HP iLO 4 User Guide

Abstract

This guide provides information about configuring, updating, and operating HP ProLiant Gen8 and Gen9 servers by using the HP iLO 4 firmware. This document is intended for system administrators, HP representatives, and HP Authorized Channel Partners who are involved in configuring and using HP iLO 4 and HP ProLiant Gen8 and Gen9 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: 684918-008
Published: September 2014
Edition: 1

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Acknowledgements

Contents

1 Introduction to iLO

Overview

The HP iLO subsystem is a standard component of HP ProLiant servers that simplifies initial server setup, server health monitoring, power and thermal optimization, and remote server administration. The HP iLO subsystem includes an intelligent microprocessor, secure memory, and a dedicated network interface. This design makes HP iLO independent of the host server and its operating system.

HP iLO enables and manages the Active Health System and also features Agentless Management. HP iLO monitors all key internal subsystems. When enabled, SNMP alerts are sent directly by HP iLO, regardless of the host operating system or whether a host operating system is installed. Embedded remote support software is available on HP ProLiant Gen8 and Gen9 servers with iLO 4, regardless of the operating system software and without installing OS agents on the server.

HP iLO features

Using HP iLO, you can 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 internal storage.
- Download the Active Health System log. You can send the log file to HP when you have an open support case.
- Manage multiple servers at one time by using the iLO Federation management features.
- 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

  In this document, 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 up to four 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.
- Implement true Agentless Management with SNMP alerts from HP iLO, regardless of the state of the host server.
- Register an HP ProLiant Gen8 or Gen9 server for HP Insight Remote Support.
- 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.
- Control iLO by using a remote management tool.

iLO web interface

The iLO web interface groups similar tasks for easy navigation and workflow. The interface is organized in a navigational tree view located on the left side of the page. The top-level branches are **Information**, **iLO Federation**, **Remote Console**, **Virtual Media**, **Power Management**, **Network**, **Remote Support**, and **Administration**. If you have a ProLiant server blade, the **BL c-Class** branch is included. When a remote management tool is used with iLO, the **<Remote Management Tool Name>** 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 **iLO Federation**, **Network**, **Remote Support**, **Administration**, and **<Remote Management Tool Name>** branches of the iLO web interface. These tasks are described in "Setting up iLO" (page 18) and "Configuring iLO" (page 37).
- Typical user tasks are available from the **Information**, **Remote Console**, **Virtual Media**, **Power Management**, **iLO Federation**, and **BL c-Class** branches of the iLO web interface. These tasks are described in "Using iLO" (page 146).

ROM-based configuration utilities

Depending on your server model, you can use iLO RBSU or the iLO 4 Configuration Utility to configure network parameters, global settings, and user accounts. On servers that support UEFI, such as the HP ProLiant DL580 Gen8 server and HP ProLiant Gen9 servers, use the iLO 4 Configuration Utility in the UEFI System Utilities. On servers that do not support UEFI, use the iLO RBSU.

iLO RBSU and the iLO 4 Configuration Utility are designed for the initial iLO setup, and are not intended for continued iLO administration. You can start these utilities when the server is booted, and you can run them remotely with the Remote Console.

To determine whether your server supports iLO RBSU or the iLO 4 Configuration Utility, see the server QuickSpecs at http://www.hp.com/go/qs/.

You can configure iLO to require users to log in when they access the ROM-based configuration utilities, or you can disable the utilities for all users. These settings can be configured in the iLO access options. Disabling iLO RBSU or the iLO 4 Configuration Utility prevents reconfiguration from the host unless the system maintenance switch is set to disable iLO security. For more information, see "Configuring access options" (page 59).

To access the ROM-based configuration utilities:

- **iLO RBSU**—Press **F8** during POST to enter iLO RBSU.
- **iLO 4 Configuration Utility**—Press **F9** during POST to enter the UEFI System Utilities, and then select **System Configuration**→**iLO 4 Configuration Utility**.

NOTE: On servers that use the system RBSU and not the UEFI System Utilities, the iLO option ROM lists the installed license and the firmware version. This information is not listed in the option ROM on UEFI systems.

iLO mobile app

The HP iLO mobile app provides access to 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 4 Scripting and Command Line Guide* describes the syntax and tools available for using iLO 4 through a command line or scripted interface.

HP RESTful API

HP iLO 4 firmware version 2.00 and later includes the HP RESTful API. The HP RESTful API is a management interface that server management tools can use to perform configuration, inventory, and monitoring of an HP ProLiant server via iLO. A REST client sends HTTPS operations to the iLO web server to `GET` and `PATCH` JSON-formatted data, and to configure supported iLO and server settings, such as the UEFI BIOS settings.

For more information about JSON, see the following website: http://www.json.org.

Some examples of the supported HTTPS operations include `GET`, `PUT`, `POST`, `PATCH`, and `DELETE`.

iLO 4 supports the HP RESTful API with HP ProLiant Gen8 and Gen9 servers.

For more information about the HP RESTful API see the following website: http://www.hp.com/go/restfulinterface/docs.

2 Setting up iLO

Overview

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 37).

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 18).

2. Connect iLO to the network.

   For more information, see "Connecting iLO to the network" (page 20).

3. If you are not using dynamic IP addressing, configure a static IP address by using iLO RBSU or the iLO 4 Configuration Utility.

   For more information, see "Setting up iLO by using iLO RBSU or the iLO 4 Configuration Utility" (page 21).

4. If you are using the local accounts feature, set up your user accounts by using iLO RBSU, the iLO 4 Configuration Utility, or the iLO web interface.

   For more information, see "Setting up iLO by using iLO RBSU or the iLO 4 Configuration Utility" (page 21) or "Setting up iLO by using the iLO web interface" (page 33).

5. Install an iLO license. For more information, see "Activating iLO licensed features" (page 33).
6. If required, install the iLO drivers.

   For more information, see "Installing the iLO drivers" (page 34).

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:

How should iLO connect to the network?

For a graphical representation and explanation of the available connections, see "Connecting iLO to the network" (page 20).

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 if a hardware failure occurs on the corporate network. In this configuration, iLO cannot be accessed directly from the corporate network.

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 or the iLO 4 Configuration Utility. For more information, see "Configuring a static IP address by using iLO RBSU" (page 21) or "Configuring a static IP address by using the iLO 4 Configuration Utility" (page 23).

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

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 accounts 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 63).

How do you want to configure iLO?

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

- Use **iLO RBSU** or the **iLO 4 Configuration Utility** when the system environment does not use DHCP, DNS, or WINS. For more information, see "Setting up iLO by using iLO RBSU or the iLO 4 Configuration Utility" (page 21).
- 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 33).

Other configuration options not discussed in this guide follow:

- **HP Intelligent Provisioning**—Press **F10** during POST to start HP Intelligent Provisioning. For information about the iLO settings you can configure, see the HP Intelligent Provisioning documentation at the following website: http://www.hp.com/go/intelligentprovisioning/docs.
- **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 a 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 4 Scripting and Command Line Guide*.

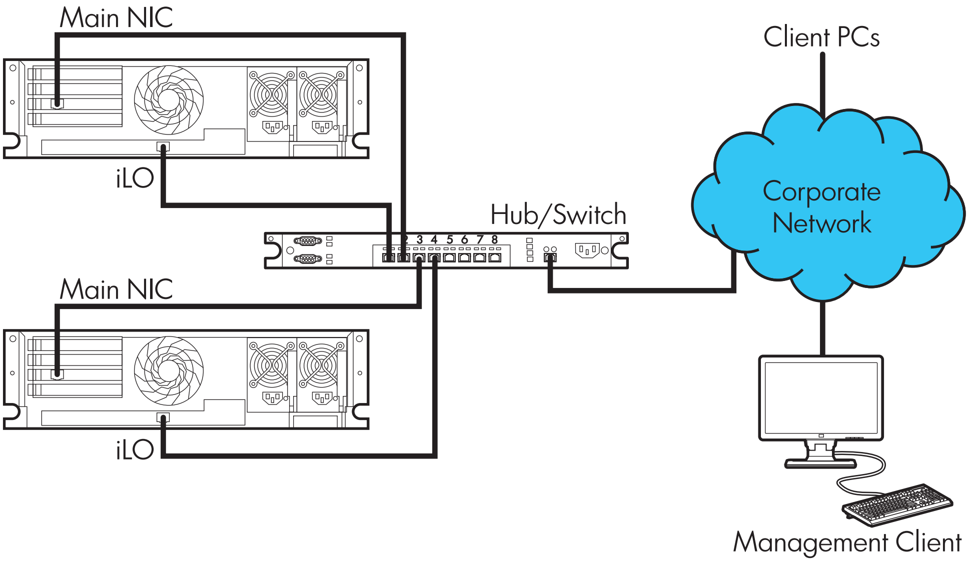
  iLO sample scripts are available at the following website: http://www.hp.com/support/iLO4.

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 20).

Figure 1 Corporate network diagram



- In a **dedicated management network**, the iLO port is on a separate network, as shown in Figure 2 (page 21).

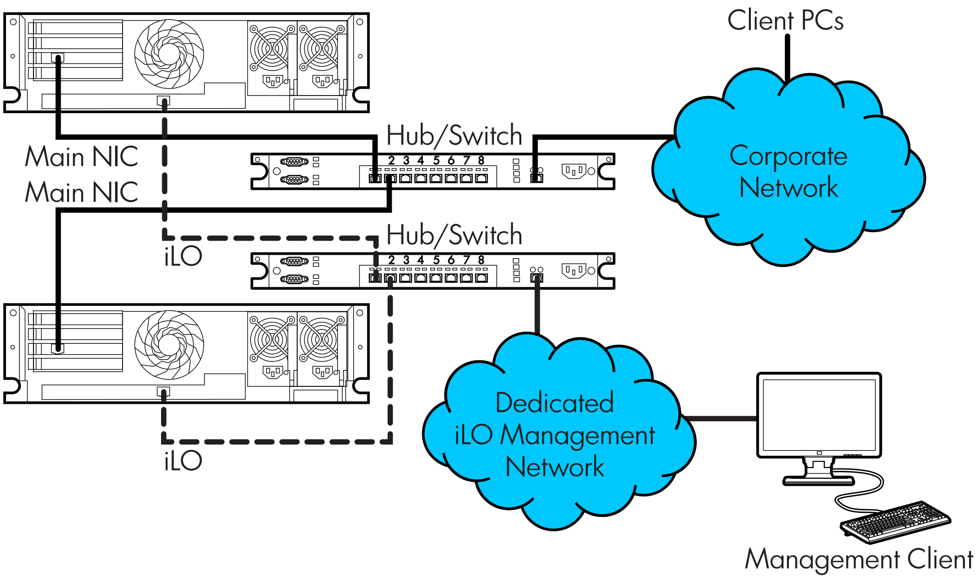


Figure 2 Dedicated management network diagram

Setting up iLO by using iLO RBSU or the iLO 4 Configuration Utility

HP recommends using iLO RBSU or the iLO 4 Configuration Utility to set up iLO for the first time and to configure iLO network parameters for environments that do not use DHCP, DNS, or WINS.

To determine whether your server supports iLO RBSU or the iLO 4 Configuration Utility, see the server QuickSpecs at http://www.hp.com/go/qs/.

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.

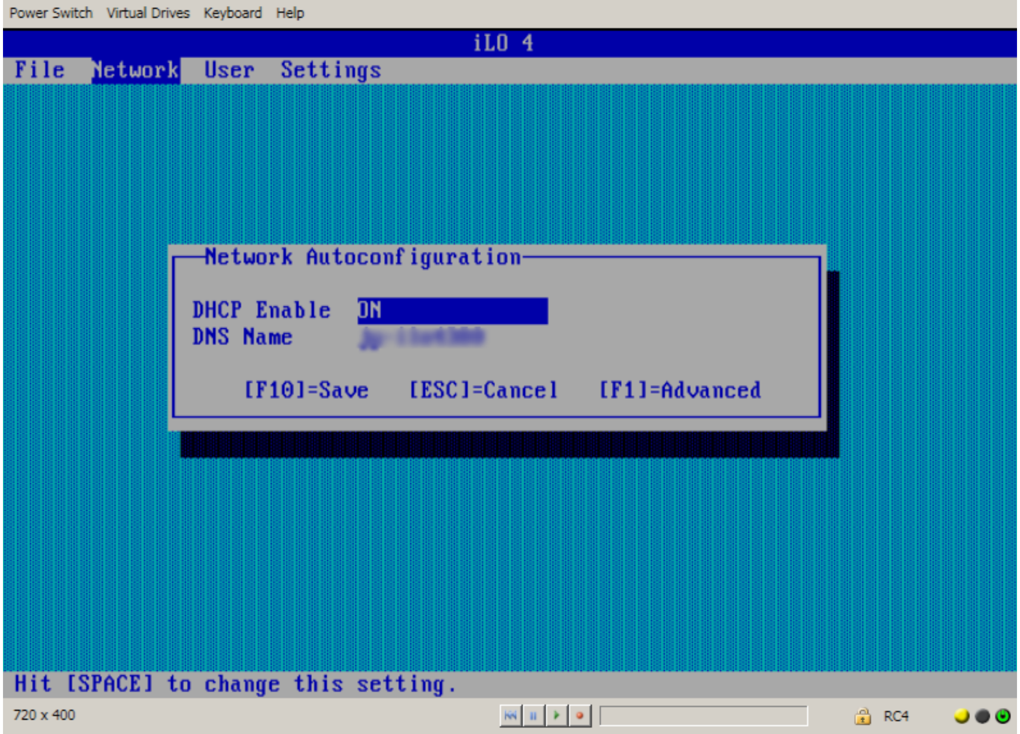
   You can use the .NET IRC or Java IRC.

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**.



Network Autoconfiguration

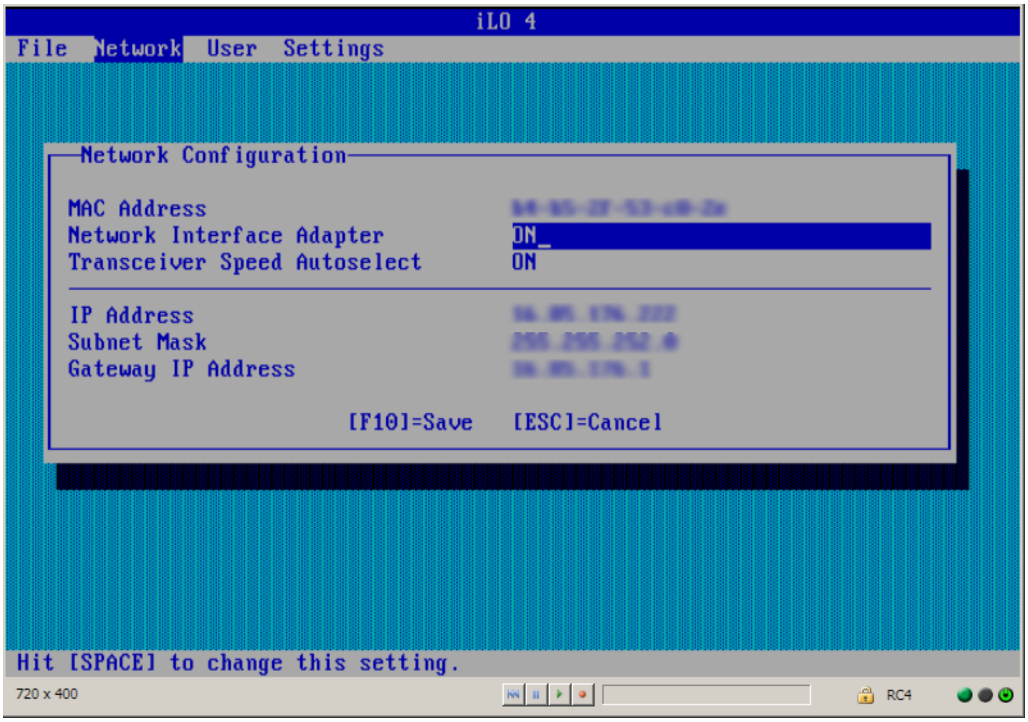
DHCP Enable ON
DNS Name [redacted]

Hit [SPACE] to change this setting.

   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.



```
Network Configuration

MAC Address                    [redacted]
Network Interface Adapter      ON_
Transceiver Speed Autoselect   ON

IP Address                     [redacted]
Subnet Mask                    [redacted]
Gateway IP Address             [redacted]

                 [F10]=Save    [ESC]=Cancel

Hit [SPACE] to change this setting.
```

   c. Press **F10** to save the changes.
6. Select **File→Exit** to exit iLO RBSU.

   The changes take effect when you exit iLO RBSU.

Configuring a static IP address by using the iLO 4 Configuration Utility

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.

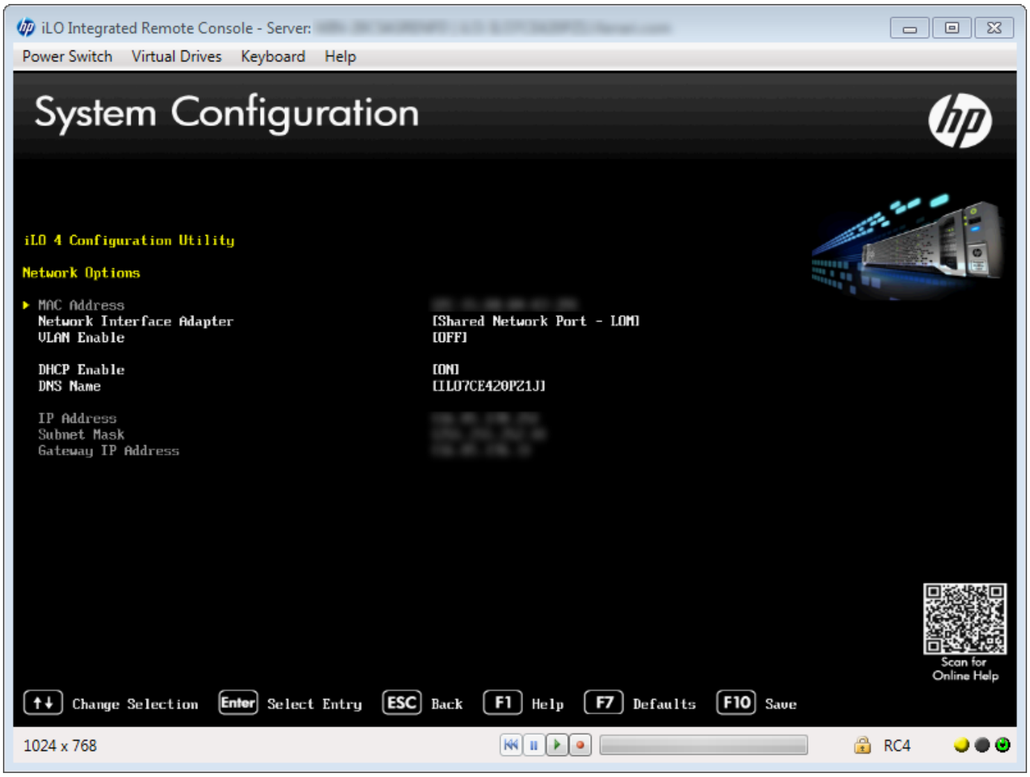
To configure a static IP address:

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 **F9** in the HP ProLiant POST screen.

   The **System Configuration** screen appears.
4. Use the up or down arrow keys and the **Enter** key to navigate to the **System Configuration→iLO 4 Configuration Utility→Network Options** screen.

   The **Network Options** screen appears.



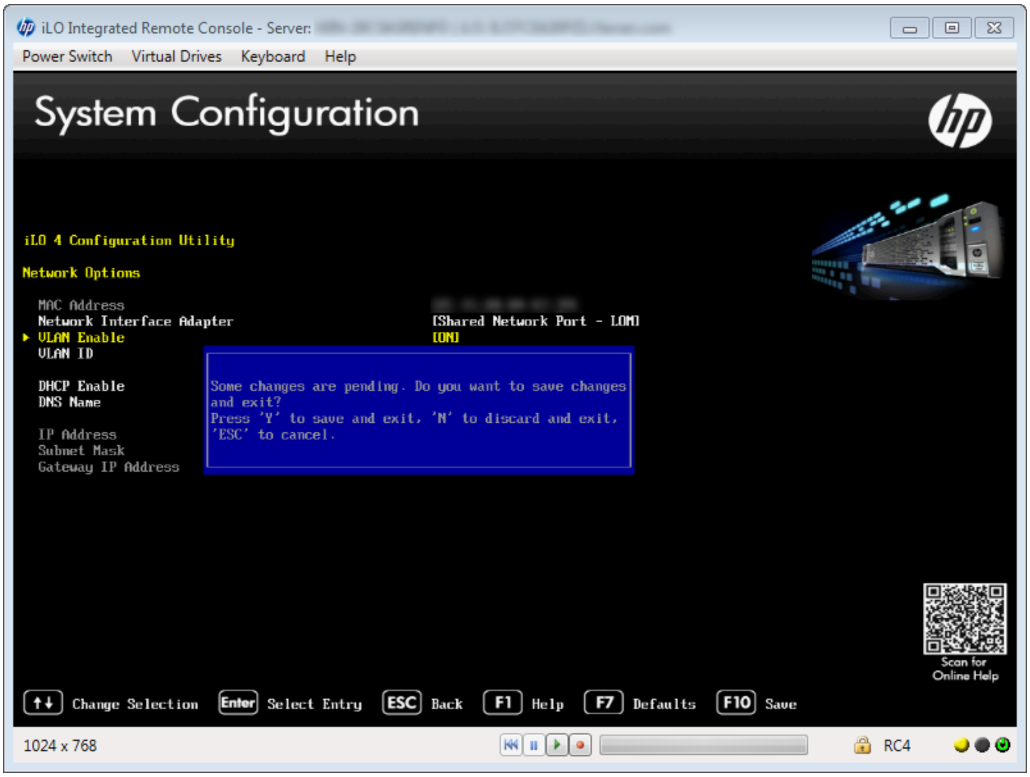
iLO Integrated Remote Console - Server: [redacted]

System Configuration

```
iLO 4 Configuration Utility

Network Options

▸ MAC Address                                      [redacted]
  Network Interface Adapter                        [Shared Network Port - LOM]
  VLAN Enable                                      [OFF]

  DHCP Enable                                      [ON]
  DNS Name                                         [ILO7CE420PZ1J]

  IP Address                                       [redacted]
  Subnet Mask                                      [redacted]
  Gateway IP Address                               [redacted]
```

5. Disable DHCP:
   a. Select **DHCP Enable**, and then press **Enter**.
   b. Select **OFF**, and then press **Enter**.
6. Enter an IP address, subnet mask, and gateway IP address:
   a. Select **IP Address**, and then press **Enter**.
   b. Type the IP address, and then press **Enter**.
   c. Select **Subnet Mask**, and then press **Enter**.
   d. Type the subnet mask address, and then press **Enter**.
   e. Select **Gateway IP Address**, and then press **Enter**.
   f. Type the gateway IP address, and then press **Enter**.
7. Press **F10** to save the changes.

   The iLO 4 Configuration Utility prompts you to confirm that you want to save all pending configuration changes.

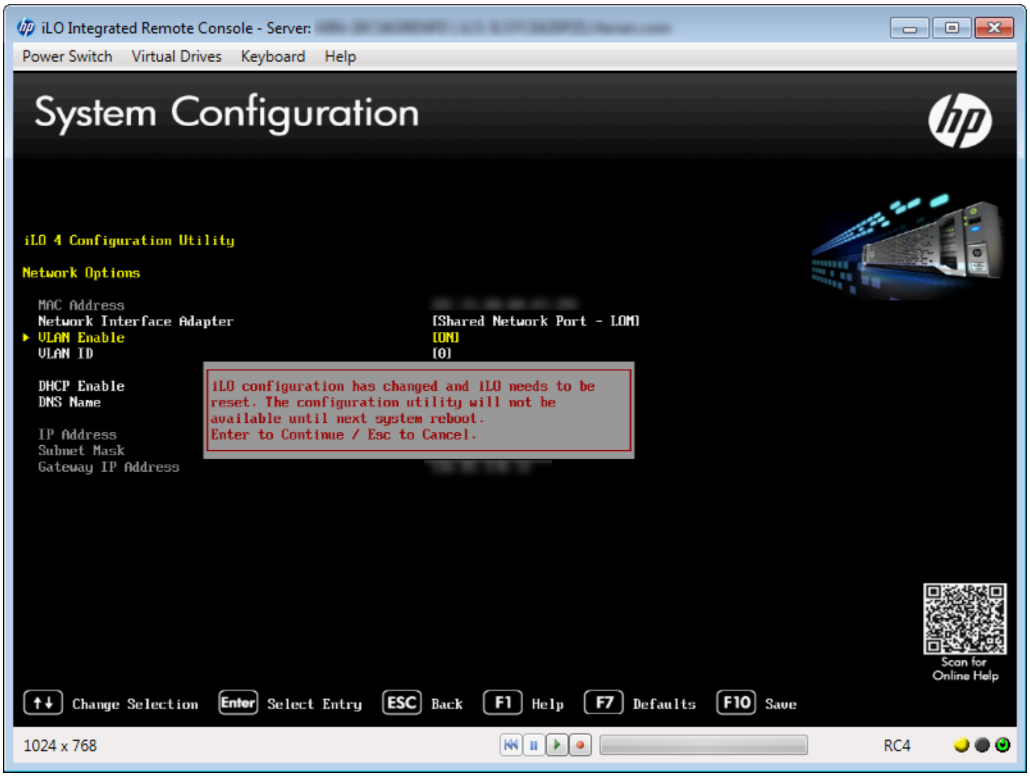


```
iLO 4 Configuration Utility

Network Options

  MAC Address                                   [redacted]
  Network Interface Adapter                     [Shared Network Port - LOM]
▸ VLAN Enable                                   [ON]
  VLAN ID

  DHCP Enable
  DNS Name

  IP Address
  Subnet Mask
  Gateway IP Address
```

```
Some changes are pending. Do you want to save changes
and exit?
Press 'Y' to save and exit, 'N' to discard and exit,
'ESC' to cancel.
```

8. Press **Y** to save and exit.

   The iLO 4 Configuration Utility notifies you that iLO must be reset in order for the changes to take effect.



```
iLO 4 Configuration Utility

Network Options

  MAC Address                                   [redacted]
  Network Interface Adapter                     [Shared Network Port - LOM]
▸ VLAN Enable                                   [ON]
  VLAN ID                                       [0]

  DHCP Enable
  DNS Name

  IP Address
  Subnet Mask
  Gateway IP Address                            [redacted]
```

```
iLO configuration has changed and iLO needs to be
reset. The configuration utility will not be
available until next system reboot.
Enter to Continue / Esc to Cancel.
```

9. Press **Enter**.

   iLO resets, and the iLO session is automatically ended. You can reconnect in approximately 30 seconds.

10. Resume the normal boot process:
    a. Start the iLO remote console.

       The iLO 4 Configuration Utility is still open from the previous session.
    b. Press **ESC** several times to navigate to the **System Configuration** page.
    c. Press **ESC** to exit the System Utilities and resume the normal boot process.

Managing iLO user accounts by using iLO RBSU

You can use iLO RBSU to add, edit, and remove local iLO user accounts.

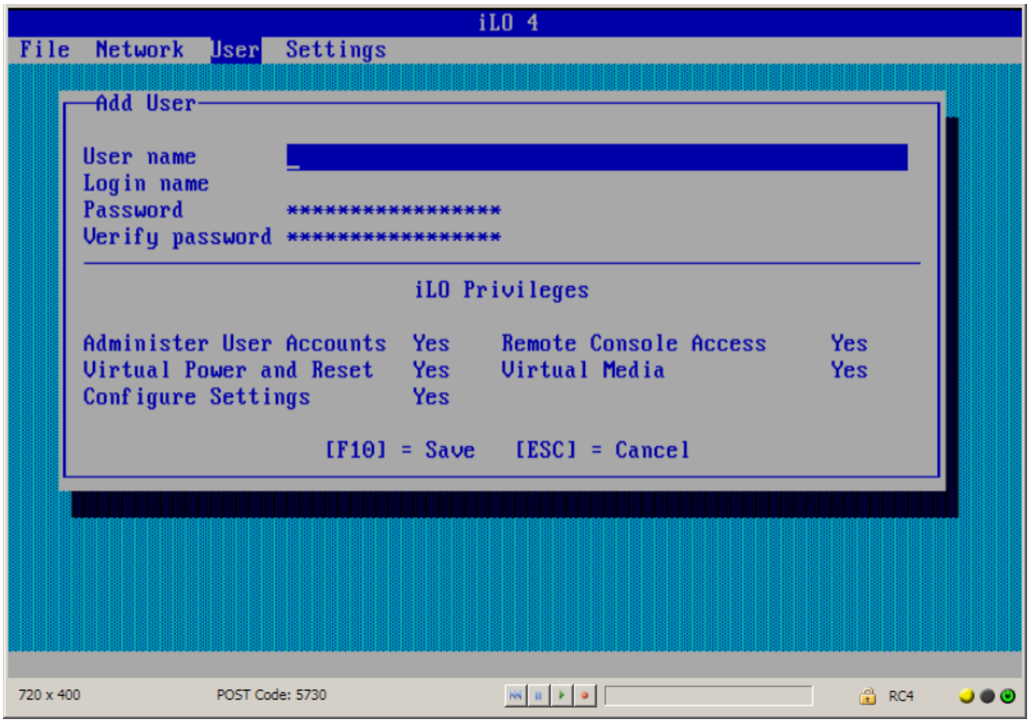
Adding user accounts

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.



```
Add User

User name
Login name
Password          *****************
Verify password   *****************

                    iLO Privileges

Administer User Accounts  Yes    Remote Console Access    Yes
Virtual Power and Reset   Yes    Virtual Media            Yes
Configure Settings        Yes

              [F10] = Save    [ESC] = Cancel
```

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 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, the iLO 4 Configuration Utility, 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

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

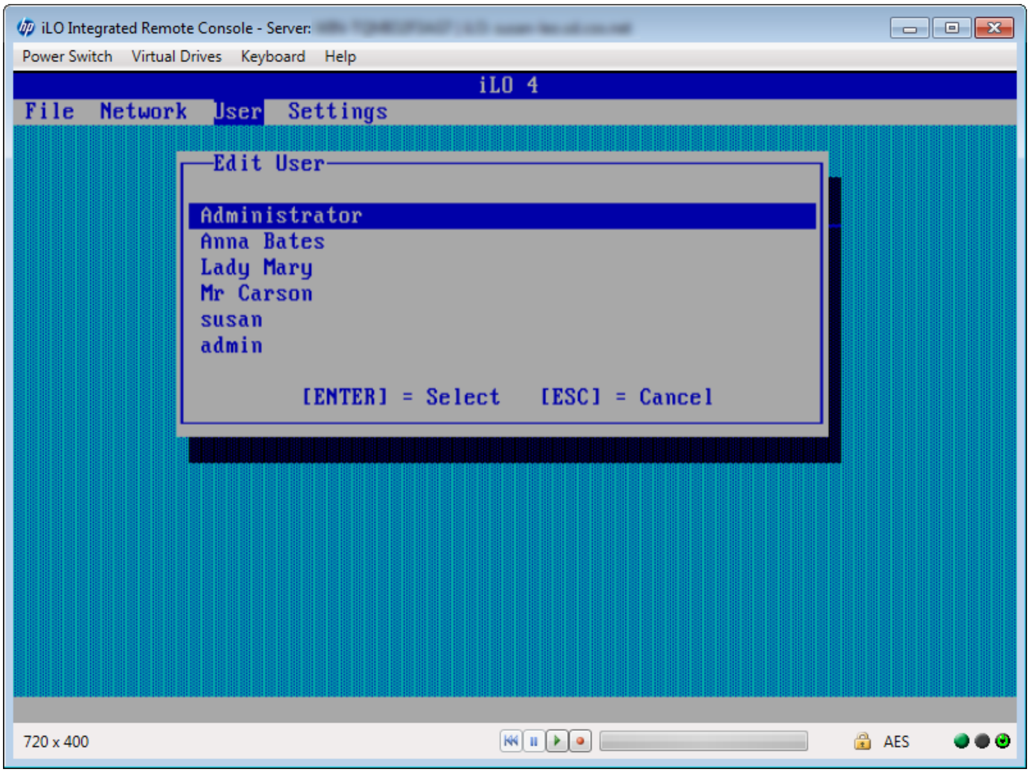
   You can use the .NET IRC or Java IRC.

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.



Edit User

Administrator
Anna Bates
Lady Mary
Mr Carson
susan
admin

[ENTER] = Select   [ESC] = Cancel

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.

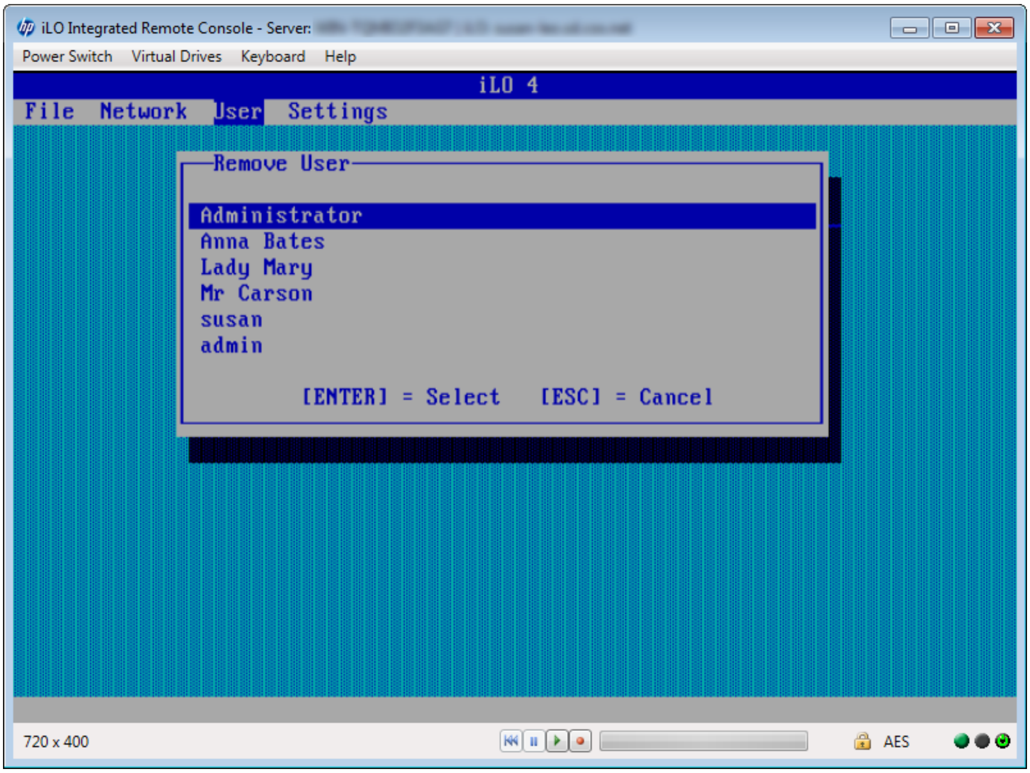
Removing user accounts

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.



```
Remove User

Administrator
Anna Bates
Lady Mary
Mr Carson
susan
admin

[ENTER] = Select    [ESC] = Cancel
```

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.

Managing iLO user accounts by using the iLO 4 Configuration Utility

You can use the iLO 4 Configuration Utility to add, edit, and remove local iLO user accounts.

Adding user accounts

You can use the iLO 4 Configuration Utility **User Management** menu to configure local iLO user accounts.

To add local iLO user accounts:

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

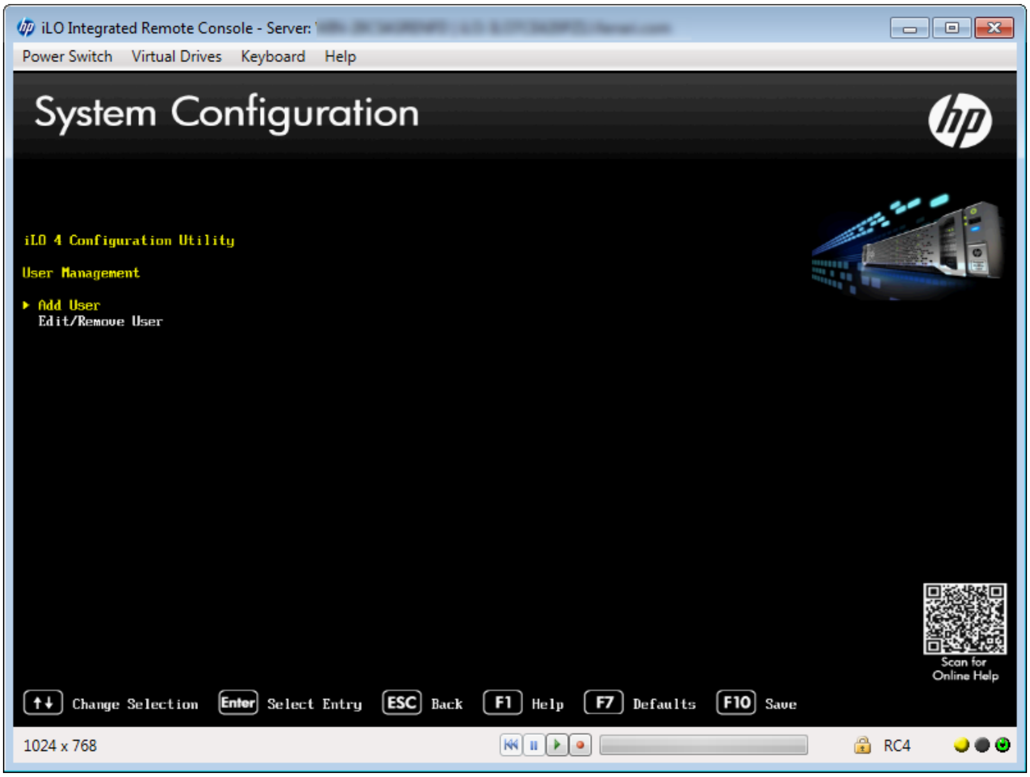
   You can use the .NET IRC or Java IRC.

2. Restart or power on the server.
3. Press **F9** in the HP ProLiant POST screen.

   The **System Utilities** screen appears.

4. From the **System Utilities** screen, select **System Configuration**→**iLO 4 Configuration Utility**→**User Management**.

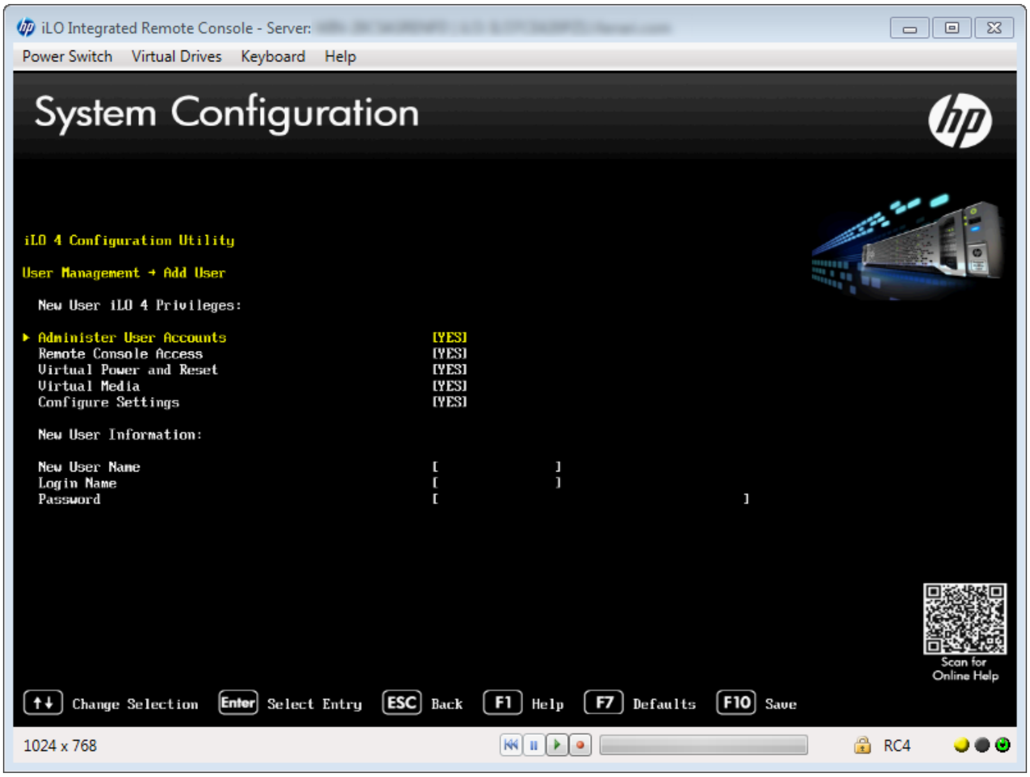
   The **User Management** screen appears.



```
System Configuration

iLO 4 Configuration Utility

User Management

▸ Add User
  Edit/Remove User

↑↓ Change Selection   Enter Select Entry   ESC Back   F1 Help   F7 Defaults   F10 Save
```

5. Select **Add User**, and then press **Enter**.

   The **User Management→Add User** screen appears.



```
System Configuration

iLO 4 Configuration Utility

User Management → Add User

  New User iLO 4 Privileges:

▸ Administer User Accounts                    [YES]
  Remote Console Access                       [YES]
  Virtual Power and Reset                     [YES]
  Virtual Media                               [YES]
  Configure Settings                          [YES]

  New User Information:

  New User Name                               [               ]
  Login Name                                  [               ]
  Password                                    [                                      ]

↑↓ Change Selection   Enter Select Entry   ESC Back   F1 Help   F7 Defaults   F10 Save
```

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 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, the iLO 4 Configuration Utility, or HPONCFG can still reconfigure iLO. Only a user who has the Administer User Accounts privilege can enable or disable this privilege.
7. Enter the following user account details:
   - **New 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 **Password Confirm** 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.
8. Create as many user accounts as needed, and then press **F10** to save the changes.
9. Press **Esc** until the main menu is displayed.
10. Select **Exit and Resume Boot** in the main menu, and then press **Enter**.
11. When prompted to confirm the request, press **Enter** to exit the utility and resume the boot process.

Editing or removing user accounts

You can use the iLO 4 Configuration Utility **User Management** menu to edit or remove local iLO user accounts.

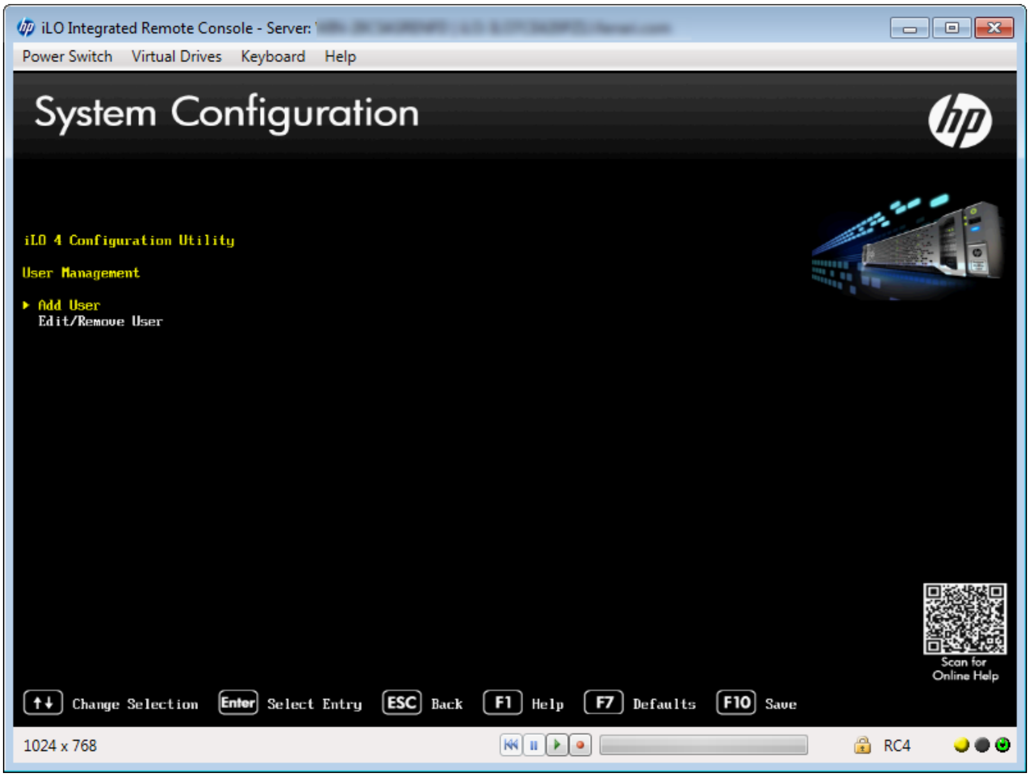
To edit or remove a local iLO user account:

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 **F9** in the HP ProLiant POST screen.

