different constraints. Using multiple restrictions and roles enables the administrator to create arbitrary, complex rights relationships with a minimum number of roles.

For example, an organization might have a security policy in which LOM administrators are allowed to use the LOM device from within the corporate network, but can reset the server only after regular business hours.

Directory administrators might be tempted to create two roles to address this situation, but extra caution is required. Creating a role that provides the required server reset rights and restricting it to after hours might allow administrators outside the corporate network to reset the server, which is contrary to most security policies.

In the example shown in Figure 107 (page 195), security policy dictates that general use is restricted to clients in the corporate subnet, and server reset capability is restricted to after hours.

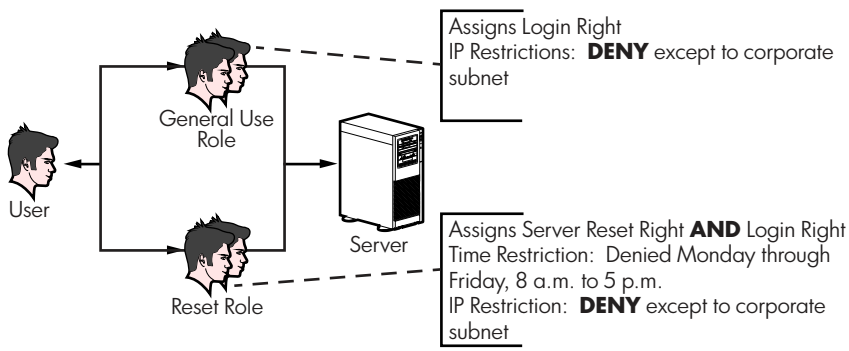
Figure 107 Creating restrictions and roles



Alternatively, the directory administrator might create a role that grants the login right and restrict it to the corporate network, and then create another role that grants only the server reset right and restrict it to after-hours operation. This configuration is easier to manage but more dangerous because ongoing administration might create another role that grants the login right to users from addresses outside the corporate network. This role might unintentionally grant the LOM administrators in the server Reset role the ability to reset the server from anywhere, if they satisfy the role's time constraints.

The previous configuration (Figure 107) meets corporate security requirements. However, adding another role that grants the login right can inadvertently grant server reset privileges from outside the corporate subnet after hours. A more manageable solution would be to restrict the Reset role and the General Use role, as shown in Figure 108 (page 195).

Figure 108 Restricting the Reset and General Use roles



Using bulk import tools

Adding and configuring large numbers of LOM objects is time consuming. HP provides several utilities to assist with these tasks.

- **HP Lights-Out Migration utility**

  The HP Lights-Out Migration utility imports and configures multiple LOM devices. It includes a GUI that provides a step-by-step approach to implementing or upgrading large numbers of management processors. HP recommends using this GUI method when upgrading several management processors. For more information, see "Using HP Directories Support for ProLiant Management Processors" (page 197).

- **HP SIM utilities**

  The HP SIM utilities enable you to perform the following tasks:

  - Manage multiple LOM devices.
  - Discover the LOM devices as management processors by using HPQLOCFG to send a RIBCL XML script file to a group of LOM devices. The LOM devices perform the actions designated by the RIBCL file and send a response to the HPQLOCFG log file. For more information, see the *HP iLO 3 Scripting and Command Line Guide*.

- **Traditional import utilities**

  Administrators familiar with tools such as LDIFDE or the NDS Import/Export Wizard can use these utilities to import or create many LOM device objects in the directory. Administrators must still configure the devices manually, as described earlier, but can do so at any time. Programmatic or scripting interfaces can also be used to create the LOM device objects in the same way as users or other objects. For information about attributes and attribute data formats when you are creating LOM objects, see "Directory services schema" (page 239).

HP Directories Support for ProLiant Management Processors utility

You can download this utility from http://www.hp.com/support/ilo3.

The HP Directories Support for ProLiant Management Processors utility (`HPLOMIG.exe`) is for customers who installed management processors and want to simplify the migration of these processors to management by directories. The utility automates some of the migration steps necessary for the management processors to support directory services. The utility can do the following:

- Discover management processors on the network.
- Upgrade the management processor firmware.
- Name the management processors to identify them in the directory.
- Create objects in the directory that correspond to each management processor, and associate them with a role.
- Configure the management processors to enable them to communicate with the directory.

Compatibility

The HP Directories Support for ProLiant Management Processors utility operates on Microsoft Windows and requires the Microsoft .NET Framework. The utility supports the following operating systems:

- Windows Server 2003 32-bit, 64-bit
- Windows Server 2008 32-bit, 64-bit
- Windows Server 2008 R2
- Windows Vista

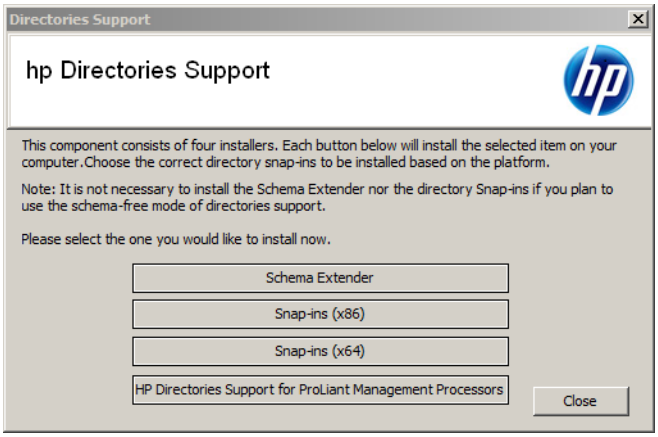
- Windows 7
- Windows 2012

HP Directories Support for ProLiant Management Processors package

The migration software, schema extender, and management snap-ins are included in the HP Directories Support for ProLiant Management Processors package. You can download the installer from http://www.hp.com/support/ilo3. To complete the migration of your management processors, you must extend the schema and install the management snap-ins before running the migration tool.

To install the migration utilities, start the installer, and then click **HP Directories Support for ProLiant Management Processors**, as shown in Figure 109 (page 197).

Figure 109 HP Directories Support for ProLiant Management Processors installer



The `HPLOMIG.exe` file, the required DLLs, the license agreement, and other files are installed in the directory `C:\Program Files\Hewlett-Packard\HP Directories Support for ProLiant Management Processors`. You can select a different directory. The installer creates a shortcut to HP Directories Support for ProLiant Management Processors on the **Start** menu and installs a sample XML file.

NOTE: If the installation utility detects that the .NET Framework is not installed, it displays an error message and exits.

Using HP Directories Support for ProLiant Management Processors

The HP Directories Support for ProLiant Management Processors utility automates the process of migrating management processors by creating objects in the directory that correspond to each management processor and associating them with a role. HP Directories Support for ProLiant Management Processors has a GUI and provides a wizard for implementing or upgrading multiple management processors.

Finding management processors

The first migration step is to discover all management processors that you want to enable for directory services. You can search for management processors by using DNS names, IP addresses, or IP address wildcards. The following rules apply to the values entered in the **Addresses** box:

- DNS names, IP addresses, and IP address wildcards must be delimited with semicolons.
- The IP address wildcard uses the asterisk (*) character in the third and fourth octet fields. For example, IP address `16.100.*.*` is valid, and IP address `16.*.*.*` is invalid.

- Ranges can also be specified using a hyphen. For example, `192.168.0.2-10` is a valid range. A hyphen is supported only in the rightmost octet.
- After you click **Find**, the utility begins pinging and connecting to port 443 (the default SSL port) to determine whether the target network address is a management processor. If the device does not respond to the ping or connect appropriately on port 443, the utility determines that it is not a management processor.

If you click **Next**, click **Back**, or exit the utility during discovery, operations on the current network address are completed, but those on subsequent network addresses are canceled.

To discover your management processors:

1. Select **Start→All Programs→Hewlett-Packard→HP Directories Support for ProLiant Management Processors.**

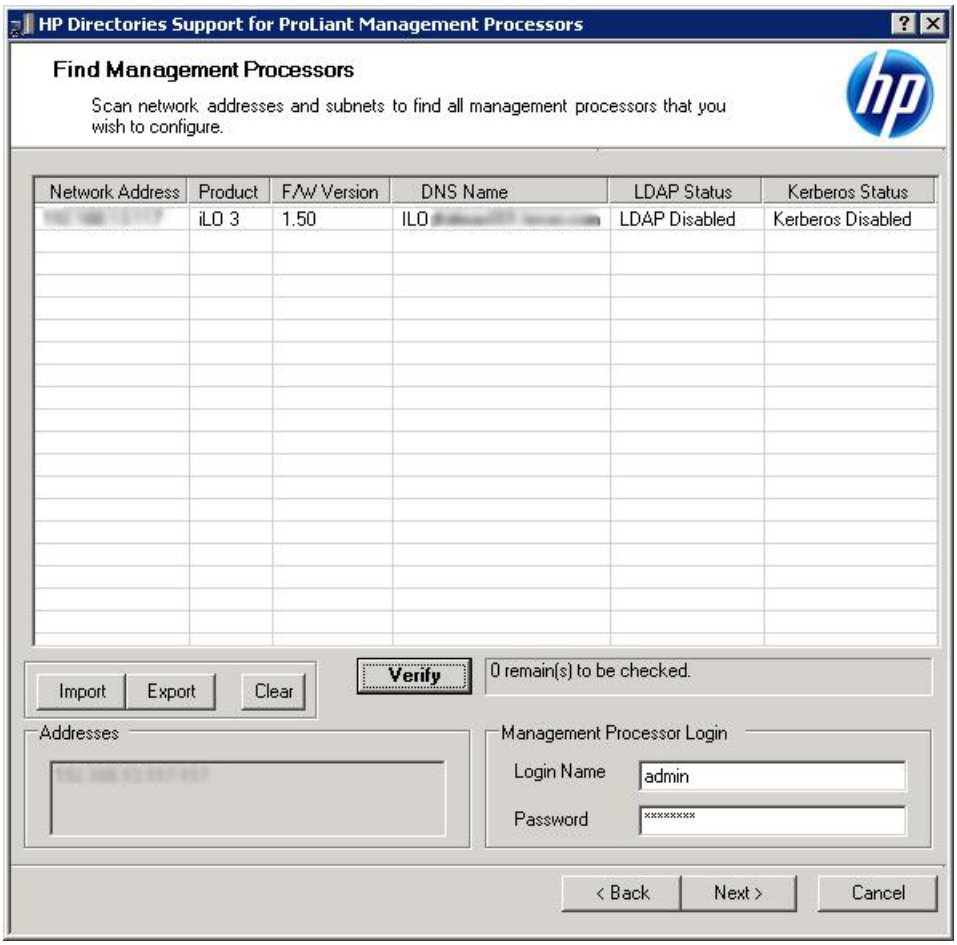
   The **Welcome** page opens.
2. Click **Next**.

   The **Find Management Processors** window opens.
3. In the **Addresses** box, enter the values to perform the management processor search.

4. Enter your iLO login name and password, and then click **Find**.

   When the search is complete, the management processors are listed and the **Find** button changes to **Verify**, as shown in Figure 110 (page 199).

Figure 110 Find Management Processors window



You can also enter a list of management processors from a file by clicking **Import**. The file is a simple text file with one management processor listed per line. The columns, which are delimited with semicolons, are as follows:

- **Network Address**
- **Product**
- **F/W Version**
- **DNS Name**
- **User Name**
- **Password**
- **LDAP Status**
- **Kerberos Status**

For example, one line might have the following information:

```
16.100.225.20;iLO;1.10;ILOTPILOT2210;user;password;Default
Schema;Kerberos Disabled
```

If, for security reasons, the user name and password cannot be included in the file, leave these columns blank, but enter the semicolons.

Upgrading firmware on management processors

The **Upgrade Firmware** page enables you to update the firmware on your iLO management processors. It also enables you to designate the location of the firmware image for each management processor by entering the path or clicking **Browse**.

NOTE: Binary images of the firmware for the management processors must be accessible from the system that is running the migration utility. These binary images can be downloaded from http://www.hp.com/support/ilo3.

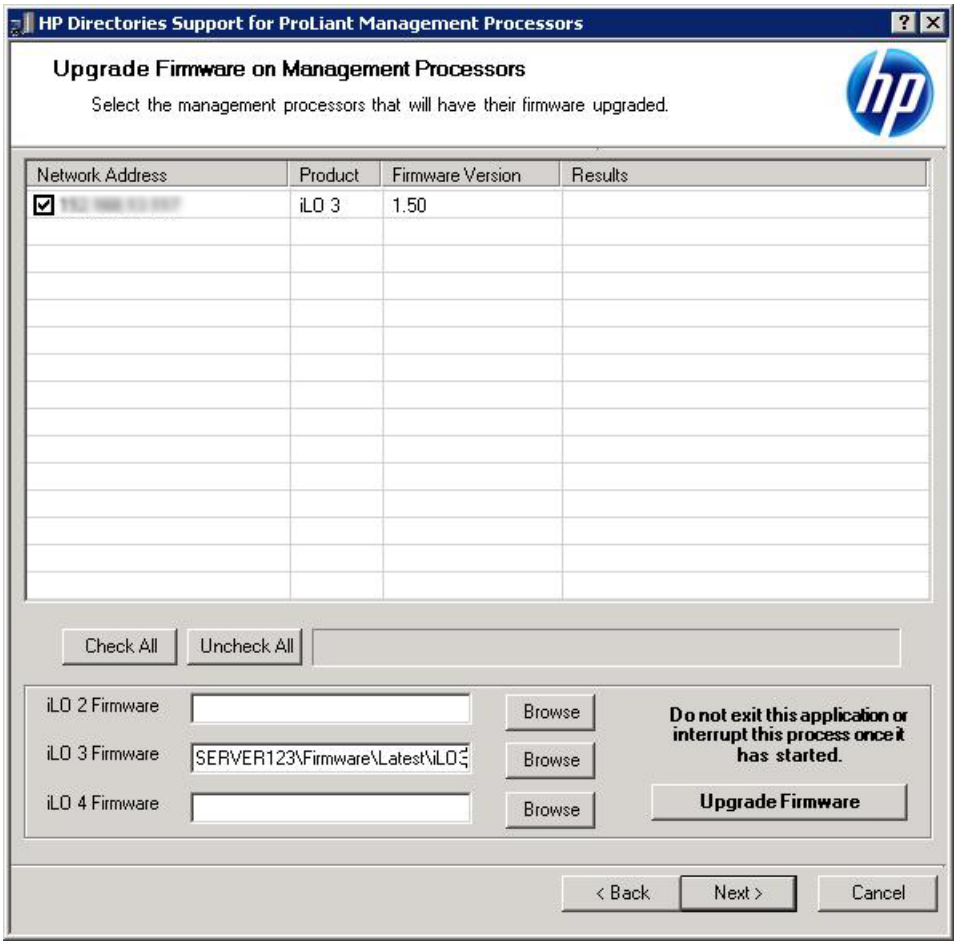
The upgrade process might take a long time, depending on the number of management processors selected. The firmware upgrade of a single management processor can take as long as 5 minutes to complete. If an upgrade fails, a message is displayed in the **Results** column, and the utility continues to upgrade the other discovered management processors.

IMPORTANT: HP recommends that you test the upgrade process and verify the results in a test environment before running the utility on a production network. An incomplete transfer of the firmware image to a management processor might result in having to locally reprogram the management processor.

To upgrade the firmware on your management processors:

1. Navigate to the **Upgrade Firmware on Management Processors** window, as shown in Figure 111 (page 200).

Figure 111 Upgrade Firmware on Management Processors window



2. Select the management processors to upgrade.
3. For each discovered management processor type, enter the correct pathname to the firmware image or browse to the image.

4. Click **Upgrade Firmware**.

   The selected management processors are upgraded. Although this utility enables you to upgrade hundreds of management processors, only 25 management processors are upgraded simultaneously. Network activity is considerable during this process.

5. After the upgrade is complete, click **Next**.

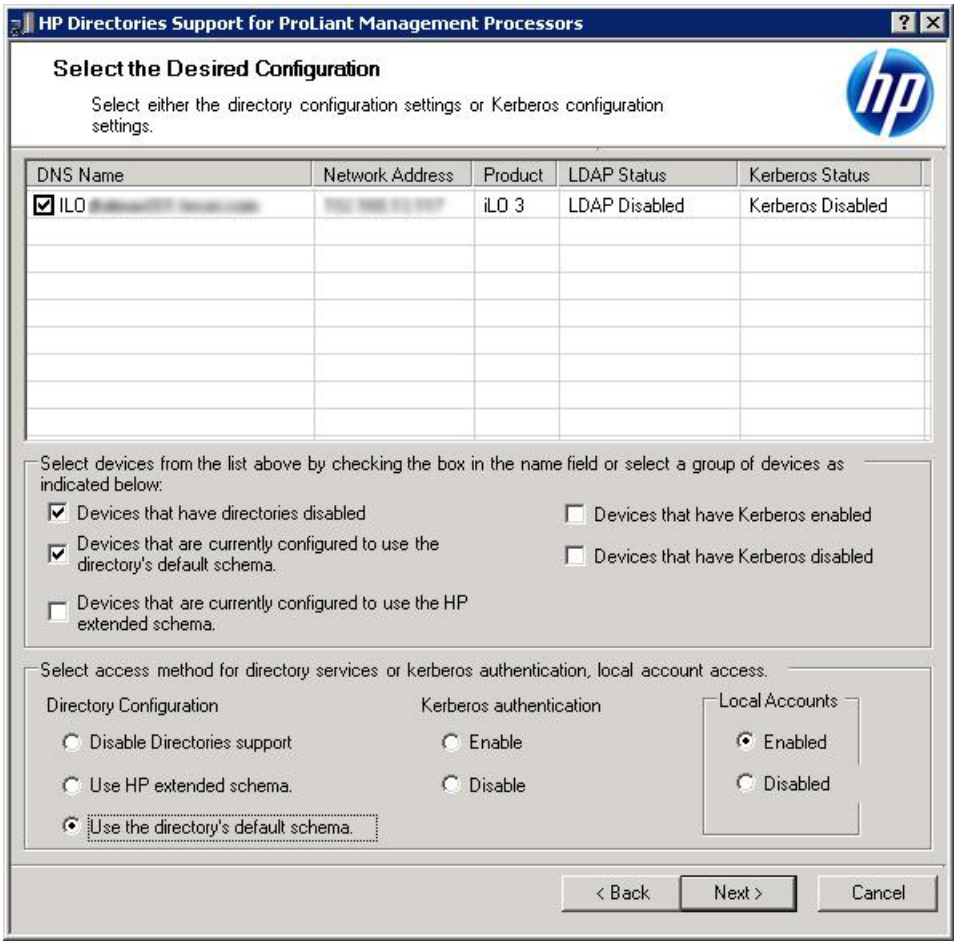
During the firmware upgrade process, all buttons are deactivated to prevent navigation. You can still close the application by clicking the X at the top right of the page. If the GUI is closed during programming of firmware, the application continues to run in the background and completes the firmware upgrade on all selected devices.

Selecting a directory access method

After you click **Next** in the **Upgrade Firmware on Management Processors** window, the **Select the Desired Configuration** window appears (Figure 112). You can select which management processors to configure (with respect to schema usage) and how to configure them. The **Select the Desired Configuration** window helps to prevent an accidental overwrite of iLOs already configured for HP schema, or iLOs that have directories turned off.

The selections you make in this window determine the windows that are displayed when you click **Next**.

Figure 112 Select the Desired Configuration window



To configure the management processor for directory services, see "Configuring directories when HP extended schema is selected" (page 202). To configure the management processor for Schema-free (default schema) directories support, see "Configuring directories when schema-free integration is selected" (page 206).

Naming management processors

The **Name the management processors** window (Figure 113) enables you to name iLO management device objects in the directory and create corresponding device objects for all management processors to be managed. You can create names by using one or more of the following:

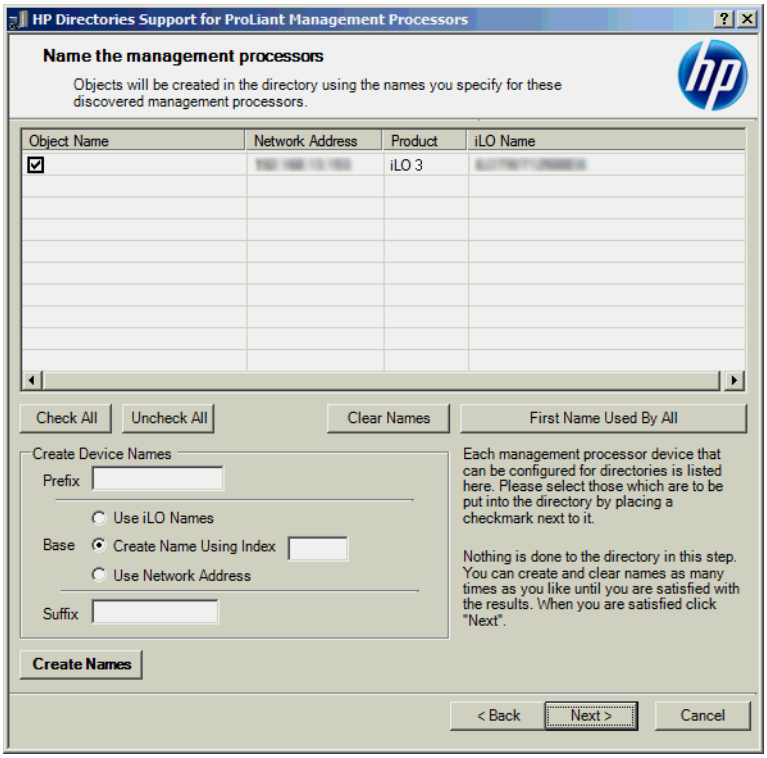
- The network address
- The DNS name
- An index
- Manual creation of the name
- The addition of a prefix to all
- The addition of a suffix to all

To name the management processors, click the **Object Name** column and enter the name, or do the following:

1. Select **Use iLO Names**, **Create Name Using Index**, or **Use Network Address**.
2. Optional: Enter the text to add (suffix or prefix) to all names.
3. Click **Create Names**.

   The names appear in the **Object Name** column as they are generated. At this point, names are not written to the directory or the management processors. The names are stored until the next HP Directories Support for ProLiant Management Processors window is displayed.
4. Optional: To change the names, click **Clear Names**, and rename the management processors.
5. When the names are correct, click **Next**.

Figure 113 Name the management processors window



Configuring directories when HP extended schema is selected

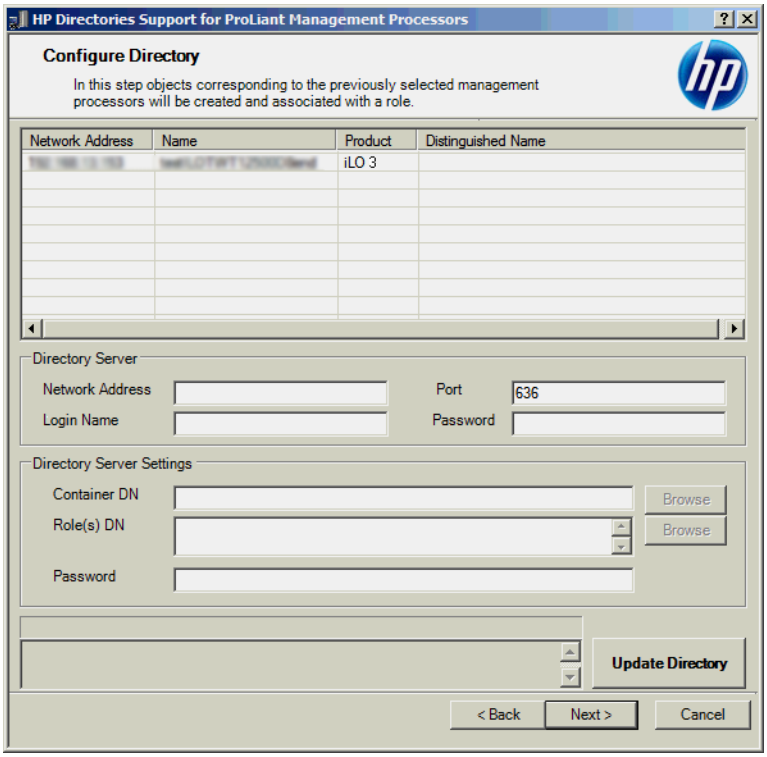
The **Configure Directory** window (Figure 114) enables you to create a device object for each discovered management processor and to associate the new device object with a previously defined

role. For example, the directory defines a user as a member of a role (such as administrator) who has a collection of privileges on a specific device object, as shown in Figure 114 (page 203).

The boxes on the **Configure Directory** window follow:

- **Network Address**—The network address of the directory server, which can be a valid DNS name or IP address.
- **Port**—The SSL port to the directory. The default port is 636. Management processors can communicate with the directory only by using SSL.
- **Login Name** and **Password**—Enter the login name and password for an account that has domain administrator access to the directory.
- **Container DN**—After you have the network address, port, and login information, you can click **Browse** to search for the container DN. The container is where the migration utility will create the management processor objects in the directory.
- **Role DN**—After you have the network address, port, and login information, you can click **Browse** to search for the role DN. The role is where the role to be associated with the device objects resides. The role must be created before you run this utility.

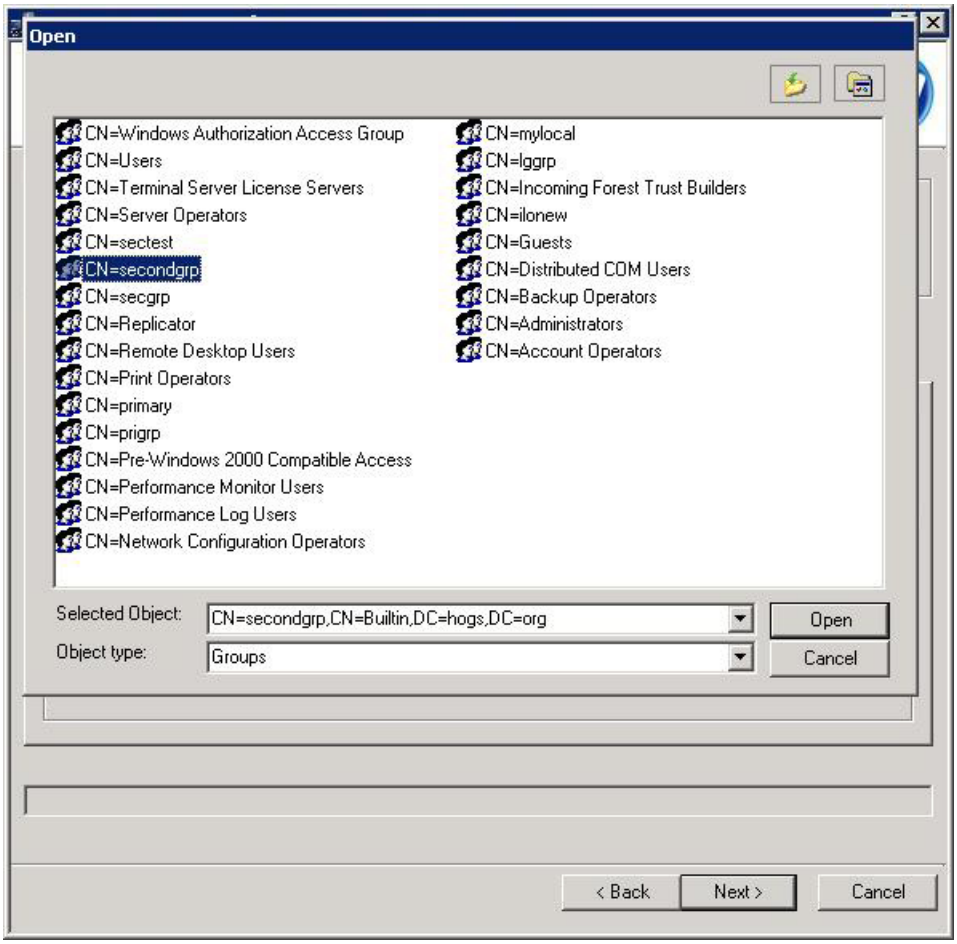
Figure 114 Configure Directory window



To configure the device objects to be associated with a role:

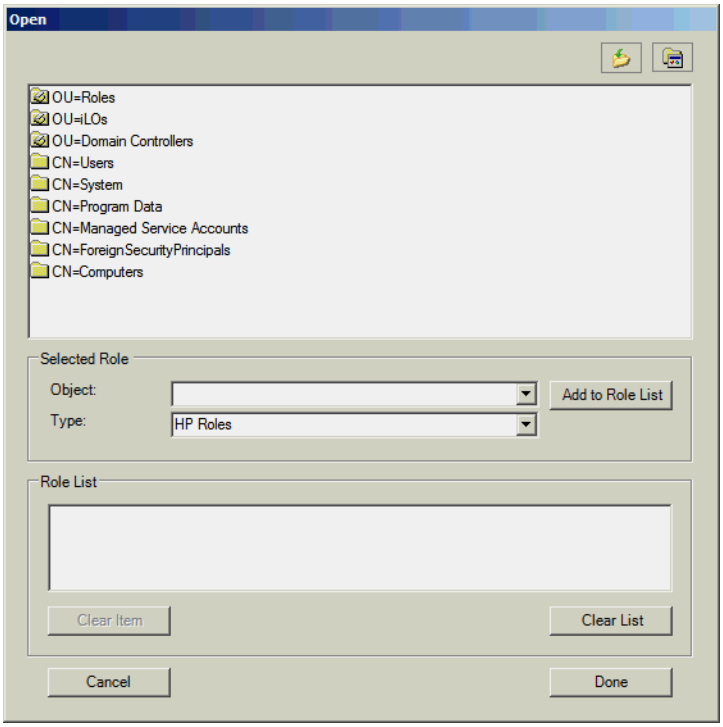
1. Enter the network address, login name, and password for the designated directory server.
2. Enter the container DN in the **Container DN** box, or click **Browse**, as shown in Figure 115 (page 204).

Figure 115 Entering the container distinguished name



3. Associate device objects with a member of a role by entering the role DN in the **Role(s) DN** box, or click **Browse**, as shown in Figure 116 (page 204).