   The **System Utilities** screen appears.
4. From the **System Utilities** screen, select **System Configuration→iLO 4 Configuration Utility→User Management**.

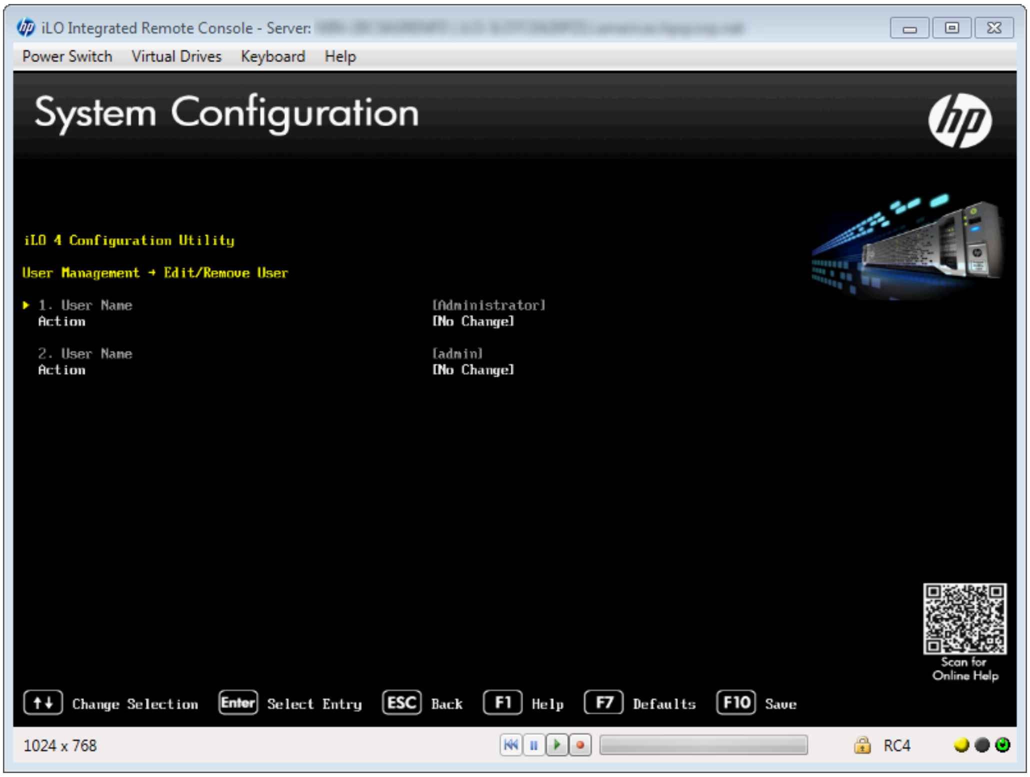
   The **User Management** screen appears.



```
iLO 4 Configuration Utility

User Management

▸ Add User
  Edit/Remove User
```

5. Select **Edit/Remove User**, and then press **Enter**.

   The **User Management→Edit/Remove User** screen appears.



```
iLO 4 Configuration Utility

User Management → Edit/Remove User

▸ 1. User Name                                    [Administrator]
  Action                                          [No Change]

  2. User Name                                    [admin]
  Action                                          [No Change]
```

6. Locate the user name that you want to edit or delete, select the **Action** menu for that user name, and then press **Enter**.

7. Select one of the following, and then press **Enter**.
   - **No Change**—Returns you to the main menu.
   - **Delete**—Deletes this user.
   - **Edit**—Edits the user.
8. Depending on your selection in Step 7, do one of the following:
   - If you selected **No Change**, no further action is needed.
   - If you selected **Delete**, the user name is marked to be deleted when you save the changes on this page.
   - If you selected **Edit**, update the login name, password, or user permissions.
9. Update as many user accounts as needed, and then press **F10** to save the changes.
10. Press **Esc** until the main menu is displayed.
11. Select **Exit and Resume Boot** in the main menu, and then press **Enter**.
12. When prompted to confirm the request, press **Enter** to exit the utility and resume the boot process.

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 33).

For information about the configuration procedures available in the iLO web interface, see "Configuring iLO" (page 37).

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 label 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.

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 66).

IMPORTANT: HP recommends changing the default password after you log in to iLO for the first time. For instructions, see "Managing iLO users by using the iLO web interface" (page 46).

If you reset iLO to the factory default settings, use the default iLO account information to log in after the reset.

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 "Installing an iLO license by using a browser" (page 45).

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 Agentless Management Service 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 (Windows, Red Hat, and SLES) and the HP website (Windows, Linux, and VMware).

- **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 following website: http://www.hp.com/support.
  2. Select a country or region and a language.

     The **HP Support** page opens.
  3. Click **Drivers & Downloads**.
  4. In the **Find my product** box, enter the server model number, and then click **Go**.

     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.
- **For Ubuntu**—Download the iLO drivers from the **mcp** section of the Software Delivery Repository 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 34)
- “Linux device driver support” (page 35)
- “VMware device driver support” (page 35)

Microsoft device driver support

When you use 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 106).

Linux device driver support

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

- **HP ProLiant Channel Interface KMOD** (`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.

Loading and removing SLES and Red Hat drivers:

ⓘ **IMPORTANT:** These drivers are standard for SUSE Linux Enterprise Server 11 and 12 and Red Hat 6 and 7.

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
```

Loading and removing Ubuntu drivers:

HP recommends subscribing to the Management Component Pack repository to ensure that your Ubuntu systems have the latest HP software.

ⓘ **IMPORTANT:** 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 procedure to load the HP System Health Application and Command Line Utilities:

1. Subscribe to the MCP.

   For instructions, see the following HP website: http://downloads.linux.hp.com/SDR/project/mcp/.
2. Enter the following command to update the repository cache: `apt-get update`.
3. Enter the following command to install the HP System Health Application and Command Line Utilities: `apt-get install hp-health`.

Use the following command to remove the HP System Health Application and Command Line Utilities:

```
apt-get remove hp-health
```

VMware device driver support

When you use 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

This chapter includes procedures for configuring iLO by using the iLO web interface and the ROM-based setup utilities.

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 4 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 server and iLO functionality with new features, improvements, and security updates.

You can update firmware by using the following methods:

- **Online firmware update**—When you use an online method to update firmware, you can perform the update without shutting down the server operating system. Online firmware updates can be performed in-band or out-of-band.
  - **In-band**—Firmware is sent to iLO from the server host operating system. The HP ProLiant Channel Interface Driver is required for in-band firmware updates. During a host-based firmware update, iLO does not verify login credentials or user privileges because the host-based utilities require a root login (Linux and VMware) or Administrator login (Windows).
  - **Out-of-band**—Firmware is sent to iLO over a network connection. Users with the Configure iLO Settings privilege can update firmware by using an out-of-band method. If the system maintenance switch is set to disable iLO security, any user can update firmware with an out-of-band method.

  For more information, see "Updating firmware by using an online method" (page 37).
- **Offline firmware update**—When you use an offline method to update the firmware, you must reboot the server by using an offline utility.

  For more information, see "Updating firmware by using an offline method" (page 38).

The following firmware types can be updated from the **Firmware Update** page:

- iLO firmware
- HP ProLiant System ROM (BIOS)
- SL Chassis Firmware (Power Management)
- Power Management Controller
- System Programmable Logic Device (CPLD)

Updating firmware by using an online method

Performing an in-band firmware update

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

- **Online ROM Flash Component**—Use an executable file to update firmware while the server is running. The executable file contains the installer and the firmware package. You can download online ROM flash components for iLO and HP ProLiant servers at the following HP website: http://www.hp.com/support/ilo4.

- **HPONCFG**—Use the HP Lights-Out Online Configuration Utility to update firmware by using XML scripts. Download the iLO or server 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/ilo4. For more information about scripting, see the *HP iLO 4 Scripting and Command Line Guide*.

  For instructions about obtaining firmware images, see "Obtaining the iLO firmware image file" (page 38) and "Obtaining supported server firmware image files" (page 39).

Performing an out-of-band firmware update

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

- **iLO web interface**—Download a supported firmware file and install it by using the iLO web interface. You can update firmware for a single server or an iLO Federation group. For instructions, see "Updating firmware by using a browser" (page 39) or "Using the iLO Federation Group Firmware Update feature" (page 194).
- **HPQLOCFG**—Use the HP Lights-Out Configuration Utility to update firmware by using XML scripts. Download the iLO or server 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/ilo4. For more information about scripting, see the *HP iLO 4 Scripting and Command Line Guide*.

  For instructions about obtaining the iLO firmware image, see "Obtaining the iLO firmware image file" (page 38).
- **HPLOMIG** (also called HP Directories Support for Management Processors)—You do not need to use directory integration to take advantage of the firmware update capabilities in HPLOMIG. 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. For more information, see "Upgrading firmware on management processors" (page 295).
- **SMASH CLP**—Access SMASH CLP through the SSH port, and use standard commands to view firmware information and update firmware.

  For more information about SMASH CLP, see the *HP iLO 4 Scripting and Command Line Guide*.

Updating firmware by using an offline method

You can use the following offline firmware update methods:

- **HP Service Pack for ProLiant**—Use the HP Service Pack for ProLiant to install firmware. 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 HP Support Center website: http://www.hp.com/go/hpsc.

2. In the **Enter a product name or number** box, enter the server model number, and then click **Go**.
3. The HP Support Center page for the server opens.
4. Click the **Drivers, Software & Firmware** link.

   A list of operating systems is displayed.
5. Click the link for the server operating system.
6. Follow the onscreen instructions to download the iLO Online ROM Flash Component file.
7. Double-click the downloaded file, and then click the **Extract** button.
8. Select a location for the extracted files, and then click **OK**.

   The name of the iLO firmware image file is similar to `ilo4_<yyy>.bin`, where `<yyy>` represents the firmware version.

Obtaining supported server firmware image files

To obtain the system ROM, Power Management Controller, and SL Chassis Manager firmware image files:

1. Navigate to the HP Support Center website: http://www.hp.com/go/hpsc.
2. In the **Enter a product name or number** box, enter the server model number, and then click **Go**.
3. The HP Support Center page for the server opens.
4. Click the **drivers, software & firmware** link.

   A list of operating systems is displayed.
5. Click the link for the server operating system.
6. Follow the onscreen instructions to download an Online ROM Flash Component file.
7. Double-click the downloaded file, and then click the **Extract** button.
8. Select a location for the extracted files, and then click **OK**.
   - The system ROM firmware image file name uses a format similar to the following: `CPQJ0123.B18`.
   - The Power Management Controller and SL Chassis Manager firmware files use the file extension `.hex`. For example, the file name might be similar to `ABCD5S95.hex`.
   - The System Programmable Logic Device (CPLD) firmware file uses the file extension `.vme`.

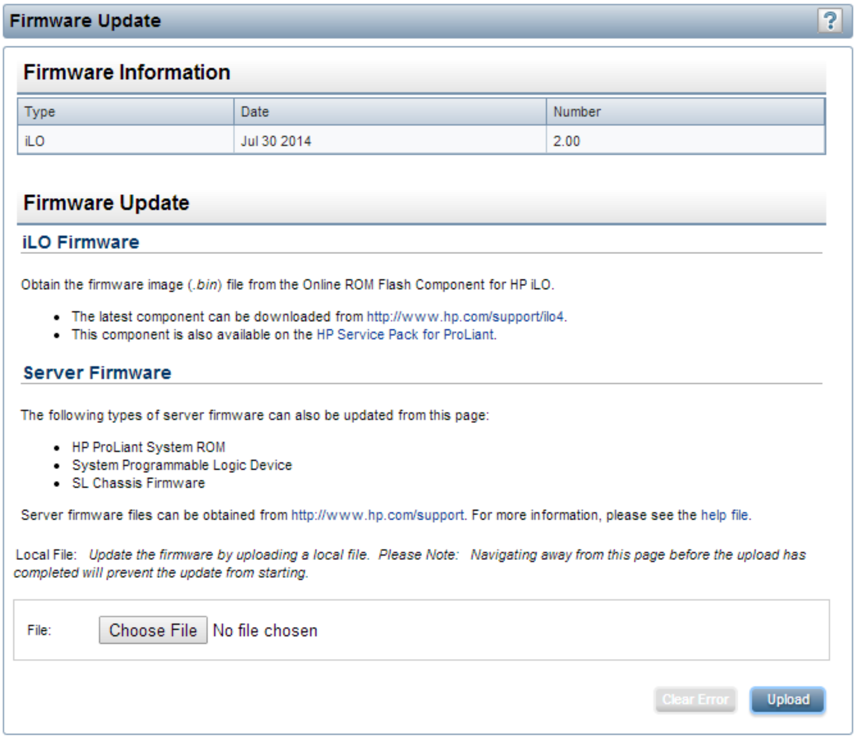
Updating firmware by using a browser

You can update firmware from any network client by using a supported browser. For a list of supported browsers, see "Using the iLO web interface" (page 146).

To update the server or iLO firmware:

1. Obtain the firmware image file. For instructions, see "Obtaining the iLO firmware image file" (page 38) or "Obtaining supported server firmware image files" (page 39).
2. Navigate to the **Administration→Firmware** page.

   The **Firmware Update** page opens.



Firmware Update

Firmware Information

Type	Date	Number
iLO	Jul 30 2014	2.00

Firmware Update

iLO Firmware

Obtain the firmware image (*.bin*) file from the Online ROM Flash Component for HP iLO.

- The latest component can be downloaded from http://www.hp.com/support/ilo4.
- This component is also available on the HP Service Pack for ProLiant.

Server Firmware

The following types of server firmware can also be updated from this page:

- HP ProLiant System ROM
- System Programmable Logic Device
- SL Chassis Firmware

Server firmware files can be obtained from http://www.hp.com/support. For more information, please see the help file.

Local File: *Update the firmware by uploading a local file. Please Note: Navigating away from this page before the upload has completed will prevent the update from starting.*

File: Choose File No file chosen

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 following message appears:

   ```
   Updating the iLO firmware will cause the iLO to reboot. This will
   terminate any connections to the iLO including Remote Console and
   Virtual Media. Updating other types of firmware might not cause iLO
   to reboot, but they might require a server reboot. The server will
   not reboot automatically.
   ```
5. Click **OK**.

   The iLO firmware receives, validates, and then flashes the firmware image.

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

IMPORTANT: Do not interrupt a firmware update. If a firmware update is interrupted or fails, attempt it again immediately.

6. For iLO firmware updates only: To start working with the new firmware, clear your browser cache, and then log in to iLO.

7. For server firmware updates only: For the new firmware to take effect, some types of firmware updates require an iLO reset, a system reset, or a server reboot. The requirements for each firmware type follow:
   - HP ProLiant System ROM (BIOS)—Requires a server reboot.
   - SL Chassis Firmware (Power Management)—Requires an SL Chassis reset, which is triggered automatically.
   - Power Management Controller—Does not require an iLO reset or server reboot.
   - System Programmable Logic Device (CPLD)—Requires a server reboot.

TIP: To confirm that the new firmware is active, check the version on the **System Information→Firmware** page.

If an error occurs during an iLO firmware update, see "Unable to upgrade iLO firmware" (page 333).

If an iLO firmware update is corrupted or canceled, and iLO is corrupted, see "iLO network Failed Flash Recovery" (page 334).

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:

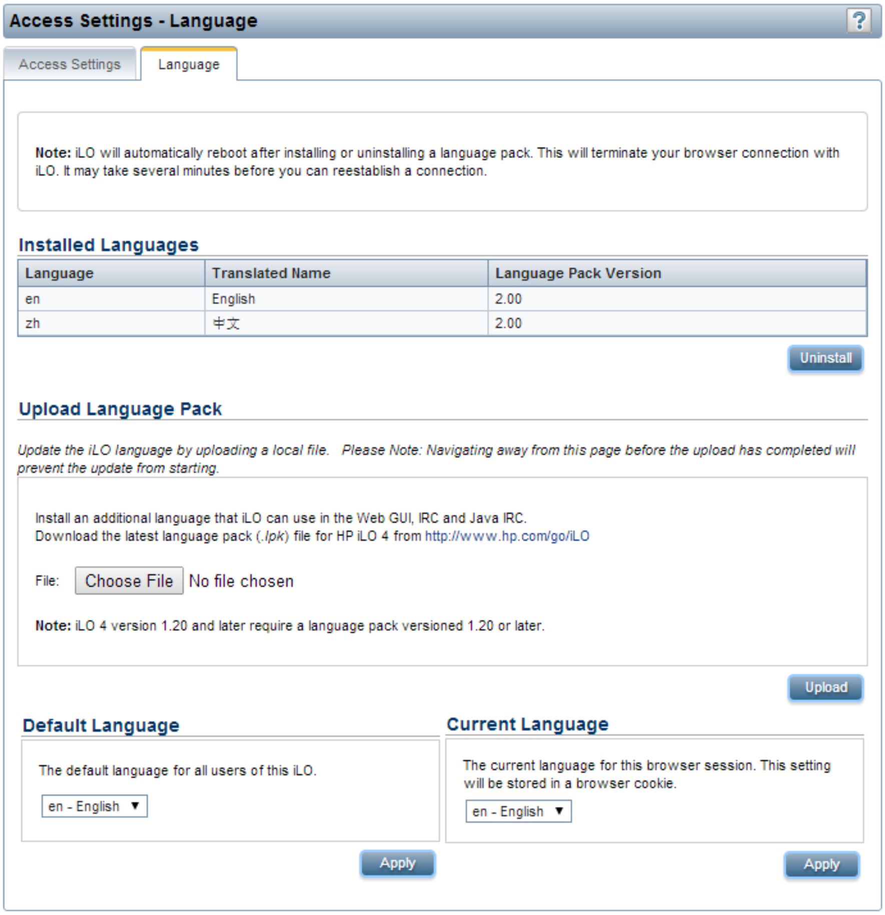
- You must have the Configure iLO Settings privilege to install a language pack.
- You can install only one language pack. Uploading a new language pack replaces the currently installed language pack, regardless of the language pack version.
- The language pack firmware is independent of the iLO firmware. 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 4 firmware version 1.20 or later requires version 1.20 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 43).

Installing a language pack

1. Navigate to the following website: http://www.hp.com/support/ilo4.
2. Download the language pack to your local computer.
3. Navigate to the **Administration→Access Settings→Language** page.



Note: iLO will automatically reboot after installing or uninstalling a language pack. This will terminate your browser connection with iLO. It may take several minutes before you can reestablish a connection.

Installed Languages

Language	Translated Name	Language Pack Version
en	English	2.00
zh	中文	2.00

Upload Language Pack

Update the iLO language by uploading a local file.   Please Note: Navigating away from this page before the upload has completed will prevent the update from starting.

Install an additional language that iLO can use in the Web GUI, IRC and Java IRC.
Download the latest language pack (*.lpk*) file for HP iLO 4 from http://www.hp.com/go/iLO

File: Choose File No file chosen

Note: iLO 4 version 1.20 and later require a language pack versioned 1.20 or later.

Default Language

The default language for all users of this iLO.

en - English ▼

Current Language

The current language for this browser session. This setting will be stored in a browser cookie.

en - English ▼

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**.

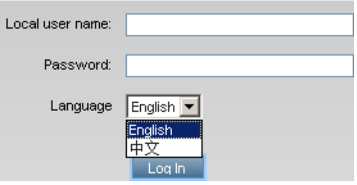
   iLO will automatically reboot after installing a language pack. This will end your browser connection with iLO.

   It might take several minutes before you can re-establish a connection.

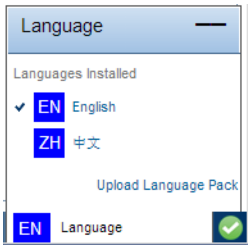
Selecting a language pack

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

- From the login page.



- From the toolbar located on the bottom right side of the iLO web interface.



- From the **Administration**→**Access Settings**→**Language** page. For instructions, see "Configuring the current language settings" (page 43).

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.
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**.

   The following message appears:

   ```
   Default language changed.
   ```

   In subsequent iLO web interface sessions, if there is no browser cookie from a previous session, and the browser or OS language is not supported, the iLO web interface uses the configured default language.

Configuring the current language settings

To set the language of the current browser session:

1. Navigate to the **Administration**→**Access Settings**→**Language** page.
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**.

   The iLO web interface for the current browser session changes to the language selected in Step 2.

Uninstalling a language pack

1. Navigate to the **Administration**→**Access Settings**→**Language** page.

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.

   It might take several minutes before you can re-establish a connection.

iLO licensing

HP iLO standard features are included with every HP ProLiant server to simplify server setup, perform health monitoring, monitor power and thermal control, and facilitate remote administration.

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

To unlock iLO licensed features, simply choose and install the license that best suits your company's infrastructure.

The following license types are available:

- **iLO Advanced**—Enables the full set of iLO features. iLO Advanced is available for all HP ProLiant Gen8 and Gen9 servers.
  - iLO Advanced Single Server License
  - iLO Advanced Electronic License
  - iLO Advanced Flexible Quantity License
  - iLO Advanced Volume License
- **iLO Essentials**—Enables the iLO Integrated Remote Console, Virtual Media, and email alerts. iLO Essentials is available on all HP ProLiant Gen8 e-series servers, Microservers, and Gen9 100 series and lower series.
- **iLO Scale-Out**—Enables the following iLO remote management features: Textcons, Power Management, Virtual Serial Port log, email alerts, and Remote Syslog. iLO Scale-Out is available on all HP ProLiant Gen8 and Gen9 SL and BL servers.

For information about 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 342).

Consider the following about iLO licenses:

- You must have the Configure iLO Settings privilege to install a license.
- 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 342).
- 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 339).
- 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:

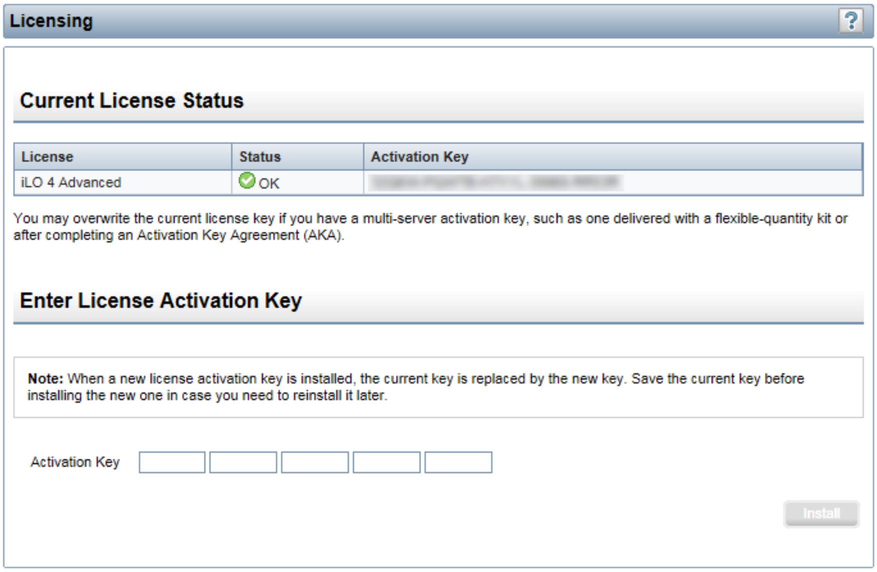
- The evaluation license activates and enables access to iLO licensed features.
- The evaluation license key is a 10-seat key, meaning it can be used on 10 different servers.
- When the evaluation period has expired, your iLO system will return to the standard functionality.
- Only one evaluation license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

   The **Licensing** page opens.



Licensing

Current License Status

License	Status	Activation Key
iLO 4 Advanced	✓ OK	[redacted]

You may overwrite the current license key if you have a multi-server activation key, such as one delivered with a flexible-quantity kit or after completing an Activation Key Agreement (AKA).

Enter License Activation Key

Note: When a new license activation key is installed, the current key is replaced by the new key. Save the current key before installing the new one in case you need to reinstall it later.

Activation Key

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

   Press the **Tab** key or click inside a segment of the **Activation Key** box to move between segments. The cursor advances automatically when you enter data into the segments of the **Activation Key** box.
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 321).

Viewing installed licenses

To view information about installed licenses, navigate to the **Administration**→**Licensing** page.

The following information is displayed for each installed license:

- **License**—The license name
- **Status**—The license status
- **Activation Key**—The installed key

Managing iLO users by using the iLO web interface

The iLO 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.

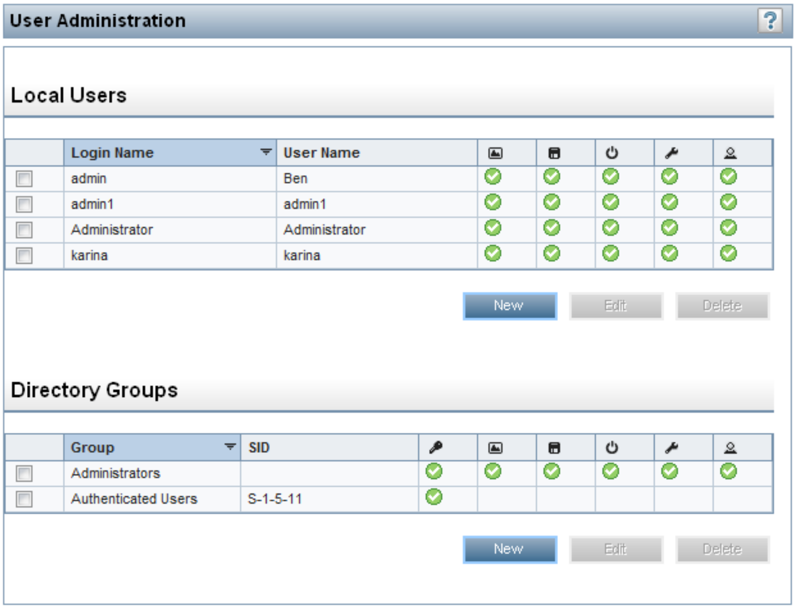
The following privileges are required for user and directory group administration:

- **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 user accounts by using iLO RBSU" (page 26).

Viewing local user accounts

To view local users, navigate to the **Administration**→**User Administration** page.



User Administration

Local Users

☐	Login Name	User Name	🖥	💾	⏻	🔧	👤
☐	admin	Ben	✓	✓	✓	✓	✓
☐	admin1	admin1	✓	✓	✓	✓	✓
☐	Administrator	Administrator	✓	✓	✓	✓	✓
☐	karina	karina	✓	✓	✓	✓	✓

Directory Groups

☐	Group	SID	🔑	🖥	💾	⏻	🔧	👤
☐	Administrators		✓	✓	✓	✓	✓	✓
☐	Authenticated Users	S-1-5-11	✓					

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 with the web interface, HPQLOCFG, or the CLI. Users who have access to iLO RBSU, the UEFI System Utilities, or 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.

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 with the web interface, HPQLOCFG, or the CLI. Users who have access to iLO RBSU, the UEFI System Utilities, or 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.

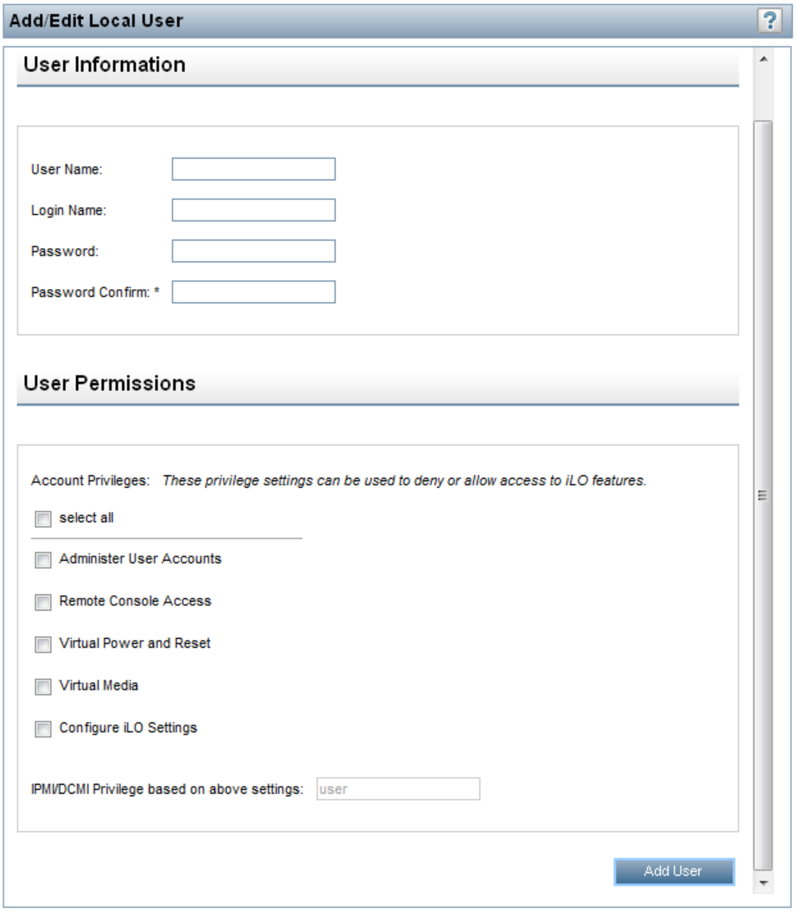
Adding or editing local user accounts

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

To add or edit a local user account:

1. Navigate to the **Administration→User Administration** page.
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.



Add/Edit Local User

User Information

User Name:

Login Name:

Password:

Password Confirm: *

User Permissions

Account Privileges: *These privilege settings can be used to deny or allow access to iLO features.*

□ select all

□ Administer User Accounts

□ Remote Console Access

□ Virtual Power and Reset

□ Virtual Media

□ Configure iLO Settings

IPMI/DCMI Privilege based on above settings: user

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 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. The maximum length for a password is 39 characters. Enter the password twice for verification.

  For more information about passwords, see "Password guidelines" (page 49).

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 46).
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 59).

IPMI/DCMI users

The iLO firmware follows the IPMI 2.0 specification. When you add 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.

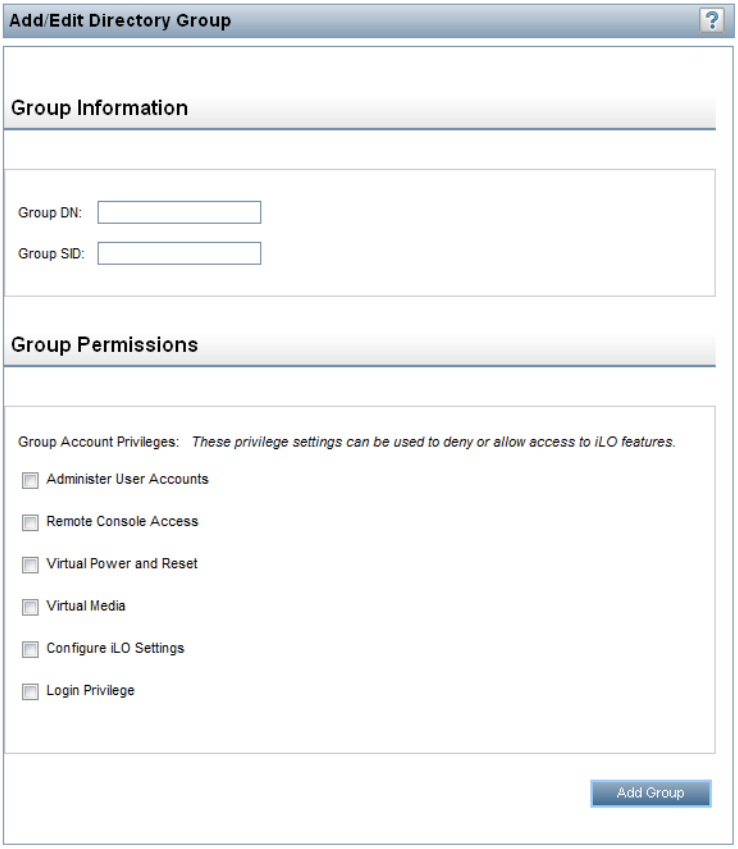
Administering directory groups

iLO enables you to view iLO directory 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.
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.



Add/Edit Directory Group

Group Information

Group DN:

Group SID:

Group Permissions

Group Account Privileges: *These privilege settings can be used to deny or allow access to iLO features.*

□ Administer User Accounts

□ Remote Console Access

□ Virtual Power and Reset

□ Virtual Media

□ Configure iLO Settings

□ Login Privilege

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. 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 add or edit 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 47).
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.
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 Federation

iLO uses multicast discovery, peer-to-peer communication, and iLO Federation groups to communicate with other iLO systems.

When data is loaded on an iLO Federation page in the iLO web interface, a request for data is sent from the iLO system running the web interface to its peers, and from those peers to other peers until all of the data for the selected iLO Federation group is retrieved.

iLO Federation network requirements

When you use iLO Federation, note the following network requirements:

- The iLO Federation features are not supported by the iLO Shared Network Port configuration.
- iLO Federation supports both IPv4 and IPv6.

  To force an iLO system to use IPv4 instead of IPv6, clear the **iLO Client Applications use IPv6 first** check box on the **Network→iLO Dedicated Network Port→IPv6** page.
- You can manage iLO systems in multiple locations if the network is configured to forward multicast traffic.
- If the switches in your network include the option to enable or disable multicast traffic, ensure that multicast traffic is enabled. This is required for iLO Federation and other HP products to discover the iLO systems on the network.
- For iLO systems that are separated by Layer 3 switches, configure the switches to forward SSDP multicast traffic between networks.
- You must configure UDP port 1900 as a firewall exception to allow iLO Federation multicast traffic.
- If you want to use server blades in an enclosure with iLO Federation, you must configure Enclosure iLO Federation Support in the Onboard Administrator web interface. This feature is supported in Onboard Administrator 4.11 or later. For more information, see the *HP iLO Federation User Guide*.
- For networks with multiple VLANs, configure the switches to allow multicast traffic between the VLANs.
  - For IPv4 networks: Enable PIM on the switch and configure it for PIM Dense Mode.
  - For IPv6 networks: Configure the switch for MLD snooping.

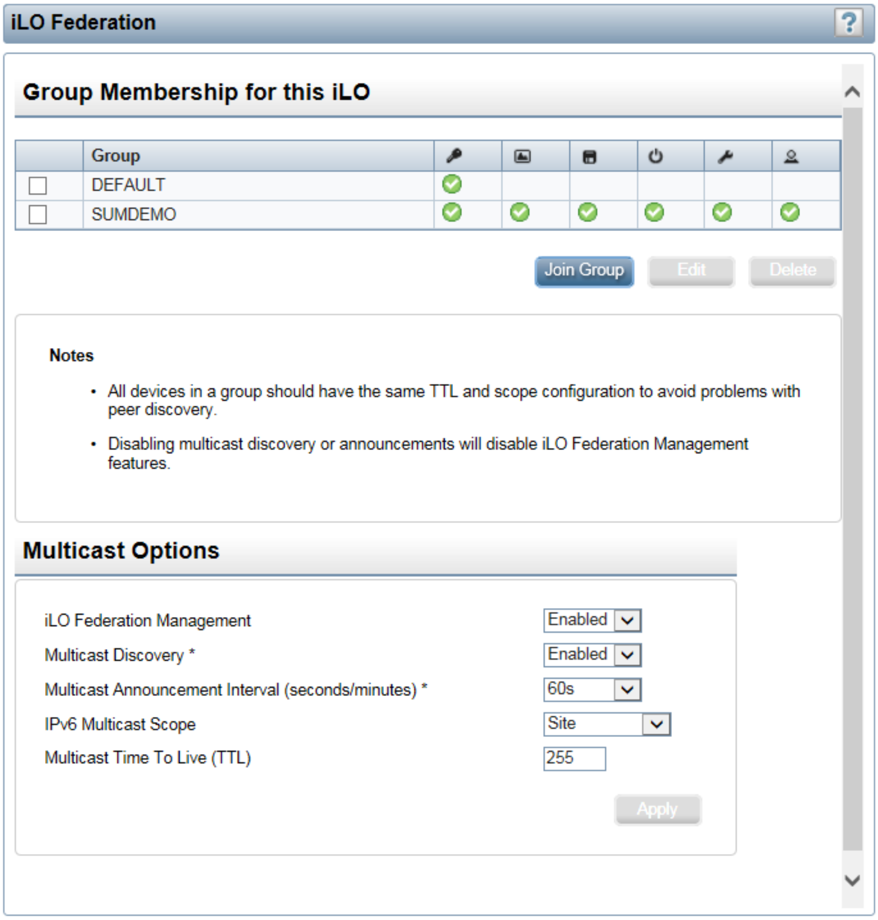
Configuring the multicast options

You must configure the multicast options for each iLO system that will be added to an iLO Federation group.

Use the following procedure to configure multicast options for one iLO system at a time. To use RIBCL scripts to view and configure multicast options for multiple iLO systems, see the *HP iLO 4 Scripting and Command Line Guide*.

You must have the Configure iLO Settings privilege to configure the multicast options.

1. Navigate to the **Administration→iLO Federation** page.



iLO Federation

Group Membership for this iLO

	Group	🔑	🖥	💾	⏻	🔧	👤
□	DEFAULT	✓					
□	SUMDEMO	✓	✓	✓	✓	✓	✓

Notes

- All devices in a group should have the same TTL and scope configuration to avoid problems with peer discovery.
- Disabling multicast discovery or announcements will disable iLO Federation Management features.

Multicast Options

iLO Federation Management	Enabled
Multicast Discovery *	Enabled
Multicast Announcement Interval (seconds/minutes) *	60s
IPv6 Multicast Scope	Site
Multicast Time To Live (TTL)	255

2. For **iLO Federation Management**, select **Enabled** or **Disabled**.

   The default setting is **Enabled**. Selecting **Disabled** disables the iLO Federation features for the local iLO system.

3. For **Multicast Discovery**, select **Enabled** or **Disabled**.

   Selecting **Disabled** disables the iLO Federation features for the local iLO system.

4. Enter a value for **Multicast Announcement Interval (seconds/minutes)**.

   This value sets the frequency at which the iLO system announces itself on the network. Each multicast announcement is approximately 300 bytes. Select a value of 30 seconds to 30 minutes. The default value is 10 minutes.

   Network changes and changes you make on this page take effect after the next multicast announcement.

   Selecting **Disabled** disables the iLO Federation features for the local iLO system.

5. Select a value for **IPv6 Multicast Scope**.

   Valid values are **Link**, **Site**, and **Organization**.

6. Enter a value for **Multicast Time To Live (TTL)**.

   This value specifies the number of switches that can be traversed before multicast discovery is stopped. The default value is 5.

7. Click **Apply** to save the settings.

IMPORTANT: To ensure that multicast discovery works correctly, make sure that all iLO systems in the same group use the same values for **Multicast Time to Live (TTL)** and **IPv6 Multicast Scope**.

Understanding iLO Federation groups

- iLO Federation groups allow iLO systems to encrypt and sign messages to other iLO systems in the same group.
- All iLO systems are automatically added to the **DEFAULT** group, which is granted the Login privilege for each group member. You can edit or delete the **DEFAULT** group membership.
- iLO Federation groups can overlap, span racks and data centers, and group servers of the same type.
- An iLO system can be a member of up to 10 iLO Federation groups.
- There is no limit on the number of iLO systems that can be in a group.
- You must have the Configure iLO Settings privilege to configure group memberships.
- You can use the iLO web interface to configure group memberships for a local iLO system or a group of iLO systems:
  - To configure group memberships for a local iLO system, see "Managing iLO Federation group memberships for the local iLO system" (page 55).
  - To configure group memberships for a group of iLO systems, see "Configuring group memberships for an iLO Federation group" (page 200).
- You can use RIBCL XML scripts to view and configure group memberships. For more information, see the *HP iLO 4 Scripting and Command Line Guide*.
- iLO systems in the same iLO Federation group must use the same version of the iLO 4 firmware.
- When you configure group memberships, you must specify the privileges that members of a group have for configuring the local managed server or the other members of the group.

  For example, if you add the local iLO system to **group1** and assign the Virtual Power and Reset privilege, the users of other iLO systems in **group1** can use the Group Power features to change the power state of the managed server.

  If the local iLO system does not grant the Virtual Power and Reset privilege to **group1**, the users of other iLO systems in **group1** cannot use the Group Power features to change the power state of the managed server.

  If the system maintenance switch is set to disable iLO security on the managed server, the users of other iLO systems in **group1** can use any iLO Federation feature to change the state of the managed server, regardless of the assigned group privileges.

Viewing iLO Federation group memberships

Use the iLO web interface to view the group memberships of a local iLO system.

You can also use RIBCL scripts to view information about groups. For more information, see the *HP iLO 4 Scripting and Command Line Guide*.

To view the group memberships of a local iLO system, navigate to the **Administration→iLO Federation** page.

The **Group Membership for this iLO** table lists the name of each group that includes the local iLO system, and the privileges granted to the group by the local iLO system. The available privileges follow:

- **Login Privilege** —Enables members of a group to log in to iLO.
- **Remote Console Access** —Enables members of a group to remotely access the host system Remote Console, including video, keyboard, and mouse control.
- **Virtual Media** —Enables members of a group to use scripted Virtual Media with the local iLO system.
- **Virtual Power and Reset** —Enables members of a group to power-cycle or reset the local iLO system.
- **Configure iLO Settings** —Enables members of a group to configure most iLO settings, including security settings, and to remotely update firmware.
- **Administer User Accounts** —Enables members of a group to add, edit, and delete iLO user accounts.

Managing iLO Federation group memberships for the local iLO system

You can configure group memberships for the local iLO system, or you can configure them for all of the members of a selected iLO Federation group. This topic describes the procedure for working with individual iLO systems. For information about managing the group memberships of iLO Federation groups, see "Configuring group memberships for an iLO Federation group" (page 200).

For more information about iLO Federation groups, see "Understanding iLO Federation groups" (page 54).

To configure group memberships for the local iLO system:

1. Navigate to the **Administration→iLO Federation** page.
2. Do one of the following:
   - Click **Join Group** to add a new group membership.
   - Select a group membership, and then click **Edit**.
3. Enter the following information:
   - **Group Name**—The group name, which can be 1 to 31 characters long.
   - **Group Key**—The group password, which can be 3 to 39 characters long.
   - **Group Key Confirm**—Confirm the group password.

   If you enter the name and key for an existing group, the local iLO system is added to that group. If you enter the name and key for a group that does not exist, the group is created and the local iLO system is added to the new group.
4. Select from the following permissions when you add or edit a group membership:
   - **Administer User Accounts**
   - **Remote Console Access**
   - **Virtual Power and Reset**
   - **Virtual Media**
   - **Configure iLO Settings**
   - **Login Privilege**

   The permissions granted to the group by the local iLO system control the tasks that users of other iLO systems in the group can perform on the managed server.

   For a description of these permissions, see "Viewing iLO Federation group memberships" (page 54).

5. Click **Join Group** or **Update Group** to save the settings.

Removing an iLO system from an iLO Federation group

Use the following procedure to remove the local iLO system from an iLO Federation group.

To use RIBCL scripts to remove group memberships, see the *HP iLO 4 Scripting and Command Line Guide*.

1. Navigate to the **Administration→iLO Federation** page.
2. Select the check box next to the group membership that you want to delete.
3. Click **Delete**.

   The following message appears:

   ```
   Are you sure you want to delete the selected group(s)?
   ```
4. Click **OK**.

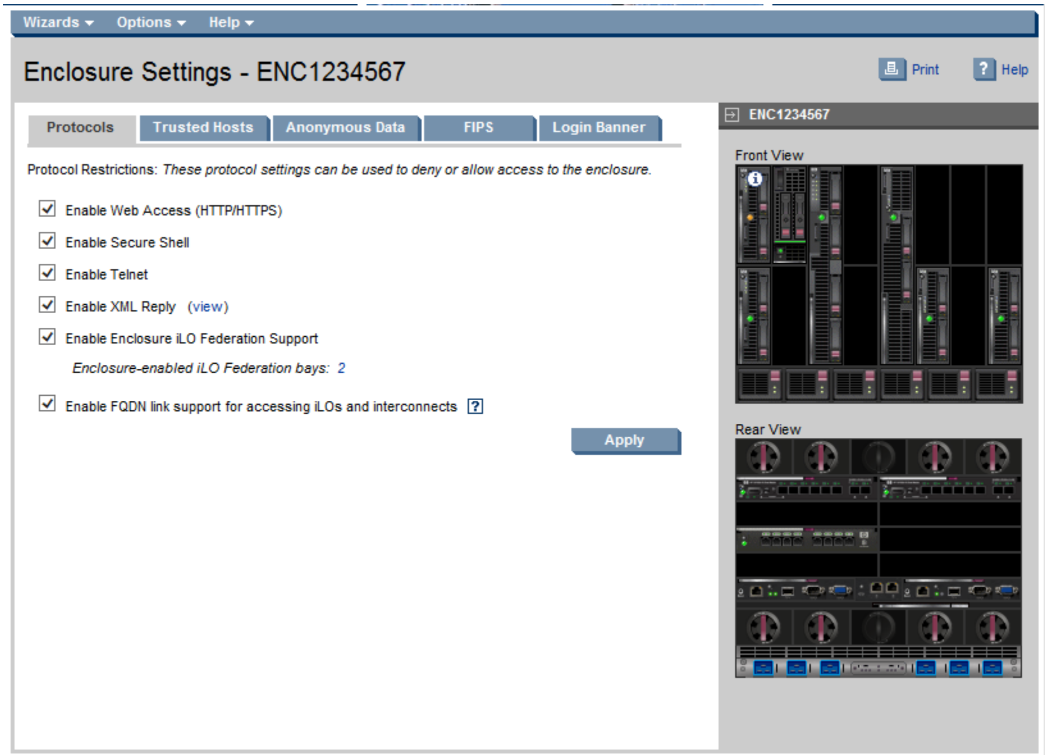
Configuring enclosure support for iLO Federation

If you want to use the iLO Federation features with server blades in an enclosure, the **Enclosure iLO Federation Support** setting must be enabled in the Onboard Administrator software. This setting is required to allow peer-to-peer communication between the server blades in an enclosure. **Enclosure iLO Federation Support** is enabled by default. Onboard Administrator 4.11 or later is required to use this feature.

Using Onboard Administrator to configure Enclosure iLO Federation Support

Use the following procedure to configure an enclosure for iLO Federation support:

1. Log in to the Onboard Administrator web interface (https://<Onboard Administrator hostname or IP address>).
2. Navigate to the **Enclosure Information→Network Access** page, and then click the **Protocols** tab.



Protocol Restrictions: *These protocol settings can be used to deny or allow access to the enclosure.*

☑ Enable Web Access (HTTP/HTTPS)

☑ Enable Secure Shell

☑ Enable Telnet

☑ Enable XML Reply (view)

☑ Enable Enclosure iLO Federation Support

Enclosure-enabled iLO Federation bays: 2

☑ Enable FQDN link support for accessing iLOs and interconnects ?

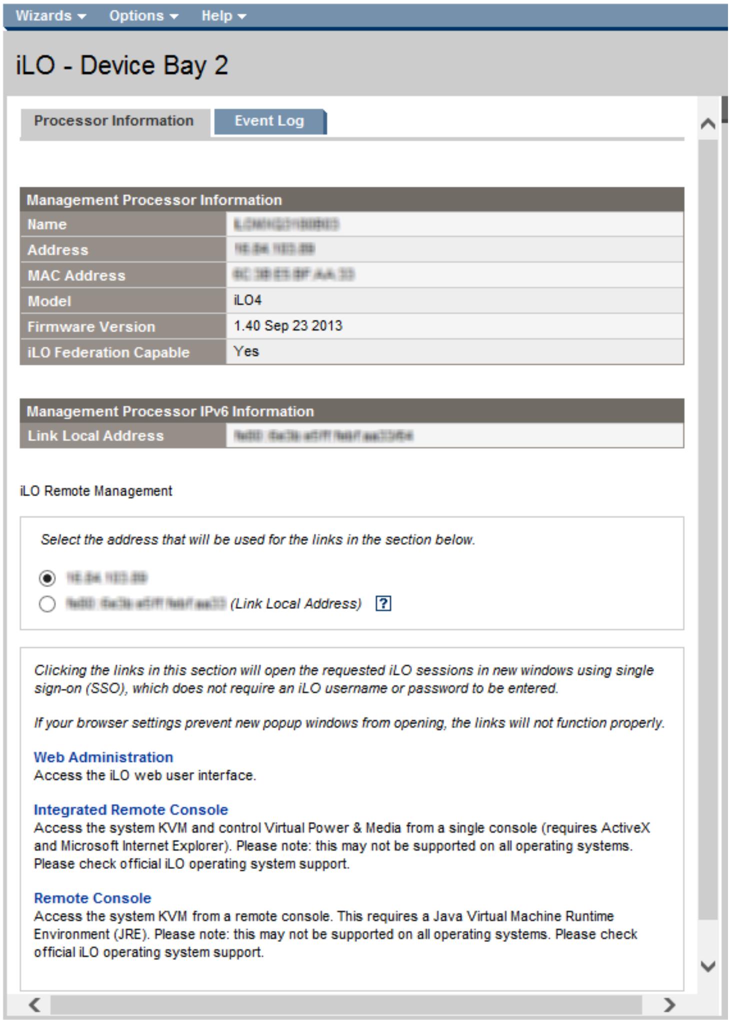
3. Select the **Enable Enclosure iLO Federation Support** check box, and then click **Apply**.

TIP: You can also use the CLI to enable or disable Enclosure iLO Federation Support. To enable the setting, enter `ENABLE ENCLOSURE_ILO_FEDERATION_SUPPORT`. To disable the setting, enter `DISABLE ENCLOSURE_ILO_FEDERATION_SUPPORT`. For information about using the Onboard Administrator CLI, see the *HP BladeSystem Onboard Administrator Command Line Interface User Guide* at the following website: http://www.hp.com/go/oa.

Verifying server blade support for iLO Federation

Use the following procedure to verify that a server blade is configured for iLO Federation support:

1. Log in to the Onboard Administrator web interface (https://<Onboard Administrator hostname or IP address>).
2. Navigate to the **Device Bays→<Device Name>→iLO** page.



iLO - Device Bay 2

Management Processor Information	
Name	[redacted]
Address	[redacted]
MAC Address	[redacted]
Model	iLO4
Firmware Version	1.40 Sep 23 2013
iLO Federation Capable	Yes

Management Processor IPv6 Information	
Link Local Address	[redacted]

iLO Remote Management

Select the address that will be used for the links in the section below.

● [redacted]

○ [redacted] *(Link Local Address)* ?

Clicking the links in this section will open the requested iLO sessions in new windows using single sign-on (SSO), which does not require an iLO username or password to be entered.

If your browser settings prevent new popup windows from opening, the links will not function properly.

Web Administration
Access the iLO web user interface.

Integrated Remote Console
Access the system KVM and control Virtual Power & Media from a single console (requires ActiveX and Microsoft Internet Explorer). Please note: this may not be supported on all operating systems. Please check official iLO operating system support.

Remote Console
Access the system KVM from a remote console. This requires a Java Virtual Machine Runtime Environment (JRE). Please note: this may not be supported on all operating systems. Please check official iLO operating system support.

3. Verify that **iLO Federation Capable** is set to **Yes**.

Configuring iLO access settings

You can modify iLO access settings, including service, IPMI/DCMI, and access options. The values 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 you can modify on the **Access Settings** page allow complete customization of the iLO external access methods for specialized environments.

Configuring service settings

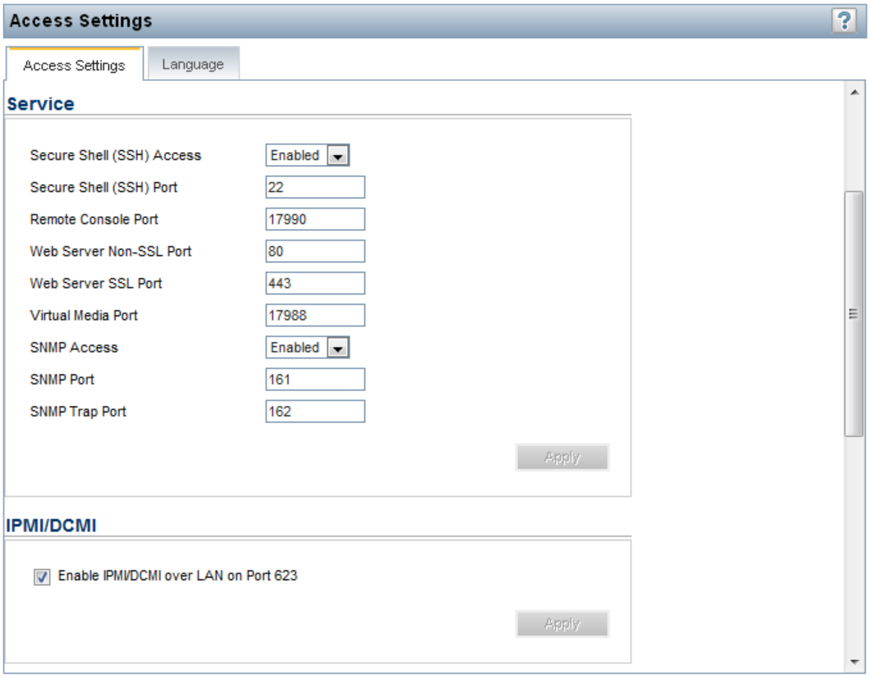
The **Service** section on the **Access Settings** page shows the **Secure Shell (SSH) Access** and **SNMP Access** settings and the TCP/IP port values.

The TCP/IP ports used by iLO are configurable, which enables compliance with site requirements and 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



Access Settings

Access Settings | Language

Service

Secure Shell (SSH) Access: Enabled
Secure Shell (SSH) Port: 22
Remote Console Port: 17990
Web Server Non-SSL Port: 80
Web Server SSL Port: 443
Virtual Media Port: 17988
SNMP Access: Enabled
SNMP Port: 161
SNMP Trap Port: 162

Apply

IPMI/DCMI

☑ Enable IPMI/DCMI over LAN on Port 623

Apply

2. Update the following settings as needed:
   - **Secure Shell (SSH) Access**—Allows you to enable or disable the SSH feature.

     SSH provides encrypted access to the iLO CLP. The default value is **Enabled**.
   - **Secure Shell (SSH) Port**—The default value is 22.
   - **Remote Console Port**—The default value is 17990.
   - **Web Server Non-SSL Port** (HTTP)—The default value is 80.
   - **Web Server SSL Port** (HTTPS)—The default value is 443.
   - **Virtual Media Port**—The default value is 17988.
   - **SNMP Access**—Specifies whether iLO should respond to external SNMP requests. The default value is **Enabled**.

     If you set **SNMP Access** to **Disabled**, iLO continues to operate, and the information displayed in the iLO web interface is updated, but no alerts are generated and SNMP access is not permitted. When **SNMP Access** is set to **Disabled**, most of the boxes on the **Administration**→**Management**→**SNMP Settings** page are unavailable and will not accept input.

- **SNMP Port**—The industry-standard (default) SNMP port is **161** for SNMP access.

  If you customize the **SNMP Port** value, some SNMP clients might not work correctly with iLO unless those clients support the use of a nonstandard SNMP port.

- **SNMP Trap Port**—The industry-standard (default) SNMP trap port is **162** for SNMP alerts (or traps).

  If you customize the **SNMP Trap Port** value, some SNMP monitoring applications (such as HP SIM) might not work correctly with iLO unless those applications support the use of a nonstandard SNMP trap port.

3. Click **Apply** to end your browser connection and restart iLO.

   It might take several minutes before you can 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.

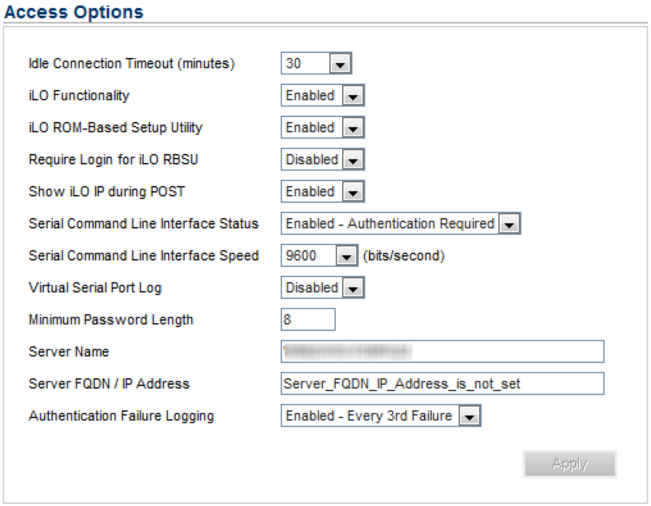
Configuring access options

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 or the iLO Configuration Utility. For instructions, see "Using the iLO RBSU" (page 134) and "Using the UEFI System Utilities iLO 4 Configuration Utility" (page 138).

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.



Access Options

Idle Connection Timeout (minutes)	30
iLO Functionality	Enabled
iLO ROM-Based Setup Utility	Enabled
Require Login for iLO RBSU	Disabled
Show iLO IP during POST	Enabled
Serial Command Line Interface Status	Enabled - Authentication Required
Serial Command Line Interface Speed	9600 (bits/second)
Virtual Serial Port Log	Disabled
Minimum Password Length	8
Server Name	[redacted]
Server FQDN / IP Address	Server_FQDN_IP_Address_is_not_set
Authentication Failure Logging	Enabled - Every 3rd Failure

3. Update the following settings as needed:
   - **Idle Connection Timeout (minutes)**—Specifies how long a user can be inactive before the iLO web interface and Remote Console session end automatically. The following settings are valid:
     - **15**, **30**, **60**, or **120** minutes—The default value is 30 minutes.
     - **Infinite**—Inactive users are not logged out.

     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**—Specifies whether iLO functionality is available. The following settings are valid:
     - **Enabled** (default)—The iLO network is available and communications with operating system drivers are active.
     - **Disabled**—The iLO network and communications with operating system drivers are terminated when **iLO Functionality** is disabled.

       To re-enable iLO functionality, disable iLO security with the system maintenance switch, and then use the iLO RBSU or the iLO 4 Configuration Utility (in the UEFI System Utilities) to set **iLO Functionality** to **Enabled**. For more information about using the system maintenance switch, see the *Maintenance and Service Guide* for your server model.

       iLO functionality cannot be disabled on server blades.
   - **iLO ROM-Based Setup Utility** or **iLO 4 Configuration Utility**—Enables or disables the iLO RBSU or the iLO 4 Configuration Utility. The following settings are valid:
     - **Enabled** (default)—On servers that support the iLO RBSU, pressing **F8** during POST starts the iLO RBSU. On servers that support UEFI, the iLO 4 Configuration Utility is available when you access the UEFI System Utilities.
     - **Disabled**—On servers that support the iLO RBSU, pressing **F8** during POST will not start the iLO RBSU. On servers that support UEFI, the iLO 4 Configuration Utility is not available when you access the UEFI System Utilities.
   - **Require Login for iLO RBSU** or **Require Login for iLO 4 Configuration Utility**—Determines whether a user-credential prompt is displayed when a user accesses the iLO RBSU or the iLO 4 Configuration Utility. The following settings are valid:
     - **Enabled**—A login dialog box opens when a user accesses the iLO RBSU or the iLO 4 Configuration Utility.
     - **Disabled** (default)—No login is required when a user accesses the iLO RBSU or the iLO 4 Configuration Utility.

- **Show iLO IP during POST**—Enables the display of the iLO network IP address during host server POST. The following settings are valid:
  - **Enabled** (default)—The iLO IP address is displayed during POST.
  - **Disabled**—The iLO IP address is not displayed during POST.
- **Serial Command Line Interface Status**—Enables you to change the login model of the CLI feature through the serial port. The following settings are valid:
  - **Enabled-Authentication Required** (default)—Enables access to the SMASH CLP command line from a terminal connected to the host serial port. Valid iLO user credentials are required.
  - **Enabled-No Authentication**—Enables access to the SMASH CLP command line from a terminal connected to the host serial port. iLO user credentials are not required.
  - **Disabled**—Disables access to the SMASH CLP command line from the host serial port. Use this option if you are planning to use physical serial devices.
- **Serial Command Line Interface Speed**—Enables you to change the speed of the serial port for the CLI feature. The following speeds (in bits per second) are valid:
  - **9600** (default)
  - **19200**
  - **38400**—This value is not supported by the iLO RBSU or the iLO 4 Configuration Utility.
  - **57600**
  - **115200**

  The serial port configuration must be set to no parity, 8 data bits, and 1 stop bit (N/8/1) for correct operation.

  The serial port speed set by this option should match the serial port speed configured in the iLO RBSU or the iLO 4 Configuration Utility.
- **Virtual Serial Port Log**—Enables or disables logging of the Virtual Serial Port.

  The following settings are valid:
  - **Enabled**—When enabled, Virtual Serial Port activity is logged to a 150-page circular buffer in the iLO memory, and can be viewed using the CLI command `vsp log`. The Virtual Serial Port buffer size is 128 KB.
  - **Disabled** (default)—Virtual Serial Port activity is not logged.

  This feature is part of an iLO licensing package. For more information, see the following website: http://www.hp.com/go/ilo/licensing.
- **Minimum Password Length**—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 characters long. The default value is 8.
- **Server Name**—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 and display the new value, save this setting, and then press **F5**.

- **Server FQDN/IP Address**—Enables you to specify the server FQDN or IP address. You can assign this value manually, but it might be overwritten by the host software when the operating system loads.
    - You can enter an FQDN or IP address that is up to 255 bytes.
    - To force the browser to refresh and display the new value, save this setting, and then press **F5**.
- **Authentication Failure Logging**—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** (default)—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 62).

4. Click **Apply** to end your browser connection and restart iLO.

    It might take several minutes before you can 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 57).
- User actions logged in the iLO Event Log. For more information, see "Using the iLO Event Log" (page 171).
- Progressive delays for failed login attempts. For more information, see "Login security" (page 66).
- Support for X.509 CA signed certificates. For more information, see "Administering SSL certificates" (page 69).
- Support for securing iLO RBSU and the iLO 4 Configuration Utility. For more information, see "iLO RBSU and iLO 4 Configuration Utility security" (page 63).
- Encrypted communication that uses SSL certificate administration. For more information, see "Administering SSL certificates" (page 69).
- Support for optional LDAP-based directory services. For more information, see "Directory services" (page 265).

Some of these options are licensed features. For more information, see "iLO licensing" (page 44).

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 20).
- Do not connect iLO directly to the Internet.
- Use a browser that has a 128-bit cipher strength.

iLO RBSU and iLO 4 Configuration Utility security

iLO RBSU and the iLO 4 Configuration Utility enable you to view and modify the iLO configuration. You can configure iLO RBSU and iLO Configuration Utility access settings by using iLO RBSU, the iLO 4 Configuration Utility, the iLO web interface, or RIBCL scripts. If the system maintenance switch is set to disable iLO security, any user can access iLO RBSU or the iLO 4 Configuration Utility, regardless of the configured access settings.

- For information about using the iLO web interface to configure iLO RBSU or the iLO 4 Configuration Utility access settings, see "Configuring access options" (page 59).
- For information about using iLO RBSU or the iLO 4 Configuration Utility to configure iLO RBSU or iLO 4 Configuration Utility access settings, see "Configuring iLO by using the ROM-based utilities" (page 133).
- For information about using RIBCL scripts to configure iLO RBSU or the iLO 4 Configuration Utility, see the *HP iLO 4 Scripting and Command Line Guide*.
- For information about using the system maintenance switch, see "Managing iLO security with the system maintenance switch" (page 64).

iLO RBSU and the iLO 4 Configuration Utility have the following security levels:

- **Login Not Required** (default)

  Anyone who has access to the host during POST can enter iLO RBSU or the iLO 4 Configuration Utility 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 or iLO 4 Configuration Utility login is required, the active configuration menus are controlled by the authenticated user access rights.

- **Disabled** (most secure)

  If iLO RBSU or the iLO 4 Configuration Utility is disabled, user access is prohibited. This prevents modification by using the iLO RBSU or the iLO 4 Configuration Utility.

To change the login requirement:

- Use the iLO web interface to edit the **Require Login for iLO RBSU** or **Require Login for iLO 4 Configuration Utility** setting. For instructions, see "Configuring access options" (page 59).
- Use the iLO RBSU or the iLO 4 Configuration Utility to edit the **Require iLO 4 RBSU Login** or **Require Login for iLO 4 Configuration Utility** setting. For instructions, see "Configuring iLO by using the ROM-based utilities" (page 133).

To enable or disable access to iLO RBSU or the iLO 4 Configuration Utility:

- Use the iLO web interface to edit the **iLO ROM-Based Setup Utility** or **iLO 4 Configuration Utility** setting. For instructions, see "Configuring access options" (page 59).
- Use the iLO RBSU or the iLO 4 Configuration Utility to edit the **iLO 4 ROM-Based Setup Utility** or **iLO 4 Configuration Utility** setting. For instructions, see "Configuring iLO by using the ROM-based utilities" (page 133).

Managing iLO security with the system maintenance switch

The iLO security setting on the system maintenance switch provides emergency access to an administrator who has physical control over the server system board. Disabling iLO security allows login access with all privileges, without a user ID and password.

The system maintenance switch is located inside the server and cannot be accessed without opening the server enclosure. When you work with the system maintenance switch, ensure that the server is powered off and disconnected from the power source. Set the switch to enable or disable iLO security, and then power on the server.

Disabling iLO security 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.

NOTE: The system maintenance switch position that controls iLO security is sometimes called the *iLO Security Override switch*.

It might be necessary to disable iLO security for the following reasons:

- iLO Functionality is 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 or the iLO 4 Configuration Utility is disabled.
- The boot block must be flashed.
- The iLO NIC is turned off, and it is not possible or convenient to run iLO RBSU or the iLO 4 Configuration Utility to turn it back on.
- Only one user name is configured, and the password is forgotten.

When you disable iLO security with the system maintenance switch:

- All security authorization verifications are disabled.
- iLO RBSU or the iLO 4 Configuration Utility runs if the host server is reset.
- iLO is not disabled and might be displayed on the network as configured.
- If iLO Functionality disabled, iLO does not log out active users 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 iLO security is disabled.
- An iLO log entry is added to record the iLO security change.
- When iLO starts after you use the system maintenance switch to enable or disable iLO security, an SNMP alert is sent if an SNMP Alert Destination is configured.

For information about how to enable and disable iLO security with the system maintenance switch, see the *Maintenance and Service Guide* for your server.

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 265).

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 46).

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 59).

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 67) and "Authorizing a new key by using the CLI" (page 68). 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.

The following SSH key formats are supported:

- **RFC 4716**

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "Administrator"
AAAAB3NzaC1kc3MAAACAT27C04Dy2zr7fWhUL7TwHDKQdEdyuAlNLIivLFP3IoKZ
ZtzF0VInP5x2VFVYmTvdVjD92CTlxxAtarOPON2qUqoOajKRtBWLmxcfqsLCT3wI
3ldxQvPYnhTYyhPQuoeJ/vYhoam+y0zi8D03pDv9KaeNA3H/zEL5mf9Ktgts8/UA
AAAVAJ4efo8ffq0hg4a/eTGEuHPCb3INAAAAgCbnhADYXu+Mv4xuXccXWP0Pcj47
7YiZgos3jt/Z0ezFX6/cN/RwwZwPC1HCsMuwsVBIqi7bvn1XczFPKOt06gVWcjFt
eBY3/bKpQkn61SGPC8AhSu8ui0KjyUZrxL4LdBrtp/K2+lm1fqXHnzDIEJ0RHg8Z
JazhY920PpkD4hNbAAAAgDN3lba1qFVl0UlRjj21MjXgr6em9TETSOO5b7SQ8hX/
Z/axobbrHCj/2s66VA/554chkVimJT2IDRRKVkcV8OVC3nb4ckpfFEZvKkAWYaiF
DLqRbHhh4qyRBIfBKQpvvhDj1aecdFbaO2UvZltMir4n8/E0hh19nfi3tjXAtSTV
---- END SSH2 PUBLIC KEY ----
```