Figure 116 Entering the role distinguished name



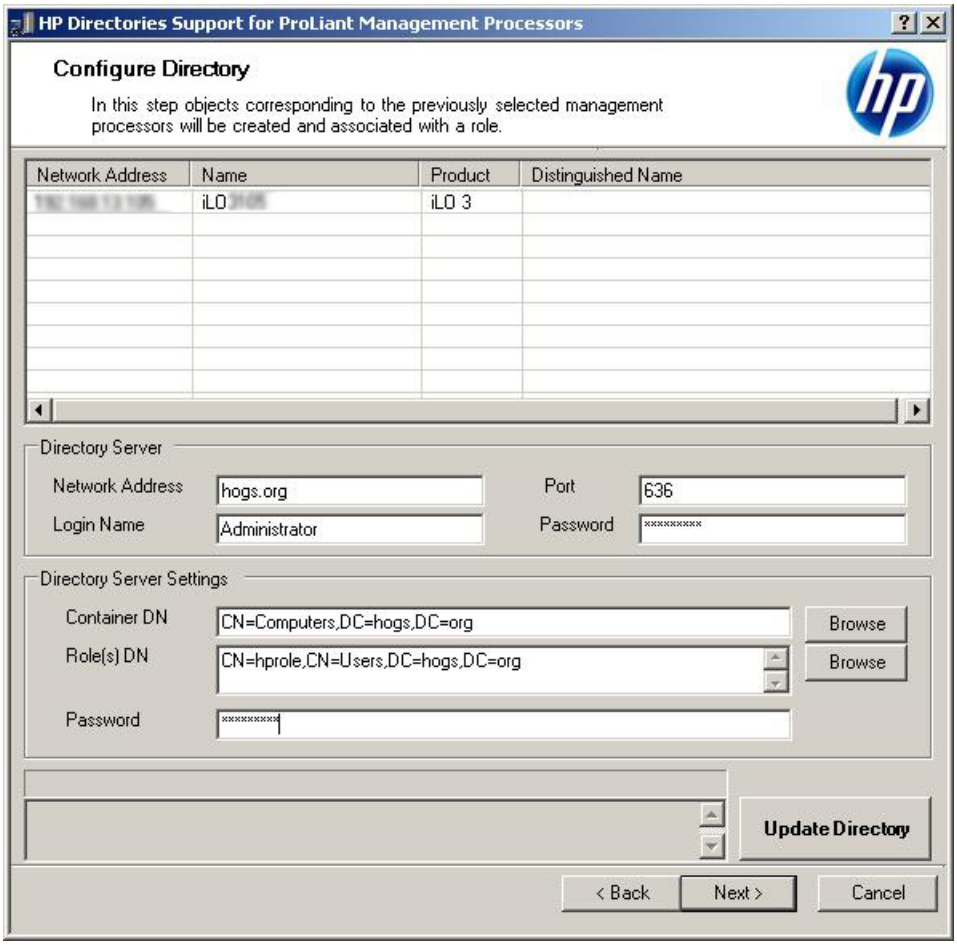
4. Click **Update Directory**.

   The utility connects to the directory, creates the management processor objects, and adds them to the selected roles.

5. After the device objects have been associated with a role, click **Next**.

   The values you entered are displayed in the **Configure Directory** window (Figure 117).

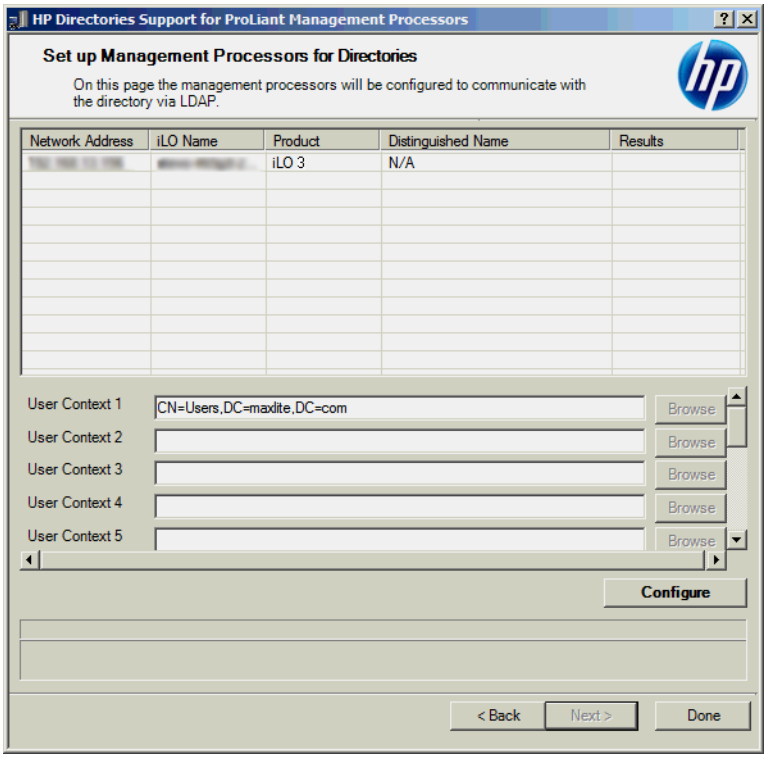
Figure 117 Configure Directory window



6. Define the user contexts.

   The user contexts define where the users who will log in to iLO are located in the LDAP structure. You can enter the organizational unit DN or click **Browse**.

Figure 118 Defining the user contexts



7. Click **Configure**, and then click **Done** when button is available.

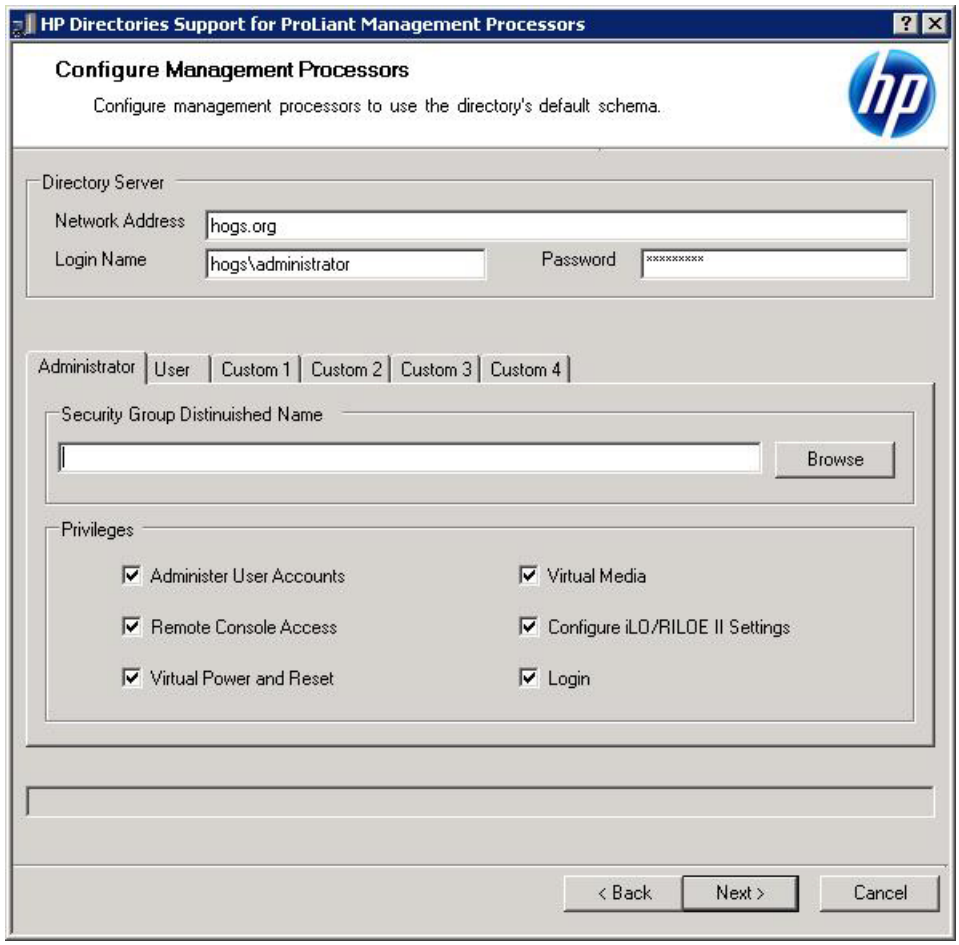
Configuring directories when schema-free integration is selected

The boxes on the **Configure Management Processors** window (Figure 119) follow:

- **Network Address**—The network address of the directory server, which can be a valid DNS name or IP address.
- **Login Name** and **Password**—Enter the login name and password for an account that has domain administrator access to the directory.
- **Security Group Distinguished Name**—The DN of the group in the directory that contains a set of iLO users with a common set of privileges. If the directory name, login name, and password are correct, you can click **Browse** to navigate to and select the group.
- **Privileges**—The iLO privileges associated with the selected group. The login privilege is implied if the user is a member of the group.

Configure Management Processors settings are stored until the next window in the wizard is displayed.

Figure 119 Configure Management Processors window



Setting up management processors for directories

The last step in the migration process is to configure the management processors to communicate with the directory. The **Set up Management Processors for Directories** window (Figure 120) enables you to create user contexts.

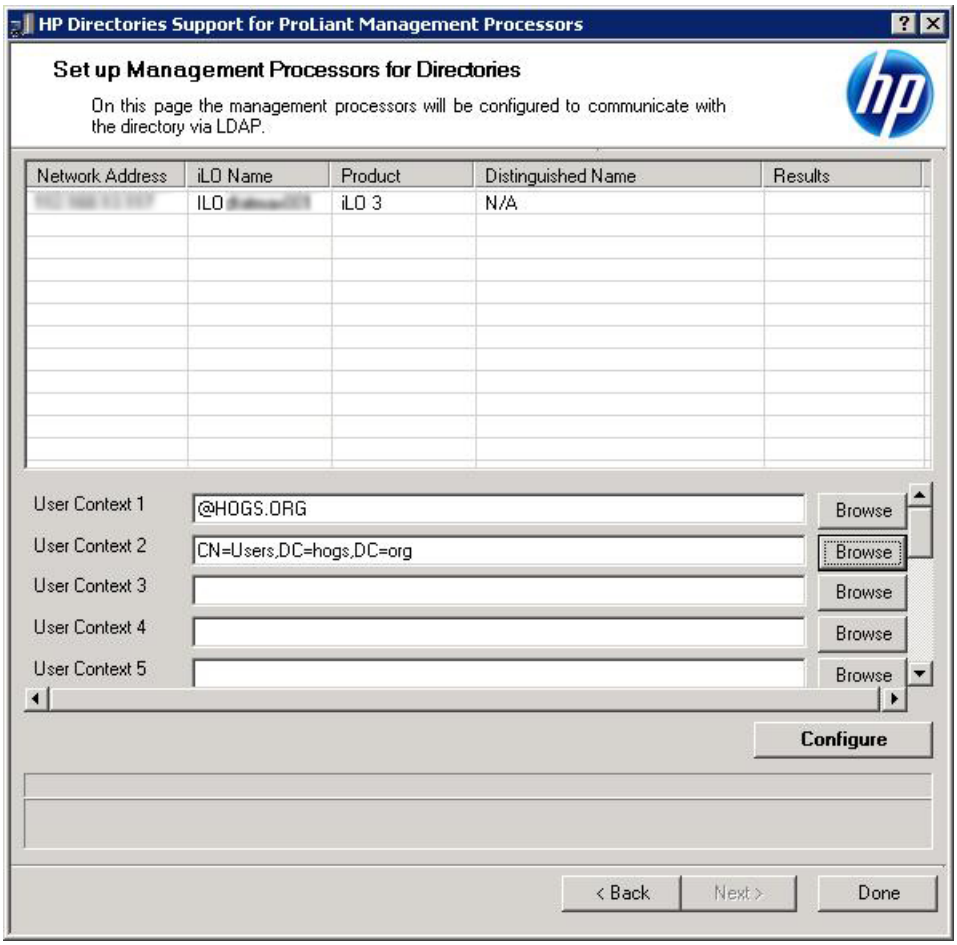
User contexts enable the user to use short names or user object names to log in, rather than the full DN. For example, having a user context such as `CN=Users,DC=iLOTEST2,DC=HP` enables user Elizabeth Bennett to log in using `Elizabeth Bennett` rather than `CN=Elizabeth Bennett,CN=Users, DC=iLOTEST2,DC=HP`. The `@` format is also supported. For example, `@iLOTEST2.HP` in a context box enables the user to log in using `ebennett` (assuming that `ebennett` is the user short name).

To configure the management processors to communicate with the directory:

1. Enter the user contexts, or click **Browse**.
2. Click **Configure**.

   The migration utility connects to all selected management processors and updates their configurations as specified. The utility supports configuring 15 user contexts. To access the user context boxes, use the scroll bar.

Figure 120 Set up Management Processors for Directories window



When you click **Configure**, the utility might display a message similar to the following:

3. Click **OK** to continue.
4. When the process is complete, click **Done**.

7 Troubleshooting

iLO 3 POST LED indicators

During the initial boot of iLO, the POST LED indicators flash to display the progress through the iLO boot process. After the boot process is complete, the HB LED flashes in one second intervals. LED indicators (1 through 6) light up after the system has booted to indicate a hardware failure. If a hardware failure is detected, reset iLO. For the location of the LED indicators, refer to the server documentation.

A runtime failure of iLO is indicated by HB remaining in either the On or Off state constantly. A runtime failure of iLO can also be indicated by a repeated flashing pattern on all eight LEDs. If a runtime error occurs, reset iLO.

The LED indicators have the following assignments:

HB	7	6	5	4	3	2	1

LED indicator	POST code (activity completed)	Description	Failure indicated
None	00	Set up chip selects	
2	02 – Normal operation	Scrub done	
HB and 2	82	Kernel launch	Subsystem startup failed if this status remains for extended period of time (~60 seconds)
5,4,3,2,1 blinking	0F	Main Error - Recovery	The main payload is corrupt, the kernel is running flash recovery.
HB, 7, and 6 steady 5,4,3,2,1 blinking	E0	Kernel Error	Failure to find and load a kernel
HB		Flashes as the iLO processor executes firmware code. It does not change the value of the lower seven LEDs.	

Kernel debugging

Use the Windows `Windbg` kernel debugger from a local test system (usually a laptop) for a host server that you want to debug. This method uses the iLO Virtual Serial Port feature.

NOTE: You must have PuTTY installed on your test system. You can download PuTTY from http://www.putty.org/.

1. Using the iLO web interface on the host server with kernel issues, navigate to the **Administration→Access Settings** page and configure the **Serial Command Line Interface Speed** setting.
2. Configure the debug options in Windows (the `boot.ini` parameters for the serial connection).

   Use `debugport=com2`, and set the baud rate to match the settings in the iLO web interface.
3. During POST, press **F9** to enter the system RBSU.
4. From the main menu, disable EMS and BIOS Serial Console.

   For detailed instructions, see the *HP ROM-Based Setup Utility User Guide*.

5. Set the Virtual Serial Port to `COM 2`.

   For detailed instructions, see the *HP ROM-Based Setup Utility User Guide*.
6. Reboot the host server to access the selection menu for the Windows debug boot option.
7. From the local test system, use PuTTY to connect to iLO and log in.

   This is a CLI connection to iLO.
8. Enter the IP address for the session host name. Use the default settings for an SSH session.

   When the PuTTY iLO CLI session opens, a user login window opens, unless the PuTTY session is configured to use private keys. For more information, see "Configuring iLO security" (page 43) and "Administering SSH keys" (page 46).

   It might take a minute for the prompt to appear.
9. At the `</>hpiLO->` prompt, enter the following command:

   ```
   windbg_enable
   ```

   This opens a socket to the Virtual Serial Port on port 3002.
10. Enter the following command to start the Windows debugger:

    ```
    windbg -k com:port=<IP-address>,ipport=3002
    ```

    `<IP-address>` is the iLO IP address, and `3002` is the socket to connect to (the raw serial data socket for iLO).

    NOTE: You can add other `windbg` command-line parameters if necessary. HP recommends using the `-b` parameter for the initial breakpoint.
11. Go to the server console (or access the iLO Remote Console), and press **Enter** to boot the debug selection on the OS load menu.

    This might take several minutes.
12. When you are finished debugging the host server, use PuTTY to connect to the CLI and turn off the debug socket to the Virtual Serial Port. Then, enter the following command:

    ```
    windbg_disable
    ```

    NOTE: You can disconnect and reconnect the Windows debugger as long as you keep the iLO debug socket enabled.

Event log entries

Table 11 (page 210) lists typical iLO event log entries.

Table 11 Event log entries

Event log entry	Description
`Server power removed`	The server power was removed.
`Browser login: <IP address>`	The IP address for the browser that logged in.
`Server power restored`	The server power was restored.
`Browser logout: <IP address>`	The IP address for the browser that logged out.
`Server reset`	The server was reset.
`Failed Browser login ? IP Address: <IP address>`	A browser login failed.
`iLO Self Test Error: #`	iLO failed an internal test. The probable cause is failure of a critical component. Further use of iLO on this server is not recommended.

Table 11 Event log entries *(continued)*

Event log entry	Description
`iLO reset`	iLO was reset.
`On-board clock set; was <#:#:#:#:#:#>`	The on-board clock was set.
`Server logged critical error(s)`	The server logged one or more critical errors.
`Event log cleared by: <User>`	A user cleared the event log.
`iLO reset to factory defaults`	LO was reset to the default settings.
`iLO ROM upgrade to <#>`	The iLO ROM was upgraded.
`iLO reset for ROM upgrade`	iLO was reset for a ROM upgrade.
`iLO reset by user diagnostics`	iLO was reset by user diagnostics.
`Power restored to iLO`	The power was restored to iLO.
`iLO reset by watchdog`	An error occurred in iLO, and iLO reset itself. If this issue persists, call customer support.
`iLO reset by host`	The server reset iLO.
`Recoverable iLO error, code <#>`	A noncritical error occurred in iLO, and iLO reset itself. If this issue persists, call customer support.
`SNMP trap delivery failure: <IP address>`	The SNMP trap did not connect to the specified IP address.
`Test SNMP trap alert failed for: <IP address>`	The SNMP trap did not connect to the specified IP address.
`Power outage SNMP trap alert failed for: <IP address>`	The SNMP trap did not connect to the specified IP address.
`Server reset SNMP trap alert failed for: <IP address>`	The SNMP trap did not connect to the specified IP address.
`Illegal login SNMP trap alert failed for: <IP address>`	The SNMP trap did not connect to the specified IP address.
`Diagnostic error SNMP trap alert failed for: <IP address>`	The SNMP trap did not connect to the specified IP address.
`Host generated SNMP trap alert failed for: <IP address>`	The SNMP trap did not connect to the specified IP address.
`Network resource shortage SNMP trap alert failed for: <IP address>`	The SNMP trap did not connect to the specified IP address.
`iLO network link up`	The network is connected to iLO.
`iLO network link down`	The network is not connected to iLO.
`iLO Firmware upgrade started by: <User>`	A user started a firmware upgrade.
`Host server reset by: <User>`	A user reset the host server.

Table 11 Event log entries *(continued)*

Event log entry	Description
`Host server powered OFF by: <User>`	A user powered off the host server.
`Host server powered ON by: <User>`	A user powered on a host server.
`Virtual Floppy in use by: <User>`	A user began using a virtual floppy.
`Remote Console login: <User>`	A user logged in to a Remote Console session.
`Remote Console Closed`	A Remote Console session was closed.
`Failed Console login - IP Address: <IP address>`	A console login failed with the specified login and IP address.
`Added User: <User>`	A local user was added.
`User Deleted by: <User>`	A local user was deleted.
`Modified User: <User>`	A local user was modified.
`Browser login: <User>`	A valid user logged in to iLO by using an Internet browser.
`Browser logout: <User>`	A valid user logged out of iLO by using an Internet browser.
`Remote Console login: <User>`	An authorized user logged in by using the Remote Console port.
`Remote Console Closed`	An authorized Remote Console user was logged out or the Remote Console port was closed after a failed login attempt.
`Failed Console login ? IP Address: <IP address>`	An unauthorized user failed three login attempts when using the Remote Console port.
`Added User: <User>`	A new entry was made to the authorized user list.
`User Deleted by: <User>`	An entry was removed from the authorized user list. The **User** section displays the user who requested the removal.
`Power Cycle (Reset): <User>`	The power was reset.
`Security Override Switch Setting is On`	The system was booted with the Security Override Switch set to On.
`Security Override Switch Setting Changed to Off`	The system was booted with the Security Override Switch changed from On to Off.
`On-board clock set; was previously [NOT SET]`	The on-board clock was set. Displays the previous time or **NOT SET** if no time was set.
`Logs full SNMP trap alert failed for: <IP address>`	The logs are full and the SNMP trap alert failed for a specified IP address.
`Security disabled SNMP trap alert failed for: <IP address>`	Security was disabled and the SNMP trap alert failed for a specified IP address.
`Security enabled SNMP trap alert failed for: <IP address>`	Security was enabled and the SNMP trap alert failed for a specified IP address.
`Virtual Floppy connected by <User>`	An authorized user connected the virtual floppy.
`Virtual Floppy disconnected by <User>`	An authorized user disconnected the virtual floppy.
`License added by: <User>`	An authorized user added a license.

Table 11 Event log entries *(continued)*

Event log entry	Description
`License removed by: <User>`	An authorized user removed a license.
`License activation error by: <User>`	A license activation error occurred.
`iLO RBSU user login: <User>`	An authorized user logged in to iLO RBSU.
`Power on request received by: <Type>`	A power request was received from one of the following: • Power Button • Wake On LAN • Automatic Power On
`Virtual NMI selected by: <User>`	An authorized user clicked the **Virtual NMI** button.
`Virtual Serial Port session started by: <User>`	An authorized user started a Virtual Serial Port session.
`Virtual Serial Port session stopped by: <User>`	An authorized user stopped a Virtual Serial Port session.
`Virtual Serial Port session login failure from: <User>`	A login failure occurred.

Hardware and software link-related issues

iLO uses standard Ethernet cabling, which includes CAT 5 UTP with RJ-45 connectors. Straight-through cabling is necessary for a hardware link to a standard Ethernet hub. Use a crossover cable for a direct PC connection.

The default DNS name is displayed on the serial number/iLO information pull tab, and can be used to locate iLO if you do not know the assigned IP address.

If you are using DHCP, the following information applies:

- The iLO management port must be connected to a network that is connected to a DHCP server, and iLO must be on the network before power is applied. DHCP sends a request soon after power is applied. If the DHCP request is not answered when iLO first boots, it will reissue the request at 90-second intervals.
- The DHCP server must be configured to provide DNS and WINS name resolution.
- In the iLO RBSU, you can press **F1** on the **Network Autoconfiguration** page for advanced options for viewing the status of iLO DHCP requests.

If you are using a static IP address, the following information applies:

- If you have a direct PC connection then you must use a static IP address because no DHCP server is present on the link.
- You can configure iLO to work with a static IP address by using iLO RBSU or the iLO web interface. For more information, see "Setting up iLO by using iLO RBSU" (page 16) or "Setting up iLO by using the iLO web interface" (page 21).

Login issues

Use the following information when attempting to resolve login issues:

- Try using the default account information, which is located on the serial number/iLO information pull tab.
- If you forget your password, it can be reset by an administrator who has the Administer User Accounts privilege.

- If an administrator forgets the administrator account password, the administrator must use the Security Override Switch or use HPONCFG to establish an administrator account and password. For instructions, see the *HP iLO 3 Scripting and Command Line Guide*.
- Check for standard issues, such as the following:
  - Does the password comply with password restrictions? For example, does the password contain case-sensitive characters?
  - Is an unsupported browser being used?

Login name and password not accepted

Solution: Verify that your login information is configured correctly. Have a user with the Administer User Accounts privilege log in and change your password. If you still cannot connect, have the user log in again and delete and re-add your user account. For instructions, see "Managing iLO users by using the iLO web interface" (page 32).

NOTE: The iLO RBSU can also be used to configure user accounts. For instructions, see "Adding user accounts" (page 18).

Directory user premature logout

Solution: To recover from a premature session timeout, log back in and continue using iLO. If the directory server is unavailable, you must use a local account.

Network errors can cause iLO to conclude that a directory connection is no longer valid. If iLO cannot detect the directory, it ends the directory connection. Any attempt to continue using the terminated connection redirects the browser to the login page.

A premature session timeout can occur during an active session if:

- The network connection is terminated.
- The directory server is shut down.

iLO management port not accessible by name

Solution: The iLO management port can register with a WINS server or DDNS server to provide the name-to-IP-address resolution required to access the iLO management port by name. The WINS or DDNS server must be up and running before the iLO management port is powered on, and the iLO management port must have a valid route to the WINS or DDNS server.

In addition, the iLO management port must be configured with the IP address of the WINS or DDNS server. You can use DHCP to configure the DHCP server with the required IP addresses. These options are enabled as factory defaults and can be changed by using the iLO RBSU or iLO web interface. For more information, see "Setting up iLO by using iLO RBSU" (page 16) or "Configuring iLO network settings" (page 69).

The clients that are used to access the iLO management port must be configured to use the same DDNS server where the IP address of the iLO management port is registered.

If you are using a WINS server and a nondynamic DNS server, access to the iLO management port might be significantly faster if you configure the DNS server to use the WINS server for name resolution. For more information, see the appropriate Microsoft documentation.

iLO RBSU unavailable after iLO and server reset

Solution: Reset the server a second time. To avoid this issue, after resetting the processor, wait a few seconds before resetting the server.

If the iLO processor is reset and the server is immediately reset, iLO firmware might not be fully initialized when the server performs its initialization and attempts to start the iLO RBSU. In this case, the iLO RBSU is unavailable, or the iLO option ROM code is skipped altogether.

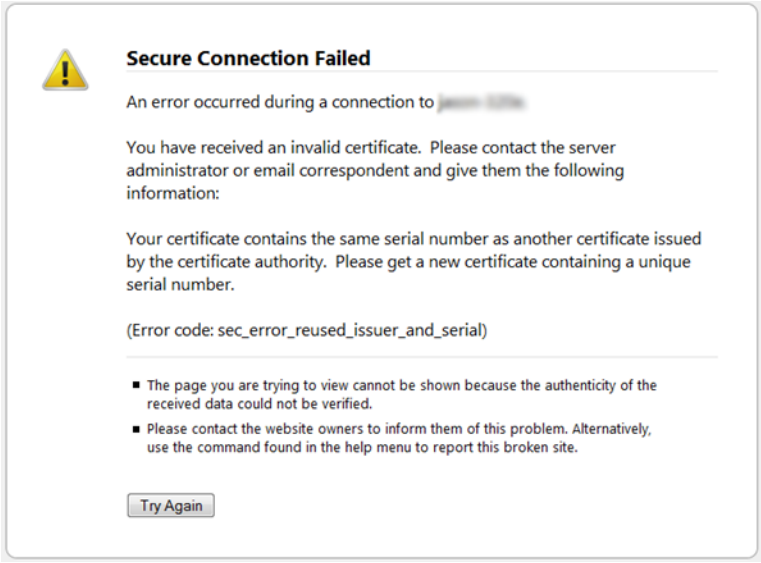
Unable to access the login page

Solution: Verify that the SSL encryption level of your browser is set to 128 bits. The SSL encryption level in iLO is set to 128 bits and cannot be changed. The browser and iLO encryption levels must be the same.

Secure Connection Failed error when using Firefox browser

When you try to connect to iLO using Firefox ESR, the following message appears (Figure 121).

Figure 121 Secure Connection Failed dialog box



Solution 1:

1. Navigate to **Tools→Options** in Firefox.
2. Click **Advanced**.
3. Click the **Encryption** tab.
4. Click **View Certificates**.

   Click the **Servers** tab, and then delete any certificates related to iLO.
5. Click the **Others** tab, and then delete any certificates related to iLO.
6. Click **OK**.
7. Start Firefox and connect to iLO.

NOTE: The steps in Solution 1 are based on Firefox ESR 17. The procedure to use might vary depending on the installed version of Firefox.

Solution 2:

1. Close the Firefox application.
2. Navigate to the Firefox `AppData` folder, and then delete all of the *.db files in all of the Firefox directories.

   The `AppData` folder is typically in the following location: `C:\\Users\<user name>\AppData\Local\Mozilla\Firefox\`

Unable to return to login page after an iLO flash or reset

Solution: Clear the browser cache and restart the browser.

Unable to access Virtual Media or graphical Remote Console

Solution: You enable the iLO Virtual Media and graphical Remote Console features by installing an optional iLO license. If a license is not installed, a message informs you that these features are not available without a license.

For details on purchasing licenses, and for a list of licensed features, see the following website: http://www.hp.com/go/ilo/licensing.

Unable to connect to iLO after changing network settings

Solution: Verify that both sides of the connection (the NIC and the switch) have the same settings for transceiver speed autoselect, speed, and duplex. For example, if one side is autoselecting the connection, the other side must use the same setting. For information about configuring the iLO network settings, see "Configuring iLO network settings" (page 69).

Unable to connect to iLO processor through NIC

Solution: If you cannot connect to the iLO processor through the NIC, try the following solutions:

- Confirm that the green LED indicator (link status) on the iLO RJ-45 connector is on. This condition indicates a good connection between the PCI NIC and the network hub.
- Look for intermittent flashes of the green LED indicator, which indicates normal network traffic.
- Run the iLO RBSU to confirm that the NIC is enabled, and verify the assigned IP address and subnet mask.
- Run the iLO RBSU, and use the **Advanced** option on the **Network Autoconfiguration** page to view the status of DHCP requests.
- Ping the IP address of the NIC from a separate network workstation.
- Attempt to connect with a browser by entering the IP address of the NIC as the URL. You can see the iLO home page from this address.
- Reset iLO.

NOTE: If a network connection is established, you might have to wait up to 90 seconds for the DHCP server request.

Unable to log in to iLO after installing iLO certificate

Solution: Do not install the iLO self-signed certificate in the browser certificate store. If you want to install the iLO certificate, request a permanent certificate from a CA and import it to iLO. For instructions, see "Administering SSL certificates" (page 48).

When you reset iLO to the factory defaults or change the iLO host name, a new self-signed certificate is generated. If the iLO self-signed certificate is installed permanently in some browsers, you might not be able to log back in to iLO after the new self-signed certificate is generated.

Unable to connect to iLO IP address

Solution: If the web browser software is configured to use a proxy server, it will not connect to the iLO IP address. To resolve this issue, configure the browser not to use the proxy server for the IP address of iLO. For example, in Internet Explorer:

1. Select **Tools→Internet Options**.
2. Click **Connections**.
3. Click **LAN settings**.

4. Click **Advanced** in the **Proxy server** section.
5. Enter the iLO IP address or DNS name in the **Exceptions** box.
6. Click **OK** to save the changes.