- **OpenSSH key format**—These keys must be one line only.

```
ssh-dss
AAAAB3NzaC1kc3MAAACAYjEd8Rk8HLCLqDIlI+RkA1UXjVS28hNSk8YDljTaJpw1VOlBirrLGPdSt0avNSz0DNQuU7gTPfjj/8c
XyHe3y95Oa3Rics1fARyLiNFGqFjr7w2ByQuoYUaXBzzghIYMQcmpc/W/kDMC0dVOf2XnfcLpcVDIm3ahVPRkxFV9WKkAAAAVAI
3J61F+oVKrbNovhoHh8pFfUa9LAAAAgA8pU5/M9F0s5QxqkEWPD6+FVz9cZ0GfwIbiuAI/9ARsizkbwRtpAlxAp6eDZKFvj3ZIy
NjcQODeYYqOvVU45AkSkLBMGjpF05cVtnWEGEvrW7mAvtG2zwMEDFSREw/V526/jR9TKzSNXTH/wqRtTc/oLotHeyV2jFZFGpxD
OvNWAAAAgFf6pvWaco3CDELmH0jT3yUkRSaDztpqtoo4D7ev7VrNPPjnKKKmpzHPmAKRxz3g5S80SfWSnWM3n/pekBa9QI9lH1r
3Lx4JoOVwTpkbwb0by4eZ2cqDw20KQ0A5J84iQE9TbPNecJ0HJtZH/K8YnFNwwYy2NSJyjLwA0TSmQEOW Administrator
```

- **iLO legacy format**—These are OpenSSH keys surrounded by the BEGIN/END headers needed for RIBCL. This format must be one line between the BEGIN SSH KEY and END SSH KEY text.

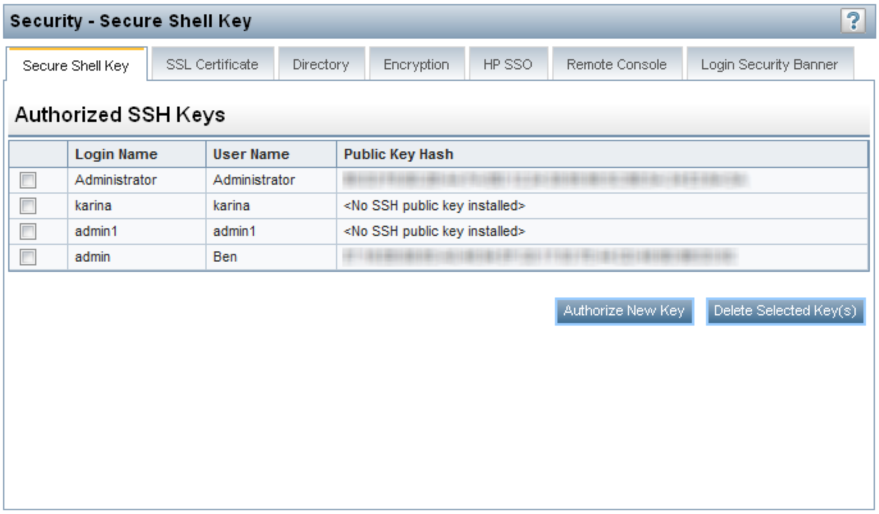
  ```
  -----BEGIN SSH KEY-----
  ssh-dss
  AAAAB3NzaC1kc3MAAACBANA45qXo9cM1asav6ApuCREt1UvP7qcMbw+sTDrx9lV22XvonwijdFiOM/0VvuzVhM9oKdGMC7sCGQr
  FV3zWDMJcIb5ZdYQSDt44X6bvlsQcAR0wNGBN9zHL6YsbXvNAsXN7uBM7jXwHwrApWVuGAI0QnwUYvN/dsE8fbEYtGZCRAAAAFQ
  DofA47q8pIRdr6epnJXSNrwJRvaQAAAIBY7MKa2uH82I0KKYTbNMi0o5mOqmqy+tg5s9GC+HvvYy/S7agpIdfJzqkpHF5EPhm0j
  KzzVxmsanO+pjju7lrE3xUxojevlokTERSCM xLa+OVVbNcgTe0xpvc/cF6ZvsHs0UWz6gXIMCQ9Pk118VMOw/tyLp42YXOaLZzG
  fi5pKAAAAIEAl7FsO7sDbPj02a5jO3qFXa762lWvu5iPRZ9cEt5WJEYwMO/ICaJVDWVOpqF9spoNb53Wl1pUARJg1ss8Ruy7YBv
  8Z1urWWAF3fYy7R/SlQqrsRYDPLM5eBkkLO28B8C6++HjLuc+hBvj90tsqeNVhpCfO9qrjYomYwnDC4m1IT4= ASmith
  -----END SSH KEY-----
  ```

Note the following when working with SSH keys:

- The previously listed sample formats are supported with the iLO web interface and the CLI. Only the iLO legacy format is supported with RIBCL scripts.
- 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 1366 bytes or less. If the key is larger than 1366 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

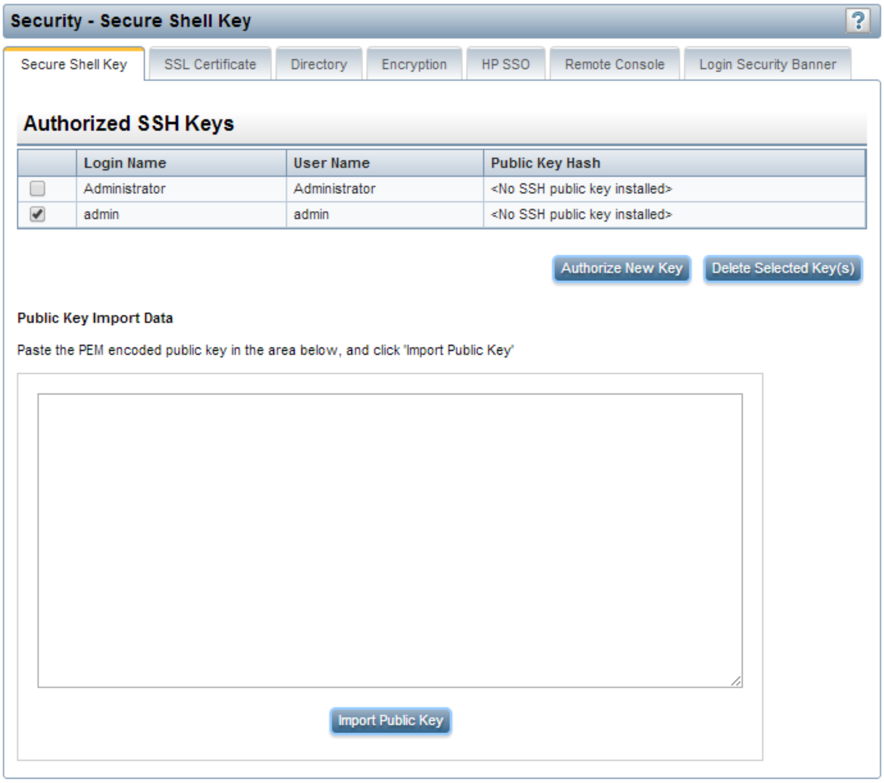
1. Generate a 2,048-bit DSA or RSA key by using `ssh-keygen`, `puttygen.exe`, or another SSH key utility.
2. Create the `key.pub` file.
3. Navigate to the **Administration→Security** page.
4. Click the **Secure Shell Key** tab.



Authorized SSH Keys

	Login Name	User Name	Public Key Hash
□	Administrator	Administrator	[redacted]
□	karina	karina	<No SSH public key installed>
□	admin1	admin1	<No SSH public key installed>
□	admin	Ben	[redacted]

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 **Public Key Import Data** box.



Authorized SSH Keys

	Login Name	User Name	Public Key Hash
□	Administrator	Administrator	<No SSH public key installed>
☑	admin	admin	<No SSH public key installed>

Public Key Import Data

Paste the PEM encoded public key in the area below, and click 'Import Public Key'

The key must be a 2,048-bit DSA or RSA key.

8. Click **Import Public Key**.

Authorizing a new key by using the CLI

1. Generate a 2,048-bit DSA or RSA SSH key by using `ssh-keygen`, `puttygen.exe`, or another SSH key utility.
2. Create the `key.pub` file.
3. Verify that **Secure Shell (SSH) Access** is enabled on the **Access Settings** page.

   For more information, see "Configuring iLO access settings" (page 57).
4. Use `Putty.exe` to open an SSH session using port 22.
5. Change to the `cd /Map1/Config1` directory.
6. Enter the following command:

   ```
   load sshkey type "oemhp_loadSSHkey -source
   <protocol://username:password@hostname:port/filename>"
   ```

   When you use this command:

   - The protocol value is required and must be HTTP or HTTPS.
   - The hostname and filename values are required.
   - The username:password and port values are optional.
   - `oemhp_loadSSHkey` is case-sensitive.

The CLI performs a cursory syntax verification of the values you enter. You must visually verify that the URL is valid. The following example shows the command structure:

```
oemhp_loadSSHkey -source http://192.168.1.1/images/path/sshkey.pub
```

Deleting SSH keys

1. Navigate to the **Administration**→**Security** page.

2. Click the **Secure Shell Key** tab.
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 4 Scripting and Command Line Guide*.

Administering SSL certificates

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

A certificate is a small data file that connects an SSL key to a server. It contains the name of the server and the server's public key. Only the server has the corresponding private key, and 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.

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 with the Configure iLO Settings privilege can customize and import a trusted certificate that is signed by a CA.

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

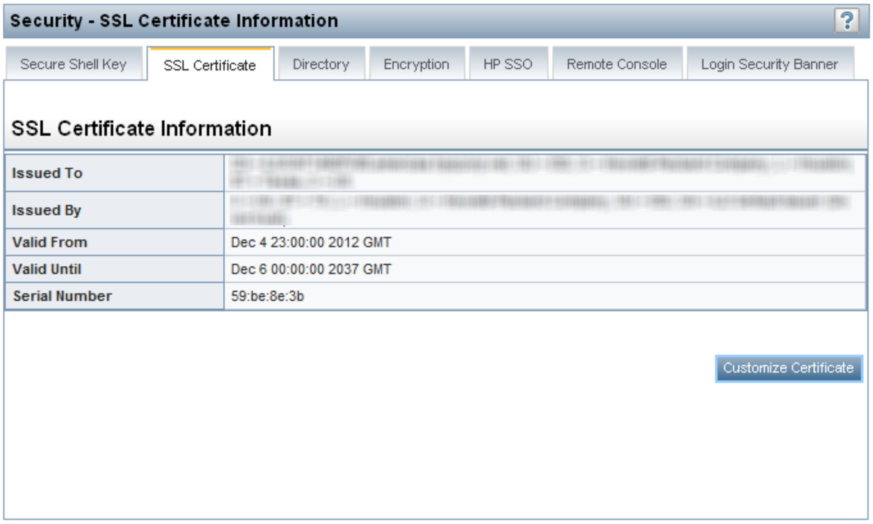
Obtaining and importing an SSL certificate

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 the factory default settings, 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 a CA.

To obtain and import a certificate:

1. Navigate to the **Administration→Security→SSL Certificate** page.



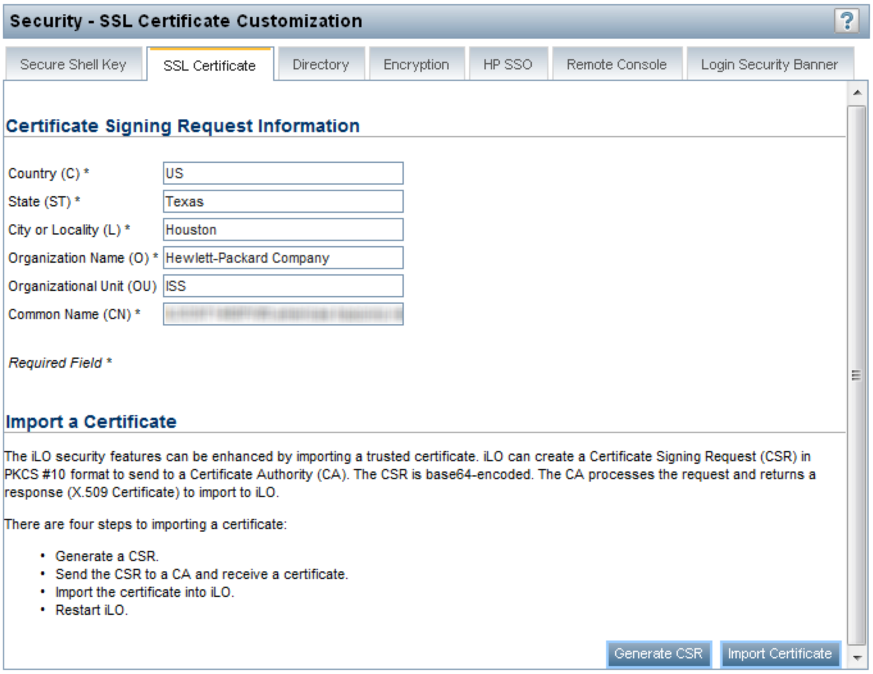
Security - SSL Certificate Information

SSL Certificate Information

Issued To	[redacted]
Issued By	[redacted]
Valid From	Dec 4 23:00:00 2012 GMT
Valid Until	Dec 6 00:00:00 2037 GMT
Serial Number	59:be:8e:3b

2. Click **Customize Certificate**.

   The **SSL Certificate Customization** page opens.



Security - SSL Certificate Customization

Certificate Signing Request Information

Country (C) *	US
State (ST) *	Texas
City or Locality (L) *	Houston
Organization Name (O) *	Hewlett-Packard Company
Organizational Unit (OU)	ISS
Common Name (CN) *	[redacted]

*Required Field **

Import a Certificate

The iLO security features can be enhanced by importing a trusted certificate. iLO can create a Certificate Signing Request (CSR) in PKCS #10 format to send to a Certificate Authority (CA). The CSR is base64-encoded. The CA processes the request and returns a response (X.509 Certificate) to import to iLO.

There are four steps to importing a certificate:

- Generate a CSR.
- Send the CSR to a CA and receive a certificate.
- Import the certificate into iLO.
- Restart iLO.

3. Enter the following information in the **Certificate Signing Request Information** section. The required boxes are marked with an asterisk (*).

   - **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.

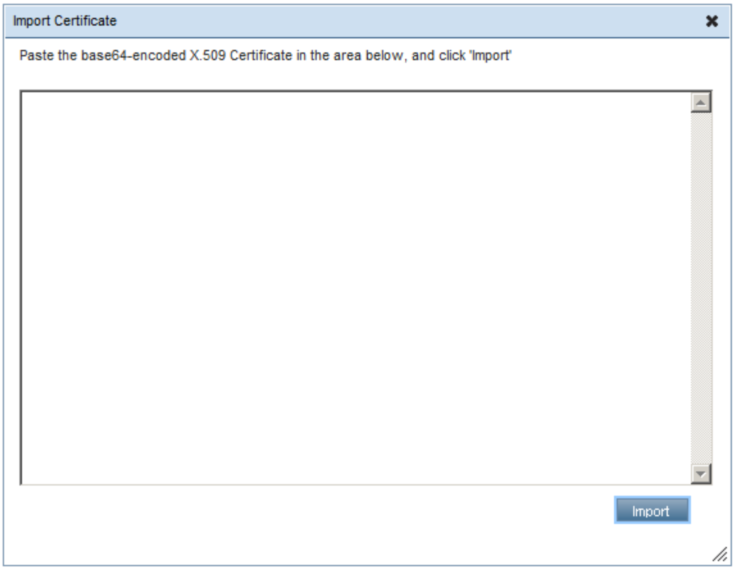
6. Select and copy the CSR text.
7. Open a browser window and navigate to a third-party CA.
8. Follow the onscreen instructions and submit the CSR to the CA.

   The CA will generate a certificate in 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.
   - The first and last lines are included in the certificate.
10. Return to the **SSL Certificate Customization** page in the iLO web interface.
11. Click the **Import Certificate** button.

    The **Import Certificate** window opens.



Paste the base64-encoded X.509 Certificate in the area below, and click 'Import'

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

    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. Reset iLO.

    For instructions, see “Using iLO diagnostics” (page 180).

Configuring directory settings

The iLO firmware connects to Microsoft Active Directory 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 265).