Blocked iLO ports

Solution: iLO communicates through several configurable TCP/IP ports. If these ports are blocked, the administrator must configure the firewall to allow for communications on these ports. For information about viewing and changing the iLO port configuration, see "Configuring iLO access settings" (page 39).

Troubleshooting alert and trap issues

Table 12 (page 217) lists the alerts and traps that might occur.

Table 12 Alerts

Alert	Description
`Test Trap`	This trap is generated when you click the **Send Test Alert** button on the **Administration→Management** page in the iLO web interface.
`Server Power Outage`	The server lost power.
`Server Reset`	The server was reset.
`Failed Login Attempt`	A remote user login attempt failed.
`General Error`	This is an error condition that is not predefined by the hard-coded MIB.
`Logs`	The circular log has been overrun.
`Security Override Switch Changed: On/Off`	The state of the Security Override Switch changed (On/Off).
`Rack Server Power On Failed`	The server could not power on because of insufficient power.
`Rack Server Power On Manual Override`	The server was forced to power on manually despite reporting insufficient power.
`Rack Name Changed`	The name of the rack was changed.
`Browser login: <user>`	The listed user logged in through a browser.
`Browser logout: <user>`	The listed user logged out through a browser.
`Remote Console login: <user>`	The listed user logged in to the Remote Console.
`Remote Console Closed`	A user closed the Remote Console.
`iLO Firmware upgrade started by <user>`	The listed user started a firmware upgrade.

Unable to receive HP SIM alarms (SNMP traps) from iLO

Solution: A user who has the Configure iLO Settings privilege must connect to iLO to configure SNMP trap parameters. When you are connected to iLO, make sure that the correct alert types and trap destinations are enabled on the **Administration→Management** page in the iLO web interface.

Incorrect authentication code

When you use a Mozilla browser, you might receive an incorrect authentication code error message, which indicates that the public or private key pair and certificate used to initiate the browser SSL session has changed. This error message might occur when you do not use a customer provided certificate because iLO generates its own self-signed certificate each time it is rebooted.

Solution: Close and restart the web browser, or install your own certificates into iLO.

Using the iLO Security Override Switch for emergency access

Solution: The iLO Security Override Switch gives emergency access to the administrator who has physical control over the server system board. Setting the iLO Security Override Switch allows login access, with all privileges, without a user ID and password.

The iLO Security Override Switch is located inside the server and cannot be accessed without opening the server enclosure. To set the iLO Security Override Switch, make sure that the server is powered off and disconnected from the power source. Set the switch, and then power on the server. To clear the iLO Security Override Switch, reverse this procedure.

When you use the iLO Security Override Switch:

- A warning message indicating that the iLO Security Override Switch is currently in use is displayed on the iLO web interface pages.
- An iLO log entry is added to record the use of the iLO Security Override Switch.
- An SNMP alert might be sent when you set or clear the iLO Security Override Switch.

Setting the iLO Security Override Switch also enables you to flash the iLO boot block if necessary. The boot block is exposed until iLO is reset. HP recommends that you disconnect iLO from the network until the reset is complete.

Depending on the server, the iLO Security Override Switch might be a single jumper or it might be a specific switch position on a DIP switch panel. For information about how to access the iLO Security Override Switch, see the server documentation.

Troubleshooting license installation

License-key installation issues might occur because of the following:

- The license key is not for iLO.
- If a license key was previously installed, an evaluation license key cannot be installed.
- The iLO firmware was not updated before the license was be installed.
- The iLO date and time are incorrect.

Troubleshooting directory issues

The following sections provide instructions for troubleshooting directory issues.

User contexts do not appear to work

Solution: Check with your network administrator. The full DN of your user object must be in the directory. Your login name appears after the first `CN=`. The remainder of the DN must appear in one of the user context boxes. User contexts are not case sensitive, and any other characters, including spaces, are part of the user context. For information about entering directory user contexts, see "Configuring directory settings" (page 51).

Directory user does not log out after directory timeout has expired

Solution: If you set the iLO **Idle Connection Timeout** to **Infinite**, the Remote Console periodically pings the firmware to verify that the connection exists. When the ping occurs, the iLO firmware queries the directory for user permissions. This periodic query keeps the directory connection active, preventing a timeout and logging the user.

Problems generating keytab by using `ktpass.exe`

Solution: If you use `ktpass.exe` to generate a keytab, you must specify a principal name by using the `-princ` argument.

Principal names are case sensitive and must be entered as follows:

`HTTP/myilo.somedomain.net@SOMEDOMAIN.NET`

- The first part is uppercase (`HTTP`).
- The middle part is lowercase (`myilo.somedomain.net`).
- The last part is uppercase (`@SOMEDOMAIN.NET`).

If you do not format the command exactly as shown, it will not work.

Here is an example of the full `ktpass.exe` command:

```
ktpass +rndPass -ptype KRB5_NT_SRV_HST -mapuser myilo$@somedomain.net
-princ HTTP/myilo.somedomain.net@SOMEDOMAIN.NET -out myilo.keytab
```

Directory login fails

Solution:

1. Log in with a local account and determine the directory server name.
2. Verify that the directory server name is a name and not an IP address.
3. Verify that you can ping the directory server name from your client.
4. Run the directory setup tests.
5. Verify that the ping was received successfully. For more information on testing directory settings, see "Running directory tests" (page 54).

Troubleshooting Remote Console issues

The following sections discuss troubleshooting Remote Console issues.

IMPORTANT: Pop-up blocking applications, which prevent the automatic opening of new windows, prevent the Remote Console from running. Disable any pop-up blocking programs before you start the Remote Console.

Java IRC applet displays red X when Firefox is used to run Java IRC on Linux client

Solution: Firefox browsers must be configured to accept cookies. For instructions on configuring Firefox, see the Firefox documentation.

Unable to navigate single cursor of Remote Console to corners of Remote Console window

In some cases, you might not be able to navigate the mouse cursor to the corners of the Remote Console window.

Solution: Right-click and drag the mouse cursor outside the Remote Console window, and then drag it back inside.

Remote Console text window not updated correctly

When you are using the Remote Console to display text windows that scroll at a high rate of speed, the text window might not be updated correctly. This error is caused by video updates occurring faster than the iLO firmware can detect and display them. Typically, only the upper left corner of the text window is updated while the rest of the text window remains static.

Solution: After the scrolling is complete, click **Refresh** to update the text window.

Mouse or keyboard not working in .NET IRC or Java IRC

Solution 1: When you open the .NET IRC or Java IRC and notice that the mouse or keyboard is not working, perform the following steps:

1. Close the .NET IRC or Java IRC.

2. Navigate to the **Power Management→Power Settings** page.
3. Clear the **Enable persistent mouse and keyboard** check box, and then click **Apply**.
4. Start the .NET IRC or Java IRC again.

Solution 2 (.NET IRC only): Some monitors do not support DirectDraw. For example, some USB VGA device drivers might disable DirectDraw on all monitors for Windows Vista and Windows 7 clients.

The .NET IRC requires DirectDraw support.

Solution 2 (Java IRC only):

1. Shut down and exit your browser.
2. Open the Java Control Panel.
3. Navigate to the **Java Runtime Environment Settings** dialog box.
4. Add the following runtime parameter:

   ```
   -Dsun.java2d.noddraw=true
   ```
5. Click **OK** and close the **Java Runtime Environment Settings** window.
6. Click **Apply**, and then click **OK** to close the Java Control Panel.

NOTE: Viewing your changes before you click **Apply** might reset the **Runtime Parameters** dialog box, causing your edits to be lost.

.NET IRC sends characters continuously after switching windows

Solution: If you have a key pressed during a .NET IRC session, and you inadvertently switch windows, the key can remain pressed in the .NET IRC session, causing the character to repeat continuously. To stop the character from repeating, click the .NET IRC session screen to bring it to the front of your desktop.

Java IRC does not display correct floppy and USB-key device

This issue occurs only with the Firefox browser.

Solution:

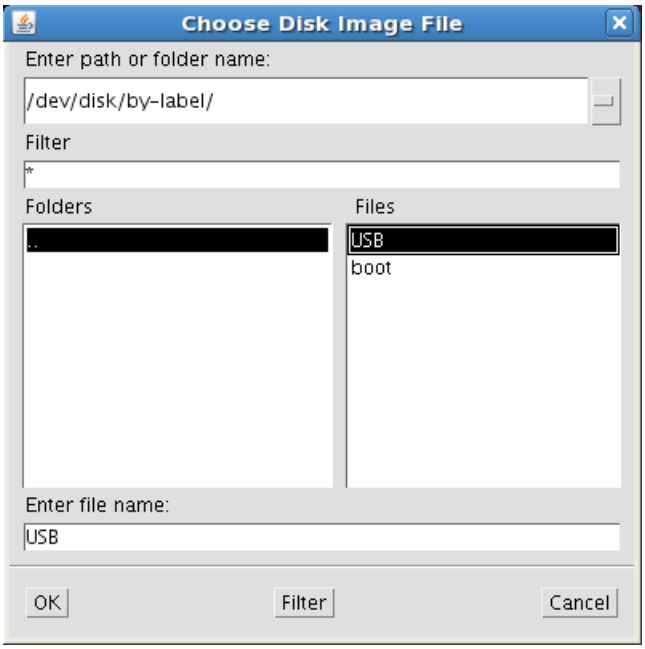
1. Make sure that Red Hat Enterprise Linux 5 or later is installed on the local client system.
2. Install the latest version of Java and configure it to connect through the Firefox browser.
3. Log in to the iLO web interface by using Firefox.
4. Insert a USB key or floppy disk on the local client system.
5. Verify that you can access the USB key or floppy disk.
6. Open a Java IRC session.
7. Select **Virtual Drives→Floppy/USB-Key**, and then select **Virtual Image**.

   The **Choose Disk Image File** dialog box opens (Figure 122).

Figure 122 Choose Disk Image File dialog box

8. Type or select the path of the USB key/floppy (`/dev/disk`) inserted in the client.
   You can also mount the USB key/floppy by label, as shown in Figure 123 (page 221).

Figure 123 Mounting the USB key by label



9. Click **OK**.

Caps Lock out of sync between iLO and Java IRC

When you log in to the Java IRC, the **Caps Lock** setting might be out of sync between iLO and the Java IRC.

Solution: Select **Keyboard**→**Caps Lock** in the Java IRC to synchronize the **Caps Lock** settings.

Num Lock out of sync between iLO and Shared Remote Console

When you log in to a Shared Remote Console session, the **Num Lock** setting might be out of sync between iLO and some of the Remote Console sessions.

Solution: Select **Keyboard→Num Lock** in the Remote Console to synchronize the **Num Lock** settings.

Keystrokes repeat unintentionally during Remote Console session

When you are using the .NET IRC or Java IRC, a keystroke might repeat unintentionally during a Remote Console session.

Solution 1: Identify and fix problems that might cause network latency.

Solution 2: Adjust the following settings on the remote machine:

- **Increase the typematic delay**—This setting controls the delay before a character repeats when you press and hold a key on the keyboard.
- **Decrease the typematic rate**—This setting controls the rate at which a character repeats when you press and hold a key on the keyboard.

NOTE: The exact name of the setting varies depending on the OS you are using. For more information about changing the typematic delay and rate, see your OS documentation.

Session leader does not receive connection request when .NET IRC is in replay mode

Solution: When a Remote Console session leader plays captured video data, the .NET IRC does not display the **Deny or Accept** message when another user attempts to access or share the .NET IRC. Instead, the new .NET IRC session waits and eventually times out. If you require access to the .NET IRC, and your request times out, contact the other user or use the Remote Console Acquire feature to take control of the IRC. For instructions, see "Acquiring the Remote Console" (page 118).

Keyboard LED does not work correctly

The client keyboard LED does not reflect the true state of the keyboard lock keys. The **Caps Lock**, **Num Lock**, and **Scroll Lock** keys are fully functional when you are using the keyboard options in the Remote Console.

Inactive .NET IRC

The iLO .NET IRC might become inactive or disconnect during periods of high activity. .NET IRC activity slows before becoming inactive. Symptoms of an affected .NET IRC include the following:

- The .NET IRC display is not updated.
- Keyboard and mouse activity is not recorded.
- Shared Remote Console requests do not register.

Although you can replay a captured file on an inactive .NET IRC, the active state of the .NET IRC is not restored.

This issue might occur when multiple users are logged in to iLO, a Virtual Media session is connected and is performing a continuous copy operation, or a .NET IRC session is open. The Virtual Media continuous copy operation takes priority and, consequently, the .NET IRC loses synchronization. Eventually, the Virtual Media connection resets multiple times and causes the USB media drive for the OS to lose synchronization with the Virtual Media client.

Solution: Reconnect to the .NET IRC and the Virtual Media. If possible, reduce the number of simultaneous iLO user sessions. If necessary, reset iLO. (The server does not need to be reset.)

.NET IRC failed to connect to server

iLO might display the message `Failed to connect to server` when it attempts to establish a .NET IRC session.

The iLO .NET IRC client waits a specified amount of time for a connection to be established with iLO. If the client server does not receive a response in this amount of time, it displays an error message.

Possible causes for this message include the following:

- The network response is delayed.
- A Shared Remote Console session is requested, but the session leader delays sending an acceptance or denial message.

Solution 1: Retry the .NET IRC connection.

Solution 2: If possible, correct the network delay and retry the .NET IRC connection.

Solution 3: If the request was for a Shared Remote Console session, attempt to contact the session leader and retry the request. If the Remote Console Acquire feature is enabled, use the Acquire feature rather than requesting a Shared Remote Console session. For more information, see "Acquiring the Remote Console" (page 118).

File not present after copy from .NET IRC virtual drives to USB key

If a user copies files from the target server to a mounted iLO virtual drive (USB key connected to a client computer running any Windows OS), the files are not visible in Windows Explorer on the client computer.

File changes on the iLO Virtual Media USB key are never seen in Windows Explorer by the user on the client computer.

Windows Explorer keeps a cached copy of the files on the USB key, and the iLO Remote Console does not notify the Windows Shell when the USB key is updated with file changes. The file changes exist on the USB drive, but if the user refreshes the Explorer window, the cached copy of the files is flushed back to the USB key, and the user will never see the file changes in Windows Explorer.

Any kind of file change made on a mounted iLO Virtual Media USB key drive from a Windows client via the Remote Console can trigger this issue.

Solution:

1. Install a USB key drive on a Windows client computer.
2. Using .NET IRC, connect the client USB key to the iLO Virtual Media drive on the target server.
3. Make file changes to the connected iLO Virtual Media drive (copy, delete, and so on).
4. Safely unmount the iLO USB Virtual Media drive on the target server so that all data is updated to the Virtual Media drive.
5. Disconnect the client USB key by using the .NET IRC.

△ **CAUTION:** Do not use Windows Explorer to refresh the contents of the USB key.

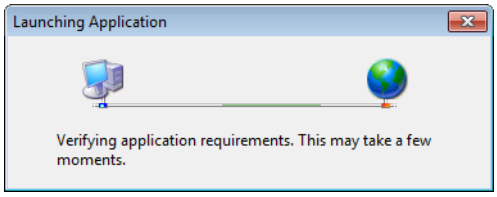
6. Safely remove the USB key from the client computer by clicking the **Safely Remove Hardware** icon in the Windows notification area. Follow the onscreen instructions.
7. Remove the USB key from the client computer.

When you connect the USB key to any computer, the file changes will be visible in Windows Explorer.

.NET IRC takes a long time to verify application requirements

When you start the .NET IRC from the iLO web interface, the following dialog box (Figure 124) appears and remains on the screen for a long time.

Figure 124 .NET IRC launch dialog box



Solution:

1. Open Internet Explorer.
2. Select **Tools→Internet Options**.

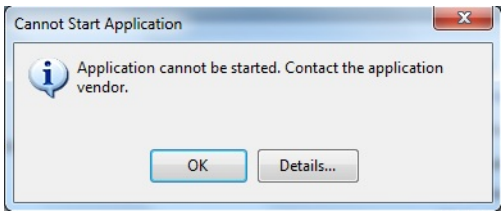
   The **Internet Options** window opens.
3. Click the **Connections** tab, and then click the **LAN settings** button.

   The **Local Area Network (LAN) Settings** window opens.
4. Clear the **Automatically detect settings** check box.
5. Optional: If needed, configure the proxy server settings.
6. Close all of the browser windows.
7. Restart the browser and start the .NET IRC.

.NET IRC fails to start

When you start the .NET IRC, the following error message appears (Figure 125).

Figure 125 .NET IRC cannot be started

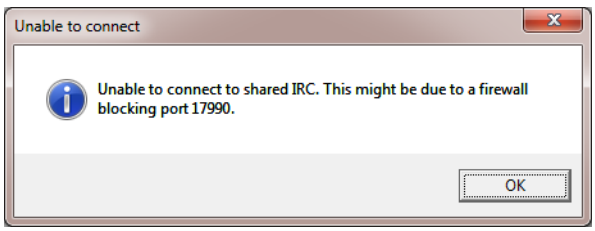


Solution: Clear the ClickOnce application cache by entering the following command from the Windows Command Prompt: **`rundll32 %windir%\system32\dfshim.dll CleanOnlineAppCache`**.

.NET IRC cannot be shared

When you try to join a shared .NET IRC session, the following error message appears (Figure 126.

Figure 126 .NET IRC firewall error



Solution 1: Make sure there is a communication route between the session leader .NET IRC client and each shared .NET IRC client.

Solution 2: Make sure the firewall settings on all clients allow an inbound connection to the Remote Console port (the default port is 17990).

Troubleshooting SSH issues

The following sections discuss troubleshooting SSH issues.

Initial PuTTY input slow

During the initial connection to iLO through a PuTTY client, input is accepted slowly for approximately 5 seconds.

Solution: Change the configuration options in the client. Clear the **Disable Nagle's algorithm** check box in the low-level TCP connection options.

PuTTY client unresponsive

When you are using a PuTTY client with the Shared Network Port, the PuTTY session might become unresponsive when a large amount of data is transferred or when you are using a Virtual Serial Port and Remote Console.

Solution: Close the PuTTY client and restart the session.

SSH text support from text-based Remote Console session

SSH access from the text-based Remote Console supports the standard 80 x 25 configuration of the text screen. This mode is compatible for the text-based Remote Console for most text-mode interfaces. Extended text configuration beyond the 80 x 25 configuration is not displayed correctly when using SSH. HP recommends configuring the text application in 80 x 25 mode or using the graphical Remote Console.

Troubleshooting video and monitor issues

The client screen resolution must be greater than the screen resolution of the remote server.

User interface does not display correctly

On ProLiant servers using Red Hat EL 4.0 and some other Linux systems and iLO 3, the text on the buttons of the user interface might be cut off along the bottom of the button. This error occurs because Mozilla Firefox does not display the text size that iLO 3 specifies for the buttons.

Solution: To display the text correctly, select **View>Text Size>Decrease** until the text appears correctly.

iLO Virtual Floppy media applet unresponsive

The iLO Virtual Floppy media applet can become unresponsive if the physical floppy diskette contains media errors.

Solution: To prevent the iLO Virtual Floppy media applet from becoming unresponsive, run a utility such as `CHKDSK.EXE` to check the physical floppy disk media for errors. If the physical media contains errors, load the floppy disk image onto a new physical floppy diskette.

Troubleshooting text-based Remote Console issues

The following sections discuss items to be aware of when attempting to resolve text-based Remote Console issues.

Unable to view Linux installer in text-based Remote Console

When installing Linux from the text console, the initial installation screen might not appear because the screen is in graphics mode.

Solution: To correct this and proceed with the installation, do one of the following:

- For most versions of Linux, enter `linux text nofb`.

  The characters that you enter do not appear.

After you enter the command, the screen changes from graphics mode to text mode, displaying the screen.

- For SLES, press **F2** and the down arrow from the text console. The text mode is selected and the screen appears.

Unable to pass data through SSH terminal

If you use an SSH terminal to access the text console, SSH might intercept keystroke data and not pass the action to the text-based Remote Console. When this occurs, it appears as if the keystroke did not perform its function.

Solution: Disable any SSH terminal shortcuts.

VSP-driven selection during the serial timeout window sends output to BIOS redirect instead of VSP

The `/etc/grub.conf` file includes an option for a serial timeout window (`terminal --timeout=10 serial console`). This setting provides a window of time to select a key stroke on the VSP or on the VGA console, and then the menu is output to the corresponding device. The BIOS serial redirect intercepts VSP keystrokes during this timeout window.

Solution: To work around this issue, do not press a key for a VSP-driven selection during the 10-second timeout or turn off BIOS redirection to the VSP.

Scrolling and text appear irregular during BIOS redirection

During BIOS redirection, the scrolling might not work properly. When you enter commands in RBSU, the text might overwrite itself on the bottom line of the terminal window.

Solution: The BIOS expects and controls a fixed 80x24 character window. When redirected to the serial port, the BIOS still expects and controls a fixed 80x24 character window. If the VSP client being used (SSH, HyperTerminal, or other terminal emulator) can resize the window to a size other than 80x24, scrolling becomes confused and the screen output appears garbled. To avoid this issue, configure the terminal emulator for a window size of exactly 80x24.

Troubleshooting miscellaneous issues

The following sections discuss troubleshooting miscellaneous hardware or software issues.

Cookie sharing between browser instances and iLO

iLO uses browser session cookies to distinguish between individual logins—each browser window appears as a separate user login—while sharing the same active session with iLO. Multiple logins can confuse the browser. This may appear to be an iLO issue, but it is typical browser behavior.

Several processes can cause a browser to open additional windows. Browser windows opened from an open browser represent different aspects of the same program in memory. Consequently, each browser window shares properties with the parent, including cookies.

Shared instances

When iLO opens another browser window (for example, the Remote Console or a help file), this window shares the same connection to iLO and the session cookie.

The iLO web server makes URL decisions based on each request received. For example, if a request does not have access rights, it is redirected to the login page, regardless of the original request. Web server-based redirection, selecting **File→New→Window**, or pressing **Ctrl+N** opens a duplicate instance of the original browser.

Cookie order

During login, the login page builds a browser session cookie that links the window to the appropriate session in the iLO firmware. The firmware tracks browser logins as separate sessions listed in the **Active Sessions** section of the **iLO Overview** page.

For example, when User1 logs in, the web server builds the initial frames view, with User1 listed in the top pane, menu items in the left pane, and page data in the lower right pane. When User1 clicks from link to link, only the menu items and page data are updated.

While User1 is logged in, if User2, opens a browser window on the same client and logs in, the second login overwrites the cookie generated in the original User1 session. Assuming that User2 is a different user account, a different current frame is built, and a new session is granted. The second session appears in the **Active Sessions** section of the **iLO Overview** page as User2.

The second login has effectively orphaned the first session by overriding the cookie generated during the User1 login. This behavior is the same as closing the User1 browser without clicking the **Sign Out** button. The User1 orphaned session is reclaimed when the session timeout expires.

Because the current user frame is not refreshed unless the browser is forced to refresh the entire page, User1 can continue navigating by using the browser window. However, the browser is now operating by using the User2 session cookie settings, even though it may not be readily apparent.

If User1 continues to navigate in this mode (User1 and User2 sharing the same process because User2 logged in and reset the session cookie), the following can occur:

- User1 session behaves consistently with the privileges assigned to User2.
- User1 activity keeps User2 session alive, but User1 session can time out unexpectedly.
- Logging out of either window causes both sessions to end. The next activity in the other window can redirect the user to the login page as if a session timeout or premature timeout occurred.
- Clicking **Sign Out** from the second session (User2) results in the following warning message:

  ```
  Logging out: unknown page to display before redirecting the user to
  the login page.
  ```

- If User2 logs out and then logs back in as User3, User1 assumes the User3 session.
- If User1 is at login, and User2 is logged in, User1 can alter the URL to redirect to the index page. It appears as if User1 has accessed iLO without logging in.

These behaviors continue as long as the duplicate windows are open. All activities are attributed to the same user, using the last session cookie set.

Displaying the current session cookie

After logging in, you can force the browser to display the current session cookie by entering the following in the URL navigation bar:

```
javascript:alert(document.cookie)
```

The first field visible is the session ID. If the session ID is the same among the different browser windows, these windows are sharing the same iLO session.

You can force the browser to refresh and reveal your true identity by pressing **F5**, selecting **View→Refresh**, or clicking the **Refresh** button.

Preventing cookie-related issues

To prevent these issues:

- Start a new browser for each login by double-clicking the browser icon or shortcut.
- Click the **Sign Out** button to close the iLO session before you close the browser window.

Unable to get SNMP information from HP SIM

Solution: The agents running on the managed server supply SNMP information to HP SIM. For agents to pass information through iLO, iLO device drivers must be installed. For installation instructions, see "Installing the iLO drivers" (page 22).

If you have installed the drivers and agents for iLO, verify that iLO and the management PC are on the same subnet. You can verify this quickly by pinging iLO from the management PC. Consult your network administrator for proper routes to access the iLO network interface.

Unable to upgrade iLO firmware

- **Solution 1**: If you attempt to upgrade the iLO firmware by using the iLO web interface, and it does not respond, does not accept the firmware upgrade, or is stopped before a successful upgrade, try reinstalling the firmware after you complete the following diagnostic steps:
  1. Attempt to connect to iLO through the web browser. If you cannot connect, there is a communication issue.
  2. Attempt to ping iLO. If you are successful, the network is working.
- **Solution 2**: If an incorrect file is used to flash the iLO firmware by using the iLO web interface, the following error message is displayed:

  ```
  The last firmware update attempt was not successful. Ready for the next update.
  ```

  If this error occurs, click the **Clear Error** button to reset the flash process, and then try the firmware update again with the correct firmware file. If you do not clear the error, the same error might occur even when you use the correct firmware file.
- **Solution 3**: If a connection error occurs after you install a firmware update by using the iLO web interface, clear the browser cache.
- **Solution 4**: Try a different firmware update method. For information about the methods that you can use to update the firmware, see "Updating firmware" (page 25).

Recovering from a failed iLO firmware update

Use this procedure to recover from a failed iLO firmware update on Linux or VMware systems.

1. Copy the iLO offline flash component to a USB drive key.
2. Set the iLO Security Override Switch to **disabled**.
3. Boot the USB drive key containing the iLO offline flash component.

   To download the HP USB Key Utility and for information on how to create a boot USB key, see the SPP documentation at http://www.hp.com/go/spp/documentation.
4. After the first screen displays, switch to text console by pressing **Ctrl+Alt+F1**.
5. Switch to the directory where the flash component is stored by entering the following command at the # prompt:

   ```
   cd /mnt/usb/components/
   ```
6. Remove the loaded iLO driver by entering the following commands:
   - ESX 4.x: `/etc/init.d/hp-snmp-agents stop /etc/init.d/hp-ilo stop`
   - ESX 3.x: `/etc/init.d/hpasm stop`
7. Run the component using the –direct option, for example:

   ```
   /CP00xxxx.scexe --direct
   ```
8. Enter `Y` at the `Continue (Y/N)?` prompt.
9. After programming is successfully completed, set the security override switch to **enabled** and reboot the server.

iLO network Failed Flash Recovery

Most firmware upgrades finish successfully. In the unlikely event of server power loss during an iLO firmware upgrade, iLO might be recoverable when power is restored.

When the computer is booting, the kernel performs image validation on the main image. If the image is corrupted or incomplete, the kernel enters Failed Flash Recovery. Failed Flash Recovery activates an FTP server within iLO. The FTP server enables you to send an image to iLO for programming. The FTP server does not provide any other services.

A network client can connect to the FTP server. The user name for the connection is **test**, and the password is **flash**. To send a firmware image to iLO, use the FTP client `PUT` command. After receiving the image, iLO validates the image. If the image is a complete, signed, and valid firmware image, the kernel begins programming the FLASH partition.

After the image is completely programmed into the FLASH partition, reset iLO by issuing the `RESET` command to the iLO FTP server.

Example:

```
F:\ilo3>ftp 192.168.1.2
Connected to 192.168.1.2.
220 FTP Recovery server ready.
User (192.168.1.2:(none)): ftp
331 Password required.
Password:
231 Logged in.
ftp> put iLO3.bin
200 Ok.
150 ready for file
226-Checking file
226-File acceptable
226-Flashing   3% complete
226-Flashing   4% complete
226-Flashing   6% complete
.
.
.
226-Flashing  97% complete
226-Flashing  99% complete
226-Flashing 100% complete
226-Flashing completed
226 Closing file
ftp: 8388608 bytes sent in 1.38Seconds 6100.81 Kbytes/sec.
ftp> quote reset
221 Goodbye (reset).
Connection closed by remote host.
ftp> quit
```

Testing SSL

The following test checks for the correct security prompt. A nonworking server will proceed to a `Page cannot be displayed` message. If this test fails, your domain controller is not accepting SSL connections and probably has not been issued a certificate.

1. Open a browser and navigate to `https://<domain controller>:636`.

   You can use <domain> instead of <domain controller>, which accesses the DNS and determines which domain controller is handling requests for the domain. Test multiple domain controllers to verify that all of them have been issued a certificate.

2. If SSL is operating correctly on the domain controller (a certificate has been issued), you are prompted with a security message that asks whether you want to proceed with accessing the site or view the server certificate. Clicking **Yes** does not display a webpage, which is normal. This process is automatic, but might require rebooting. To avoid rebooting:
   a. Open the MMC.
   b. Add the certificates snap-in.
   c. When prompted, select **Computer Account** for the type of certificates you want to view.
   d. Click **OK** to return to the certificates snap-in.
   e. Select the **Personal**→**Certificates** folder.
   f. Right-click the folder and select **Request New Certificate**.
   g. Verify that the **Type** is domain controller, and click **Next** until a certificate is issued.

You can also use the Microsoft `Ldp.exe` tool to verify SSL connections. For more information about the LDP tool, see your Microsoft documentation.

An old certificate can cause issues with SSL on the domain controller when it points to a previously trusted CA with the same name. This situation is rare but might happen if a certificate service is added and removed, and then added again on the domain controller. To remove old certificates and issue a new one, follow the instructions in step 2.

Resetting iLO

In some cases, it might be necessary to reset iLO; for example, if iLO is not responding to the browser.

iLO might reset itself in certain instances. For example, an internal iLO watchdog timer resets if the firmware detects an iLO issue. If a firmware upgrade is completed or a network setting is changed, iLO also resets.