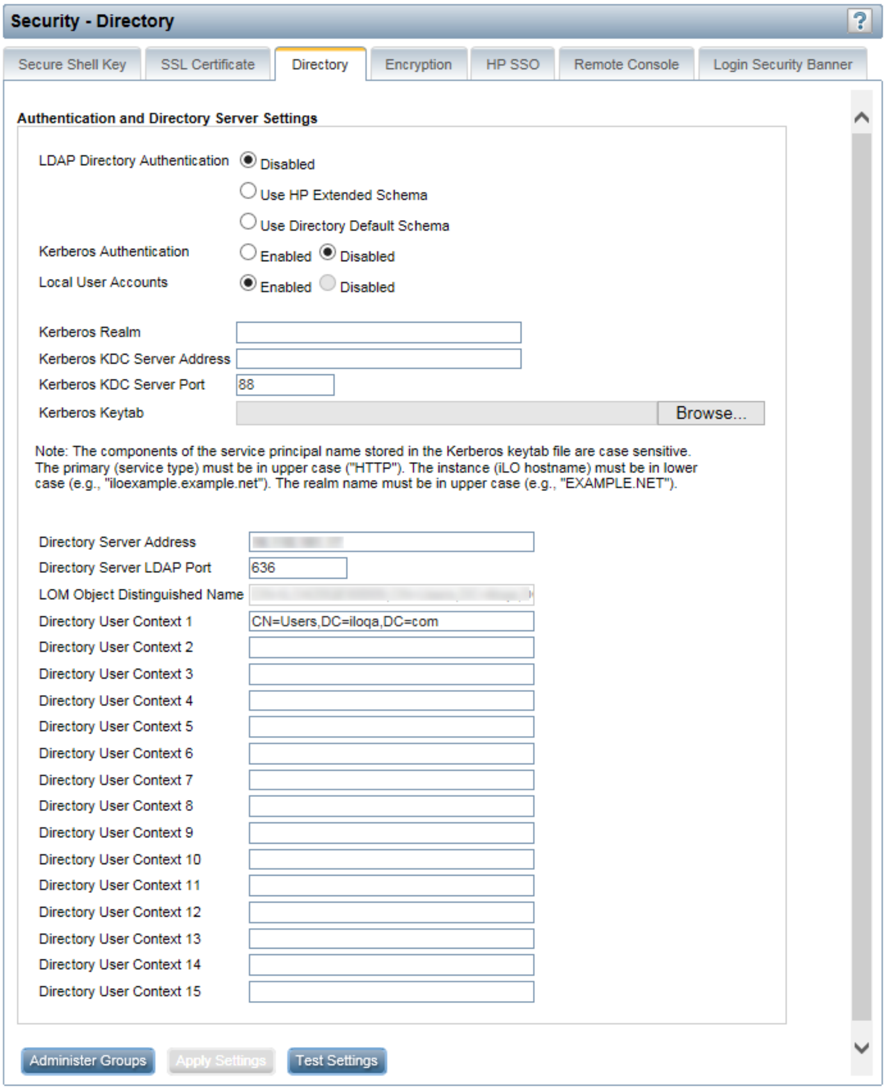
Locally stored user accounts (listed on the **User Administration** page) can be active when iLO directory support is enabled. This enables both local-based and directory-based user access. Typically, you can delete local user accounts (with the exception of an emergency access account) after iLO is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



Authentication and Directory Server Settings

LDAP Directory Authentication ● Disabled ○ Use HP Extended Schema ○ Use Directory Default Schema

Kerberos Authentication ○ Enabled ● Disabled

Local User Accounts ● Enabled ○ Disabled

Kerberos Realm

Kerberos KDC Server Address

Kerberos KDC Server Port 88

Kerberos Keytab

Note: The components of the service principal name stored in the Kerberos keytab file are case sensitive. The primary (service type) must be in upper case ("HTTP"). The instance (iLO hostname) must be in lower case (e.g., "iloexample.example.net"). The realm name must be in upper case (e.g., "EXAMPLE.NET").

Directory Server Address [redacted]

Directory Server LDAP Port 636

LOM Object Distinguished Name [redacted]

Directory User Context 1 CN=Users,DC=iloqa,DC=com

Directory User Context 2

Directory User Context 3

Directory User Context 4

Directory User Context 5

Directory User Context 6

Directory User Context 7

Directory User Context 8

Directory User Context 9

Directory User Context 10

Directory User Context 11

Directory User Context 12

Directory User Context 13

Directory User Context 14

Directory User Context 15

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 or disables 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.
   - **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 define 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 75).
6. Optional: Click **Administer Groups** to navigate to the **User Administration** page, where you can configure directory groups.

   For information about group administration, see “Administering directory groups” (page 50).

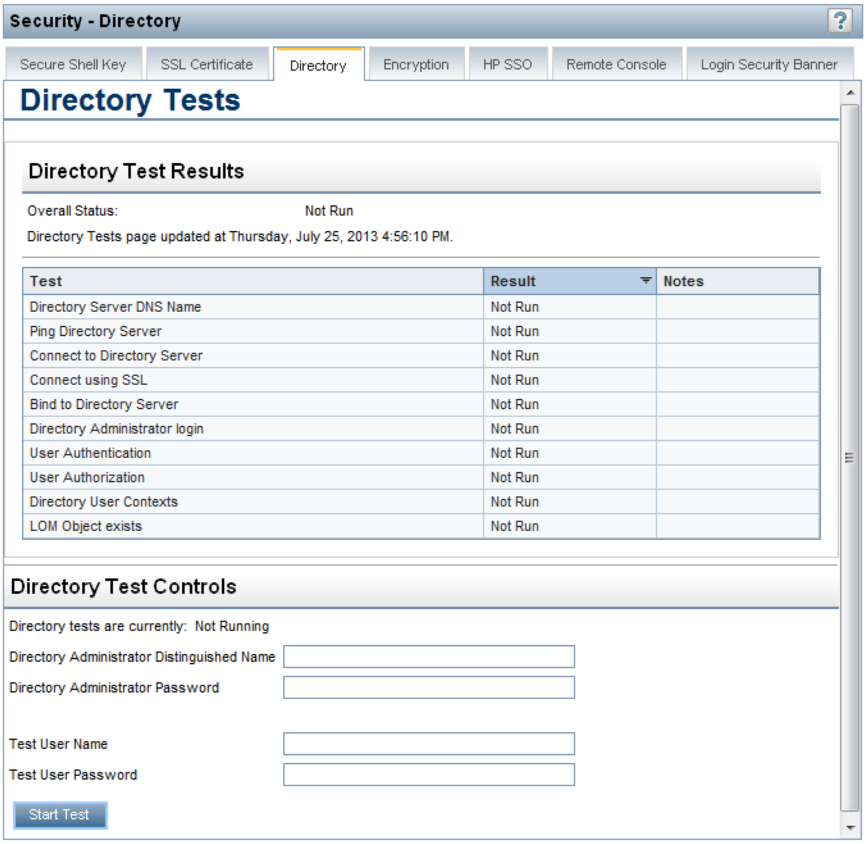
Running directory tests

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.



Directory Tests

Directory Test Results

Overall Status: Not Run

Directory Tests page updated at Thursday, July 25, 2013 4:56:10 PM.

Test	Result	Notes
Directory Server DNS Name	Not Run	
Ping Directory Server	Not Run	
Connect to Directory Server	Not Run	
Connect using SSL	Not Run	
Bind to Directory Server	Not Run	
Directory Administrator login	Not Run	
User Authentication	Not Run	
User Authorization	Not Run	
Directory User Contexts	Not Run	
LOM Object exists	Not Run	

Directory Test Controls

Directory tests are currently: Not Running

Directory Administrator Distinguished Name

Directory Administrator Password

Test User Name

Test User Password

   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 detected issues. After your directory settings are configured correctly, you do not need to rerun these tests. The **Directory Tests** page does not require you to log 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 the right 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. This name does not need 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.

  For more information about the iLO directory tests, see "About the iLO directory tests" (page 78).
- **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 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 **Stop Test** to cancel the current tests, or click **Refresh** 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 75).

About the iLO directory tests

Descriptions of the directory tests follow:

- **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:

  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 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 does 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.

  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 test 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.

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 AES256-CBC, 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.

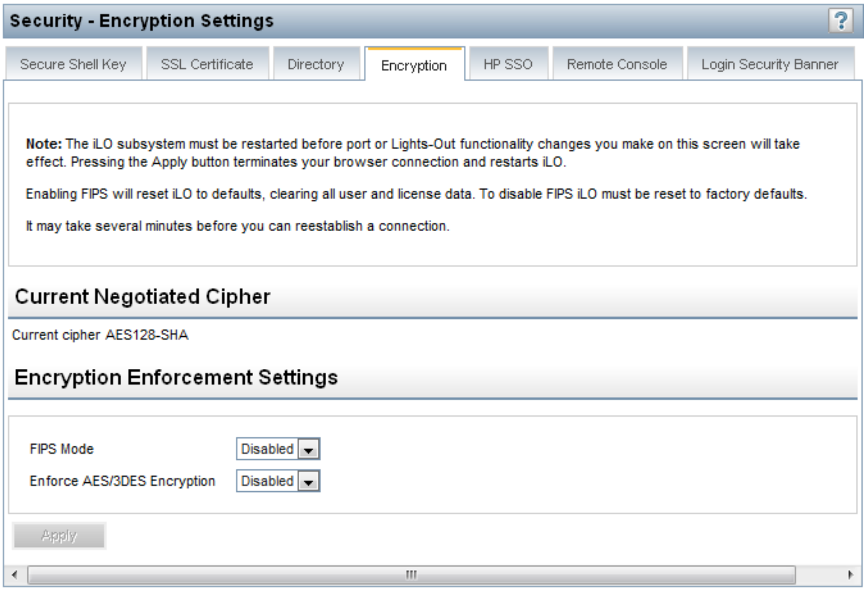
Version 1.20 and later of the iLO 4 firmware supports FIPS Mode.

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 4 1.20 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.



Note: The iLO subsystem must be restarted before port or Lights-Out functionality changes you make on this screen will take effect. Pressing the Apply button terminates your browser connection and restarts iLO.

Enabling FIPS will reset iLO to defaults, clearing all user and license data. To disable FIPS iLO must be reset to factory defaults.

It may take several minutes before you can reestablish a connection.

Current Negotiated Cipher

Current cipher AES128-SHA

Encryption Enforcement Settings

FIPS Mode: Disabled

Enforce AES/3DES Encryption: Disabled

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.
2. Change the **Enforce AES/3DES Encryption** setting to **Enabled** or **Disabled**.

IMPORTANT: Java Runtime Environment 8 or later is required when **Enforce AES/3DES Encryption** is set to **Enabled**.

3. Click **Apply** to end your browser connection and restart iLO.

   It might take several minutes before you can 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 4 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 69).

   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.
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 4 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 89).

You can also use XML configuration and control scripts to enable FIPS mode. For more information, see the *HP iLO 4 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, iLO RBSU, or the iLO 4 Configuration Utility.

For instructions, see "Resetting iLO to the factory default settings by using iLO RBSU" (page 311), "Resetting iLO to the factory default settings by using the iLO 4 Configuration Utility" (page 312), or the *HP iLO 4 Scripting and Command Line Guide*.

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

Using HP SSO

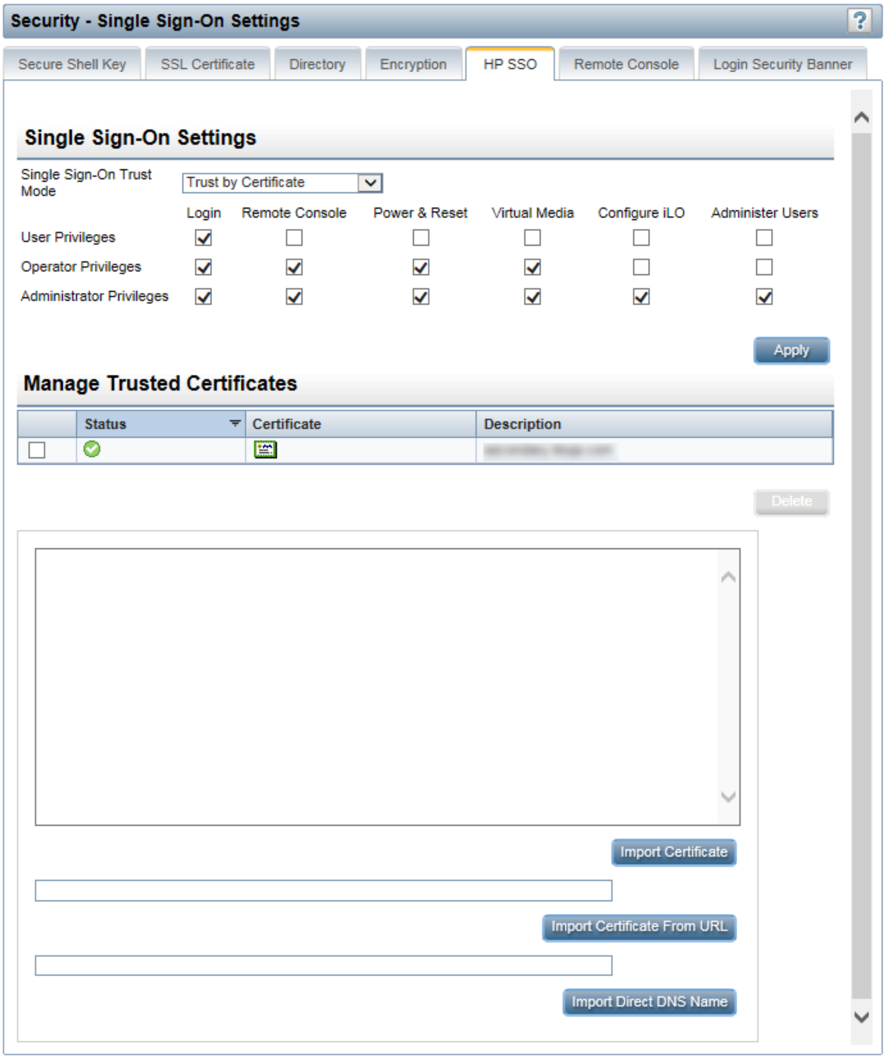
HP SSO enables you to browse directly from an HP SSO-compliant application (such as HP SIM and HP OneView) to iLO, bypassing an intermediate login step. To use SSO, you must have a supported version of an HP SSO-compliant application, you might need iLO 4 1.20 or later, and you must configure the iLO processor to trust the SSO-compliant application.

iLO contains support for HP SSO applications to determine the minimum SSO certificate requirements. 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.

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 iLO for HP SSO

1. Navigate to the **Administration→Security→HP SSO** page.



Single Sign-On Settings

Single Sign-On Trust Mode: Trust by Certificate

	Login	Remote Console	Power & Reset	Virtual Media	Configure iLO	Administer Users
User Privileges	☑	□	□	□	□	□
Operator Privileges	☑	☑	☑	☑	□	□
Administrator Privileges	☑	☑	☑	☑	☑	☑

Manage Trusted Certificates

	Status	Certificate	Description
□	✓	▤	[redacted]

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 46).

   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 information about adding certificates and DNS names, see "Adding trusted certificates" (page 86).

   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 certificate (if any are installed).The possible status values follow:
  - ✓—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.

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.
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 a certificate by entering 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 86).

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.

NOTE: iLO 4 1.20 or later might be required to install the larger certificates used with recent versions of HP SIM.

NOTE: HP SIM 7.3.2 or later supports 2048-bit 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 trusted 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.
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?
   ```

   IMPORTANT: If you delete the certificate of a remote management system, you might experience impaired functionality when using the remote management system with iLO.

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.

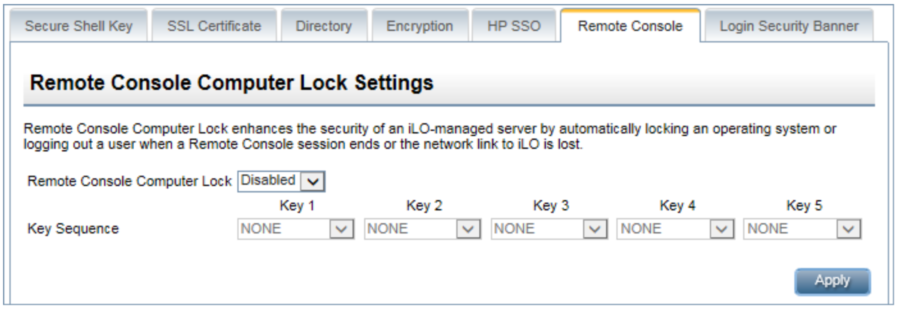
Configuring Remote Console Computer Lock settings

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.



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.

Remote Console Computer Lock: Disabled

	Key 1	Key 2	Key 3	Key 4	Key 5
Key Sequence	NONE	NONE	NONE	NONE	NONE

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 1 (page 88):

Table 1 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

Table 1 Remote Console Computer Lock keys *(continued)*

END	**F11**	\	**s**
PG_UP	**F12**	**]**	**t**
PG_DN	**" " (space)**	**'**	**u**
ENTER	**'**	**a**	**v**
TAB	**,**	**b**	**w**
BREAK	**-**	**c**	**x**
BACKSPACE	**.**	**d**	**y**
NUM PLUS	**/**	**e**	**z**
NUM MINUS	**0**	**f**	

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

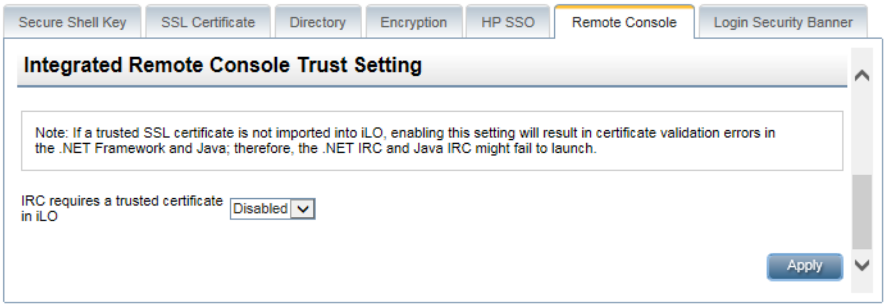
Configuring the Integrated Remote Console Trust setting (.NET IRC)

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.



Integrated Remote Console Trust Setting

Note: If a trusted SSL certificate is not imported into iLO, enabling this setting will result in certificate validation errors in the .NET Framework and Java; therefore, the .NET IRC and Java IRC might fail to launch.

IRC requires a trusted certificate in iLO: Disabled

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**.

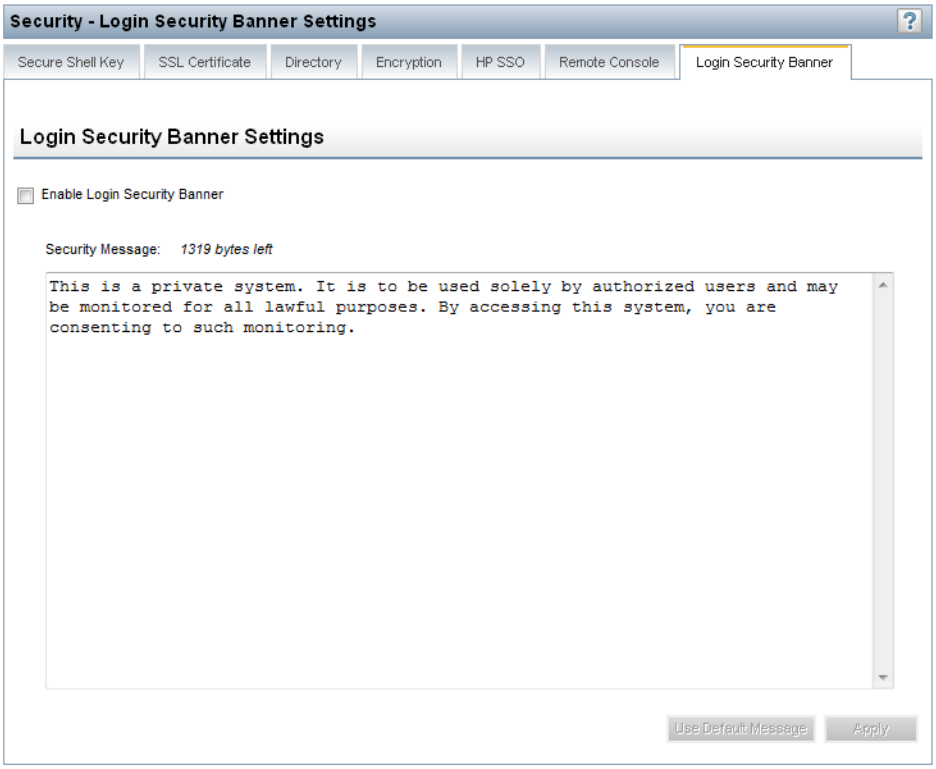
Configuring the Login Security Banner

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.



☐ Enable Login Security Banner

Security Message: *1319 bytes left*

```
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.
```

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.
   ```

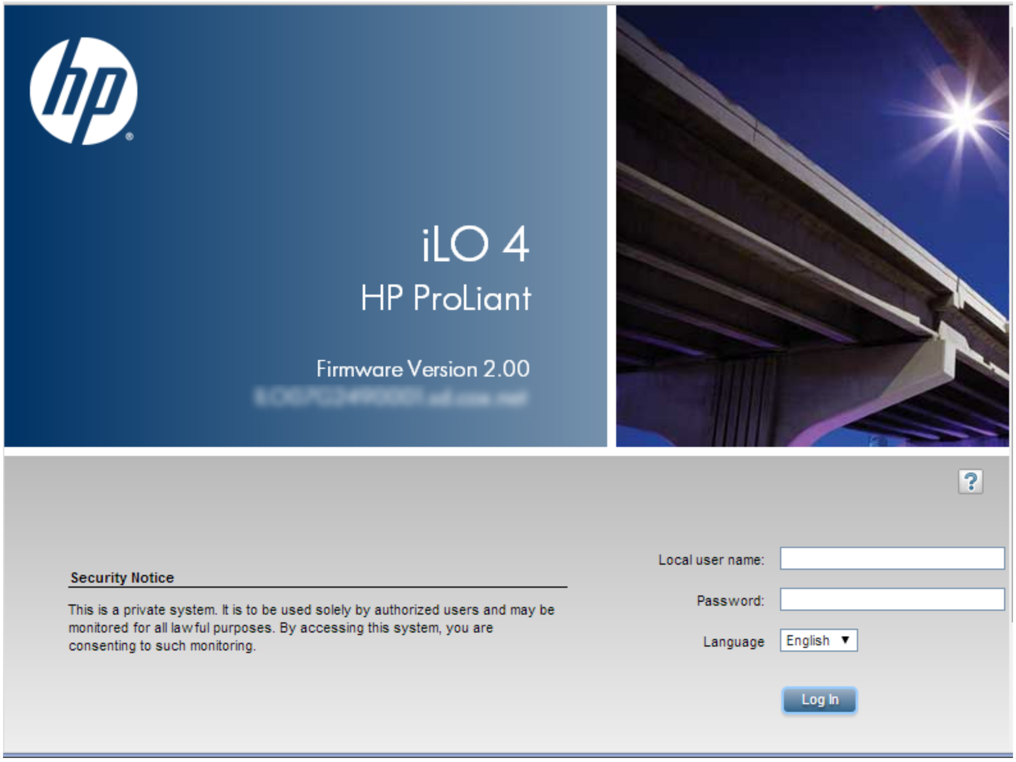
3. Optional: To customize the security message, enter a custom message in the **Security Message** text box.

   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.



[redacted]

Security Notice

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.

Managing the iLO network settings

iLO provides the following options for network connection:

- **iLO Dedicated Network Port**—Uses an independent NIC that is dedicated to iLO network traffic only. When supported, this port uses an RJ-45 jack (labeled **iLO**) on the back of the server.
- **Shared Network Port LOM**—Uses a permanently-installed NIC that is built into the server. This NIC normally handles server network traffic, and it can be configured to handle iLO network traffic at the same time via a common RJ-45 connector.
- **Shared Network Port FlexibleLOM**—Uses an optional NIC that plugs into a special slot on the server. This NIC normally handles server network traffic, and it can be configured to handle iLO network traffic at the same time via a common RJ-45 connector.

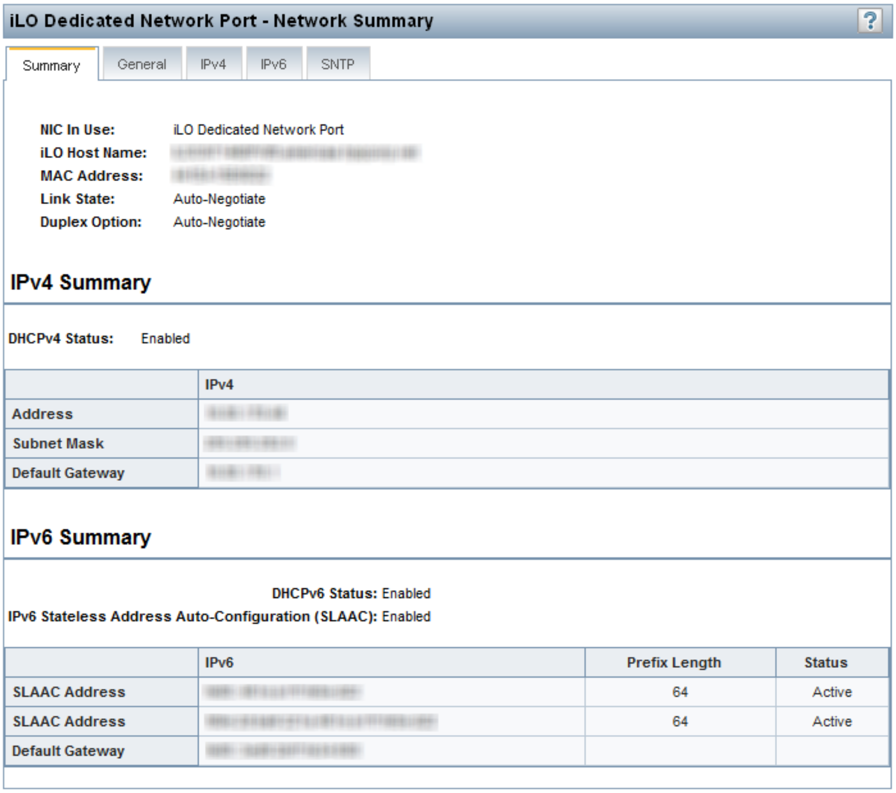
To view or configure the network settings in the iLO web interface, select the active NIC in the navigation tree (**Network→iLO Dedicated Network Port** or **Network→Shared Network Port**), and then view or edit the network settings on the following pages:

- **Network Summary**—For more information, see "Viewing the network configuration summary" (page 92).
- **Network General Settings**—For more information, see "Viewing the network configuration summary" (page 92).
- **IPv4 Settings**—For more information, see "Configuring IPv4 settings" (page 97).
- **IPv6 Settings**—For more information, see "Configuring IPv6 settings" (page 99).
- **SNTP Settings**—For more information, see "Configuring SNTP settings" (page 103).

If you select the inactive port option, the following message is displayed on the **Network Summary** page: `iLO is not configured to use this NIC.`

Viewing the network configuration summary

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



NIC In Use: iLO Dedicated Network Port
iLO Host Name: [redacted]
MAC Address: [redacted]
Link State: Auto-Negotiate
Duplex Option: Auto-Negotiate

IPv4 Summary

DHCPv4 Status: Enabled

	IPv4
Address	[redacted]
Subnet Mask	[redacted]
Default Gateway	[redacted]

IPv6 Summary

DHCPv6 Status: Enabled
IPv6 Stateless Address Auto-Configuration (SLAAC): Enabled

	IPv6	Prefix Length	Status
SLAAC Address	[redacted]	64	Active
SLAAC Address	[redacted]	64	Active
Default Gateway	[redacted]		

The summary information follows:

- **NIC in Use**—The name of the active 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 setting 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 93).

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 (iLO Dedicated Network Port only) 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).

  For more information about IPv6 support, see "Configuring IPv6 settings" (page 99).
- **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 99).

Configuring general network settings

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

Configuring the iLO Hostname Settings

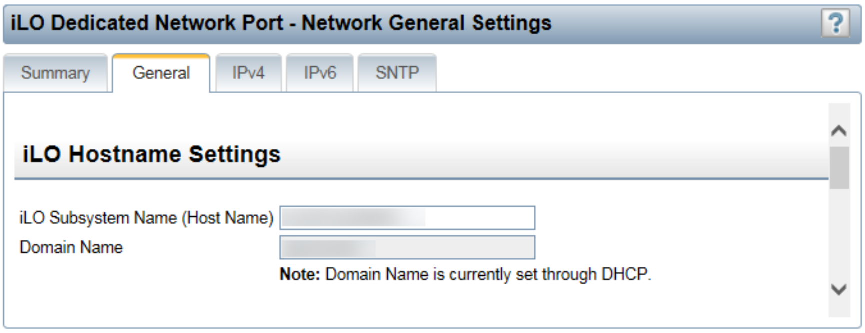
When you configure the **iLO Hostname Settings**, note the following iLO subsystem-name limitations:

- **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.

To configure the **iLO Hostname Settings**:

1. Navigate to the **Network→iLO Dedicated Network Port** or **Network→Shared Network Port** page.
2. Click the **General** tab.



iLO Dedicated Network Port - Network General Settings

iLO Hostname Settings

iLO Subsystem Name (Host Name)

Domain Name

Note: Domain Name is currently set through DHCP.

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.
   - **Domain Name**—The iLO domain name. If DHCP is not used, enter a domain name.

   IMPORTANT: When the iLO Dedicated Network port is selected, you must disable the following iLO settings to use a static domain name: **Use DHCPv4 Supplied Domain Name** and **Use DHCPv6 Supplied Domain Name**. For information about configuring these settings, see the "Configuring IPv4 settings" (page 97) and "Configuring IPv6 settings" (page 99).

   When the iLO Shared Network port is selected, you must disable the following iLO setting to use a static domain name: **Use DHCPv4 Supplied Domain Name**. For information about configuring this setting, see the "Configuring IPv4 settings" (page 97).

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

   It might take several minutes before you can re-establish a connection.

Understanding the iLO network port configuration options

iLO provides the following options for network connection:

- **iLO Dedicated Network Port**—Uses an independent NIC that is dedicated to iLO network traffic only. When supported, this port uses an RJ-45 jack (labeled **iLO**) on the back of the server.
- **Shared Network Port LOM**—Uses a permanently-installed NIC that is built into the server. This NIC normally handles server network traffic, and it can be configured to handle iLO network traffic at the same time via a common RJ-45 connector.
- **Shared Network Port FlexibleLOM**—Uses an optional NIC that plugs into a special slot on the server. This NIC normally handles server network traffic, and it can be configured to handle iLO network traffic at the same time via a common RJ-45 connector.

NOTE: For information about the NICs your server supports, see the server QuickSpecs at http://www.hp.com/go/qs/.

When configuring the iLO network connection options, observe the following:

- Only one of the Dedicated Network Port or Shared Network Port options can be enabled at a time because iLO supports only one active NIC connection.
- By default, the iLO Shared Network Port uses port 1 on the server NIC. Depending on the server configuration, this NIC might be a LOM or FlexibleLOM adapter. The port number corresponds to the label on the NIC, which might be different from the numbering in the operating system. iLO 4 2.00 and later allows you to select a different port if your server and NIC support port selection. If a port other than port 1 is selected for Shared Network Port use, and that configuration is not supported by your server, iLO will switch back to port 1 when it starts.
- Access to iLO via IPv6 is not currently supported when the Shared Network Port is enabled.
- 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. On these servers, the iLO firmware defaults to the Shared Network Port.
- 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 that the iLO Shared Network Port is connected to for auto-negotiation.

  If the switch port that iLO is connected to is configured for 1Gb/s, please 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.
- Disabling the iLO Shared Network Port does not completely disable the system NIC—server network traffic can still pass through the NIC port. When the iLO Shared Network Port is disabled, any traffic going to or originating from iLO will not pass through the Shared Network Port.
- If the Shared Network Port is enabled, you cannot modify the link state or duplex options. When using Shared Network Port configurations, these settings must be managed in the operating system.

Configuring the NIC settings

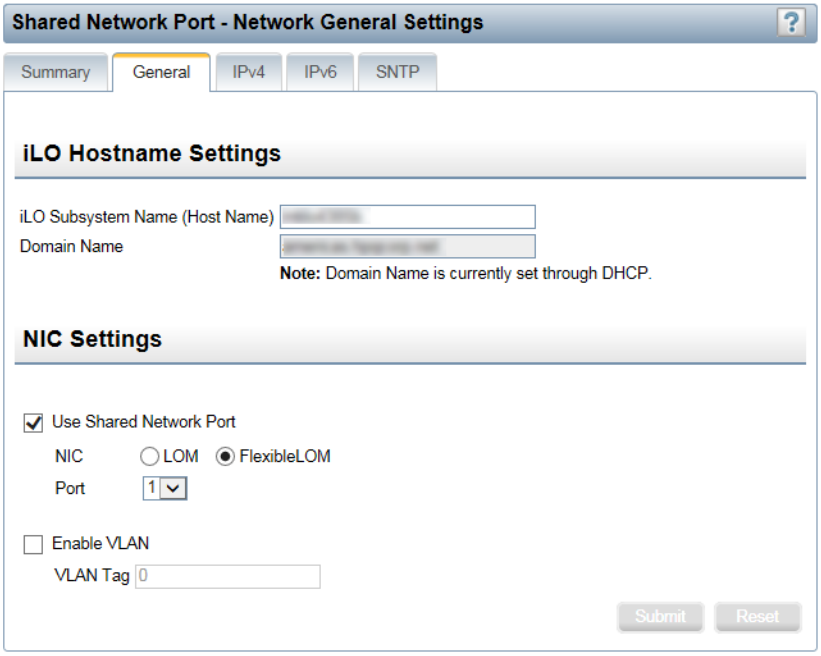
Use the **NIC Settings** section of the **Network General Settings** tab to enable the iLO Shared Network Port or the iLO Dedicated Network Port, and to configure the associated NIC settings.

You can also configure the NIC settings by using the following methods:

- **iLO RBSU** (on servers that support iLO RBSU)—For more information, see "Configuring iLO by using the ROM-based utilities" (page 133).
- **iLO 4 Configuration Utility** (on servers that support the HP UEFI System Utilities)—For more information, see"Configuring iLO by using the ROM-based utilities" (page 133).
- **XML scripting**—For more information, see the *HP iLO 4 Scripting and Command Line Guide*.
- **SMASH CLP**—For more information, see the *HP iLO 4 Scripting and Command Line Guide*.

Enabling the iLO Shared Network Port through the iLO web interface

1. Connect the Shared Network Port LOM or FlexibleLOM port to a LAN.
2. Navigate to the **Network→Shared Network Port** page.
3. Click the **General** tab.



Shared Network Port - Network General Settings

iLO Hostname Settings

iLO Subsystem Name (Host Name) [redacted]

Domain Name [redacted]

Note: Domain Name is currently set through DHCP.

NIC Settings

☑ Use Shared Network Port

NIC ○ LOM ● FlexibleLOM

Port 1

□ Enable VLAN

VLAN Tag 0

4. Select the **Use Shared Network Port** check box.
5. Depending on the server configuration, select **LOM**, or **FlexibleLOM**.
6. Select a value from the **Port** menu.

IMPORTANT: Selecting a port number other than 1 works only if the configuration is supported by both the server and the network adapter. If you enter an invalid port number, port 1 is used.

7. To use a VLAN, select the **Enable VLAN** check box.

   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.

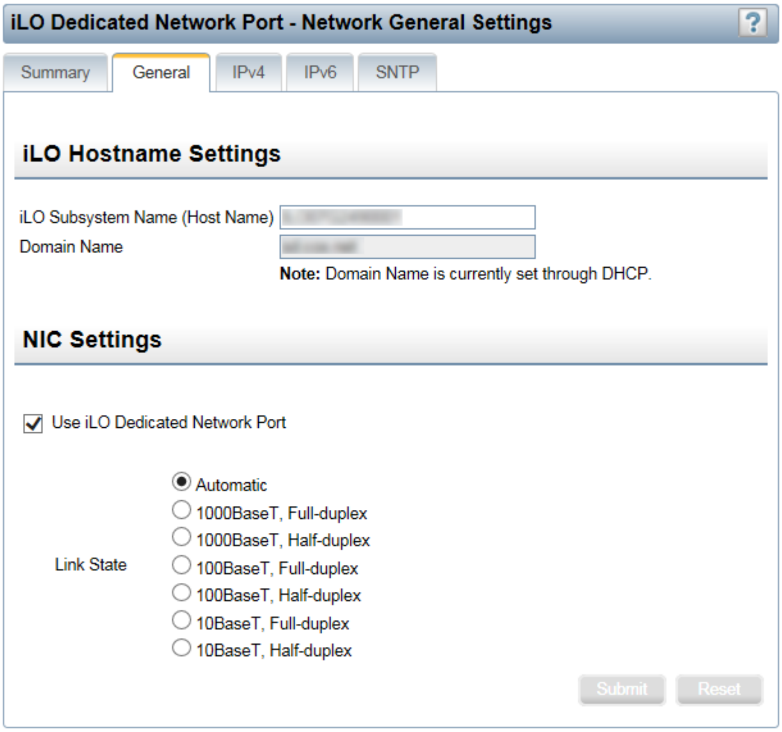
8. If you enabled VLAN, enter a **VLAN Tag**. All network devices that you want to communicate with each other must have the same VLAN tag. The VLAN tag can be any number between 1 and 4094.
9. Click **Submit** to save the changes.
10. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart iLO.

    It might take several minutes before you can re-establish a connection.

After iLO resets, the Shared Network Port is active. Any network traffic going to or originating from iLO is directed through the Shared Network Port LOM or FlexibleLOM port.

Enabling the iLO Dedicated Network Port through the iLO web interface

1. Connect the iLO Dedicated Network Port to a LAN from which the server is managed.
2. Navigate to the **Network→iLO Dedicated Network Port** page.
3. Click the **General** tab.



iLO Dedicated Network Port - Network General Settings

iLO Hostname Settings

iLO Subsystem Name (Host Name) [redacted]

Domain Name [redacted]

Note: Domain Name is currently set through DHCP.

NIC Settings

☑ Use iLO Dedicated Network Port

Link State
- ● Automatic
- ○ 1000BaseT, Full-duplex
- ○ 1000BaseT, Half-duplex
- ○ 100BaseT, Full-duplex
- ○ 100BaseT, Half-duplex
- ○ 10BaseT, Full-duplex
- ○ 10BaseT, Half-duplex

4. Select the **Use iLO Dedicated Network Port** check box.
5. Select a **Link State**.

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

   NOTE: This setting is not available on server blades.

   The available settings follow:

   - **Automatic** (default)—Enables iLO to negotiate the highest supported link speed and duplex settings when connected to the network
   - **1000BaseT, Full-duplex**—Forces a 1 Gb connection that uses full duplex (not supported for BL c-Class servers)
   - **1000BaseT, Half-duplex**—Forces a 1 Gb connection that uses half duplex (not supported for BL c-Class servers)

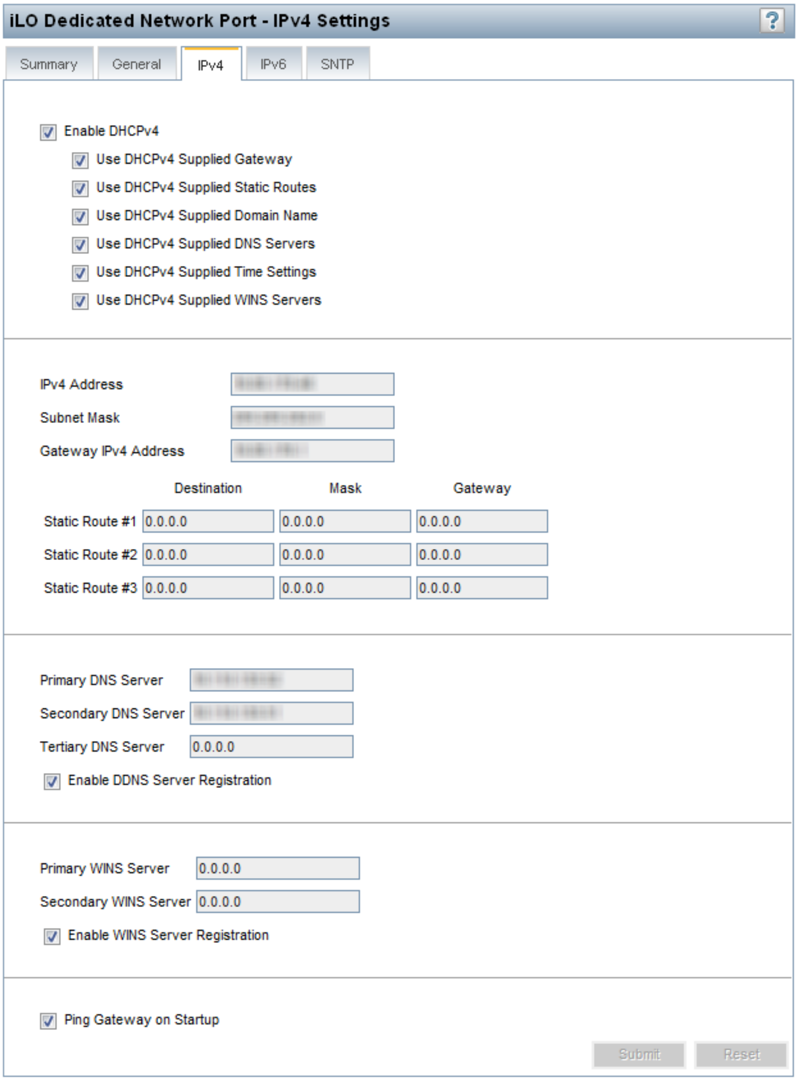
     1000BaseT, Half-duplex is not a standard setting, and few switches support it. If you use this setting, ensure that the switch is configured to support 1000BaseT, Half-duplex.
   - **100BaseT, Full-duplex**—Forces a 100 Mb connection using full duplex
   - **100BaseT, Half-duplex**—Forces a 100 Mb connection 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
6. Click **Submit** to save the changes.
7. If you are finished configuring the iLO network settings on the **General**, **IPv4**, **IPv6**, and **SNTP** tabs, click **Reset** to restart iLO.

   It might take several minutes before you can 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.



☑ Enable DHCPv4

- ☑ Use DHCPv4 Supplied Gateway
- ☑ Use DHCPv4 Supplied Static Routes
- ☑ Use DHCPv4 Supplied Domain Name
- ☑ Use DHCPv4 Supplied DNS Servers
- ☑ Use DHCPv4 Supplied Time Settings
- ☑ Use DHCPv4 Supplied WINS Servers

IPv4 Address [redacted]

Subnet Mask [redacted]

Gateway IPv4 Address [redacted]

	Destination	Mask	Gateway
Static Route #1	0.0.0.0	0.0.0.0	0.0.0.0
Static Route #2	0.0.0.0	0.0.0.0	0.0.0.0
Static Route #3	0.0.0.0	0.0.0.0	0.0.0.0

Primary DNS Server [redacted]

Secondary DNS Server [redacted]

Tertiary DNS Server 0.0.0.0

☑ Enable DDNS Server Registration

Primary WINS Server 0.0.0.0

Secondary WINS Server 0.0.0.0

☑ Enable WINS Server Registration

☑ Ping Gateway on Startup

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 93).
     - **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.

   It might take several minutes before you can re-establish a connection.

Configuring IPv6 settings

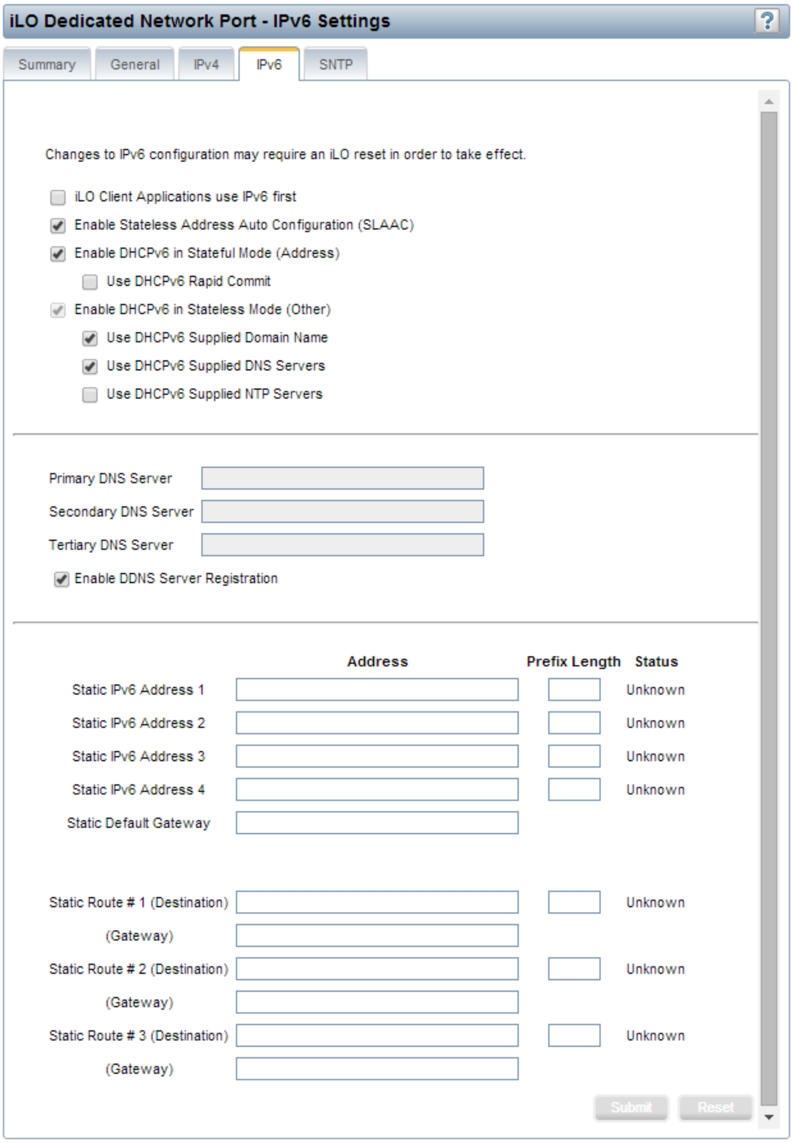
Use the iLO Dedicated Network Port **IPv6 Settings** page to configure IPv6 settings for iLO. You must have the Configure iLO Settings privilege to make changes on this page.

When using IPv6, note the following:

- IPv6 is not supported in the Shared Network Port configuration.
- If you downgrade the iLO firmware from version 1.30 or later to version 1.2x, the IPv6 settings will be reset to the default values.
- For a list of the iLO features that support IPv6, see "iLO features that support IPv6" (page 102).

To configure the IPv6 settings:

1. Navigate to the **Network→iLO Dedicated Network Port** page.
2. Click the **IPv6** tab.



iLO Dedicated Network Port - IPv6 Settings

Changes to IPv6 configuration may require an iLO reset in order to take effect.

☐ iLO Client Applications use IPv6 first
☑ Enable Stateless Address Auto Configuration (SLAAC)
☑ Enable DHCPv6 in Stateful Mode (Address)
☐ Use DHCPv6 Rapid Commit
☑ Enable DHCPv6 in Stateless Mode (Other)
☑ Use DHCPv6 Supplied Domain Name
☑ Use DHCPv6 Supplied DNS Servers
☐ Use DHCPv6 Supplied NTP Servers

Primary DNS Server
Secondary DNS Server
Tertiary DNS Server
☑ Enable DDNS Server Registration

	Address	Prefix Length	Status
Static IPv6 Address 1			Unknown
Static IPv6 Address 2			Unknown
Static IPv6 Address 3			Unknown
Static IPv6 Address 4			Unknown
Static Default Gateway			
Static Route # 1 (Destination)			Unknown
(Gateway)			
Static Route # 2 (Destination)			Unknown
(Gateway)			
Static Route # 3 (Destination)			Unknown
(Gateway)			

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 Domain Name**—Select this check box to use the DHCPv6 server-supplied domain name.
  - **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.

   It might take several minutes before you can re-establish a connection.

iLO features that support IPv6

IPv6 is supported by iLO 4 1.20 and later in the iLO Dedicated Network Port configuration. It is not supported with the Shared 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.

The following features support the use of IPv6:

- IPv6 Static Address Assignment
- IPv6 SLAAC Address Assignment
- IPv6 Static Route Assignment
- IPv6 Static Default Gateway Entry
- DHCPv6 Stateful Address Assignment
- DHCPv6 Stateless DNS, Domain Name, and NTP Configuration
- Integrated Remote Console
- Onboard Administrator Single Sign-On
- HP-SIM Single Sign-On
- Web Server
- SSH Server
- SNTP Client
- DDNS Client
- RIBCL over IPv6
- SNMP
- AlertMail
- Remote Syslog
- WinDBG Support
- HPQLOCFG/HPLOMIG over an IPv6 connection
- Scriptable Virtual Media
- CLI/RIBCL key import over an IPv6 connection
- Authentication using LDAP and Kerberos over IPv6
- iLO Federation

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

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 server blades only)

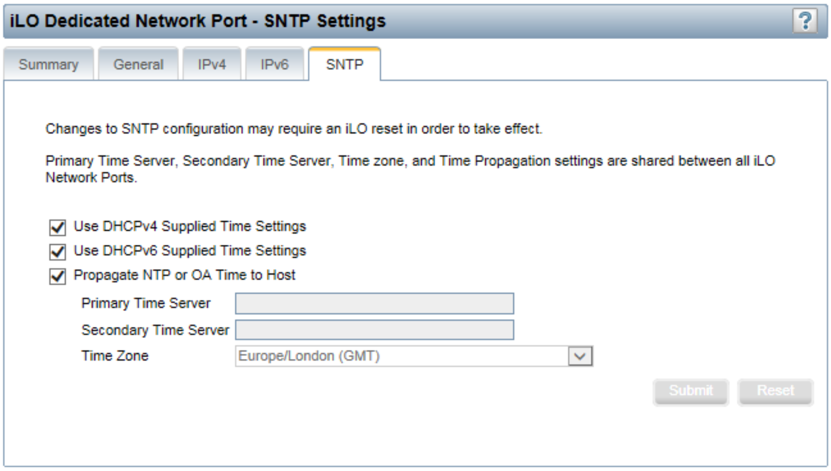
To use iLO SNTP, you must have at least one NTP server available on your management network.

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.



iLO Dedicated Network Port - SNTP Settings

Changes to SNTP configuration may require an iLO reset in order to take effect.

Primary Time Server, Secondary Time Server, Time zone, and Time Propagation settings are shared between all iLO Network Ports.

☑ Use DHCPv4 Supplied Time Settings
☑ Use DHCPv6 Supplied Time Settings
☑ Propagate NTP or OA Time to Host

Primary Time Server
Secondary Time Server
Time Zone: Europe/London (GMT)

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 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 Onboard Administrator 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.

   It might take several minutes before you can 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).

Using iLO NIC auto-selection

The iLO NIC auto-selection feature enables iLO to automatically select between the iLO Dedicated Network Port and the iLO Shared Network port. At startup, iLO searches for network activity on the available ports, and automatically selects one for use based on network activity.

This feature enables you to use a common pre-configuration for all of your HP ProLiant Gen9 servers. For example, if you have several servers, some might be installed into a data center where iLO is contacted by using the iLO Dedicated Network Port, and others might be installed a data center where iLO is contacted by using the Shared Network Port. When you use iLO NIC auto-selection, you can install a server in either data center and iLO will select the correct network port.

HP ProLiant Gen9 servers with iLO 4 2.00 or later support NIC auto-selection.

At iLO startup, when iLO NIC auto-selection is enabled:

- If iLO was just connected to power, it tests the iLO Dedicated Network Port first.
- If iLO was just reset, it tests the last used iLO network port first.
- When testing a network port, if iLO detects network activity, then that port is selected for use. If network activity is not found after approximately 100 seconds, iLO switches to the opposite network port and begins testing there. iLO alternates testing between the iLO Dedicated Network Port and the iLO Shared Network Port until network activity is detected. An iLO reset occurs each time iLO switches between network ports for testing purposes.

△ **CAUTION:** If any of the physical NICs are connected to an unsecured network, it might be possible for unauthorized access attempts to occur when iLO is alternating between the iLO Dedicated Network Port and iLO Shared Network Port. HP strongly recommends that whenever iLO is connected to any network:

  - Use strong passwords for iLO access.
  - Never connect the iLO Dedicated Network Port to an unsecured network.
  - If the iLO Shared Network Port is connected to an unsecured network, use VLAN tagging on the iLO portion of the shared NIC, and make sure that the VLAN is connected to a secure network only.

- When iLO is searching for an active network port, the server UID LED is illuminated. If iLO is reset during the search, the UID LED flashes for 5 seconds, followed by the UID LED being illuminated continuously until an active port is selected or iLO is reset.
- When a server supports both LOM and FlexibleLOM Shared Network Port connections to iLO, iLO will test only the option that was selected during configuration. It will not alternate testing between LOM and FlexibleLOM options.

  For information about configuring the Shared Network Port options, see "Enabling the iLO Shared Network Port through the iLO web interface" (page 95).
- If NIC auto-selection is configured to search for DHCP address assignment activity, but only one of the iLO network ports has DHCP enabled, iLO tests for received data packet activity on the port that is not configured for DHCP.

Configuring iLO NIC auto-selection

To enable the NIC auto-selection feature, do the following:

1. Configure both iLO network ports.

   Before enabling and using the NIC auto-selection feature, both iLO network ports must be configured for their respective network environments.
2. Enable the feature using the CLI command `oemhp_nicautosel` or by adding the ILO_NIC_AUTO_SELECT command to your MOD_NETWORK_SETTINGS script.

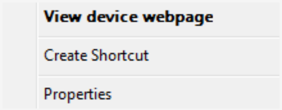
   For instructions, see the *HP iLO 4 Scripting and Command Line Guide*.
3. Arrange server cabling as desired, and then reset iLO.

   The change to NIC auto-selection does not take effect until iLO is reset.

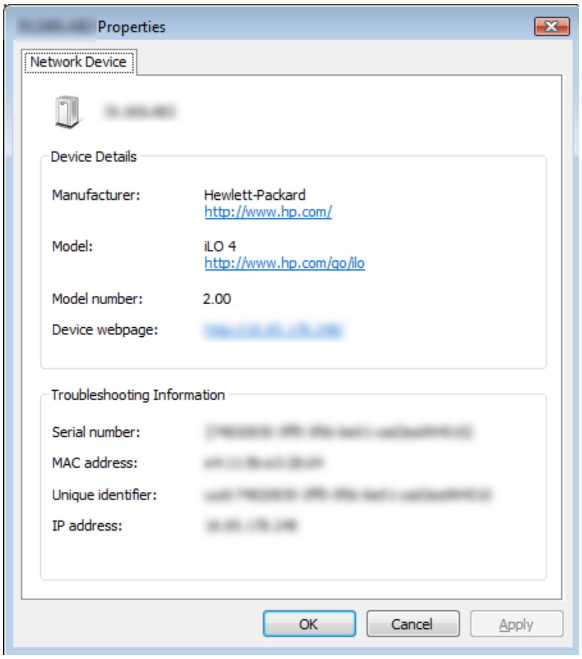
Viewing iLO systems in the Windows Network folder

If UPnP is configured, iLO systems on the same network as a Windows system are displayed in the Windows **Network** folder.

- To start the web interface for an iLO system, right-click the system in the Windows **Network** folder, and then select **View device webpage**.



- To view the properties of an iLO system, right-click the icon in the Windows **Network** folder, and then select **Properties**.



[redacted]

Device Details

Manufacturer: Hewlett-Packard http://www.hp.com/

Model: iLO 4 http://www.hp.com/go/ilo

Model number: 2.00

Device webpage: [redacted]

Troubleshooting Information

Serial number: [redacted]

MAC address: [redacted]

Unique identifier: [redacted]

IP address: [redacted]

The **Properties** window includes the following:

- **Device Details**—iLO software manufacturer and version information. Click the **Device weblog** link to start the iLO web interface.
- **Troubleshooting Information**—The iLO serial number, MAC address, UUID, and IP address.

Configuring iLO Management settings

With iLO 3 and earlier, SNMP management used the HP Insight Management Agents running on the server operating system. With iLO 4, you can use either Agentless Management or the Insight Management Agents. The default configuration uses Agentless Management.

iLO 4 Agentless Management uses out-of-band communication for increased security and stability. With Agentless Management, health monitoring and alerting is built into the system and begins working the moment a power cord is connected to the server. This feature runs on the iLO hardware, independent of the operating system and processor. Additional operating system data is collected when AMS is installed.

The **Management – SNMP Settings** page allows you to configure the iLO settings for SNMP, 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. For more information, see “Installing AMS or the Insight Management Agents” (page 107).

Table 2 (page 107) provides a comparison of the information provided by the HP ProLiant Gen8 and Gen9 server configurations.

Table 2 Information provided by Agentless Management and Insight Management Agents

Component	Agentless Management without AMS[1]	Agentless Management with AMS[1]	Insight Management Agents[1]
Server health	• Fans • Temperatures • Power supplies • Memory • CPU • Gen9 only: Smart Storage battery monitoring	• Fans • Temperatures • Power supplies • Memory • CPU • Gen9 only: Smart Storage battery monitoring	• Fans • Temperatures • Power supplies • Memory • CPU
Storage	• Smart Array • SMART Drive Monitoring (connected to Smart Array) • Internal and external drives connected to Smart Array	• Smart Array • iSCSI SAS/SATA HBA[2] • SMART Drive Monitoring (connected to Smart Array and SAS HBA) • Internal and external drives connected to Smart Array	• Smart Array • SAS/SATA HBA/RAID • Fibre Channel/iSCSI • SMART Drive Monitoring (connected to Smart Array and SAS HBA) • Tape • External storage
NIC	• MAC addresses for embedded NICs	• MAC and IP address for standup and embedded NICs • Link up/link down traps[2]	• MAC and IP addresses for standup and embedded NICs • Teaming information • Link up/link down traps • VLAN information
Other	• iLO data • Firmware inventory	• iLO data • OS information (host MIB)[2] • Firmware inventory • Driver/service inventory • Logging events to OS logs[3]	• OS information (host MIB) • iLO data • Performance data • User-configurable thresholds • Logging events to OS logs • Clustering information
Pre-failure warranty alerts	• Memory • Drives (physical and logical)	• Memory • Drives (physical and logical)	• Memory • Drives (physical and logical) • CPU

[1] The **Agentless Management without AMS** column represents the basic iLO configuration without AMS or the Insight Management Agents. HP ProLiant Gen8 and Gen9 server configurations with AMS or the Insight Management Agents provide the same information as the basic iLO configuration, as well as the information that is listed in the **Agentless Management with AMS** and **Insight Management Agents** columns.

[2] The data supplied by Agentless Management is not as extensive as the data supplied by the SNMP agents.

[3] iLO 4 1.10 and later supports AMS-based OS logging for Linux (var/message/log), Solaris, and VMware.

Installing AMS or the Insight Management Agents

AMS is installed automatically when you perform an operating system installation using HP Intelligent Provisioning or the HP Service Pack for ProLiant. Follow the instructions in this section if AMS is not installed or if you want to use the Insight Management Agents.

When you are using Agentless Management and AMS, note the following:

- To verify AMS installation, see “Verifying the AMS installation” (page 108).
- HP does not recommend installing AMS at the same time as the Insight Management Agents and WMI Providers.
- If you must run AMS with the Insight Management Agents on Linux systems, start the `hp-ams` daemon process first, and then decrease the number of traditional agents (for example, `cmasm2d`) running on the system. For more information about AMS on Linux systems, see the manpage for `hpHelper`, the AMS daemon process.
- When you install AMS on Windows systems, the Agentless Management Service Control Panel is installed. You can use the Control Panel to configure SNMP settings, to enable or disable AMS, and to remove AMS.
- AMS writes operating system configuration information and critical events to the Active Health System Log.
- Use one of the following methods to obtain the AMS software or the Insight Management Agents:
  - **HP Service Pack for ProLiant (Windows, Red Hat, SLES)**—Navigate to the following website to download the SPP: http://www.hp.com/go/spp.

    For instructions on using the HP Service Pack for ProLiant to install AMS or the Insight Management Agents, see the Service Pack for ProLiant documentation.
  - **HP Support Center (Windows, Red Hat, SLES, VMware)**
    1. Navigate to the technical support page on the HP website: http://www.hp.com/support.
    2. Select a country or region.

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

       In the search box, enter the server model number.

       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.
  - **Software Delivery Repository (Ubuntu)**—Download AMS or the Insight Management Agents from the **mcp** section of the Software Delivery Repository at http://downloads.linux.hp.com/SDR/index.html.
  - **Software Delivery Repository (VMware)**—Download AMS or the Insight Management Agents from the **vibsdepot** section of the Software Delivery Repository website at http://downloads.linux.hp.com/SDR/index.html.

    AMS is also included in the customized HP VMware ISO images that are released on HP Software Depot (http://www.hp.com/go/softwaredepot).

Verifying the AMS installation

Use the following procedures to verify the AMS installation on Windows, Linux, and VMware systems.

Verifying AMS installation: Windows

To verify that AMS is enabled on a Windows system:

1. Open the Windows Control Panel.

   If the Agentless Management Service Control Panel is present, then AMS is installed.
2. Open the Agentless Management Service Control Panel.
3. Click the **Service** tab.

   If AMS is enabled, the following message appears:

   ```
   Agentless Management Service (AMS) is enabled.
   ```

Verifying AMS installation: SUSE and Red Hat

To verify that AMS is installed on a SUSE or Red Hat system, enter the following command:

```
rpm -qi hp-ams
```

To verify that AMS is running on a SUSE or Red Hat system, enter the following command:

```
service hp-ams status
```

Verifying AMS installation: VMware

To verify that AMS is installed on a VMware system:

1. Access the VMware host from the VMware vSphere Client.
2. Navigate to the server's **Inventory**→**Configuration**→**Health Status** tab.
3. Click the plus sign (+) next to **Software Components**.

   The software installed on the host is listed. The AMS component includes the string `hp-ams`.

   NOTE: The full name of the AMS component is different for each supported version of ESX/ESXi.

To verify that AMS is running on a VMware system, enter the following command:

```
service hp-ams status
```

Verifying AMS installation: Ubuntu

To verify that AMS is installed on an Ubuntu system, enter the following command:

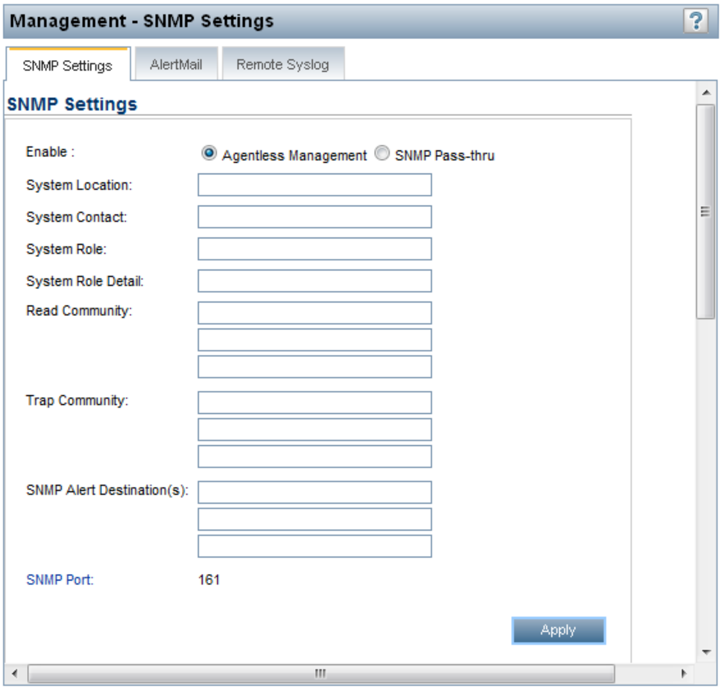
```
dpkg -l hp-ams
```

To verify that AMS is running on an Ubuntu system, enter the following command:

```
sudo service hp-ams status
```

Configuring SNMP settings

1. Navigate to the **Administration**→**Management** page.
2. Click the **SNMP Settings** tab.



Management - SNMP Settings

SNMP Settings

Enable : ● Agentless Management ○ SNMP Pass-thru

System Location:

System Contact:

System Role:

System Role Detail:

Read Community:

Trap Community:

SNMP Alert Destination(s):

SNMP Port: 161

3. Select the SNMP setting:
   - **Agentless Management** (default)—Use SNMP agents running on iLO to manage the server. SNMP requests sent by the client to iLO over the network are fulfilled by iLO. This setting does not affect 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. This setting does not affect alerts.
4. Enter the following information:
   - **System Location** (Agentless Management only)—A string of up to 49 characters that specifies the physical location of the server.
   - **System Contact** (Agentless Management only)—A string of up to 49 characters that specifies the system administrator or server owner. The string can include a name, email address, or phone number.
   - **System Role** (Agentless Management only)—A string of up to 64 characters that describes the server role or function.
   - **System Role Detail** (Agentless Management only)—A string of up to 512 characters that describes specific tasks that the server might perform.
   - **Read Community** (Agentless Management only)—The configured SNMP read-only community string.

     Read Community supports the following formats:
     - A community string (for example, `public`).
     - A community string followed by an IP address or FQDN (for example, `public 192.168.0.1`).

       Use this option to specify that SNMP access will be allowed from the specified IP address or FQDN. For iLO 4 1.10 or later, you can enter an IPv4 address or FQDN.
   - **Trap Community**—The configured SNMP trap community string.

- **SNMP Alert Destination(s)**—The IP addresses or FQDNs of up to three remote management systems that will receive SNMP alerts from iLO.

  NOTE: Typically, you enter the HP SIM server console IP address in one of the **SNMP Alert Destination(s)** boxes.

  When SNMP Alert Destinations are configured using FQDN, and DNS provides both IPv4 and IPv6 addresses for those FQDNs, iLO will send traps to the address specified by the **iLO Client Applications use IPv6 first** setting on the network configuration **IPv6** page. If **iLO Client Applications use IPv6 first** is selected, traps will be sent to IPv6 addresses (when available). When **iLO Client Applications use IPv6 first** is not selected, traps will be sent to IPv4 addresses (when available).

- **SNMP Port**—The port used for SNMP communications. This value is read-only, but can be modified on the **Administration→Access Settings** page.

  Click the **SNMP Port** link to navigate to the **Administration→Access Settings** page. For more information, see "Configuring iLO access settings" (page 57).

5. Click **Apply** to save the configuration.

Configuring SNMPv3 Users

iLO 4 1.20 or later supports SNMPv3 authentication when you use Agentless Management.

The following security features of SNMPv3 enable secure data collection from SNMP agents:

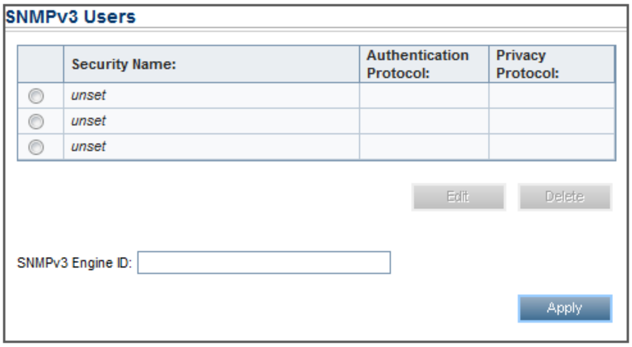
- Message integrity prevents tampering during packet transmission.
- Encryption prevents packet snooping.
- Authentication ensures that packets are from a valid source.

By default, SNMPv3 supports the User-based Security Model. With this model, security parameters are configured at both the agent level and the manager level. Messages exchanged between the agent and the manager are subject to a data integrity check and data origin authentication.

iLO supports three user profiles in which you can set the SNMPv3 USM parameters.

To edit SNMPv3 user profiles:

1. Navigate to the **Administration→Management** page.
2. Click the **SNMP Settings** tab and scroll to the **SNMPv3 Users** section.



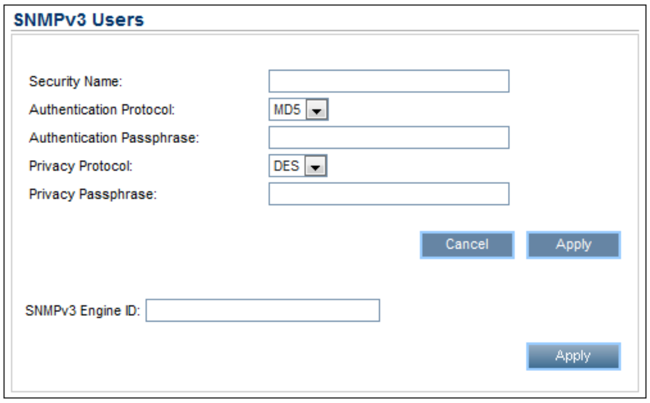
SNMPv3 Users

	Security Name:	Authentication Protocol:	Privacy Protocol:
○	unset		
○	unset		
○	unset		

SNMPv3 Engine ID:

3. Select a user profile in the **SNMPv3 Users** section, and then click **Edit**.

   The iLO web interface updates to show the SNMPv3 user options.



Authentication Protocol: MD5

Privacy Protocol: DES

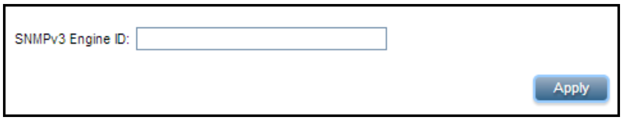
4. Enter the following information:
   - **Security Name**—The user profile name. Enter an alphanumeric string of 1 to 32 characters.
   - **Authentication Protocol**—Sets the message digest algorithm to use for encoding the authorization passphrase. The message digest is calculated over an appropriate portion of an SNMP message, and is included as part of the message sent to the recipient. Select **MD5** or **SHA**.
   - **Authentication Passphrase**—Sets the passphrase to use for sign operations. Enter a value of 8 to 49 characters.
   - **Privacy Protocol**—Sets the encryption algorithm to use for encoding the privacy passphrase. A portion of an SNMP message is encrypted before transmission. Select **AES** or **DES**.
   - **Privacy Passphrase**—Sets the passphrase used for encrypt operations. Enter a value of 8 to 49 characters.
5. Click **Apply** to save the user profile.

Configuring the SNMPv3 Engine ID

The **SNMPv3 Engine ID** sets the unique identifier of an SNMP engine belonging to an SNMP agent entity. You can configure this value when **Agentless Management** is selected.

To configure the SNMPv3 Engine ID:

1. Navigate to the **Administration→Management** page.
2. Click the **SNMP Settings** tab and scroll to the **SNMPv3 Users** section.



3. Enter a value in the **SNMPv3 Engine ID** box.

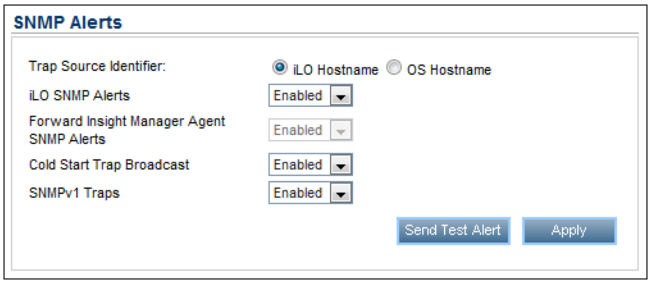
   This value must be a hexadecimal string of 6 to 32 characters, and must be an even number of characters, excluding the preceding `0x` (for example, `0x01020304abcdef`).
4. Click **Apply**.

Configuring SNMP alerts

You can configure the Trap Source Identifier, iLO SNMP alerts, forwarding of Insight Management Agent SNMP alerts, Cold Start Trap broadcast, and SNMPv1 traps.

To configure SNMP alerts:

1. Navigate to the **Administration→Management** page.
2. Click the **SNMP Settings** tab and scroll to the **SNMP Alerts** section.


SNMP Alerts

Trap Source Identifier: ● iLO Hostname ○ OS Hostname

iLO SNMP Alerts: Enabled

Forward Insight Manager Agent SNMP Alerts: Enabled

Cold Start Trap Broadcast: Enabled

SNMPv1 Traps: Enabled

3. Configure the **Trap Source Identifier** by selecting **iLO Hostname** or **OS Hostname**.

   This setting determines the host name that is used in the SNMP-defined **sysName** variable when iLO generates SNMP traps. The default setting is **iLO Hostname**.

   NOTE: The host name is an OS construct and does not remain persistent with the server when the hard drives are moved to a new server platform. The iLO **sysName**, however, remains persistent with the system board.

4. 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. If this option is disabled, no traps will be sent to the configured SNMP alert destinations.
   - **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.
   - **Cold Start Trap Broadcast**—When this option is enabled, Cold Start Trap is broadcast to a subnet broadcast address if no valid trap destinations are configured.

     The Cold Start Trap is broadcast when any of the following conditions is met:

     - **SNMP Alert Destinations** are not configured.
     - iLO failed to resolve all of the **SNMP Alert Destinations** to IP addresses.

     The subnet broadcast address for an IPv4 host is obtained by performing a bitwise logical `OR` operation between the bit complement of the subnet mask and the host IP address. For example, the host `192.168.1.1`, which has the subnet mask `255.255.252.0`, has the broadcast address `192.168.1.1 | 0.0.3.255 = 192.168.3.255`.
   - **SNMPv1 Traps**—When enabled, SNMPv1 traps are sent to the remote management systems configured in the **SNMP Alert Destination(s)** boxes.

5. 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.

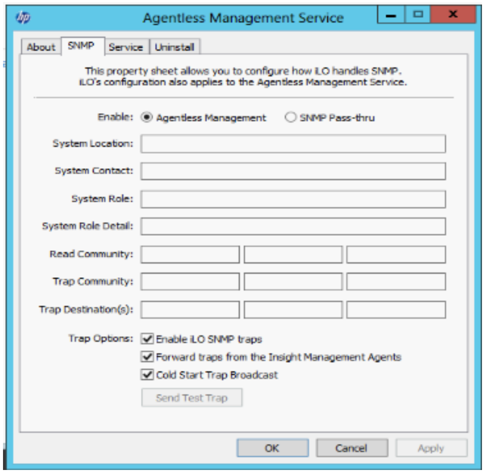
   Test alerts include an Insight Management SNMP trap, and are used to verify the network connectivity of iLO in HP SIM. Only users with the Configure iLO Settings privilege can send test alerts.

   After the alert is generated, a confirmation dialog box opens. Check the HP SIM console for receipt of the alert.

6. Click **Apply** to save the configuration.

Using the AMS Control Panel to configure SNMP and SNMP alerts (Windows only)

1. Open the Agentless Management Service Control Panel.
2. Click the **SNMP** tab.



This property sheet allows you to configure how iLO handles SNMP.
iLO's configuration also applies to the Agentless Management Service.

Enable: ● Agentless Management ○ SNMP Pass-thru

System Location:

System Contact:

System Role:

System Role Detail:

Read Community:

Trap Community:

Trap Destination(s):

Trap Options: ☑ Enable iLO SNMP traps
☑ Forward traps from the Insight Management Agents
☑ Cold Start Trap Broadcast

3. Update the SNMP settings.

   For a description of the available settings, see "Configuring SNMP settings" (page 109) and "Configuring SNMP alerts" (page 112).

4. Optional: Click **Send Test Trap** to generate a test alert and send it to the TCP/IP addresses in the **Trap 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 that have 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

Table 3 (page 114) lists the SNMP traps that you can generate with iLO and HP ProLiant Gen8 and Gen9 servers.

For more information about these SNMP traps, see the following files in the Insight Management MIB update kit for HP SIM:

- `cpqida.mib`
- `cpqhost.mib`
- `cpqhlth.mib`
- `cpqsm2.mib`
- `cpqide.mib`
- `cpqscsi.mib`
- `cpqnic.mib`
- `cpqstsys.mib`
- `cpqstdeq.mib`

Table 3 SNMP traps

SNMP trap name	Description
Cold Start Trap 0	SNMP has been initialized, the system has completed POST, or AMS has started.
Authentication Failure Trap 4	SNMP has detected an authentication failure.

Table 3 SNMP traps *(continued)*

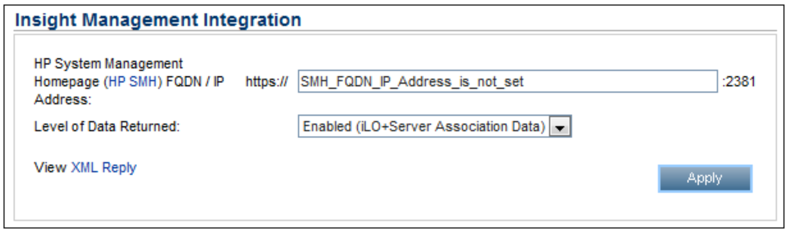
SNMP trap name	Description
cpqSeCpuStatusChange 1006	An uncorrectable machine check exception has been detected in a processor.
cpqDa6CntlrStatusChange 3033	A change has been detected in the status of the Smart Array controller.
cpqDa6LogDrvStatusChange 3034	A change has been detected in the status of a Smart Array logical drive.
cpqDa6AccelStatusChange 3038	A change has been detected in the status of a Smart Array cache module.
cpqDa6AccelBadDataTrap 3039	The Smart Array cache module has lost backup power.
cpqDa6AccelBatteryFailed 3040	The Smart Array cache module backup power has failed.
cpqDa7PhyDrvStatusChange 3046	A change has been detected in the status of a Smart Array physical drive.
cpqDa7SpareStatusChange 3047	A change has been detected in the status of a Smart Array spare drive.
cpqDaPhyDrvSSDWearStatusChange 3049	A change has been detected in the SSD wear status of a Smart Array physical drive.
cpqHe3ThermalConfirmation 6026	The server was shut down due to a thermal anomaly and is now operational.
cpqHe3PostError 6027	One or more POST errors have occurred.
cpqHe3FltTolPowerRedundancyLost 6032	The fault-tolerant power supplies have lost redundancy for the specified chassis.
cpqHe3FltTolPowerSupplyInserted 6033	A fault-tolerant power supply has been inserted.
cpqHe3FltTolPowerSupplyRemoved 6034	A fault-tolerant power supply has been removed.
cpqHe3FltTolFanDegraded 6035	The fault-tolerant fan condition has been set to **Degraded**.
cpqHe3FltTolFanFailed 6036	The fault-tolerant fan condition has been set to **Failed**.
cpqHe3FltTolFanRedundancyLost 6037	The fault-tolerant fans have lost redundancy.
cpqHe3FltTolFanInserted 6038	A fault-tolerant fan has been inserted.
cpqHe3FltTolFanRemoved 6039	A fault-tolerant fan has been removed.
cpqHe3TemperatureDegraded 6041	The temperature status has been set to **Degraded**, and the temperature is outside the normal operating range. Depending on the system configuration, this system might be shut down.
cpqHe3TemperatureOk 6042	The temperature status has been set to **OK**.
cpqHe4FltTolPowerSupplyOk 6048	The fault-tolerant power supply condition has been reset to **OK**.
cpqHe4FltTolPowerSupplyDegraded 6049	The fault-tolerant power supply condition has been set to **Degraded**.
cpqHe4FltTolPowerSupplyFailed 6050	The fault-tolerant power supply condition has been set to **Failed**.
cpqHeResilientMemMirroredMemoryEngaged 6051	The Advanced Memory Protection subsystem has detected a memory fault. Mirrored Memory has been activated.
cpqHe3FltTolPowerRedundancyRestore 6054	The fault-tolerant power supplies have returned to a redundant state.
cpqHe3FltTolFanRedundancyRestored 6055	The fault-tolerant fans have returned to a redundant state.
cpqHe5CorrMemReplaceMemModule 6064	Memory errors have been corrected, but the memory module should be replaced.

Table 3 SNMP traps *(continued)*

SNMP trap name	Description
cpqHe4FltTolPowerSupplyACpowerloss 6069	The fault-tolerant power supply in the specified chassis and bay reported AC power loss.
cpqHeSysBatteryFailed 6070	The HP Smart Storage battery has failed.
cpqHeSysBatteryRemoved 6071	The HP Smart Storage battery has been removed.
cpqSs6FanStatusChange 8029	A change has been detected in the fan status of the storage system.
cpqSs6TempStatusChange 8030	A change has been detected in the temperature status of the storage system.
cpqSs6PwrSupplyStatusChange 8031	A change has been detected in the power status of the storage system.
cpqSm2ServerReset 9001	The server power has been reset.
cpqSm2UnauthorizedLoginAttempts 9003	The maximum unauthorized login attempt threshold has been exceeded.
cpqSm2SelfTestError 9005	iLO 4 has detected a Self Test Error.
cpqSm2SecurityOverrideEngaged 9012	iLO 4 has detected that the security override jumper has been toggled to the engaged position.
cpqSm2SecurityOverrideDisengaged 9013	iLO 4 has detected that the security override jumper has been toggled to the disengaged position.
cpqSm2ServerPowerOn 9017	The server has been powered on.
cpqSm2ServerPowerOff 9018	The server has been powered off.
cpqSm2ServerPowerOnFailure 9019	A request was made to power on the server, but the server could not be powered on because of a failure condition.
cpqSm2IrsCommFailure 9020	Communication with Insight Remote Support or Insight Online has failed.
cpqHo2GenericTrap 11003	Generic trap. Verifies 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 on the SNMP console.
cpqHo2PowerThresholdTrap 11018	A power threshold has been exceeded.
cpqHoMibHealthStatusArrayChangeTrap 11020	A change in the health status of the server has occurred.
cpqSasPhyDrvStatusChange 5022	AMS detected a change in the status of an SAS or SATA physical drive.
cpqIdeAtaDiskStatusChange 14004	AMS detected a change in the status of an ATA disk drive.
cpqNic3ConnectivityRestored 18011	AMS detected that connectivity was restored to a logical network adapter.
cpqNic3ConnectivityLost 18012	AMS detected that the status of a logical network adapter changed to **Failed**.

Configuring Insight Management integration

1. Navigate to the **Administration→Management** page.
2. Click the **SNMP Settings** tab and scroll to the **Insight Management Integration** section.



Insight Management Integration

HP System Management Homepage (HP SMH) FQDN / IP Address: https:// SMH_FQDN_IP_Address_is_not_set :2381

Level of Data Returned: Enabled (iLO+Server Association Data)

View XML Reply

3. Configure the **HP System Management Homepage (HP SMH) FQDN/IP Address**.

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

   Enter the FQDN or IP address 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.

4. 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.

5. Optional: Click **View XML Reply** to view the response that is returned to HP SIM when it requests iLO management processor identification by using the provided address.
6. Click **Apply** to save the changes.

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

Configuring AlertMail settings

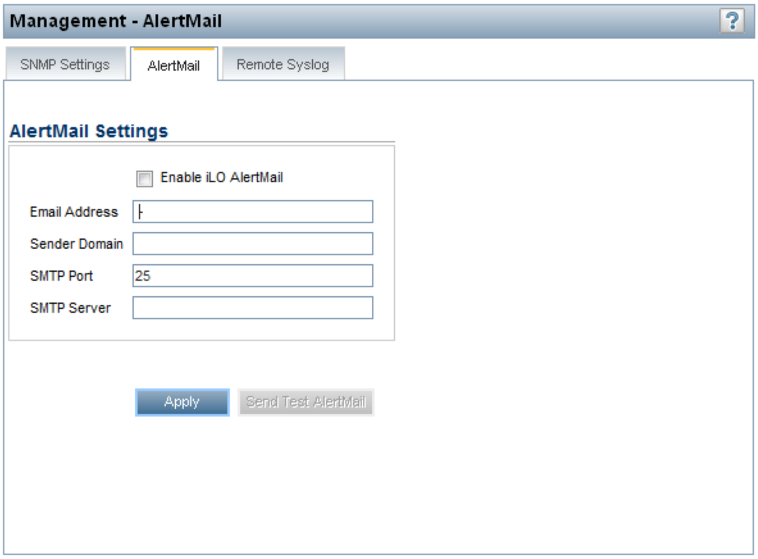
iLO AlertMail enables you to configure iLO to send alert conditions detected independently of the host operating system to a specified email address. iLO mail alerts include major host system events.

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

Enabling AlertMail

1. Navigate to the **Administration→Management→AlertMail** page.



AlertMail Settings

☐ Enable iLO AlertMail

Email Address
Sender Domain
SMTP Port 25
SMTP Server

2. Select the **Enable iLO AlertMail** check box.
3. Enter the following information:
   - **Email Address**—The destination email address for iLO email alerts. This string can be up to 63 characters and should be in standard email address format. You can enter only one email address.
   - **Sender Domain**—The domain name specified in the sender (From) email address. The sender email address is formed by using the iLO name as host name, and the subject string as domain name. If no domain name is specified, the iLO domain name, which may not be accepted by all SMTP servers, is used. This string can be up to 63 characters.
   - **SMTP Port**—The port that the SMTP server will use for unauthenticated SMTP connections. The default value is 25.
   - **SMTP Server**—The IP address or DNS name of the SMTP server or the MSA. This server cooperates with the MTA to deliver the email. This string can be up to 63 characters.
4. Optional: Click **Send Test AlertMail** to send a test message to the configured email address.

   This button is available only when AlertMail is enabled.
5. Click **Apply** to save the changes.

Disabling AlertMail

1. Navigate to the **Administration→Management→AlertMail** page.
2. Clear the **Enable iLO AlertMail** check box.
3. Click **Apply** to save the changes.

Configuring Remote Syslog settings

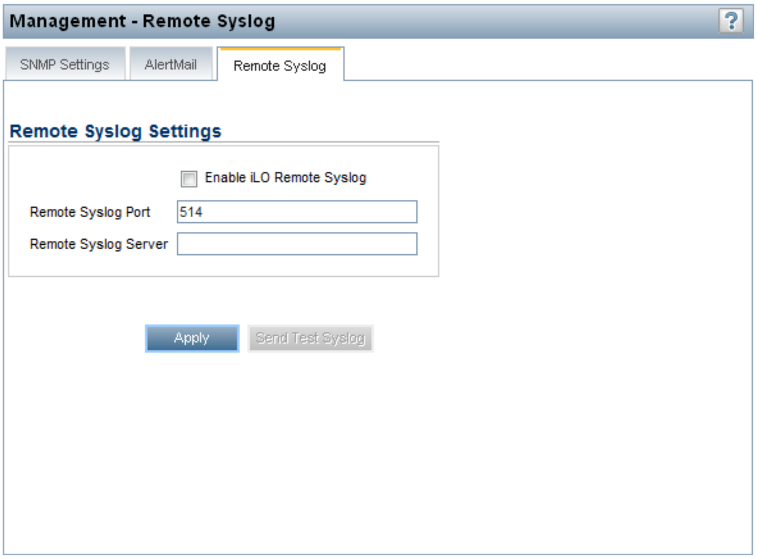
The Remote Syslog feature allows iLO to send event notification messages to Syslog servers. The iLO firmware Remote Syslog includes the IML and iLO Event Log.

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

Enabling iLO Remote Syslog

1. Navigate to the **Administration→Management→Remote Syslog** page.



Management - Remote Syslog

Remote Syslog Settings

□ Enable iLO Remote Syslog

Remote Syslog Port: 514

Remote Syslog Server:

2. Select the **Enable iLO Remote Syslog** check box.
3. Enter the following information:
   - **Remote Syslog Port**—The port number through which the Syslog server is listening.

     The default value is 514.
   - **Remote Syslog Server**—The IP address, FQDN, IPv6 name, or short name of the server running the Syslog service. This string can be up to 127 characters.

     On Linux systems, system events are logged by a tool called syslog. This tool should be installed on all Linux systems. You can set a syslog server on a remote system that will act as a central logging system for iLO systems. This way, if the iLO Remote Syslog feature is enabled in iLO, it can send its logs to the syslog server.
4. Optional: Click **Send Test Syslog** to send a test message to the configured syslog server.

   This button is available only when iLO Remote Syslog is enabled.
5. Click **Apply** to save the changes.

Disabling iLO Remote Syslog

1. Navigate to the **Administration→Management→Remote Syslog** page.
2. Clear the **Enable iLO Remote Syslog** check box.
3. Click **Apply** to save the changes.

Configuring remote support

HP remote support overview

HP has developed a service and support solution that integrates the following:

- An online, personalized dashboard (HP Insight Online)
- 24x7 remote support with HP Insight Remote Support software and Insight Online direct connect capability

When you use the embedded Remote Support functionality with an HP ProLiant server, you can choose from the following configuration options:

Configuration options

- **Insight Online direct connect**—Register a server to communicate directly with Insight Online without the need to set up an Insight Remote Support centralized Hosting Device in your local environment. Insight Online will be your primary interface for remote support information.