To reset iLO, use one of the following methods:

- Click **Reset** on the **Information**→**Diagnostics** page in the iLO web interface. For more information, see "Using iLO diagnostics" (page 112).
- Use the CLI or HPONCFG. For instructions, see the *HP iLO 3 Scripting and Command Line Guide*.
- The HP Insight Management Agents 5.40 and later have the ability to reset iLO. Select the **Reset iLO** option on the **HP Management Agent** page in the iLO section.
- Click **Apply** on the **Network**→**iLO Dedicated Network Port or Shared Network Port**→**General** page to manually force the iLO management processor to reset. If the **Apply** button is not available, change a setting, change it back, and then click **Apply** to reset iLO without changing the configuration.

If none of these methods is available or working as expected, you must power down the server and disconnect the power supplies completely.

Resetting iLO to the factory default settings by using iLO RBSU

To reset iLO to the factory default settings:

△ **CAUTION:** This operation clears all user and license data.

1. Optional: If you access the server remotely, start an iLO remote console session.
   You can use the .NET IRC or Java IRC.
2. Restart or power on the server.
3. Press **F8** in the HP ProLiant POST screen.
   iLO RBSU starts.

4. Select **File→Set Defaults**.

   iLO RBSU prompts you to confirm the request.

5. Press **F10** to continue.

   iLO RBSU displays the following message:

   ```
   After setting to factory defaults, iLO 3 will be reset and  this utility will exit.
   ```

6. Press **Enter**.

   iLO resets and the server boot process finishes.

NOTE: If a server has an installed iLO Advanced license when you perform this procedure, the iLO Advanced icon might be selected when the server boot process finishes. The icon will be set correctly after POST completes, or after the server is shut down, powered off, and then powered on again.

Server name still present after System Erase Utility is executed

The server name, as shown on the **iLO Overview** page, is the installed host operating system name. If the Insight Management Agents are installed on the server, the agents will obtain the host name and update it on the iLO web interface page.

To remove the server name after the redeployment of a server, do one of the following:

- Load the HP Insight Management Agents to update the server name.
- Use the iLO RBSU **Reset to Factory Defaults** feature to clear the server name.

CAUTION: This procedure clears all iLO configuration information, not just the **Server Name** information.

- Change the server name on the **Administration→Access Settings→Access Options** page in the iLO web interface.

Certificate error when navigating to iLO web interface

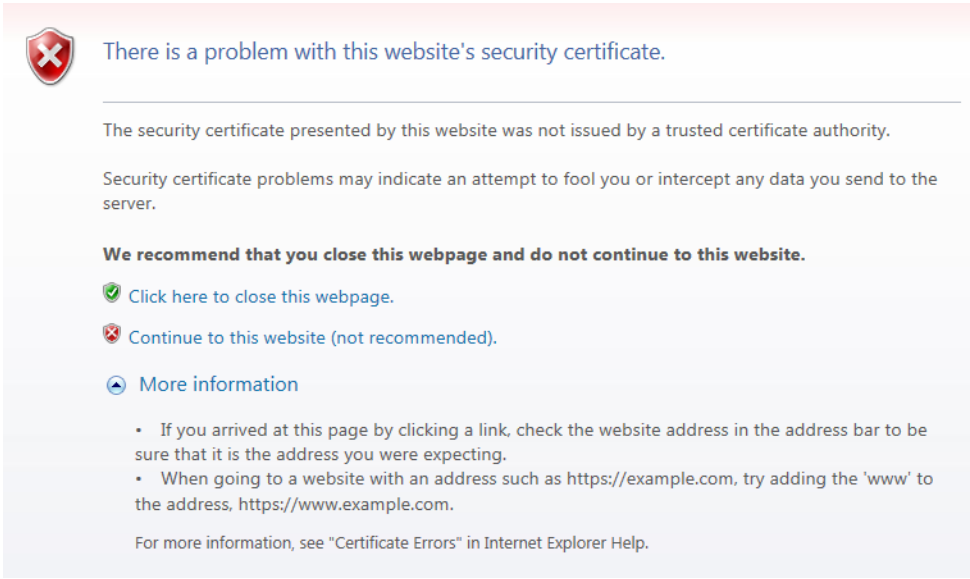
Issue: When you point your browser to the iLO web interface, a certificate error appears.

Suggested action: Use one of the following procedures to resolve the error.

Resolving a browser certificate error: Internet Explorer

1. Click the **Continue to this website (not recommended)** link, as shown in Figure 127 (page 232)

Figure 127 Internet Explorer security certificate warning



2. Log in to the iLO web interface.
3. Navigate to the **Administration→Security→SSL Certificate** page.
4. Click **Customize Certificate**.
5. Enter the following information in the **Certificate Signing Request (CSR) Information** section. The required boxes are marked with an asterisk (*) in the GUI.
   - **Country (C)**—The two-character country code that identifies the country where the company or organization that owns this iLO subsystem is located
   - **State (ST)**—The state where the company or organization that owns this iLO subsystem is located
   - **City or Locality (L)**—The city or locality where the company or organization that owns this iLO subsystem is located
   - **Organization Name (O)**—The name of the company or organization that owns this iLO subsystem
   - **Organizational Unit (OU)**—(Optional) The unit within the company or organization that owns this iLO subsystem
   - **Common Name (CN)**—The FQDN of this iLO subsystem
6. Click **Generate CSR**.

   The following message is displayed:

   ```
   The iLO subsystem is currently generating a Certificate Signing
   Request (CSR). This may take 10 minutes or more. In order to view
   the CSR, wait 10 minutes or more, and then click the Generate CSR
   button again.
   ```
7. After 10 minutes or more, click the **Generate CSR** button.

   A new window displays the CSR.
8. Select and copy the CSR text.
9. Open a browser window and navigate to a third-party CA.

10. Follow the onscreen instructions and submit the CSR to the CA.

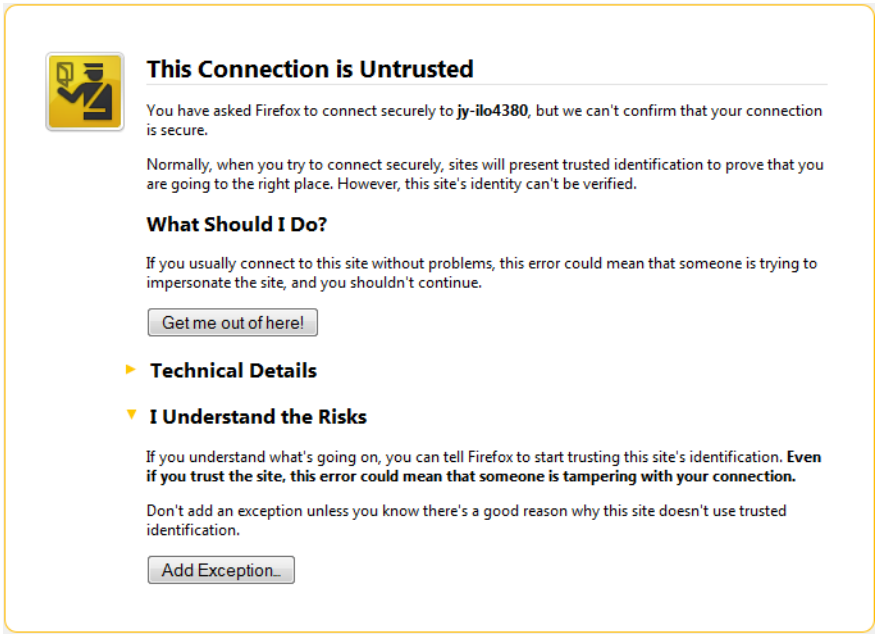
    The CA will generate a certificate in the PKCS #10 format.
11. After you obtain the certificate, ensure the following:
    - The CN matches the iLO FQDN. This is listed as the **iLO Hostname** on the **Information→Overview** page.
    - The certificate is generated as a Base64-encoded X.509 certificate, and is in the RAW format.
    - The first and last lines are included in the certificate.
12. Return to the **Customize Certificate** page in the iLO web interface.
13. Click the **Import Certificate** button.

    The **Import Certificate** window opens.
14. Paste the certificate into the text box, and then click the **Import** button.
15. Restart iLO.

Resolving a browser certificate error: Firefox

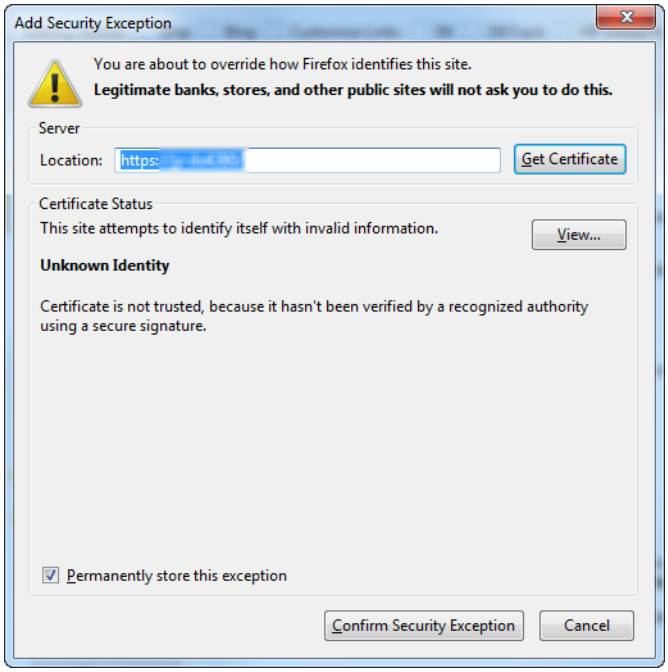
1. Click the **I Understand the Risks** link to expand the section, and then click **Add Exception**, as shown in Figure 128 (page 233).

Figure 128 Firefox untrusted connection dialog box



2. In the **Add Security Exception** dialog box, enter `https://<iLO hostname or IP address>` in the **Location** box, as shown in Figure 129 (page 234).

Figure 129 Firefox Add Security Exception dialog box



3. Click **Confirm Security Exception** to resolve the security warning.
   The security exception is saved, and the iLO login screen appears.
4. Log in to iLO.

8 Support and other resources

Information to collect before you contact HP

Be sure to have the following information available before you contact HP:

- Software product name
- Hardware product model number
- Operating system type and version
- Applicable error message
- Third-party hardware or software
- Technical support registration number (if applicable)

How to contact HP

Use the following methods to contact HP technical support:

- See the Contact HP worldwide website:
  http://www.hp.com/go/assistance
- Use the `Get Help from HP` link on the HP Support Center website:
  http://www.hp.com/go/hpsc
- In the United States, call +1 800 334 5144 to contact HP by telephone. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, conversations might be recorded or monitored.

Registering for Software Technical Support and Update Service

Insight Management software products include 1 year of 24 x 7 HP Software Technical Support and Update Service. This service provides access to HP technical resources for assistance in resolving software implementation or operations problems.

The service also provides access to software updates and reference manuals in electronic format.

With this service, iLO Advanced and iLO Advanced for BladeSystem customers benefit from expedited problem resolution as well as proactive notification and delivery of software updates. For more information about this service, see the following website: http://www.hp.com/services/insight.

If you received a license entitlement certificate, registration for this service occurs after online redemption of the license certificate or key.

How to use Software Technical Support and Update Service

After you are registered, you will receive a service contract in the mail. The contract contains the Customer Service phone number and your SAID. You will need your SAID when you call for technical support. By using your SAID, you can also go to the HP Support Center website to view your contract online.

HP Support Center

Join the discussion. The HP Support Center at http://www.hp.com/go/hpsc is a community-based, user-supported tool for HP customers to participate in discussions among the customer community about HP products. For discussions related to iLO Advanced and iLO Advanced for BladeSystem software, see the **Management Software and System Tools** area.

HP authorized resellers

For the name of the nearest HP authorized reseller, see the following sources:

- In the United States, see the HP U.S. service locator website: http://www.hp.com/service_locator
- In other locations, see the Contact HP worldwide website: http://www.hp.com/go/assistance

Related information

Documents

- *HP iLO 3 Scripting and Command Line Guide*
- *HP iLO 3 Release Notes*
- *HP ROM-Based Setup Utility User Guide*
- *HP Scripting Toolkit for Linux User Guide*
- *HP Scripting Toolkit for Windows User Guide*
- *HP Smart Update Firmware DVD User Guide*
- *HP Smart Update Manager User Guide*
- *HP Service Pack for ProLiant User Guide*
- *HP Insight Management Agents User Guide*
- *HP Insight Management Agents Installation Guide*
- *HP Systems Insight Manager User Guide*
- *HP BladeSystem Onboard Administrator User Guide*

Websites

- HP iLO: http://www.hp.com/go/ilo
- HP Operating Systems and Virtualization Software Support for ProLiant Servers: http://www.hp.com/go/supportos.
- HP SUM: http://www.hp.com/go/hpsum
- HP Service Pack for ProLiant: http://www.hp.com/go/spp/documentation
- HP Systems Insight Manager: http://www.hp.com/go/hpsim
- HP Onboard Administrator: http://www.hp.com/go/oa
- HP VMware Vibs Depot :http://vibsdepot.hp.com

9 Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hp.com). Include the document title and part number, version number, or the URL when submitting your feedback.

A iLO license options

Table 13 (page 238) lists the features that are included with each iLO license.

Table 13 iLO 3 license options

Feature	iLO Standard	iLO Standard for BladeSystem	iLO Advanced for BladeSystem	iLO Advanced
Platform Support	All (except BL)	BL	BL	All (except BL)
Embedded Health System	X	X	X	X
Virtual Power Buttons	X	X	X	X
IPMI Over LAN/DCMI	X	X	X	X
Web-Based GUI	X	X	X	X
SSH Command Line Interface	X	X	X	X
RIBCL	X	X	X	X
Virtual Serial Port	X	X	X	X
IPv6	X	X	X	X
Integrated Remote Console (IRC/Virtual KVM, Supports Text & Graphics)	Pre-OS only	X	X	X
Global Team Collaboration via Integrated Remote Console			X	X
Integrated Remote Console Record and Playback			X	X
Virtual Media via Integrated Remote Console		X	X	X
Scripted Virtual Media			X	X
Text-based Remote Console via SSH (Textcons)			X	X
Directory Service Authentication			X	X
Kerberos Authentication			X	X
Advanced Power Management (Power History Graphs, Dynamic Power Capping)			X	X

B Directory services schema

This appendix describes the classes and attributes that are used to store Lights-Out management authorization data in the directory service.