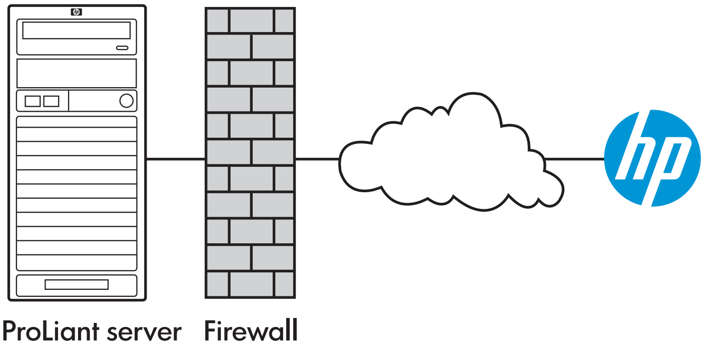
  Insight Online is an HP Support Center feature that enables you to view your remotely monitored devices anywhere, anytime. It provides a personalized dashboard for simplified tracking of IT operations and support information, including a mobile dashboard for monitoring when you are on the go. For more information, see http://www.hp.com/go/insightonline/info.

  For HP ProLiant Gen8 servers, the direct connect configuration is available in iLO 4 1.40 and later.

  For HP ProLiant Gen9 servers, the direct connect configuration is available in iLO 4 2.00 and later.

  Figure 3 (page 120) shows the direct connect configuration with an HP ProLiant server.

  Figure 3 Insight Online direct connect

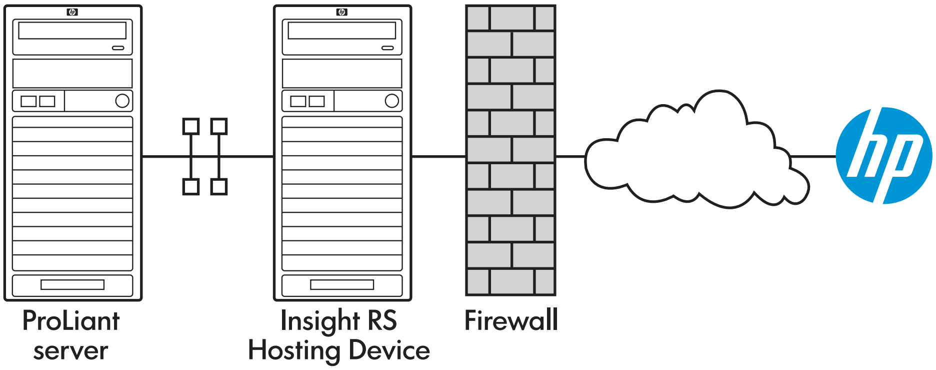
- **Insight Remote Support central connect**—Register a server to communicate with HP through an Insight Remote Support centralized Hosting Device in your local environment. All configuration and service event information is routed through the Hosting Device. This information can be viewed using the local Insight RS Console or the web-based view in Insight Online (if it is enabled in Insight RS).

  For HP ProLiant Gen8 servers, the central connect configuration is available in iLO 4 1.10 and later.

  For HP ProLiant Gen9 servers, the central connect configuration is available in iLO 4 2.00 and later.

  Figure 4 (page 120) shows the central connect configuration with an HP ProLiant server.

  Figure 4 Insight Remote Support central connect

Data collected by Insight Remote Support

By registering for Insight Remote Support, you agree to send registration, service events, configuration, and Active Health System data to HP. All data collected and sent to HP will be used to provide remote support and quality improvement. The collected data is managed according to the HP privacy statement, available at http://www.hp.com/go/privacy.

When a server is registered for Insight Remote Support, iLO or the Insight RS Hosting Device sends Active Health System information to HP every 7 days, and sends configuration information every 30 days. The following information is sent to HP:

- **Registration**—During server registration, iLO collects data to uniquely identify the server hardware. This data is sent to the Insight RS Hosting Device (Insight Remote Support central connect) or directly to HP (Insight Online direct connect).

  Registration data includes the following:

  - Server model
  - Serial number
  - iLO NIC address

  For more information about registering for Remote Support, see "Registering for Insight Remote Support central connect" (page 126) or "Registering for Insight Online direct connect" (page 123).

- **Service events**—When service events are recorded, iLO collects data to uniquely identify the relevant hardware component. This data is sent to the Insight RS Hosting Device (Insight Remote Support central connect) or directly to HP (Insight Online direct connect).

  Service event data includes the following:

  - Server model
  - Serial number
  - Part number of the hardware component
  - Description, location, and other identifying characteristics of the hardware component

  For more information, see "Working with Insight Remote Support service events" (page 128).

- **Configuration**—During data collection, iLO collects data to enable proactive advice and consulting. This data is sent to the Insight RS Hosting Device (Insight Remote Support central connect) or directly to HP (Insight Online direct connect).

  Configuration data includes the following:

  - Server model
  - Serial number
  - Processor model, speed, and utilization
  - Storage capacity, speed, and utilization
  - Memory capacity, speed, and utilization
  - Firmware/BIOS
  - Installed drivers, services, and applications (if AMS is installed)

For more information, see “Viewing and sending Remote Support data collection information” (page 131).

- **Active Health System**—During data collection, iLO collects data about the health, configuration, and runtime telemetry of the server. This information is used for troubleshooting issues and closed-loop quality analysis.

  For information about the data that is collected, see “Using the HP Active Health System” (page 177).

Using Insight Remote Support with HP Proactive Care service

HP Proactive Care service customers must register their HP ProLiant Gen8 and Gen9 servers for Insight Remote Support central connect or Insight Online direct connect in order to receive the following HP Proactive Care services features: Proactive Scan and Firmware/Software Version Report and recommendations.

- The direct connect option requires the installation of AMS.
- The central connect option requires the installation of AMS or the SNMP/WBEM agents.

For more information about the HP Proactive Care service, see the following website: http://www.hp.com/services/proactivecarecentral.

Prerequisites

Before registering, verify that the following prerequisites are met:

- A supported version of the iLO firmware is installed.

  For HP ProLiant Gen8 servers:

  ◦ Version 1.40 or later is required for Insight Online direct connect registration.

  ◦ Version 1.10 or later is required for Insight Remote Support central connect registration.

  For HP ProLiant Gen9 servers:

  ◦ Version 2.00 or later is required for Insight Online direct connect and Insight Remote Support central connect registration.

- Optional: AMS is installed and the operating system is running on the server that you want to register.

  HP recommends installing AMS. For more information about AMS, see “Installing AMS or the Insight Management Agents” (page 107).

  HP Proactive Care services customers only: AMS installation is required in order to receive the following HP Proactive Care services features: Proactive Scan and Firmware/Software Version Report and recommendations.

  AMS is one way in which iLO can obtain the name of the server. If iLO cannot obtain the server name, the displayed server name in Insight Online and Insight RS is derived from the server serial number. If you do not install AMS, do one of the following to ensure that the server name is displayed correctly in Insight Online and Insight RS:

  ◦ For Windows systems only, start the operating system. Insight Online and Insight RS will use the Windows computer name to identify the server.

  ◦ Configure the **Server Name** on the **Administration**→**Access Settings** page in the iLO web interface.

  NOTE: The server name is displayed in Insight Online and Insight RS, and can be viewed by HP Support and your authorized service provider, reseller/distributor, and installer. To protect your privacy, do not use sensitive information in the name of the HP ProLiant Gen8 or Gen9 server.

- The HP ProLiant iLO 3/4 Channel Interface Driver is installed.

  For more information, see "Installing the iLO drivers" (page 34).

- The iLO time zone is set.

  For instructions, see "Configuring SNTP settings" (page 103).

- For Insight Online direct connect only: A DNS server is configured in iLO.

  This is required for communication between iLO and Insight Online.

  For instructions, see "Configuring IPv4 settings" (page 97) and "Configuring IPv6 settings" (page 99).

- For Insight Remote Support central connect only: A supported version of the Insight RS software is installed and configured on the Insight RS Hosting Device.

  HP ProLiant Gen8 servers are supported with Insight RS 7.0.9 or later.

  HP ProLiant Gen9 servers are supported with Insight RS 7.1 or later.

  For Insight RS device support information, see the following website: http://h17007.www1.hp.com/us/en/enterprise/servers/supportmatrix/insight_rs.aspx.

- For Insight Remote Support central connect only: The RIBCL protocol credentials for the server are configured in the Insight RS Console.

  For more information about the RIBCL protocol credentials, see the *HP Insight Remote Support Installation and Configuration Guide*.

Registering for Insight Remote Support by using the iLO web interface

HP Insight Remote Support provides automatic submission of hardware events to HP to prevent downtime and enable faster issue resolution. You can register directly to HP or through an Insight RS Hosting Device.

Registering for Insight Online direct connect

Use this procedure to register an HP ProLiant server for Insight Online direct connect remote support. When you register for Insight Online direct connect, you must complete steps in both the iLO web interface and the Insight Online portal.

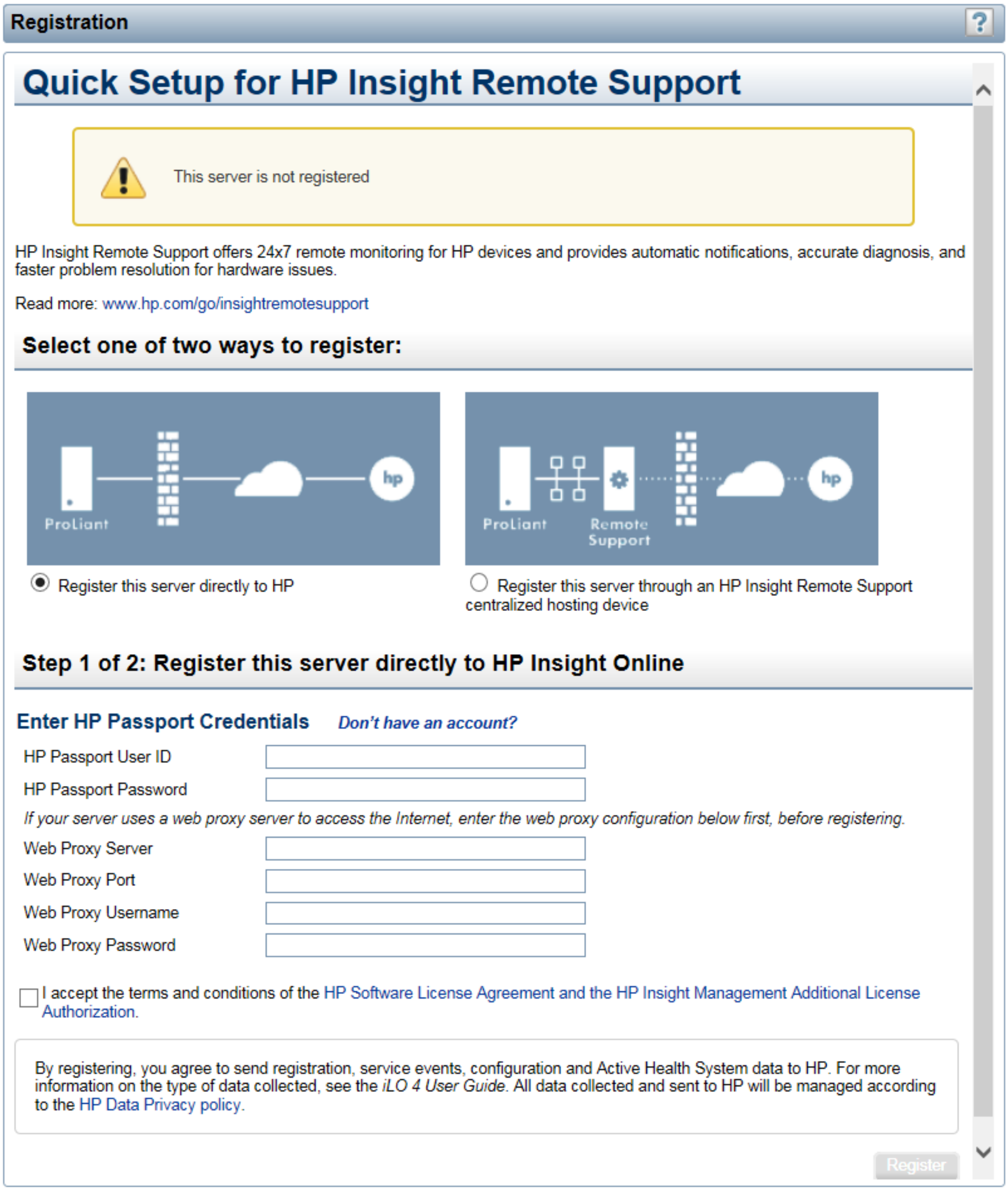
You must have the Configure iLO Settings privilege to modify the iLO remote support settings.

1. Verify that the server meets the prerequisites for using the Insight Remote Support solution.

   For more information, see "Prerequisites" (page 122).

2. Navigate to the **Remote Support→Registration** page.
3. Select **Register this server directly to HP**.

   The page refreshes to show the Insight Online direct connect registration options.



Quick Setup for HP Insight Remote Support

This server is not registered

HP Insight Remote Support offers 24x7 remote monitoring for HP devices and provides automatic notifications, accurate diagnosis, and faster problem resolution for hardware issues.

Read more: www.hp.com/go/insightremotesupport

Select one of two ways to register:

● Register this server directly to HP

○ Register this server through an HP Insight Remote Support centralized hosting device

Step 1 of 2: Register this server directly to HP Insight Online

Enter HP Passport Credentials *Don't have an account?*

HP Passport User ID	
HP Passport Password	

If your server uses a web proxy server to access the Internet, enter the web proxy configuration below first, before registering.

Web Proxy Server	
Web Proxy Port	
Web Proxy Username	
Web Proxy Password	

☐ I accept the terms and conditions of the HP Software License Agreement and the HP Insight Management Additional License Authorization.

By registering, you agree to send registration, service events, configuration and Active Health System data to HP. For more information on the type of data collected, see the *iLO 4 User Guide*. All data collected and sent to HP will be managed according to the HP Data Privacy policy.

4. Enter your HP Passport credentials in the **HP Passport User ID** and **HP Passport Password** boxes.

IMPORTANT: In most cases, your HP Passport user ID is the same as the email address you used during the HP Passport registration process. If you changed your user ID in the HP Support Center, be sure to enter your user ID and not your email address.

5. Optional: Enter the following information if the HP ProLiant server uses a web proxy server to access the Internet:
   - **Web Proxy Server**
   - **Web Proxy Port**
   - **Web Proxy Username**
   - **Web Proxy Password**
6. Select the check box **I accept the terms and conditions of the HP Software License Agreement and the HP Insight Management Additional License Authorization**.

NOTE: You can view these documents at http://www.hp.com/go/SWLicensing.

7. Click **Register**.

   Clicking **Register** is Step 1 of a two-step registration process. Step 2 is completed in Insight Online.

   By registering, you agree to send registration, service events, configuration, and Active Health System data to HP. For more information about the type of data collected, see "Data collected by Insight Remote Support" (page 121). All data collected and sent to HP will be managed according to the HP Privacy Statement, which you can review at the following website: http://www.hp.com/go/privacy.

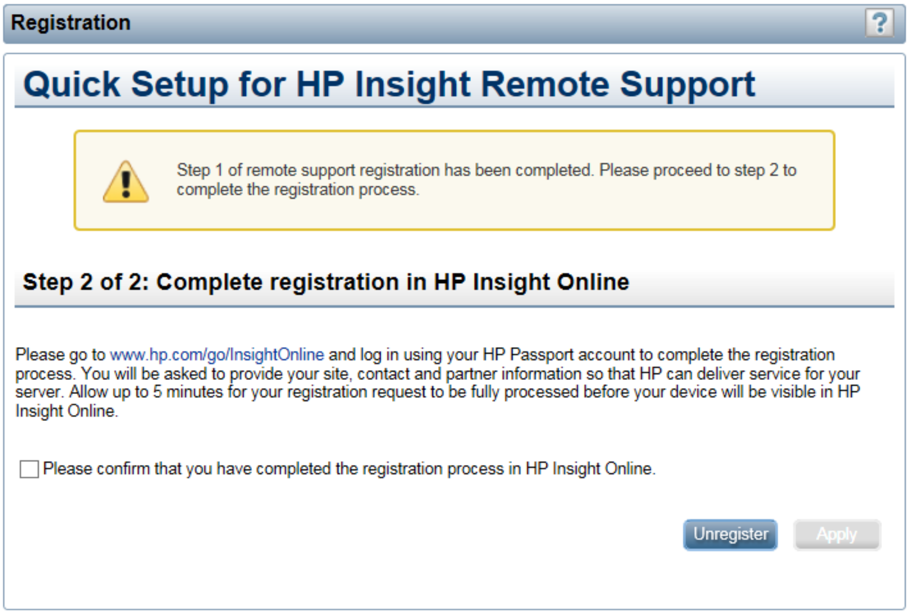
   When Step 1 is completed, the following message appears:

   ```
   Step 1 of remote support registration has been completed. Please
   proceed to step 2 to complete the registration process.
   ```

   Allow up to 5 minutes for your registration request to be fully processed.
8. Navigate to the Insight Online website at http://www.hp.com/go/InsightOnline, and then log in with your HP Passport account credentials.
9. Follow the onscreen instructions in Insight Online, and provide your site, contact, and partner information so HP can deliver service for your HP ProLiant server.

   TIP: To streamline the process when you have multiple servers to register, complete Step 1 for all of the servers, and then complete Step 2 for all of the servers during one Insight Online session.

   For detailed instructions, see the *HP Insight Remote Support and Insight Online Setup Guide for HP ProLiant Servers and HP BladeSystem c-Class Enclosures*.
10. Return to the **Remote Support→Registration** page in the iLO web interface, select the check box **Please confirm that you have completed the registration process in HP Insight Online**, and then click **Apply**.



Quick Setup for HP Insight Remote Support

Step 1 of remote support registration has been completed. Please proceed to step 2 to complete the registration process.

Step 2 of 2: Complete registration in HP Insight Online

Please go to www.hp.com/go/InsightOnline and log in using your HP Passport account to complete the registration process. You will be asked to provide your site, contact and partner information so that HP can deliver service for your server. Allow up to 5 minutes for your registration request to be fully processed before your device will be visible in HP Insight Online.

□ Please confirm that you have completed the registration process in HP Insight Online.

TIP: You can use RIBCL XML scripts to complete this step for a group of HP ProLiant servers. For more information, see the *HP iLO 4 Scripting and Command Line Guide*.

A message similar to the following appears:

```
Successfully registered!
```

`HP Passport User ID used to register this server: <HP Passport User ID>.`

11. Optional: Send a test event to confirm the connection between iLO and Insight Remote Support.

    For instructions, see "Sending a test service event" (page 129).

12. Optional: If you want to receive email alerts about system events, configure AlertMail on the **Administration→Management→AlertMail** page.

    For more information, see "Configuring AlertMail settings" (page 117).

You can also register a server for Insight Online direct connect by using the following:

- XML configuration and control scripts. For instructions, see the *HP iLO 4 Scripting and Command Line Guide*.
- Intelligent Provisioning. For instructions, see the Intelligent Provisioning documentation at the following website: http://www.hp.com/go/intelligentprovisioning/docs.

Editing the web proxy settings

Proxy settings must be maintained to enable an HP ProLiant server to continue to send Insight Remote Support data to HP. If the proxy settings change, use the following procedure to edit them:

1. Navigate to the **Remote Support→Registration** page.
2. Update the following settings, as needed:
    - **Web Proxy Server**
    - **Web Proxy Port**
    - **Web Proxy Username**
    - **Web Proxy Password**
3. Click **Apply**.

Registering for Insight Remote Support central connect

Use this procedure to register an HP ProLiant server for Insight Remote Support central connect.

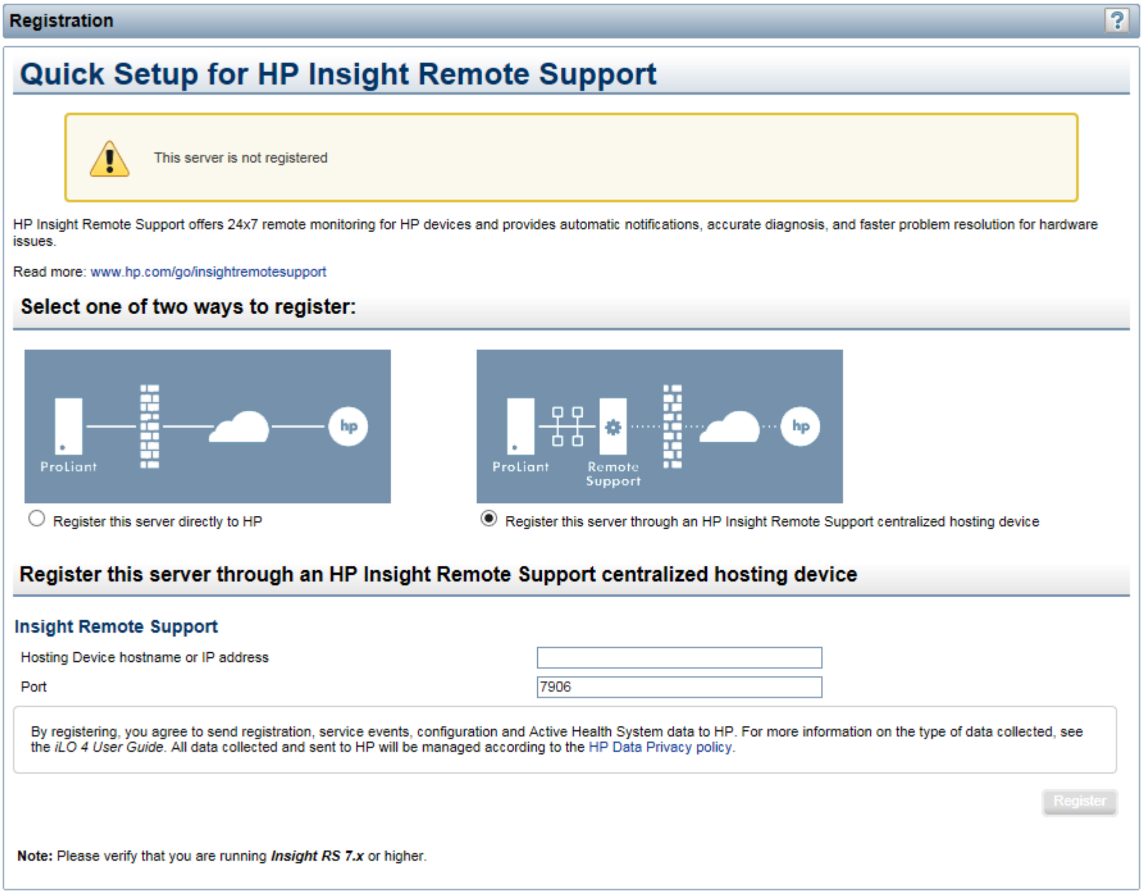
You must have the Configure iLO Settings privilege to modify the iLO remote support settings.

1. Verify that the server meets the prerequisites for using Insight Remote Support.

    For more information, see "Prerequisites" (page 122).

2. Navigate to the **Remote Support→Registration** page.
3. Select **Register this server through an HP Insight Remote Support centralized hosting device**.

    The page refreshes to show the Insight Remote Support central connect registration options.



Quick Setup for HP Insight Remote Support

This server is not registered

HP Insight Remote Support offers 24x7 remote monitoring for HP devices and provides automatic notifications, accurate diagnosis, and faster problem resolution for hardware issues.

Read more: www.hp.com/go/insightremotesupport

Select one of two ways to register:

○ Register this server directly to HP

● Register this server through an HP Insight Remote Support centralized hosting device

Register this server through an HP Insight Remote Support centralized hosting device

Insight Remote Support

Hosting Device hostname or IP address	
Port	7906

By registering, you agree to send registration, service events, configuration and Active Health System data to HP. For more information on the type of data collected, see the *iLO 4 User Guide*. All data collected and sent to HP will be managed according to the HP Data Privacy policy.

Note: Please verify that you are running ***Insight RS 7.x*** or higher.

4. Enter the Insight RS **Hosting Device hostname or IP address** and **Port** number.

   The default port is 7906.

5. Click **Register**.

   By registering, you agree to send registration, service events, configuration, and Active Health System data to HP. For more information about the type of data collected, see "Data collected by Insight Remote Support" (page 121). All data collected and sent to HP will be managed according to the HP Privacy Statement, which you can review at the following website: http://www.hp.com/go/privacy.

   A message similar to the following appears:

   ```
   Successfully registered! Insight Remote Support hosting server:
   <cms.mycompany.com:port>.
   ```

   where `<cms.mycompany.com:port>` is the Insight RS Hosting Device host name or IP address and port number.

6. Optional: Send a test event to confirm the connection between iLO and Insight Remote Support.

   For instructions, see "Sending a test service event" (page 129).

You can also register a server for Insight Remote Support central connect by using the following:

- XML configuration and control scripts. For instructions, see the *HP iLO 4 Scripting and Command Line Guide*.
- Intelligent Provisioning. For instructions, see the Intelligent Provisioning documentation at the following website: http://www.hp.com/go/intelligentprovisioning/docs.
- Insight RS Console. For instructions, see the *HP Insight Remote Support Monitored Devices Configuration Guide*.

Unregistering from Insight Remote Support by using the iLO web interface

The process to unregister from remote support depends on whether you used the Direct Connect or Central Connect registration method.

Unregistering from Insight Online direct connect

Use this procedure to discontinue monitoring of an HP ProLiant server that is registered for Insight Online direct connect.

You must have the Configure iLO Settings privilege to modify the remote support settings.

1. Navigate to the **Remote Support→Registration** page in the iLO web interface.
2. Click **Unregister**.

   The following message appears:

   ```
   Are you sure you want to unregister and disable automated support?
   ```
3. Click **OK**.

   The following message appears:

   ```
   Un-registration in progress. Please wait...
   ```

   When the process is completed, the following message appears:

   ```
   This server is not registered.
   ```

Unregistering from Insight Remote Support central connect

Use this procedure to discontinue monitoring of an HP ProLiant server that is registered for Insight Remote Support central connect.

You must have the Configure iLO Settings privilege to modify the remote support settings.

1. Log in to the Insight RS Console.
2. Do one of the following:
   - To stop monitoring an HP ProLiant server temporarily, select the server on the **Devices→Device Summary** tab in the Insight RS Console, and then select **ACTIONS→DISABLE SELECTED**.

     NOTE: Unregistering the server directly from the iLO web interface is the same as temporarily disabling the server in the Insight RS Console.
   - To stop monitoring an HP ProLiant server permanently, delete the server from the Insight RS Console. To delete the server, select it on the **Device Summary** tab, and then select **ACTIONS→DELETE SELECTED**.
3. Navigate to the **Remote Support→Registration** page in the iLO web interface.
4. Verify that the server is unregistered.

Working with Insight Remote Support service events

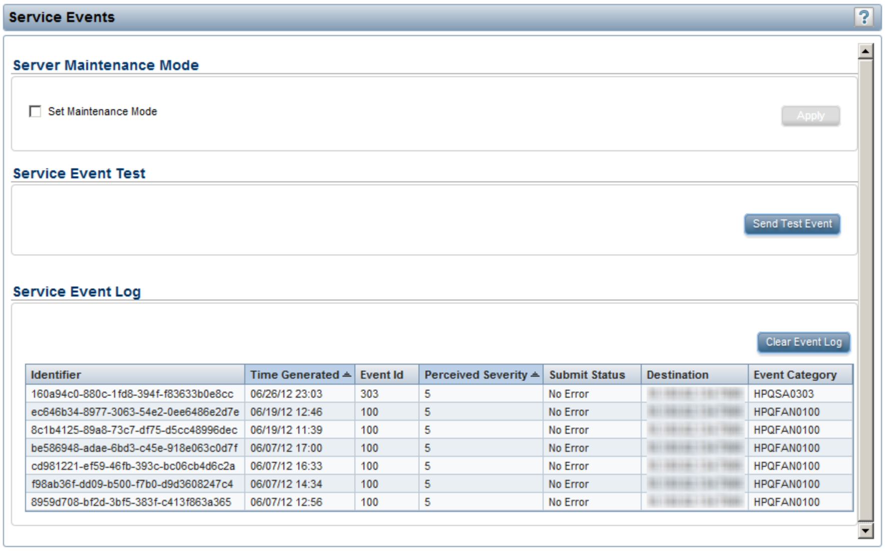
Use the **Remote Support →Service Events** page to monitor service events, send test events, and set maintenance mode. You must have the Configure iLO Settings privilege to make changes on this page.

When iLO detects a hardware failure—for example, a problem with a memory DIMM or fan—a service event is generated. When a server is registered for Insight Remote Support, the service event details are recorded in the **Service Event Log**, and the service event is sent to directly to Insight Online (direct connect) or to the Insight RS Hosting Device (central connect) which forwards it to HP. When HP receives a service event, a support case is opened (if warranted).

Using maintenance mode

Use maintenance mode when you are performing maintenance on a server. In maintenance mode, any events or messages that are sent to Insight RS or Insight Online are flagged to indicate that the event requires no action. This helps HP to determine whether to open a support case.

1. Navigate to the **Remote Support→Service Events** page.



□ Set Maintenance Mode

Identifier	Time Generated ⏶	Event Id	Perceived Severity ⏶	Submit Status	Destination	Event Category
160a94c0-880c-1fd8-394f-f83633b0e8cc	06/26/12 23:03	303	5	No Error	[redacted]	HPQSA0303
ec646b34-8977-3063-54e2-0ee6486e2d7e	06/19/12 12:46	100	5	No Error	[redacted]	HPQFAN0100
8c1b4125-89a8-73c7-df75-d5cc48996dec	06/19/12 11:39	100	5	No Error	[redacted]	HPQFAN0100
be586948-adae-6bd3-c45e-918e063c0d7f	06/07/12 17:00	100	5	No Error	[redacted]	HPQFAN0100
cd981221-ef59-46fb-393c-bc06cb4d6c2a	06/07/12 16:33	100	5	No Error	[redacted]	HPQFAN0100
f98ab36f-dd09-b500-f7b0-d9d3608247c4	06/07/12 14:34	100	5	No Error	[redacted]	HPQFAN0100
8959d708-bf2d-3bf5-383f-c413f863a365	06/07/12 12:56	100	5	No Error	[redacted]	HPQFAN0100

2. Select the **Set Maintenance Mode** check box.
3. Select a time from the **Expires in** menu.
4. Click **Apply**.

   iLO displays the following message:

   ```
   Server Maintenance Mode set.
   ```

   Maintenance mode ends automatically when the specified amount of time has passed. The following message appears:

   ```
   Server Maintenance Mode cleared.
   ```

TIP: To end maintenance mode early, select the **Clear Maintenance Mode** check box, and then click **Apply**.

Sending a test service event

You can send a test event to verify that your Insight Remote Support configuration is working correctly.

1. Navigate to the **Remote Support→Service Events** page.
2. Click **Send Test Event**.

   The following message appears:

   ```
   Are you sure you want to send a test event?
   ```

3. Click **OK**.

   The following messages appear:

   ```
   Test Service Event Transmission initiated.
   ```

   ```
   Service Event transmission in progress.
   ```

   When the transmission is completed, the test event is listed in the **Service Event Log**, the Insight RS Console (central connect only), and Insight Online.

   If the test is successful, the **Submit Status** in the **Service Event Log** displays the text `No Error`.

   The **Time Generated** column in the **Service Event Log** shows the date and time based on the configured iLO time zone.

Viewing the Service Event Log

To view the **Service Event Log**, navigate to the **Remote Support→Service Events** page.

The **Service Event Log** displays the following information for each service event:

- **Identifier**—A unique string that identifies the service event.
- **Time Generated**—The time the service event was generated. This column shows the date and time based on the configured iLO time zone.
- **Event ID**—A unique number for the service event type. Table 4 (page 130) lists the possible service events.

Table 4 Service event types

Event ID	Description
1	Generic Test Service Event
100	Fan Failed Service Event
200	Power Supply Failed Service Event
300	Physical Disk Drive Service Event
301	Smart Array Controller Accelerator Battery Failure Event
302	Smart Array Controller Accelerator Board Status Changed Event
303	Smart Array Controller Status Changed Event
400	Memory Module Failed or Predicted to Fail Event

- **Perceived Severity**—The severity of the event indication (for example, 5-Major, 7-Fatal).
- **Submit Status**—The status of the event submission. If the status is `No error`, the event was submitted successfully.
- **Destination**—For Insight Remote Support central connect configurations, the host name or IP address and port of the Insight RS Hosting Device that received the service event. For Insight Online direct connect configurations, the value **HP Insight Online** is displayed.
- **Event Category**—The category of the event that matches the Message ID description in the message registry.

Clearing the Service Event Log

1. Navigate to the **Remote Support→Service Events** page.
2. Click **Clear Event Log**.

   The following message appears:

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

3. Click **OK**.

   The following message appears:

   ```
   Service Event Log has been cleared.
   ```

Viewing and sending Remote Support data collection information

Use the **Remote Support→Data Collections** page to view information about the data that is sent to HP when a server is registered for Remote Support. You can also send data collection information manually from this page.

Sending data collection information

Depending on whether you use Insight Online direct connect or Insight Remote Support central connect, iLO or the Insight RS Hosting Device sends server configuration information to HP for analysis and proactive services in accordance with your warranty and service agreements.

- For Insight Online direct connect, this data is transmitted every 30 days. You cannot edit or delete the data collection schedule.
- For Insight Remote Support central connect, the data transmission frequency is configured in the Insight RS Console on the Insight RS Hosting Device. For information about configuring the data collection schedule, see the Insight RS online help.

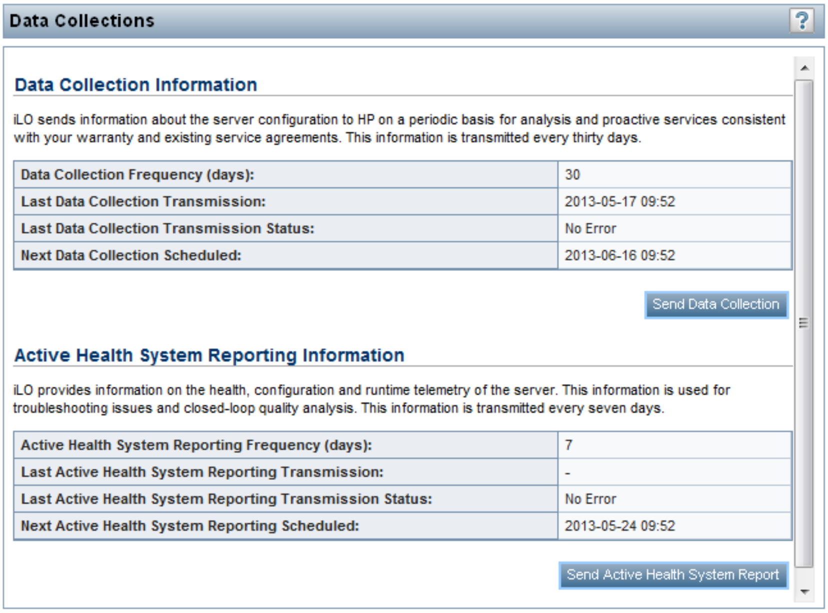
The **Data Collection Information** section of the **Remote Support→Data Collections** page displays the following information:

- **Last Data Collection Transmission**—The date and time of the last data collection.
- **Last Data Collection Transmission Status**—The status of the last data transmission.
- **Data Collection Frequency (days)** (Insight Online direct connect only)—The frequency (in days) at which data is sent to HP.
- **Next Data Collection Scheduled** (Insight Online direct connect only)—The next date and time when data will be sent to HP.

Users with the Configure iLO Settings privilege can send data collection information to HP at any time.

To send data collection information immediately:

1. Navigate to the **Remote Support→Data Collections** page.



Data Collections

Data Collection Information

iLO sends information about the server configuration to HP on a periodic basis for analysis and proactive services consistent with your warranty and existing service agreements. This information is transmitted every thirty days.

Data Collection Frequency (days):	30
Last Data Collection Transmission:	2013-05-17 09:52
Last Data Collection Transmission Status:	No Error
Next Data Collection Scheduled:	2013-06-16 09:52

Active Health System Reporting Information

iLO provides information on the health, configuration and runtime telemetry of the server. This information is used for troubleshooting issues and closed-loop quality analysis. This information is transmitted every seven days.

Active Health System Reporting Frequency (days):	7
Last Active Health System Reporting Transmission:	-
Last Active Health System Reporting Transmission Status:	No Error
Next Active Health System Reporting Scheduled:	2013-05-24 09:52

2. Click **Send Data Collection**.

   The following message appears:

   ```
   Are you sure you want to send a Data Collection?
   ```

3. Click **OK**.

   The following messages appear:

   ```
   Data Collection Transmission initiated.
   ```

   ```
   Data Collection Transmission in progress.
   ```

   When the transmission is completed, the **Last Data Collection Transmission** and **Last Data Collection Transmission Status** are updated. The date and time are based on the configured iLO time zone.

Sending Active Health System reporting information

Depending on whether you use Insight Online direct connect or Insight Remote Support central connect, iLO or the Insight RS Hosting Device sends information about the server's health, configuration, and run-time telemetry to HP. This information is used for troubleshooting issues and closed-loop quality analysis.

- For Insight Online direct connect configurations, this data is transmitted every 7 days. You cannot edit or delete the data collection schedule.
- For Insight Remote Support central connect configurations, this data is transmitted every 7 days. You can change the day of the week for data collection transmission from the Insight RS Console. For information about configuring the data collection schedule, see the Insight RS online help.

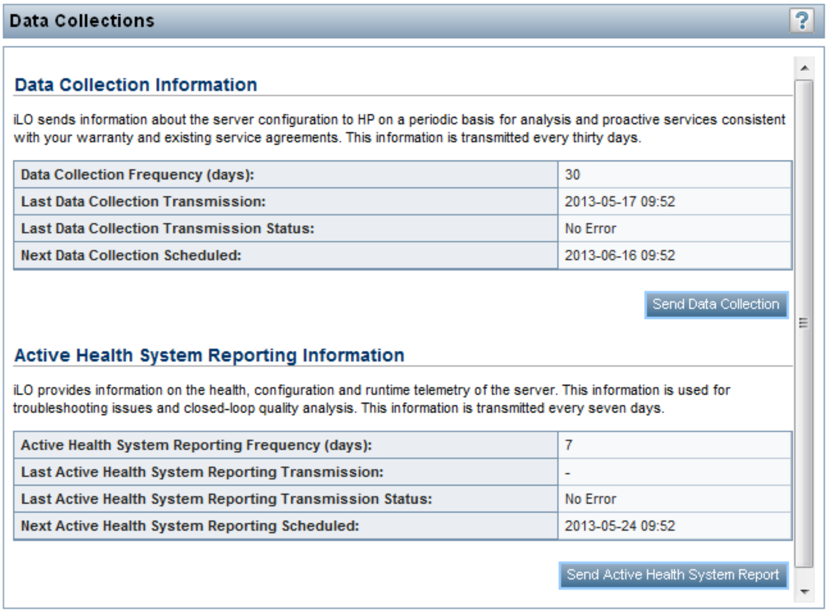
The **Active Health System Reporting Information** section on the **Remote Support→Data Collections** page displays the following information:

- **Last Active Health System Reporting Transmission**—The date and time of the last Active Health System report.
- **Last Active Health System Reporting Transmission Status**—The status of the last data transmission.
- **Active Health System Reporting Frequency (days)** (Insight Online direct connect only)—The frequency (in days) at which Active Health System data is sent to HP.
- **Next Active Health System Reporting Scheduled** (Insight Online direct connect only)—The next date and time when Active Health System data will be sent to HP.

Users with the Configure iLO Settings privilege can send Active Health System information to HP at any time.

To send Active Health System information immediately:

1. Navigate to the **Remote Support→Data Collections** page.



Data Collection Information

iLO sends information about the server configuration to HP on a periodic basis for analysis and proactive services consistent with your warranty and existing service agreements. This information is transmitted every thirty days.

Data Collection Frequency (days):	30
Last Data Collection Transmission:	2013-05-17 09:52
Last Data Collection Transmission Status:	No Error
Next Data Collection Scheduled:	2013-06-16 09:52

Active Health System Reporting Information

iLO provides information on the health, configuration and runtime telemetry of the server. This information is used for troubleshooting issues and closed-loop quality analysis. This information is transmitted every seven days.

Active Health System Reporting Frequency (days):	7
Last Active Health System Reporting Transmission:	-
Last Active Health System Reporting Transmission Status:	No Error
Next Active Health System Reporting Scheduled:	2013-05-24 09:52

2. Click **Send Active Health System Report**.

   The following message appears:

   ```
   Are you sure you want to send an Active Health System report?
   ```

3. Click **OK**.

   The following messages appear:

   ```
   Active Health System Transmission initiated.
   ```

   ```
   Active Health System Transmission in progress.
   ```

   The collected data includes Active Health System information from the last 7 days.

   When the transmission is completed, the **Last Active Health System Reporting Transmission** and **Last Active Health System Reporting Transmission Status** are updated. The date and time are based on the configured iLO time zone.

NOTE: You can also download Active Health System information manually and send it to HP. For instructions, see "Using the HP Active Health System" (page 177).

Configuring iLO by using the ROM-based utilities

You can use ROM-based utilities to configure iLO. The ROM-based utility embedded in the system ROM of your HP ProLiant server depends on your server model.

- HP ProLiant Gen8 servers, except for the DL580 Gen8 server, have the iLO RBSU software embedded in the system ROM.

  For information about using iLO RBSU, see "Using the iLO RBSU" (page 134).

- HP ProLiant Gen9 servers and the DL580 Gen8 server have the HP UEFI System Utilities software embedded in the system ROM.

  For information about using the iLO Configuration Utility in the UEFI System Utilities, see "Using the UEFI System Utilities iLO 4 Configuration Utility" (page 138).

Using the iLO RBSU

This section provides general use instructions and instructions for configuring iLO with the iLO RBSU. For other iLO setup and troubleshooting procedures that you can perform with the iLO RBSU, see the following:

- "Setting up iLO by using iLO RBSU or the iLO 4 Configuration Utility" (page 21)
- "Troubleshooting miscellaneous issues" (page 333)

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 134)
   - "Configuring DNS/DHCP settings" (page 136)
   - "Configuring global settings by using iLO RBSU" (page 137)
   - "Configuring serial CLI options by using iLO RBSU" (page 138)
   - "Resetting iLO to the factory default settings by using iLO RBSU" (page 311)
   - "Managing iLO user accounts by using iLO RBSU" (page 26)

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.

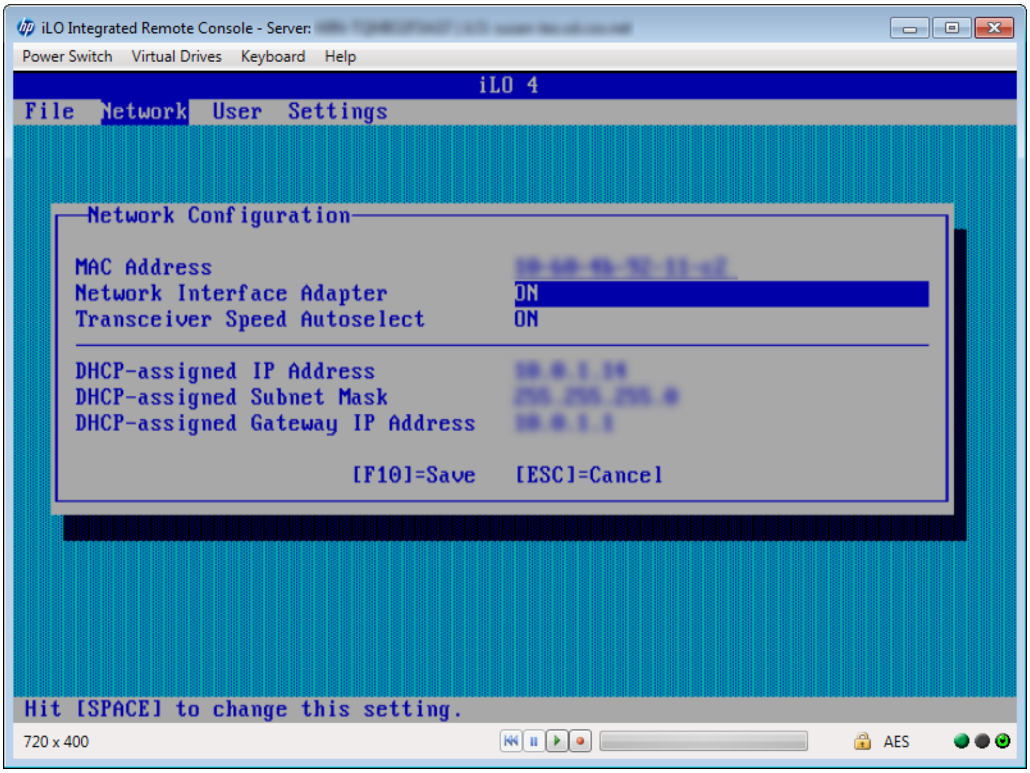
To configure NIC and TCP/IP settings:

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



```
                              iLO 4
File  Network  User  Settings

  Network Configuration

   MAC Address                          [redacted]
   Network Interface Adapter            ON
   Transceiver Speed Autoselect         ON

   DHCP-assigned IP Address             [redacted]
   DHCP-assigned Subnet Mask            [redacted]
   DHCP-assigned Gateway IP Address     [redacted]

                      [F10]=Save    [ESC]=Cancel

Hit [SPACE] to change this setting.
```

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** to enable the iLO Dedicated Network Port. Select a Shared Network Port option to use the Shared Network Port. Selecting **OFF** disables all network interfaces to iLO.

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

     For more information about the iLO network interface adapter settings, see“Understanding the iLO network port configuration options” (page 94).

   - **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. This option is available only when **Network Interface Adapter** is set to **ON**.
   - **Transceiver Speed Manual Setting** (iLO Dedicated Network Port only)—Sets the link speed for the iLO network interface. This option is available only when **Network Interface Adapter** is set to **ON** and **Transceiver Speed Autoselect** is set to **OFF**.
   - **Transceiver Duplex Setting** (iLO Dedicated Network Port only)—Sets the link duplex setting for the iLO network interface. This option is available only when **Network Interface Adapter** is set to **ON** and **Transceiver Speed Autoselect** is set to **OFF**.
   - **VLAN Enable** (Shared Network Port only)—Enables the VLAN feature.

     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. This option is available only when **Network Interface Adapter** is set to **Shared Network Port**.

   - **VLAN ID** (Shared Network Port only)—If you enabled VLAN, enter a VLAN tag. 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. This option is available only when **Network Interface Adapter** is set to a Shared Network Port option.

- **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.

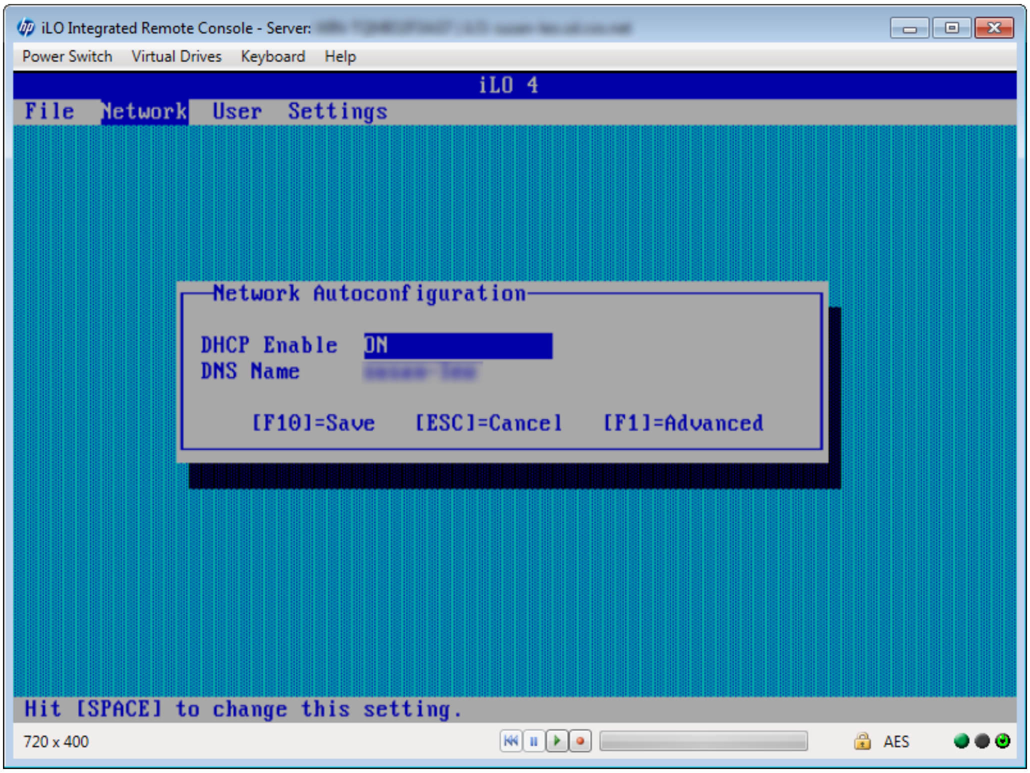
To configure DNS and DHCP settings:

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.



iLO Integrated Remote Console - Server: [redacted]

Network Autoconfiguration

DHCP Enable ON
DNS Name [redacted]

[F10]=Save [ESC]=Cancel [F1]=Advanced

Hit [SPACE] to change this setting.

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`).

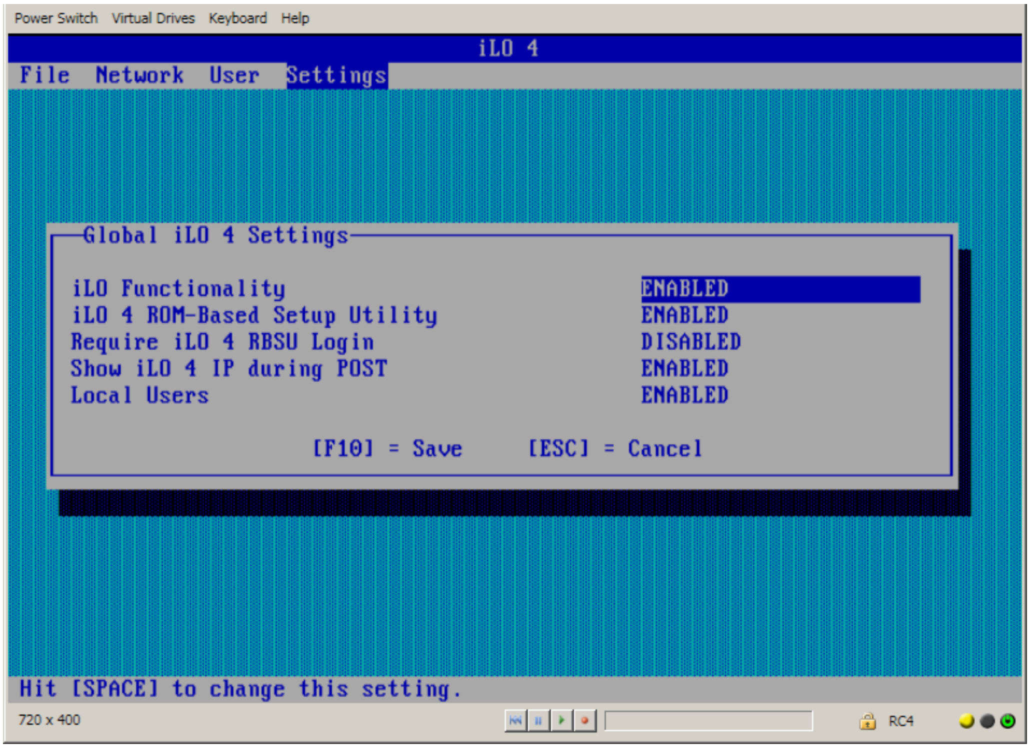
     This name can be used only if DHCP and DNS are configured to connect to the iLO subsystem name instead of the IP address.
6. Press **F10** to save your changes.
7. Select **File**→**Exit** to exit iLO RBSU.

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 4 Settings** menu opens.



```
Global iLO 4 Settings

iLO Functionality                          ENABLED
iLO 4 ROM-Based Setup Utility              ENABLED
Require iLO 4 RBSU Login                   DISABLED
Show iLO 4 IP during POST                  ENABLED
Local Users                                ENABLED

          [F10] = Save      [ESC] = Cancel

Hit [SPACE] to change this setting.
```

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 Functionality**
   - **iLO 4 ROM-Based Setup Utility**
   - **Require iLO 4 RBSU Login**
   - **Show iLO 4 IP during POST**
   - **Local Users**

   For more information about the first four options in the list, see "Configuring access options" (page 59).

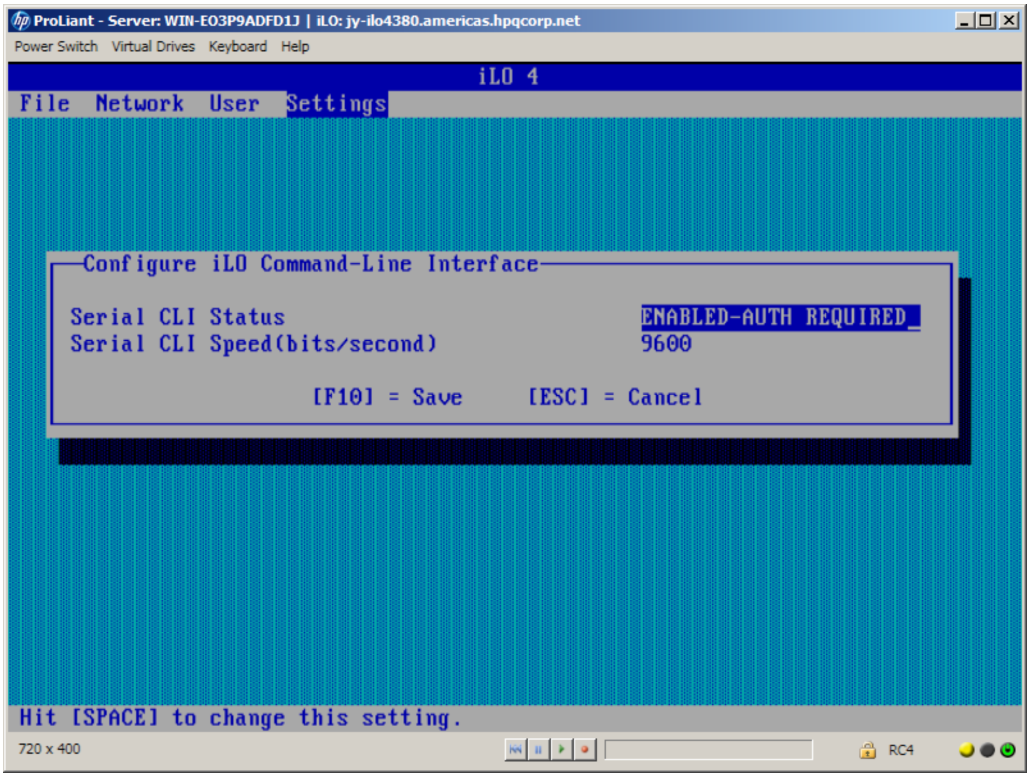
For more information about the last option in the list, see "Configuring authentication and directory server settings" (page 73).

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.


ProLiant - Server: WIN-E03P9ADFD1J | iLO: jy-ilo4380.americas.hpqcorp.net
Power Switch Virtual Drives Keyboard Help
iLO 4
File Network User Settings
720 x 400
RC4

```
Configure iLO Command-Line Interface

Serial CLI Status                          ENABLED-AUTH REQUIRED
Serial CLI Speed(bits/second)              9600

              [F10] = Save      [ESC] = Cancel

Hit [SPACE] to change this setting.
```

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 "Configuring iLO access settings" (page 57).
7. Press **F10** to save the settings.
8. Select **File**→**Exit** to close iLO RBSU.

Using the UEFI System Utilities iLO 4 Configuration Utility

For general instructions about using the UEFI System Utilities, see the *HP UEFI System Utilities User Guide*.

This section provides general use instructions and instructions for configuring iLO with the iLO 4 Configuration Utility. For other iLO setup and troubleshooting procedures that you can perform with the iLO 4 Configuration utility, see the following:

- "Setting up iLO by using iLO RBSU or the iLO 4 Configuration Utility" (page 21)
- "Troubleshooting miscellaneous issues" (page 333)

Accessing the iLO 4 Configuration Utility menu

You can access the iLO 4 Configuration Utility from the physical system console, or by using an iLO remote console session.

To access the **iLO 4 Configuration Utility** menu:

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

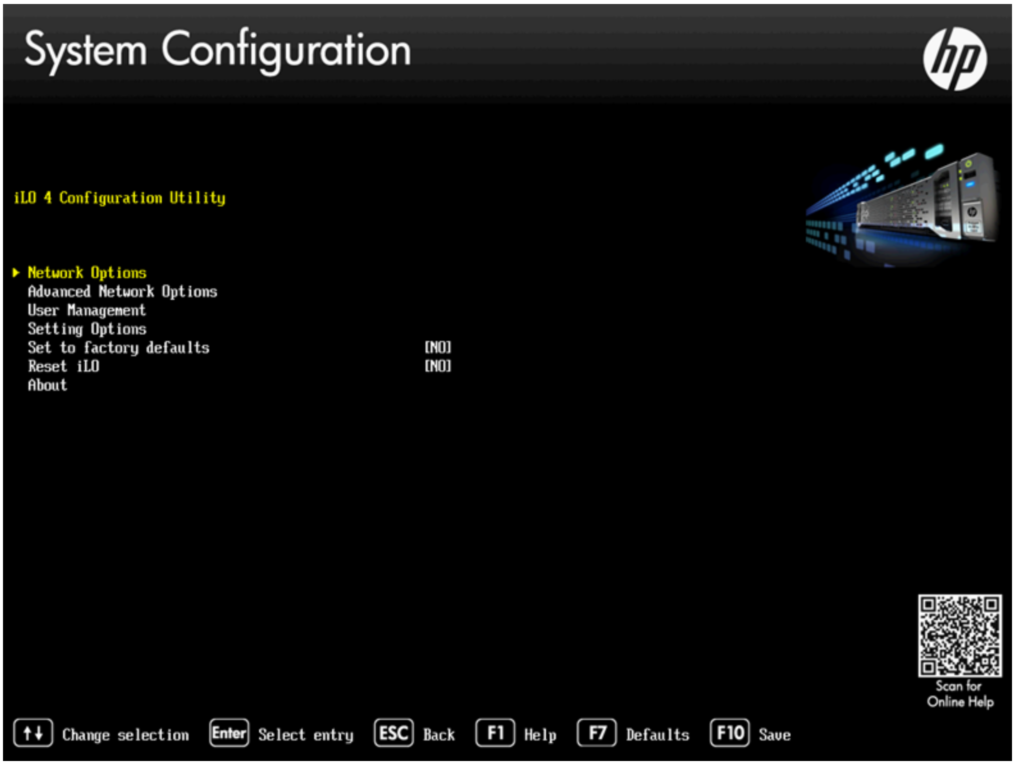
   You can use the .NET IRC or Java IRC.

2. Restart or power on the server.
3. Press **F9** in the HP ProLiant POST screen.

   The **System Utilities** screen appears.

4. From the **System Utilities** screen, select **System Configuration**→**iLO 4 Configuration Utility**.

   The **iLO 4 Configuration Utility** screen appears.



Set to factory defaults [NO]
Reset iLO [NO]

5. Select an option, and then press **Enter**.

   You can use the iLO 4 Configuration Utility to perform the following tasks:

   - “Configuring Network Options” (page 140)
   - “Configuring Advanced Network Options” (page 141)
   - “Managing iLO user accounts by using the iLO 4 Configuration Utility” (page 29)
   - “Configuring access settings by using the iLO 4 Configuration Utility” (page 143)
   - “Viewing information about iLO by using the iLO 4 Configuration Utility” (page 144)
   - “Resetting iLO to the factory default settings by using the iLO 4 Configuration Utility” (page 312)
   - “Resetting iLO by using the iLO 4 Configuration Utility” (page 309)

Configuring Network Options

You can use the iLO 4 Configuration Utility **Network Options** menu to configure basic iLO network options.

To configure iLO network options:

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

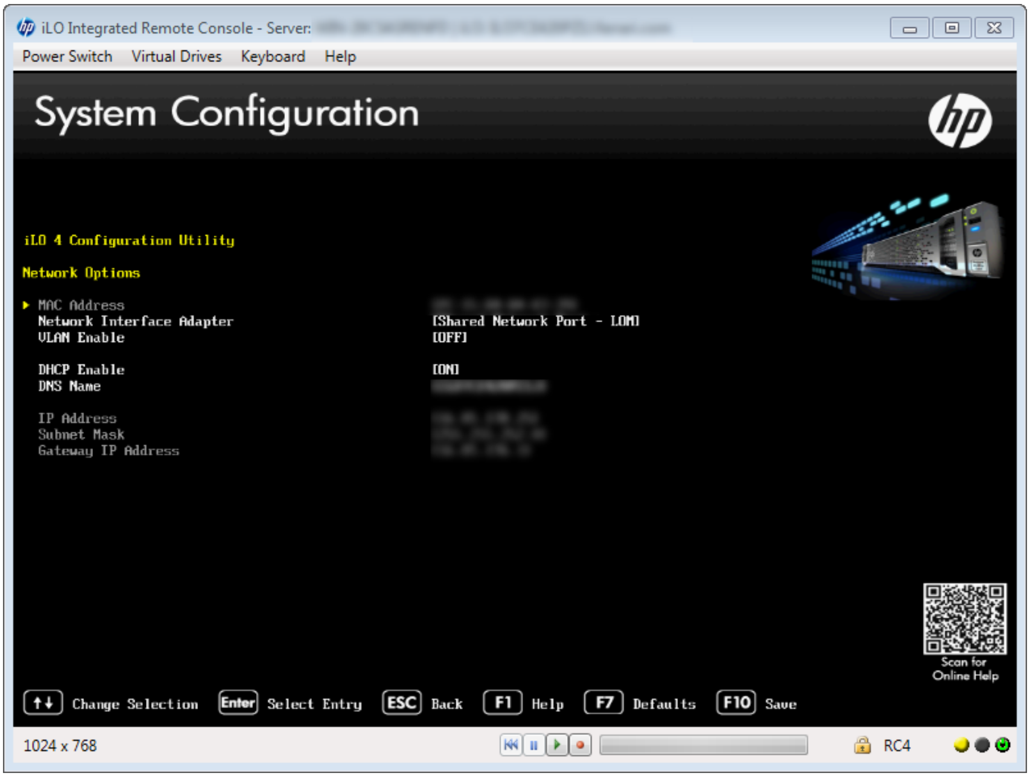
   You can use the .NET IRC or Java IRC.

2. Restart or power on the server.
3. Press **F9** in the HP ProLiant POST screen.

   The **System Utilities** screen appears.

4. From the **System Utilities** screen, select **System Configuration→iLO 4 Configuration Utility→Network Options**.

   The **Network Options** screen appears.



iLO Integrated Remote Console - Server: [redacted]

System Configuration

iLO 4 Configuration Utility

Network Options

```
▸ MAC Address                         [redacted]
  Network Interface Adapter           [Shared Network Port - LOM]
  VLAN Enable                         [OFF]

  DHCP Enable                         [ON]
  DNS Name                            [redacted]

  IP Address                          [redacted]
  Subnet Mask                         [redacted]
  Gateway IP Address                  [redacted]
```

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** to enable the iLO Dedicated Network Port. Select **Shared Network Port** to use the Shared Network Port. Selecting **OFF** disables all network interfaces to iLO.

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

     For more information about the iLO network interface adapter settings, see“Understanding the iLO network port configuration options” (page 94).
   - **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. This option is available only when **Network Interface Adapter** is set to **ON**.
   - **Transceiver Speed Manual Setting** (iLO Dedicated Network Port only)—Sets the link speed for the iLO network interface. This option is available only when **Network Interface Adapter** is set to **ON** and **Transceiver Speed Autoselect** is set to **OFF**.
   - **Transceiver Duplex Setting** (iLO Dedicated Network Port only)—Sets the link duplex setting for the iLO network interface. This option is available only when **Network Interface Adapter** is set to **ON** and **Transceiver Speed Autoselect** is set to **OFF**.
   - **VLAN Enable** (Shared Network Port only)—Enables the VLAN feature.

     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. This option is available only when **Network Interface Adapter** is set to **Shared Network Port**.
   - **VLAN ID** (Shared Network Port only)—If you enabled VLAN, enter a VLAN tag. 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. This option is available only when **Network Interface Adapter** is set to **Shared Network Port**.
   - **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.
   - **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. Press **Esc** until the main menu is displayed.
8. Select **Exit and Resume Boot** in the main menu, and then press **Enter**.
9. When prompted to confirm the request, press **Enter** to exit the utility and resume the boot process.

Configuring Advanced Network Options

You can use the iLO 4 Configuration Utility **Advanced Network Options** menu to configure advanced iLO network options.

To configure advanced iLO network options:

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

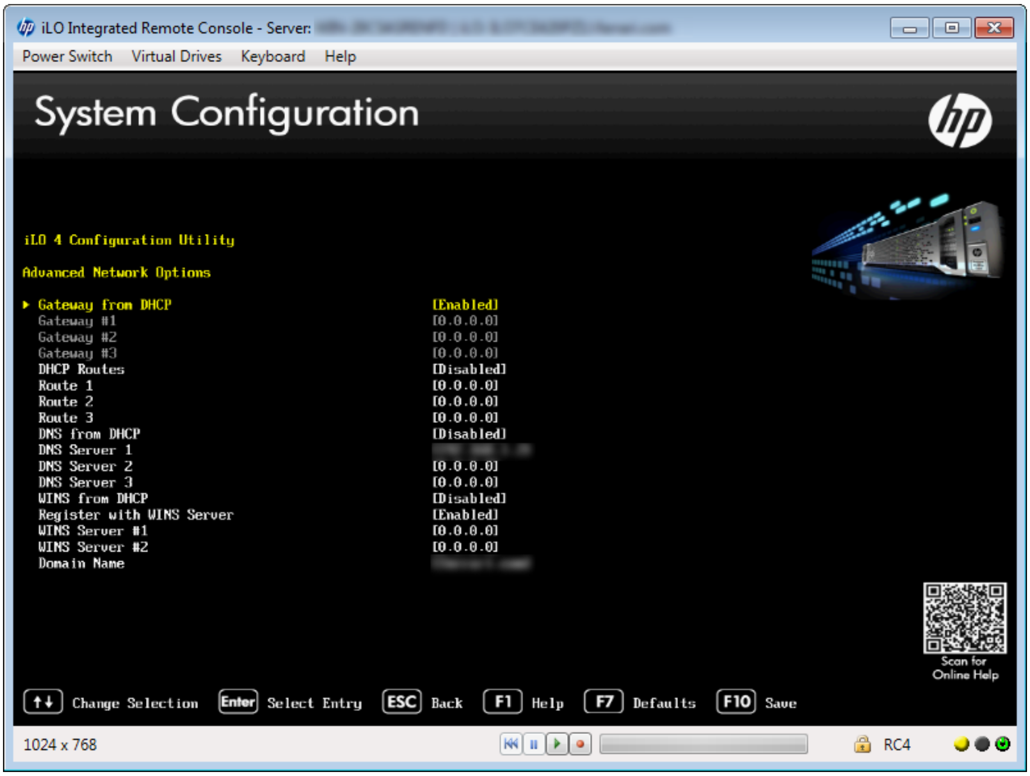
   You can use the .NET IRC or Java IRC.

2. Restart or power on the server.
3. Press **F9** in the HP ProLiant POST screen.

   The **System Utilities** screen appears.

4. From the **System Utilities** screen, select **System Configuration→iLO 4 Configuration Utility→Advanced Network Options**.

   The **Advanced Network Options** screen appears.



```
iLO 4 Configuration Utility

Advanced Network Options

▶ Gateway from DHCP                                  [Enabled]
  Gateway #1                                         [0.0.0.0]
  Gateway #2                                         [0.0.0.0]
  Gateway #3                                         [0.0.0.0]
  DHCP Routes                                        [Disabled]
  Route 1                                            [0.0.0.0]
  Route 2                                            [0.0.0.0]
  Route 3                                            [0.0.0.0]
  DNS from DHCP                                      [Disabled]
  DNS Server 1                                       [redacted]
  DNS Server 2                                       [0.0.0.0]
  DNS Server 3                                       [0.0.0.0]
  WINS from DHCP                                     [Disabled]
  Register with WINS Server                          [Enabled]
  WINS Server #1                                     [0.0.0.0]
  WINS Server #2                                     [0.0.0.0]
  Domain Name                                        [redacted]
```

5. View or update the following values, as needed:
   - **Gateway from DHCP**—Specifies whether iLO uses a DHCP server-supplied gateway.
   - **Gateway #1**, **Gateway #2**, and **Gateway #3**—If **Gateway from DHCP** is disabled, enter up to three iLO gateway IP addresses.
   - **DHCP Routes**—Specifies whether iLO uses the DHCP server-supplied static routes.
   - **Route 1**, **Route 2**, and **Route 3**—If **DHCP Routes** is disabled, enter the iLO static route destination, mask, and gateway addresses.
   - **DNS from DHCP**—Specifies whether iLO uses the DHCP server-supplied DNS server list.
   - **DNS Server 1**, **DNS Server 2**, **DNS Server 3**—If **DNS from DHCP** is disabled, enter the primary, secondary, and tertiary DNS servers.
   - **WINS from DHCP**—Specifies whether iLO uses the DHCP server-supplied WINS server list.
   - **Register with WINS Server**—Specifies whether iLO registers its name with a WINS server.

- **WINS Server #1** and **WINS Server #2**—If **WINS from DHCP** is disabled, enter the primary and secondary WINS servers.
- **Domain Name**—The iLO domain name. If DHCP is not used, enter a domain name.

6. Press **F10** to save the changes.
7. Press **Esc** until the main menu is displayed.
8. Select **Exit and Resume Boot** in the main menu, and then press **Enter**.
9. When prompted to confirm the request, press **Enter** to exit the utility and resume the normal boot process.

Configuring access settings by using the iLO 4 Configuration Utility

You can use the iLO 4 Configuration Utility **Setting Options** menu to configure iLO access settings.

To configure iLO access settings:

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

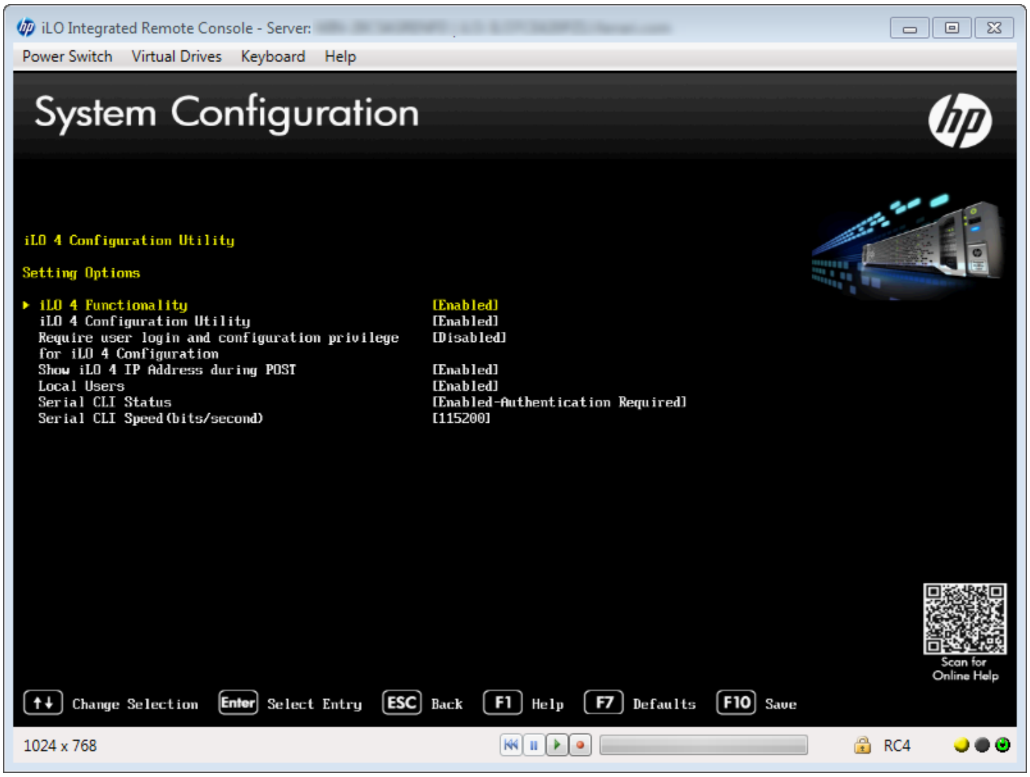
   You can use the .NET IRC or Java IRC.

2. Restart or power on the server.
3. Press **F9** in the HP ProLiant POST screen.

   The **System Utilities** screen appears.

4. From the **System Utilities** screen, select **System Configuration**→**iLO 4 Configuration Utility**→**Setting Options**.

   The **Setting Options** screen appears.



```
iLO 4 Configuration Utility

Setting Options

▸ iLO 4 Functionality                               [Enabled]
  iLO 4 Configuration Utility                       [Enabled]
  Require user login and configuration privilege    [Disabled]
  for iLO 4 Configuration
  Show iLO 4 IP Address during POST                 [Enabled]
  Local Users                                       [Enabled]
  Serial CLI Status                                 [Enabled-Authentication Required]
  Serial CLI Speed(bits/second)                     [115200]
```

5. View or update the following values, as needed:
   - **iLO 4 Functionality**—The iLO network and communications with operating system drivers are terminated when iLO functionality is disabled.

     To re-enable iLO functionality, disable iLO security with the system maintenance switch, and then use the iLO 4 Configuration Utility to set **iLO Functionality** to **Enabled**.
   - For more information about using the system maintenance switch, see the *Maintenance and Service Guide* for your server model.

     NOTE: The iLO functionality cannot be disabled on blade servers.
   - **iLO 4 Configuration Utility**—Enables or disables the iLO 4 Configuration Utility. If this option is set to **Disabled**, the iLO 4 Configuration Utility menu item is not available when you access the UEFI System Utilities.
   - **Require Login for iLO 4 Configuration**—Determines whether a user-credential prompt is displayed when a user accesses the iLO 4 Configuration Utility. If this setting is **Enabled**, a login dialog box opens when you access the iLO 4 Configuration Utility.
   - **Show iLO 4 IP Address during POST**—Enables the display of the iLO network IP address during host server POST.
   - **Local Users**—Enables or disables local user account access.
   - **Serial CLI Status**—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 Required**—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 CLI Speed (bits/second)**—This setting lets you 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**. You need to set the serial port configuration to no parity, 8 data bits, and 1 stop bit (N/8/1) for correct operation.

     NOTE: The 38400 speed is supported in the iLO web interface, but is not currently supported by the iLO 4 Configuration Utility.
6. Press **F10** to save the changes.
7. Press **Esc** until the main menu is displayed.
8. Select **Exit and Resume Boot** in the main menu, and then press **Enter**.
9. When prompted to confirm the request, press **Enter** to exit the utility and resume the boot process.

Viewing information about iLO by using the iLO 4 Configuration Utility

You can use the iLO 4 Configuration Utility **About** menu to view iLO information.

To view iLO information:

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

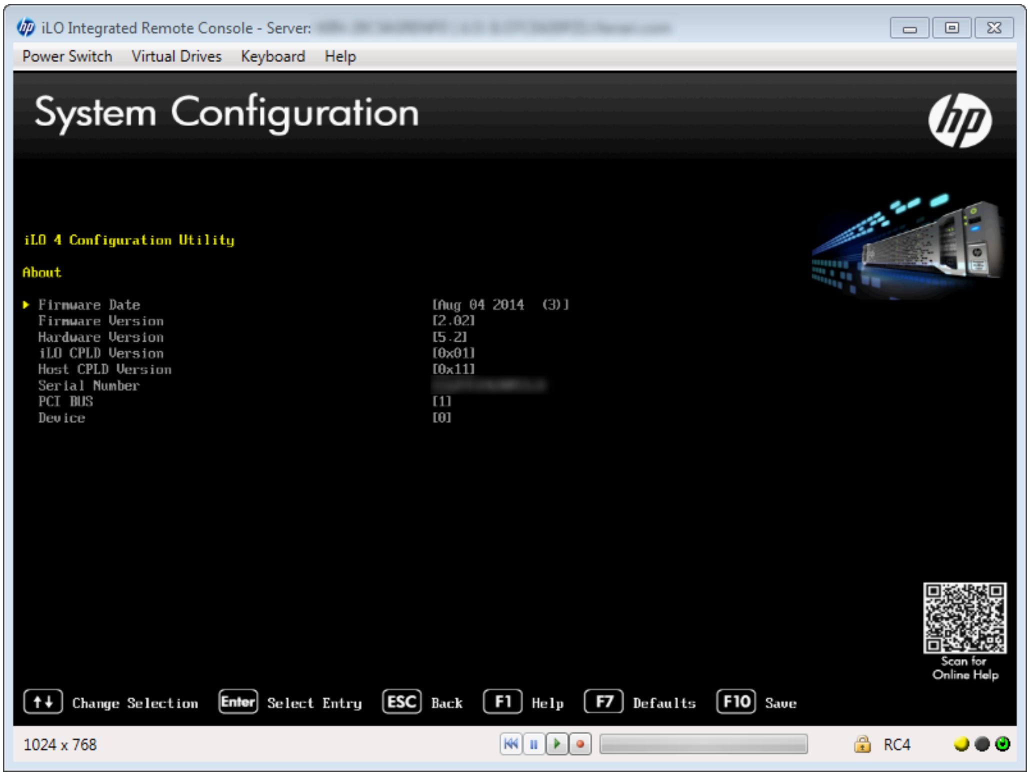
   You can use the .NET IRC or Java IRC.
2. Restart or power on the server.

3. Press **F9** in the HP ProLiant POST screen.

   The **System Utilities** screen appears.

4. From the **System Utilities** screen, select **System Configuration→iLO 4 Configuration Utility→About**.

   The **About** screen appears.



```
iLO 4 Configuration Utility

About

▸ Firmware Date                                    [Aug 04 2014  (3)]
  Firmware Version                                 [2.02]
  Hardware Version                                 [5.2]
  iLO CPLD Version                                 [0x01]
  Host CPLD Version                                [0x11]
  Serial Number                                    [redacted]
  PCI BUS                                          [1]
  Device                                           [0]
```

   This screen includes the following information:

   - **Firmware Date**—The iLO firmware revision date.
   - **Firmware Version**—The iLO firmware version.
   - **iLO CPLD Version**—The iLO complex programmable logic device version.
   - **Host CPLD Version**—The ProLiant server complex programmable logic device version.
   - **Serial Number**—The iLO serial number.
   - **RBSU Date**—The iLO 4 Configuration Utility revision date.
   - **PCI BUS**—The PCI bus to which the iLO processer is attached.
   - **Device**—The device number assigned to iLO in the PCI bus.

5. Press **Esc** until the main menu is displayed.
6. Select **Exit and Resume Boot** in the main menu, and then press **Enter**.
7. When prompted to confirm the request, press **Enter** to exit the utility and resume the boot process.

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 4 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 manage iLO. You can also use a Remote Console, scripting, or the CLP.

Browser support

The iLO web interface requires a browser that supports JavaScript. For a list of supported browsers, see Table 5 (page 146).

Table 5 Supported browsers

iLO version	Internet Explorer	Firefox	Chrome
iLO 4 1.01	7, 8, 9	3.6, ESR 10	
iLO 4 1.05	7, 8, 9	ESR 10	Chrome (latest version)
iLO 4 1.10	7, 8, 9	ESR 10	Chrome (latest version)
iLO 4 1.13	7, 8, 9	ESR 10	Chrome (latest version)
iLO 4 1.20	7, 8, 9	ESR 10	Chrome (latest version)
iLO 4 1.30	8, 9, 10	ESR 17	Chrome (latest version)
iLO 4 1.40	8, 10	ESR 24	Chrome (latest version)
iLO 4 1.50	8, 11	ESR 24	Chrome (latest version)
iLO 4 2.00	8, 11	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 the iLO web interface

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 89).
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 entered incorrect login information.
  - 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).
- Your user account is not a valid iLO account.
- Your user account has been deleted, disabled, or locked out.
- The password for the user 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 entering 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. This option is available only if a language pack is installed.
- **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.

Starting a remote management tool

When iLO is under the control of a remote management tool, the iLO web interface displays a message similar to the following on the iLO login page:

```
Warning! Some iLO settings are managed by <remote management tool name>.
Changes made directly in iLO will be out of sync with the centralized
settings.
```

The name of the remote management tool is a link. Click the link to start the remote management tool.

Language pack support

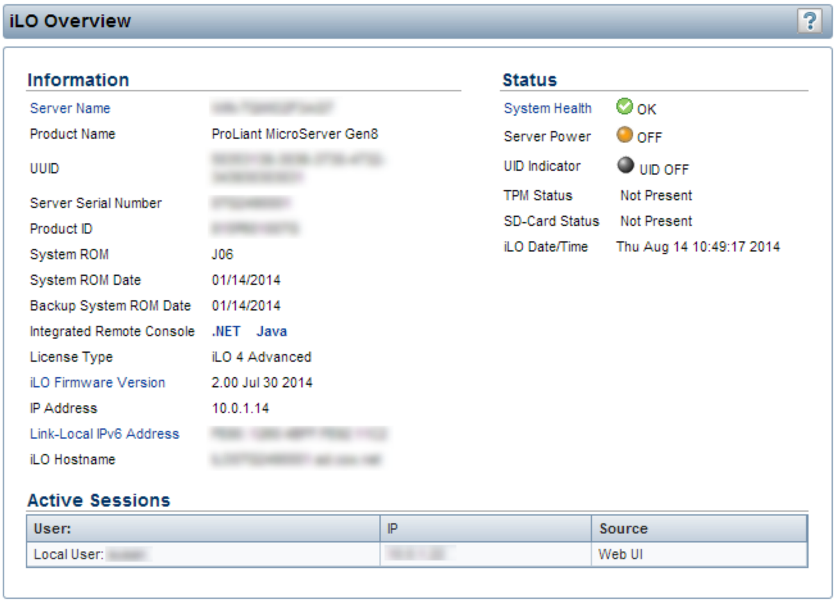
If a language pack is currently installed in iLO, a language menu is available on the login screen for you to select the language for the iLO session. This selection is saved in a browser cookie for future use.

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.



iLO Overview

Information

Server Name	[redacted]
Product Name	ProLiant MicroServer Gen8
UUID	[redacted]
Server Serial Number	[redacted]
Product ID	[redacted]
System ROM	J06
System ROM Date	01/14/2014
Backup System ROM Date	01/14/2014
Integrated Remote Console	.NET Java
License Type	iLO 4 Advanced
iLO Firmware Version	2.00 Jul 30 2014
IP Address	10.0.1.14
Link-Local IPv6 Address	[redacted]
iLO Hostname	[redacted]

Status

System Health	OK
Server Power	OFF
UID Indicator	UID OFF
TPM Status	Not Present
SD-Card Status	Not Present
iLO Date/Time	Thu Aug 14 10:49:17 2014

Active Sessions

User:	IP	Source
Local User: [redacted]	[redacted]	Web UI

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 or the UEFI System Utilities 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.
- **Chassis Serial Number**—The serial number of the SL chassis that contains the server node. This information is displayed for SL servers with SL Chassis firmware version 6.0 or later.
- **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 or the UEFI System Utilities during POST.
- **System ROM**—The family of the active system ROM.
- **System ROM Date**—The date of the active system ROM.

- **Backup System ROM Date**—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 180).
- **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 202).
- **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→Firmware** page. For more information about firmware, see "Updating firmware" (page 37).
- **IP Address**—The network IP address of the iLO subsystem.
- **Link-Local IPv6 Address**—The SLAAC link-local address of the iLO subsystem. 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.

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 151).
- **Server Power**—The server power state (**ON** or **OFF**).
- **UID Indicator**—The state of the UID. The UID helps you identify and locate a server, 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.
- **SD-Card Status**—The current status of the internal SD card. If present, the number of blocks in the SD card is displayed.

  On nonblade servers, SD cards are not hot-pluggable. Use the following procedure to insert an SD card:

1. Power down the server.
2. Remove the top cover.
3. Insert or remove the SD card.

- **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.

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)

NOTE: When a group power cap is set, you might see an unexpected session in the **Active Sessions** list on the **iLO Overview** page and in the iLO Event Log. This session is displayed with the IP address 127.0.0.1. This temporary session is created by the group power capping feature when it obtains the data that is required to maintain the power cap. This session can be ignored. It will be removed from the **Active Sessions** list within a minute.

Viewing iLO system information

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

The information that you can view depends on whether you are using Agentless Management or SNMP Pass-thru, and whether AMS is installed. For more information, see "Configuring iLO Management settings" (page 106).

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

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.

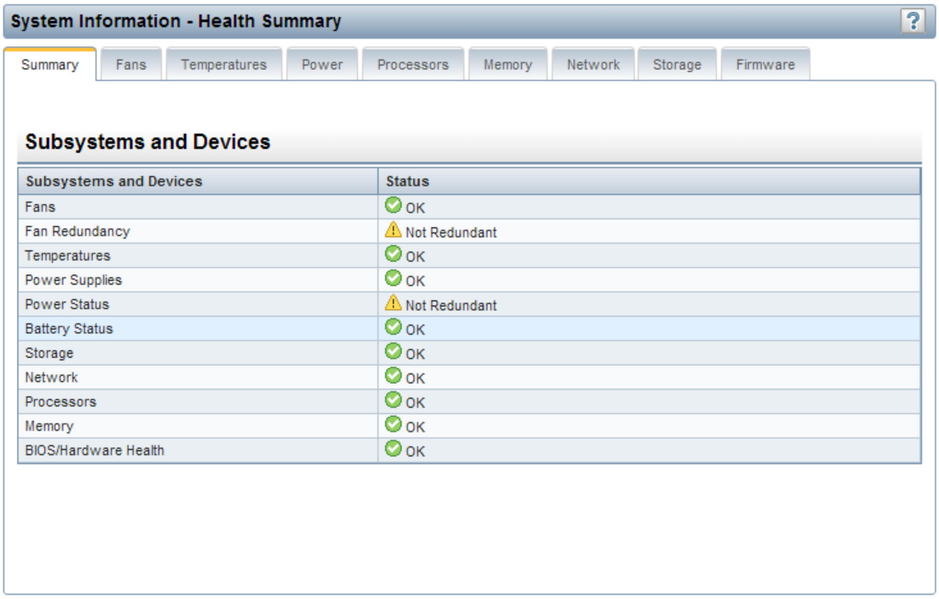
Redundancy information is available for the following items in the list:

- **Fan Redundancy**
- **Power Status**

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

- **BIOS/Hardware Health**
- **Fans**
- **Memory**
- **Network**
- **Power Supplies**
- **Processors**
- **Storage**

- **Temperatures**
- **Battery Status** (HP ProLiant Gen9 servers only)



Subsystems and Devices

Subsystems and Devices	Status
Fans	✓ OK
Fan Redundancy	⚠ Not Redundant
Temperatures	✓ OK
Power Supplies	✓ OK
Power Status	⚠ Not Redundant
Battery Status	✓ OK
Storage	✓ OK
Network	✓ OK
Processors	✓ OK
Memory	✓ OK
BIOS/Hardware Health	✓ OK

The possible status values follow:

- ✓ **Redundant**—There is a backup component for the device or subsystem.
- ✓ **OK**—The device or subsystem is working correctly.
- ⚠ **Not Redundant**—There is no backup component for the device or subsystem.
- ⚠ **Degraded**—The device or subsystem is operating at a reduced capacity.