HP Management Core LDAP OID classes and attributes

Changes made to the schema during the schema setup process include changes to the following:

- Core classes
- Core attributes

Core classes

Class name	Assigned OID
hpqTarget	1.3.6.1.4.1.232.1001.1.1.1.1
hpqRole	1.3.6.1.4.1.232.1001.1.1.1.2
hpqPolicy	1.3.6.1.4.1.232.1001.1.1.1.3

Core attributes

Attribute name	Assigned OID
hpqPolicyDN	1.3.6.1.4.1.232.1001.1.1.2.1
hpqRoleMembership	1.3.6.1.4.1.232.1001.1.1.2.2
hpqTargetMembership	1.3.6.1.4.1.232.1001.1.1.2.3
hpqRoleIPRestrictionDefault	1.3.6.1.4.1.232.1001.1.1.2.4
hpqRoleIPRestrictions	1.3.6.1.4.1.232.1001.1.1.2.5
hpqRoleTimeRestriction	1.3.6.1.4.1.232.1001.1.1.2.6

Core class definitions

The following tables define the HP Management core classes.

hpqTarget

OID	1.3.6.1.4.1.232.1001.1.1.1.1
Description	This class defines target objects, providing the basis for HP products that use directory-enabled management.
Class type	Structural
SuperClasses	user
Attributes	hpqPolicyDN - 1.3.6.1.4.1.232.1001.1.1.2.1 hpqRoleMembership - 1.3.6.1.4.1.232.1001.1.1.2.2
Remarks	None

hpqRole

OID	1.3.6.1.4.1.232.1001.1.1.1.2
Description	This class defines role objects, providing the basis for HP products that use directory-enabled management.
Class type	Structural
SuperClasses	group
Attributes	hpqRoleIPRestrictions - 1.3.6.1.4.1.232.1001.1.1.2.5 hpqRoleIPRestrictionDefault - 1.3.6.1.4.1.232.1001.1.1.2.4 hpqRoleTimeRestriction - 1.3.6.1.4.1.232.1001.1.1.2.6 hpqTargetMembership - 1.3.6.1.4.1.232.1001.1.1.2.3
Remarks	None

hpqPolicy

OID	1.3.6.1.4.1.232.1001.1.1.1.3
Description	This class defines policy objects, providing the basis for HP products that use directory-enabled management.
Class Type	Structural
SuperClasses	top
Attributes	hpqPolicyDN - 1.3.6.1.4.1.232.1001.1.1.2.1
Remarks	None

Core attribute definitions

The following tables define the HP Management core class attributes.

hpqPolicyDN

OID	1.3.6.1.4.1.232.1001.1.1.2.1
Description	Distinguished name of the policy that controls the general configuration of this target
Syntax	Distinguished Name - 1.3.6.1.4.1.1466.115.121.1.12
Options	Single valued
Remarks	None

hpqRoleMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.2
Description	Provides a list of hpqRole objects that belong to this object
Syntax	Distinguished Name - 1.3.6.1.4.1.1466.115.121.1.12
Options	Multivalued
Remarks	None

hpqTargetMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.3
Description	Provides a list of hpqTarget objects that belong to this object
Syntax	Distinguished Name - 1.3.6.1.4.1.1466.115.121.1.12
Options	Multivalued
Remarks	None

hpqRoleIPRestrictionDefault

OID	1.3.6.1.4.1.232.1001.1.1.2.4
Description	A Boolean that represents access by unspecified clients and that partially specifies rights restrictions under an IP network address constraint
Syntax	Boolean - 1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	If this attribute is `TRUE`, IP restrictions will be satisfied for unexceptional network clients. If this attribute is `FALSE`, IP restrictions will be unsatisfied for unexceptional network clients.

hpqRoleIPRestrictions

OID	1.3.6.1.4.1.232.1001.1.1.2.5
Description	Provides a list of IP addresses, DNS names, domains, address ranges, and subnets that partially specify right restrictions under an IP network address constraint
Syntax	Octet String - 1.3.6.1.4.1.1466.115.121.1.40
Options	Multivalued
Remarks	This attribute is used only on role objects. IP restrictions are satisfied when the address matches and general access is denied. They are unsatisfied when the address matches and general access is allowed. Values are an identifier byte followed by a type-specific number of bytes that specify a network address. • For IP subnets, the identifier is <0x01>, followed by the IP network address in network order, followed by the IP network subnet mask in network order. For example, the IP subnet 127.0.0.1/255.0.0.0 would be represented as <0x01 0x7F 0x00 0x00 0x01 0xFF 0x00 0x00 0x00>. For IP ranges, the identifier is <0x02>, followed by the lower bound IP address, followed by the upper bound IP address. Both are inclusive and in network order. For example, the IP range 10.0.0.1 to 10.0.10.255 would be represented as <0x02 0x0A 0x00 0x00 0x01 0x0A 0x00 0x0A 0xFF>. • For DNS names or domains, the identifier is <0x03>, followed by the ASCII encoded DNS name. DNS names can be prefixed with an * (ASCII 0x2A), to indicate they must match all names that end with the specified string. For example, the DNS domain *.acme.com is represented as <0x03 0x2A 0x2E 0x61 0x63 0x6D 0x65 0x2E 0x63 0x6F 0x6D>. General access is allowed.

hpqRoleTimeRestriction

OID	1.3.6.1.4.1.232.1001.1.1.2.6
Description	A 7-day time grid, with 30-minute resolution, which specifies rights restrictions under a time constraint
Syntax	Octet String {42} - 1.3.6.1.4.1.1466.115.121.1.40
Options	Single valued
Remarks	This attribute is used only on role objects. Time restrictions are satisfied when the bit that corresponds to the current local time of the device is 1 and unsatisfied when the bit is 0. • The least significant bit of the first byte corresponds to Sunday, from midnight to 12:30 a.m. • Each more significant bit and sequential byte corresponds to the next consecutive half-hour blocks within the week. • The most significant (eighth) bit of the 42nd byte corresponds to Saturday at 11:30 p.m. to Sunday at midnight.

Lights-Out Management specific LDAP OID classes and attributes

The following schema attributes and classes might depend on attributes or classes defined in the HP Management core classes and attributes.

Lights-Out Management classes

Class name	Assigned OID
hpqLOMv100	1.3.6.1.4.1.232.1001.1.8.1.1

Lights-Out Management attributes

Class name	Assigned OID
hpqLOMRightLogin	1.3.6.1.4.1.232.1001.1.8.2.3
hpqLOMRightRemoteConsole	1.3.6.1.4.1.232.1001.1.8.2.4
hpqLOMRightVirtualMedia	1.3.6.1.4.1.232.1001.1.8.2.6
hpqLOMRightServerReset	1.3.6.1.4.1.232.1001.1.8.2.5
hpqLOMRightLocalUserAdmin	1.3.6.1.4.1.232.1001.1.8.2.2
hpqLOMRightConfigureSettings	1.3.6.1.4.1.232.1001.1.8.2.1

Lights-Out Management class definitions

The following table defines the Lights-Out Management core class.

hpqLOMv100

OID	1.3.6.1.4.1.232.1001.1.8.1.1
Description	This class defines the rights and settings used with HP Lights-Out Management products.
Class Type	Auxiliary
SuperClasses	None

Attributes	hpqLOMRightConfigureSettings - 1.3.6.1.4.1.232.1001.1.8.2.1 hpqLOMRightLocalUserAdmin - 1.3.6.1.4.1.232.1001.1.8.2.2 hpqLOMRightLogin - 1.3.6.1.4.1.232.1001.1.8.2.3 hpqLOMRightRemoteConsole - 1.3.6.1.4.1.232.1001.1.8.2.4 hpqLOMRightServerReset - 1.3.6.1.4.1.232.1001.1.8.2.5 hpqLOMRightVirtualMedia - 1.3.6.1.4.1.232.1001.1.8.2.6
Remarks	None

Lights-Out Management attribute definitions

The following tables define the Lights-Out Management core class attributes.

hpqLOMRightLogin

OID	1.3.6.1.4.1.232.1001.1.8.2.3
Description	Login right for HP Lights-Out Management products
Syntax	Boolean - 1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	Meaningful only on role objects. If `TRUE`, members of the role are granted the right.

hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.4
Description	Remote Console right for Lights-Out Management products. Meaningful only on role objects.
Syntax	Boolean - 1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is used only on role objects. If this attribute is `TRUE`, members of the role are granted the right.

hpqLOMRightVirtualMedia

OID	1.3.6.1.4.1.232.1001.1.8.2.6
Description	Virtual Media right for HP Lights-Out Management products
Syntax	Boolean - 1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is only used on role objects. If this attribute is `TRUE`, members of the role are granted the right.

hpqLOMRightServerReset

OID	1.3.6.1.4.1.232.1001.1.8.2.5
Description	Remote Server Reset and Power Button right for HP Lights-Out Management products
Syntax	Boolean - 1.3.6.1.4.1.1466.115.121.1.7

Options	Single valued
Remarks	This attribute is used only on role objects. If this attribute is `TRUE`, members of the role are granted the right.

hpqLOMRightLocalUserAdmin

OID	1.3.6.1.4.1.232.1001.1.8.2.2
Description	Local User Database Administration right for HP Lights-Out Management products.
Syntax	Boolean - 1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is used only on role objects. If this attribute is `TRUE`, members of the role are granted the right.

hpqLOMRightConfigureSettings

OID	1.3.6.1.4.1.232.1001.1.8.2.1
Description	Configure Devices Settings right for HP Lights-Out Management products.
Syntax	Boolean - 1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is used only on role objects. If this attribute is `TRUE`, members of the role are granted the right.

C OID support for certificates

This appendix shows the OIDs supported by iLO certificates.

Table 14 OIDs supported by iLO certificates

rsaEncryption	1.2.840.113549.1.1.1
md2WithRSAEncryption	1.2.840.113549.1.1.2
md5WithRSAEncryption	1.2.840.113549.1.1.4
sha1WithRSAEncryption	1.2.840.113549.1.1.5
md2	1.2.840.113549.2.2
md5	1.2.840.113549.2.5
sha1	1.3.14.3.2.26
dsaEncryption	1.2.840.10040.4.1
sha1WithDSAEncryption	1.2.840.10040.4.3
pkcs7_data	1.2.840.113549.1.7.1
pkcs7_signedData	1.2.840.113549.1.7.2
commonName	2.5.4.3
countryName	2.5.4.6
localityName	2.5.4.7
stateOrProvinceName	2.5.4.8
organizationName	2.5.4.10
organizationalUnitName	2.5.4.11
emailAddress	1.2.840.113549.1.9.1
emailAddressRFC1274	0.9.2342.19200300.100.1.3
authorityKeyIdentifier	2.5.29.35
subjectKeyIdentifier	2.5.29.14
keyUsage	2.5.29.15
privateKeyUsagePeriod	2.5.29.16
certificatePolicies	2.5.29.32
policyMappings	2.5.29.33
subjectAltName	2.5.29.17
issuerAltName	2.5.29.18
subjectDirectoryAttributes	2.5.29.9
basicConstraints	2.5.29.19
nameConstraints	2.5.29.30
policyConstraints	2.5.29.36
extKeyUsage	2.5.29.37
crlDistributionPoints	2.5.29.31

Table 14 OIDs supported by iLO certificates *(continued)*

ikeIntermediate	1.3.6.1.5.5.8.2.2
extensionRequest	1.2.840.113549.1.9.14
domainComponent	0.9.2342.19200300.100.1.25

Glossary

.NET IRC	.NET version of the Integrated Remote Console.
3DES	Triple DES, the Data Encryption Standard cipher algorithm.
ABEND	Abnormal End.
ACPI	Advanced Configuration and Power Interface.
AES	Advanced Encryption Standard.
AMP	Advanced Memory Protection.
ARP	Address Resolution Protocol.
ASR	Automatic Server Recovery.
BMC	Baseboard management controller.
CA	Certificate authority.
CLP	Command Line Protocol.
CN	Common Name.
COM port	Communication port.
cookie	A small, unscriptable text file placed on your hard drive by a website to preserve specific settings. When you return to the site, your system opens the cookie with the previously saved settings so they can be passed along to the site. Cookies are also used to store session data temporarily.
CR	Certificate request.
CSR	Certificate signing request.
DCMI	Data Center Manageability Interface.
DDNS	Dynamic Domain Name System.
DHCP	Dynamic Host Configuration Protocol.
DHE	Diffie–Hellman key exchange.
DIMM	Dual In-line Memory Module.
DLL	Dynamic-link library.
DMTF	Distributed Management Task Force.
DN	Distinguished name.
DNS	Domain Name System.
DSA	Digital Signature Algorithm.
DVO	Digital Video Out.
ECC	Error Correcting Code.
EDO	Extended Data Out.
EMS	Emergency Management Services.
FMSO	Flexible Single Master Operation.
FQDN	Fully Qualified Domain Name.
GMT	Greenwich Mean Time.
GRUB	Grand Unified Bootloader.
HEM	High Efficiency Mode.
HP SIM	HP Systems Insight Manager.
HPLOMIG	HP Lights-Out Migration Utility, also called HP Directories Support for Management Processors.
HPONCFG	HP Lights-Out Online Configuration Utility.
HPQLOCFG	HP Lights-Out Configuration Utility.
ICMP	Internet Control Message Protocol.
IIS	Internet Information Services.

iLO	Integrated Lights-Out.
IML	Integrated Management Log.
IPMI	Intelligent Platform Management Interface.
IRC	Integrated Remote Console.
ISO	International Organization for Standardization.
Java IRC	Java version of the Integrated Remote Console.
JRE	Java Runtime Environment.
KCS	Keyboard Controller Style.
KDC	Key Distribution Center.
KDE	K Desktop Environment (for Linux).
KVM	Keyboard, video, and mouse.
LDAP	Lightweight Directory Access Protocol.
LILO	Linux Loader.
LOM	Lights-Out Management.
MAC	Media Access Control.
MIB	Management Information Base. A database of managed objects accessed by network management protocols. An SNMP MIB is a set of parameters that an SNMP management station can query or set in the SNMP agent of a network device (for example, a router).
MIME	Multipurpose Internet Mail Extensions.
MMC	Microsoft Management Console.
NDS	Novell Directory Services.
NMI	Non-maskable interrupt.
NTLM	NT Local Machine.
OA	Onboard Administrator.
OU	Organizational Unit.
PAL	Programmable Array Logic.
PKCS	Public-Key Cryptography Standards.
POST	Power-On Self Test.
RBSU	ROM-Based Setup Utility. Pressing **F9** starts the system ROM RBSU, and pressing **F8** starts the iLO RBSU.
RDRAM	Rambus Dynamic Random Access Memory.
RIBCL	Remote Insight Board Command Language.
RPM	RPM Package Manager.
RSA	An algorithm for public-key cryptography.
SAID	Service Agreement Identifier.
SAS	Serial Attached SCSI.
SATA disk	Serial ATA (SATA) disk. The evolution of the ATA (IDE) interface that changes the physical architecture from parallel to serial and from primary-secondary (master-slave) to point-to-point. Unlike parallel ATA interfaces that connect two drives; one configured as primary (master), the other as secondary (slave), each SATA drive is connected to its own interface.
SD	Secure Digital.
SHA	Secure Hash Algorithm.
SID	Security Identifier.
SLES	SUSE Linux Enterprise Server
SMASH	System Management Architecture for Server Hardware.
SMS	System Management Software.

SNMP	Simple Network Management Protocol.
SNTP	Simple Network Time Protocol.
SPN	Service Principal Name.
SPP	HP Service Pack for ProLiant.
SSD	Solid-State Drive.
SSH	Secure Shell.
SSL	Secure Sockets Layer.
SSO	Single Sign-On.
SUM	Software Update Manager.
TPM	Trusted Platform Module.
UDP	User Datagram Protocol.
UHCI	Universal Host Controller Interface.
UID	Unit Identification.
UPN	User Principal Name.
UPS	Uninterruptible Power Supply.
USB	Universal Serial Bus.
UTC	Coordinated Universal Time.
UTP	Unshielded Twisted Pair.
UUID	Universally Unique Identifier.
WBEM	Web-Based Enterprise Management.
WINS	Windows Internet Naming Service.

Index

J

K

L

T

U

V

W