  NOTE: Previous versions of iLO used a status of **Mismatched** to indicate the presence of mismatched power supplies. iLO 4 displays the power supply status as **Degraded** when mismatched power supplies are installed.

  If you boot a server with nonredundant fans or power supplies, the system health status is listed as **OK**. However, if a redundant fan or power supply fails while the system is booted, the system health status is listed as **Degraded** until you replace the fan or power supply.

- ✖ **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.
- ▼ **Link Down**—The network link is down.
- ▨ **Not Installed**—The subsystem or device is not installed.

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 server 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.

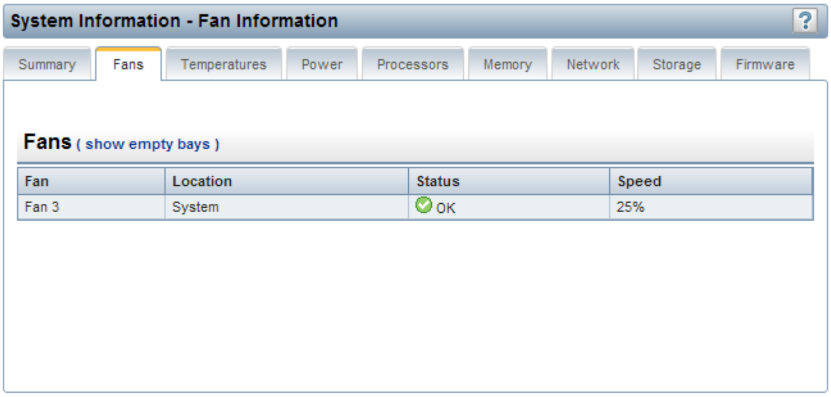
The information displayed on this page varies depending on the server type.

On servers that support fan redundancy, empty fan bays are hidden. To view the empty fan bays, click **show empty bays**. When empty fan bays are displayed, click hide empty bays to hide them.

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

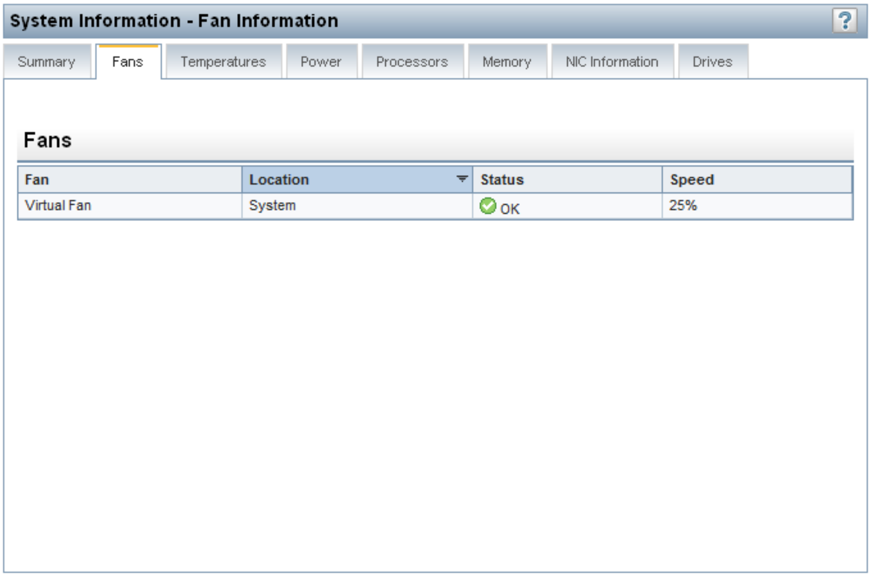


Fans (show empty bays)

Fan	Location	Status	Speed
Fan 3	System	✓ OK	25%

- **Server blades**—ProLiant server blades use the enclosure fans to provide cooling because they do not have internal fans. The enclosure fans are called “virtual fans” on the **Fans** tab. The virtual fan reading represents the cooling amount that a server blade is requesting from the enclosure. The server blade calculates the amount of required cooling 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



Fans

Fan	Location	Status	Speed
Virtual Fan	System	✓ OK	25%

Viewing temperature information

The **Temperature Information** page includes a temperature graph and a table that 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.

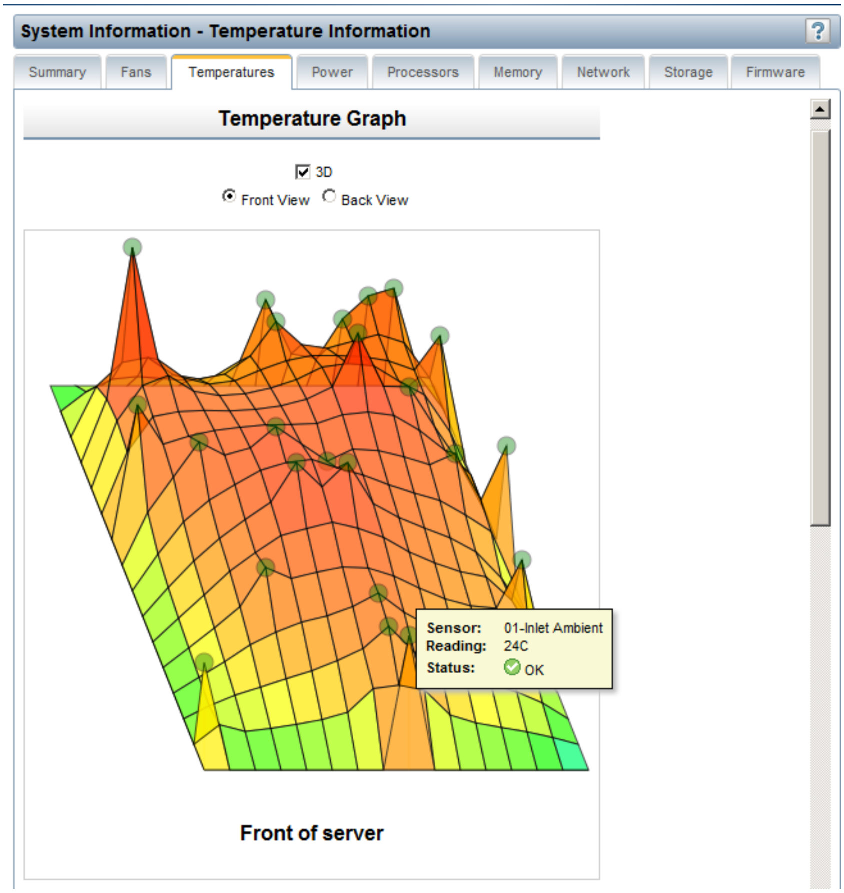
- If the temperature exceeds the caution threshold, the fan speed is increased to maximum.
- If the temperature exceeds the caution threshold for 60 seconds, a graceful server shutdown is attempted.
- If the temperature exceeds the critical threshold, the server is shut down immediately to prevent permanent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

To view the temperature graph, navigate to the **Information→System Information** page, and then click the **Temperatures** tab.



System Information - Temperature Information

Temperature Graph

☑ 3D

● Front View ○ Back View

Sensor: 01-Inlet Ambient
Reading: 24C
Status: ✓ OK

Front of server

Viewing the graph:

- The circles on the graph correspond to the sensors listed in the **Sensor Data** table.
- Move the mouse over a circle on the graph to view the sensor ID, status, and temperature reading.
- The color on the graph is a gradient that ranges from green to red. Green represents a temperature of 0°C and red represents the critical threshold. As the temperature of a sensor increases, the graph color changes from green to amber, and then to red when the temperature approaches the critical threshold.

Customizing the graph:

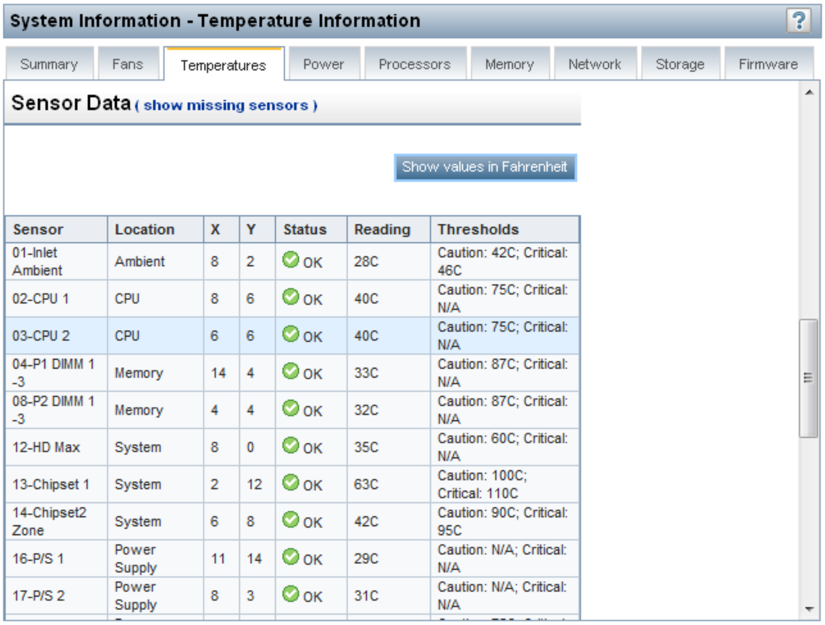
- Select the **3D** check box to display a three-dimensional graph.
- Clear the **3D** check box to display a two-dimensional graph.
- Select **Front View** or **Back View** to display the sensors located at the front or back of the server.

Viewing temperature sensor data

To view temperature sensor data, navigate to the **Information→System Information** page, and then click the **Temperatures** tab.

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.

By default, sensors that are not installed are hidden. To view the missing sensors, click **show missing sensors**. When missing sensors are displayed, click **hide missing sensors** to hide them.


System Information - Temperature Information
?
Summary
Fans
Temperatures
Power
Processors
Memory
Network
Storage
Firmware
Sensor Data (show missing sensors)
Show values in Fahrenheit

Sensor	Location	X	Y	Status	Reading	Thresholds
01-Inlet Ambient	Ambient	8	2	✓ OK	28C	Caution: 42C; Critical: 46C
02-CPU 1	CPU	8	6	✓ OK	40C	Caution: 75C; Critical: N/A
03-CPU 2	CPU	6	6	✓ OK	40C	Caution: 75C; Critical: N/A
04-P1 DIMM 1 -3	Memory	14	4	✓ OK	33C	Caution: 87C; Critical: N/A
08-P2 DIMM 1 -3	Memory	4	4	✓ OK	32C	Caution: 87C; Critical: N/A
12-HD Max	System	8	0	✓ OK	35C	Caution: 60C; Critical: N/A
13-Chipset 1	System	2	12	✓ OK	63C	Caution: 100C; Critical: 110C
14-Chipset2 Zone	System	6	8	✓ OK	42C	Caution: 90C; Critical: 95C
16-P/S 1	Power Supply	11	14	✓ OK	29C	Caution: N/A; Critical: N/A
17-P/S 2	Power Supply	8	3	✓ OK	31C	Caution: N/A; Critical: N/A

The **Sensor Data** table displays the following information:

- **Sensor**—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.

  The ID of the temperature sensor in the **Sensor** column helps to pinpoint the location, providing detailed information about the DIMM or memory area.
- **X**—The x-coordinate of the temperature sensor.
- **Y**—The y-coordinate of the temperature sensor.
- **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, it 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 server before the high temperature causes an electronic component failure.

Viewing power information

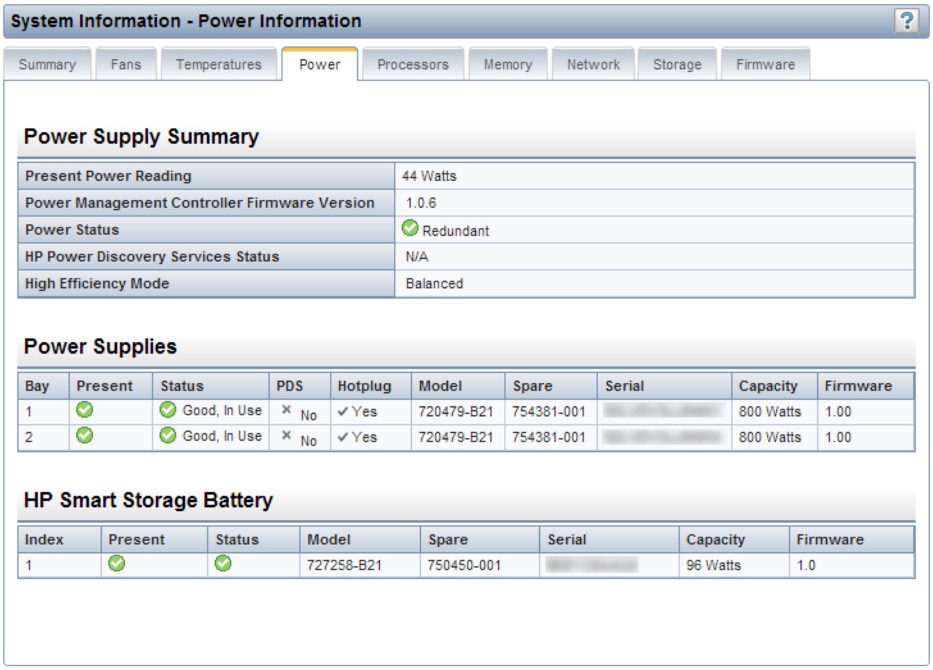
iLO monitors the power supplies in the server to ensure the longest available uptime of the server and operating system. Power supplies might be affected by brownouts and other electrical conditions, or AC cords might be unplugged accidentally. These conditions result in a loss of redundancy if redundant 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.

The iLO processor is an essential component of the HP Power Discovery Services infrastructure. The iLO processor communicates with the HP Intelligent Power Distribution Unit (iPDU) attached to each HP Platinum Plus Power Supply to determine rack and data center power redundancy. When the iLO processor is part of the HP Power Discovery Services infrastructure, it will intelligently report external server input power redundancy status and individual (internal) power supply status.

For more information about HP power supply options, see the following website: http://www.hp.com/go/rackandpower.

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



Power Supply Summary

Present Power Reading	44 Watts
Power Management Controller Firmware Version	1.0.6
Power Status	✓ Redundant
HP Power Discovery Services Status	N/A
High Efficiency Mode	Balanced

Power Supplies

Bay	Present	Status	PDS	Hotplug	Model	Spare	Serial	Capacity	Firmware
1	✓	✓ Good, In Use	× No	✓ Yes	720479-B21	754381-001	[redacted]	800 Watts	1.00
2	✓	✓ Good, In Use	× No	✓ Yes	720479-B21	754381-001	[redacted]	800 Watts	1.00

HP Smart Storage Battery

Index	Present	Status	Model	Spare	Serial	Capacity	Firmware
1	✓	✓	727258-B21	750450-001	[redacted]	96 Watts	1.0

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

- **Rack servers (DL, ML)**—The page displays the following sections: **Power Supply Summary**, **Power Supplies**, and **HP Power Discovery Services iPDU Summary** (if available).
- **Rack servers (SL)**—The page displays the following sections: **Power Supply Summary** and **Power Supplies**.
- **Server blades**—The page displays the following sections: **Power Readings** and **Power Microcontroller**.

Power Supply Summary (all rack servers)

The **Power Supply Summary** section includes the following information:

- **Present Power Reading**—When HP Common Slot Power Supplies are present, the most recent power reading from the server is displayed. Other power supplies do not provide this data.

  Although this value is typically equal to the sum of all active power supply outputs, there might be some small variance as a result of reading the individual power supplies. This value is a guideline value and is not as accurate as the values presented on the iLO **Power Management** pages. For more information, see "Viewing server power usage" (page 240).

- **Power Management Controller Firmware Version**—The firmware version of the power management controller. The server must be powered on for iLO to determine the firmware version. This feature is not available on all servers.

- **Power Status**—The overall status of the power supplied to the server.

  - If the server power supplies are connected to a nonintelligent power source, this section displays the status of the internal server power supplies.

  - If the server power supplies are connected to HP Discovery Services through an HP iPDU, this section displays the status of the power supplied to the internal server power supplies.

  Possible **Power Status** values follow:

  - **Redundant**—Indicates whether the power supplies are in a redundant state. If HP Power Discovery Services is integrated into the infrastructure, the **Power Status** box indicates whether the externally supplied power to the internal power supplies is redundant.

  - **Not Redundant**—Indicates that at least one of the power supplies or iPDUs (in the case of HP Power Discovery Services) is not supplying power to the server. The most common reason for this status is a loss of input power to the power supply. Another reason for this status is a configuration with multiple power supplies connected to the same iPDU. In this case, the individual power supply status is **Good, In Use**, but the **Power Status** value is **Not Redundant** because the loss of input power to the iPDU would lead to a total loss of power to the server.

  - **N/A**—This server does not have redundant power supply capability.

- **HP Power Discovery Services Status**—Possible values follow:

  - **Redundant**—The server is configured for a redundant iPDU configuration.

  - **Not Redundant**—There are not sufficient iPDUs to support redundancy, or the server's power supplies are connected to the same iPDU.

  - **N/A**—No iPDUs were discovered.

  NOTE: When the iLO processor or the server is reset, the iPDU discovery process can take a few minutes to complete.

- **High Efficiency Mode**—The redundant power supply mode that will be used if redundant power supplies are configured.

  High Efficiency Mode improves the power efficiency of the server 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, 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 or the UEFI System Utilities. You cannot modify these settings through iLO. For more information, see the *HP ROM-Based Setup Utility User Guide* or the *HP UEFI System Utilities User Guide*.

NOTE: If High Efficiency Mode is configured to use an unsupported mode, you might experience decreased power supply efficiency.

The redundant power supply modes follow:

- **N/A**—Not applicable.
- **Balanced Mode**—Delivers power equally across 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.
- **Not Supported**—The installed power supplies do not support High Efficiency Mode.

Power Supplies (ML and DL servers only)

The **Power Supplies** section for ML and DL servers includes the following information:

- **Bay**—The bay number of the power supply.
- **Present**—Whether a power supply is installed.
- **Status**—The status of the power supply.
- **PDS**—Whether the installed power supply is enabled for HP Power Discovery Services.

  PDS is an enhancement to the HP iPDU technology. If the server power supply is connected to an iPDU, an additional summary table on this page displays the linked iPDUs. For more information about HP Power Discovery Services and iPDUs, see the following website: http://www.hp.com/go/ipd.

  NOTE: Some power supplies do not provide information for all of the values on this page. If a power supply does not provide information for a value, **N/A** is displayed.

- **Hotplug**—Whether the power supply bay supports swapping the power supply when the server is powered on. If the value is **Yes**, and the power supplies are redundant, the power supply can be removed or replaced when the server is powered on.
- **Model**—The model number of the power supply.
- **Spare**—The part number of the spare power supply.
- **Serial**—The serial number of the power supply.
- **Capacity**—The capacity of the power supply (watts).
- **Firmware**—The installed power supply firmware.

Power Supplies (SL servers only)

The **Power Supplies** section for SL servers displays the name, location, and status of the installed power supplies. The possible status values follow:

- **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. Make sure 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.

HP Power Discovery Services iPDU Summary (ML and DL servers only)

The **HP Power Discovery Services iPDU Summary** section is displayed only if the server power supplies are connected to an iPDU.

After iLO is reset, or when an iPDU is attached, it takes approximately 2 minutes for the iLO web interface to display the **HP Power Discovery Services iPDU Summary** table. This delay is caused by the iPDU discovery process. The following information is displayed in the table:

- **Bay**—The power supply bay number.
- **Status**—The overall communication-link status and rack input power redundancy, as determined by the iPDU. Possible values follow:
  - **iPDU Redundant**—This **Good** status indicates that the server is connected to at least two different iPDUs.
  - **iPDU Not Redundant**—This **Caution** status indicates that the server is not connected to at least two different iPDUs. Typically, this status is displayed when one of the following conditions occurs:
    - An iPDU link is not established for all power supplies.
    - Two or more power supplies are connected to the same iPDU.

      The iPDU MAC address and serial number are identical for power supplies whose input power comes from the same iPDU. If one power supply is waiting for a connection to be established, the iPDU is listed as **Not Redundant**.
  - **Waiting for connection**—This **Informational** status indicates one or more of the following conditions:
    - The wrong power cord was used to connect the power supply to the iPDU.
    - The iPDU and the iLO processor are in the process of connecting. This process can take up to 2 minutes after the iLO processor or the iPDU is reset.
    - The iPDU module does not have a network (or IP) address.
- **Part Number**—The iPDU part number.
- **Serial**—The iPDU serial number.
- **MAC Address**—The MAC address of the iPDU network port. This value helps you to uniquely identify each connected iPDU, because each iPDU has a unique MAC address.
- **iPDU Link**—The iPDU HTTP address (if available). Click the link in this column to open the HP Intelligent Modular PDU web interface.

Power Readings (BL servers only)

The **Power Readings** section for BL servers includes the following information:

Present Power Reading—The most recent power reading from the server.

Although this value is typically equal to the sum of all active power supply outputs, there might be some small variance as a result of reading the individual power supplies. This value is a guideline value and is not as accurate as the values presented on the **Power Management** pages. For more information, see "Viewing server power usage" (page 240).

Power Microcontroller (BL servers only)

The **Power Microcontroller** section for BL servers includes the following information:

Firmware Version—The firmware version of the power management controller. The server must be powered on for iLO to determine the firmware version.

HP Smart Storage Battery (Gen9 servers only)

The **HP Smart Storage Battery** section includes the following information:

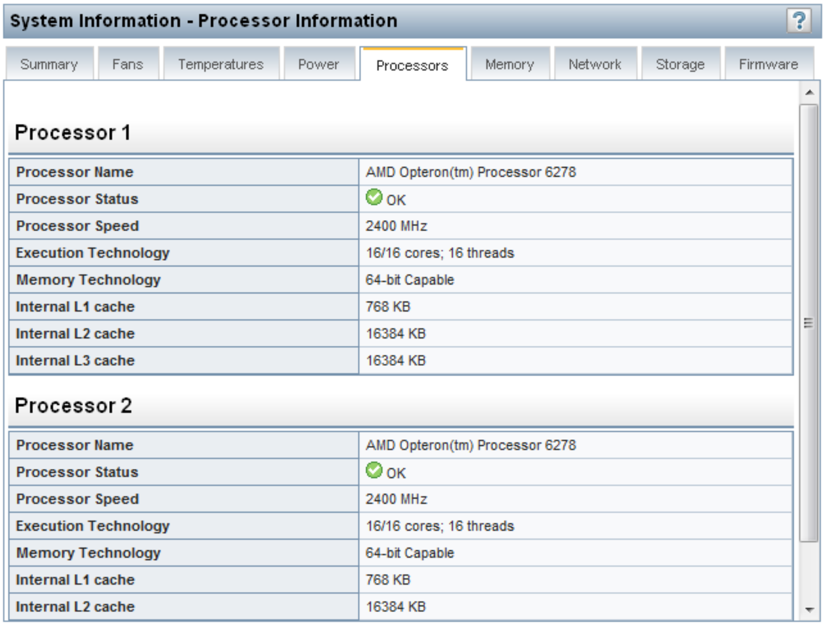
- **Index**—The battery index number.
- **Present**—Whether a battery is installed.
- **Status**—The battery status.
- **Model**—The battery model number.
- **Spare**—The part number of the spare battery.
- **Serial**—The battery serial number.
- **Capacity**—The battery capacity.
- **Firmware**—The installed battery 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.



Processor 1

Processor Name	AMD Opteron(tm) Processor 6278
Processor Status	✓ OK
Processor Speed	2400 MHz
Execution Technology	16/16 cores; 16 threads
Memory Technology	64-bit Capable
Internal L1 cache	768 KB
Internal L2 cache	16384 KB
Internal L3 cache	16384 KB

Processor 2

Processor Name	AMD Opteron(tm) Processor 6278
Processor Status	✓ OK
Processor Speed	2400 MHz
Execution Technology	16/16 cores; 16 threads
Memory Technology	64-bit Capable
Internal L1 cache	768 KB
Internal L2 cache	16384 KB

The following information is displayed:

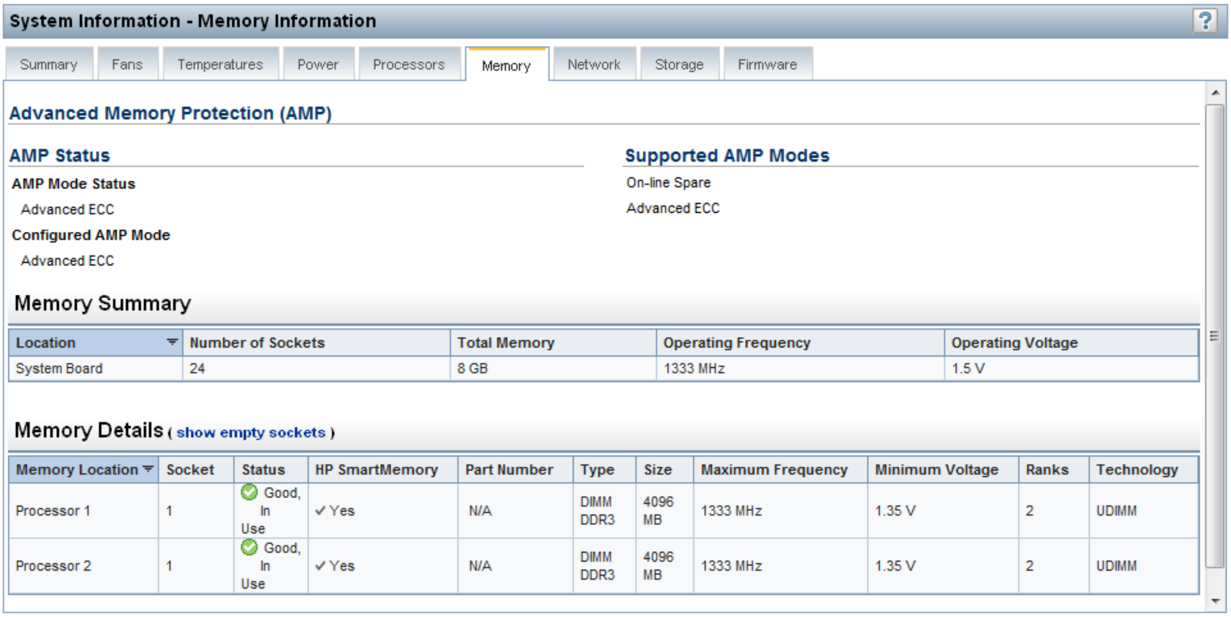
- **Processor Name**—The name of the processor
- **Processor Status**—The health status of the processor
- **Processor Speed**—The speed of the processor
- **Execution Technology**—Information about the processor cores and threads
- **Memory Technology**—The processor memory capabilities
- **Internal 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 summary of the system memory. When server power is off, AMP data is unavailable, and only memory modules present at POST are displayed.

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.



System Information - Memory Information

Advanced Memory Protection (AMP)

AMP Status

AMP Mode Status

Advanced ECC

Configured AMP Mode

Advanced ECC

Supported AMP Modes

On-line Spare

Advanced ECC

Memory Summary

Location	Number of Sockets	Total Memory	Operating Frequency	Operating Voltage
System Board	24	8 GB	1333 MHz	1.5 V

Memory Details (show empty sockets)

Memory Location	Socket	Status	HP SmartMemory	Part Number	Type	Size	Maximum Frequency	Minimum Voltage	Ranks	Technology
Processor 1	1	✓ Good, In Use	✓ Yes	N/A	DIMM DDR3	4096 MB	1333 MHz	1.35 V	2	UDIMM
Processor 2	1	✓ Good, In Use	✓ Yes	N/A	DIMM DDR3	4096 MB	1333 MHz	1.35 V	2	UDIMM

Advanced Memory Protection

This section displays the following information:

- **AMP Mode Status**—The status of the AMP subsystem. The following states are supported:
  - **Other/Unknown**—The system does not support AMP, or the management software cannot determine the status.
  - **Not Protected**—The system supports AMP, but the feature is disabled.
  - **Protected**—The system supports AMP. The feature is enabled but not engaged.
  - **Degraded**—The system was protected, but AMP is engaged. Therefore, AMP is no longer available.
  - **DIMM ECC** —The system is protected by DIMM ECC only.
  - **Mirroring**—The system is protected by AMP in the mirrored mode. No DIMM faults have been detected.
  - **Degraded Mirroring**—The system is protected by AMP in the mirrored mode. One or more DIMM faults have been detected.
  - **On-line Spare**—The system is protected by AMP in the hot spare mode. No DIMM faults have been detected.
  - **Degraded On-line Spare**—The system is protected by AMP in the hot spare mode. One or more DIMM faults have been detected.
  - **RAID-XOR**—The system is protected by AMP in the XOR memory mode. No DIMM faults have been detected.
  - **Degraded RAID-XOR**—The system is protected by AMP in the XOR memory mode. One or more DIMM faults have been detected.
  - **Advanced ECC**—The system is protected by AMP in the Advanced ECC mode.
  - **Degraded Advanced ECC**—The system is protected by AMP in the Advanced ECC mode. One or more DIMM faults have been detected.

    - **LockStep**—The system is protected by AMP in the LockStep mode.
    - **Degraded LockStep**—The system is protected by AMP in the LockStep mode. One or more DIMM faults have been detected.
- **Configured AMP Mode**—The active AMP mode. The following modes are supported:
    - **None/Unknown**—The management software cannot determine the AMP fault tolerance, or the system is not configured for AMP.
    - **On-line Spare**—A single spare bank of memory is set aside at boot time. If enough ECC errors occur, the spare memory is activated and the memory that is experiencing the errors is disabled.
    - **Mirroring**—The system is configured for mirrored memory protection. All memory banks are duplicated in mirrored memory, as opposed to only one for online spare memory. If enough ECC errors occur, the spare memory is activated and the memory that is experiencing the errors is disabled.
    - **RAID-XOR**—The system is configured for AMP with the XOR engine.
    - **Advanced ECC**—The system is configured for AMP with the Advanced ECC engine.
    - **LockStep**—The system is configured for AMP with the LockStep engine.
- **Online Spare (Rank Sparing)**—The system is configured for Online Spare Rank AMP.
- **Online Spare (Channel Sparing)**—The system is configured for Online Spare Channel AMP.
- **Intersocket Mirroring**—The system is configured for mirrored intersocket AMP between the memory of two processors or boards.
- **Intrasocket Mirroring—**The system is configured for mirrored intrasocket AMP between the memory of a single processor or board.
- **Supported AMP Modes**—The following modes are supported:
    - **RAID-XOR**—The system can be configured for AMP using the XOR engine.
    - **Dual Board Mirroring**—The system can be configured for mirrored advanced memory protection in a dual memory board configuration. The mirrored memory can be swapped with memory on the same memory board or with memory on the second memory board.
    - **Single Board Mirroring**—The system can be configured for mirrored advanced memory protection in a single memory board.
    - **Advanced ECC**—The system can be configured for Advanced ECC.
    - **Mirroring**—The system can be configured for mirrored AMP.
    - **On-line Spare**—The system can be configured for online spare AMP.
    - **LockStep**—The system can be configured for LockStep AMP.
    - **Online Spare (Rank Sparing)**—The system can be configured for Online Spare Rank AMP.
    - **Online Spare (Channel Sparing)**—The system can be configured for Online Spare Channel AMP.
    - **Intersocket Mirroring**—The system can be configured for mirrored intersocket AMP between the memory of two processors or boards.

  - **Intrasocket Mirroring—**The system can be configured for mirrored intrasocket AMP between the memory of a single processor or board.
  - **None**—The system cannot be configured for AMP.

Memory Summary

This section shows a summary of the memory that was installed and operational at POST.

- **Location**—The slot or processor on which the memory board, cartridge, or riser is installed. Possible values follow:
  - **System Board**—There is no separate memory board slot. All DIMMs are installed on the motherboard.
  - **Board Number**—There is a memory board slot available. All DIMMs are installed on the memory board.
  - **Processor Number**—The processor on which the memory DIMMs are installed.
  - **Riser Number**—The riser on which the memory DIMMs are installed.
- **Number of Sockets**—The number of memory module sockets present on the memory board, cartridge, or riser.
- **Total Memory**—The size of the memory for this board, cartridge, or riser, including memory recognized by the operating system and memory used for spare, mirrored, or XOR configurations.
- **Operating Frequency**—The frequency at which the memory on the memory board, cartridge, or riser operates.
- **Operating Voltage**—The voltage at which the memory on the memory board, cartridge, or riser operates.

Memory Details

This section shows the memory modules on the host that were installed and operational at POST. Unpopulated module positions are also listed. Various resilient memory configurations can change the actual memory inventory from what was sampled at POST. In systems that have a high number of memory modules, all module positions might not be listed.

By default, empty memory sockets are hidden. To view the empty memory sockets, click **show empty sockets**. When empty memory sockets are displayed, click **hide empty sockets** to hide them.

- **Memory Location**—The slot or processor on which the memory module is installed.
- **Socket**—The memory module socket number.
- **Status**—The memory module status and whether the module is in use.
- **HP SmartMemory**—Whether the memory module is HP SmartMemory. Possible values are **Yes** and **No**. If no memory module is installed, the value **N/A** is displayed.

  If the value **No** is displayed, the listed module is not an HP SmartMemory module. The memory module will function, but it has no warranty, and it might not perform as well as an HP SmartMemory module.

  For more information about HP SmartMemory, see http://www.hp.com/go/memory.
- **Part Number**—The memory module part number.

  NOTE: This value is displayed only for HP SmartMemory modules.

- **Type**—The type of memory installed. Possible values follow:
  - **Other**—Memory type cannot be determined.
  - **Board**—Memory module is permanently mounted (not modular) on a system board or memory expansion board.
  - **CPQ single width module**
  - **CPQ double width module**
  - **SIMM**
  - **PCMCIA**
  - **Compaq-specific**
  - **DIMM**
  - **Small outline DIMM**
  - **RIMM**
  - **SRIMM**
  - **FB-DIMM**
  - **DIMM DDR**
  - **DIMM DDR2**
  - **DIMM DDR3**
  - **DIMM DDR4** (Gen9 servers only)
  - **FB-DIMM DDR2**
  - **FB-DIMM DDR3**
  - **N/A**—Memory module is not present.
- **Size**—The size of the memory module, in MB.
- **Maximum Frequency**—The maximum frequency at which the memory module can operate.
- **Minimum Voltage**—The minimum voltage at which the memory module can operate.
- **Ranks**—The number of ranks in the memory module.
- **Technology**—The memory module technology. Possible values follow:
  - **Unknown**—Memory technology cannot be determined.
  - **N/A**—Memory module is not present.
  - **Fast Page**
  - **EDO**
  - **Burst EDO**
  - **Synchronous**
  - **RDRAM**

- ◦ **RDIMM**
- ◦ **UDIMM**
- ◦ **LRDIMM**

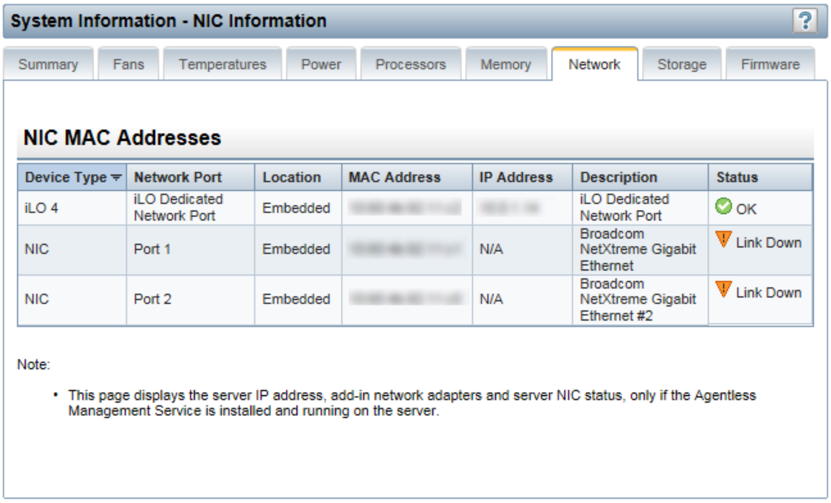
Viewing network information

The **NIC Information** page displays read-only information about the integrated and add-in 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.

The server IP address, add-in network adapters, and server NIC status are displayed only if the Agentless Management Service is installed and running on the server.

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



NIC MAC Addresses

Device Type	Network Port	Location	MAC Address	IP Address	Description	Status
iLO 4	iLO Dedicated Network Port	Embedded	[redacted]	[redacted]	iLO Dedicated Network Port	✓ OK
NIC	Port 1	Embedded	[redacted]	N/A	Broadcom NetXtreme Gigabit Ethernet	⚠ Link Down
NIC	Port 2	Embedded	[redacted]	N/A	Broadcom NetXtreme Gigabit Ethernet #2	⚠ Link Down

Note:

- This page displays the server IP address, add-in network adapters and server NIC status, only if the Agentless Management Service is installed and running on the server.

The following information is displayed:

- **Device Type**—The device type is one of the following:
  - ◦ **iLO 4**—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.
- **Network Port**—The configured network port.
- **Location**—The location of the NIC adapter on the system board.
- **MAC Address**—The port MAC address.
- **IP Address**—The host IP address.
- **Description**—A description of the NIC.
- **Status**—The NIC status.

Viewing storage information

The **Storage Information** page displays information about HP Smart Array controllers, drive enclosures, the attached logical drives, and the physical drives that constitute the logical drives.

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 information displayed on this page depends on your storage configuration. Some storage configurations will not display information for every category.

To expand or collapse the data, click **Expand All** or **Collapse All**, respectively.

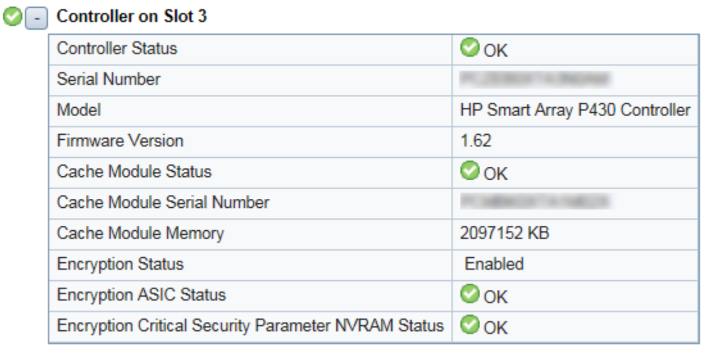
To view storage information:

1. Navigate to the **Information→System Information** page.
2. Click the **Storage** tab.
3. Select one of the following options:
   - **Logical View**—Select this option to view configured logical drives and associated physical drives. This view does not show physical drives that are not configured as part of an array, or spare drives.
   - **Physical View**—Select this option to view physical drives. This view does not show logical drives.

A description of each section on the **Storage Information** page follows.

Controllers

This section provides information about the HP Smart Array controllers.



✓ - **Controller on Slot 3**

Controller Status	✓ OK
Serial Number	[redacted]
Model	HP Smart Array P430 Controller
Firmware Version	1.62
Cache Module Status	✓ OK
Cache Module Serial Number	[redacted]
Cache Module Memory	2097152 KB
Encryption Status	Enabled
Encryption ASIC Status	✓ OK
Encryption Critical Security Parameter NVRAM Status	✓ OK

The top-level controller status is a combination of the controller hardware status and the status of cache modules, enclosures, and physical, logical, and spare drives associated with the controller. If the controller hardware status is **OK**, and any associated hardware has a failure, the top-level controller status changes to **Major Warning** or **Degraded**, depending on the failure type. If the controller hardware has a **Failed** status, the top-level controller status is **Failed**.

The following information is displayed for each HP Smart Array controller:

- Controller location—Slot number or system board
- Controller status—Controller hardware status (**OK** or **Failed**)
- Controller serial number
- Controller model name and number
- Controller firmware version
- Cache module status
- Cache module serial number
- Cache module memory

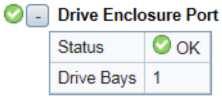
The following status information is displayed for controllers that support encryption:

- **Encryption Status**—The following values are possible:
  - **Enabled**
  - **Not Enabled**
  - **Enabled—Local Mode**—This value is displayed when you do not use a remote key management server.
- **Encryption ASIC Status**—Indicates whether the ASIC encryption self tests for the controller passed or failed. A failed status indicates that the controller is not encrypted.
- **Encryption Critical Security Parameter NVRAM Status**—Indicates whether the controller successfully detected the critical security parameter NVRAM. A failed status means that the controller is not encrypted.

NOTE: The encryption settings for an HP Smart Array controller can be configured by using the HP Smart Storage Administrator software. For instructions, see the HP Smart Storage Administrator documentation.

Drive Enclosures

This section provides information about the drive enclosures attached to an HP Smart Array controller.



✓ - Drive Enclosure Port 2I Box 1

Status	✓ OK
Drive Bays	1

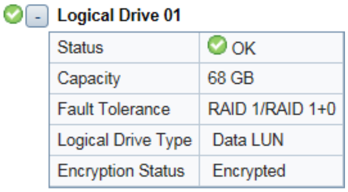
The following information is listed for each drive enclosure:

- Enclosure port and box numbers
- Enclosure status
- Number of drive bays
- Serial number
- Model number
- Firmware version

Some enclosures do not have all of the listed properties, and some storage configurations do not have drive enclosures.

Logical Drives

This section is available when the **Logical View** option is selected on the **System Information – Storage Information** page.



✓ - Logical Drive 01

Status	✓ OK
Capacity	68 GB
Fault Tolerance	RAID 1/RAID 1+0
Logical Drive Type	Data LUN
Encryption Status	Encrypted

The following information is listed for the logical drives attached to an HP Smart Array controller:

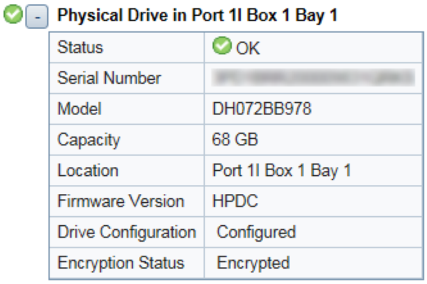
- Logical drive number
- Logical drive status

- Logical drive capacity
- Fault tolerance
- Logical Drive Type
- Encryption status

NOTE: Logical drives must be configured through the HP Smart Storage Administrator software before they can be displayed on the **System Information – Storage Information** page. For more information, see the HP Smart Storage Administrator documentation.

Physical Drives

The information listed in this section depends on whether the **Logical View** or **Physical View** option is selected. When using **Logical View**, physical drives that are configured as part of an array are listed. When using **Physical View**, all physical drives are listed.



✓ - Physical Drive in Port 1I Box 1 Bay 1

Status	✓ OK
Serial Number	[redacted]
Model	DH072BB978
Capacity	68 GB
Location	Port 1I Box 1 Bay 1
Firmware Version	HPDC
Drive Configuration	Configured
Encryption Status	Encrypted

When a physical drive has a **Failed** status, this status does not affect the overall storage health status. Only logical drives affect the storage health status.

The following information is listed for the physical drives attached to an HP Smart Array controller:

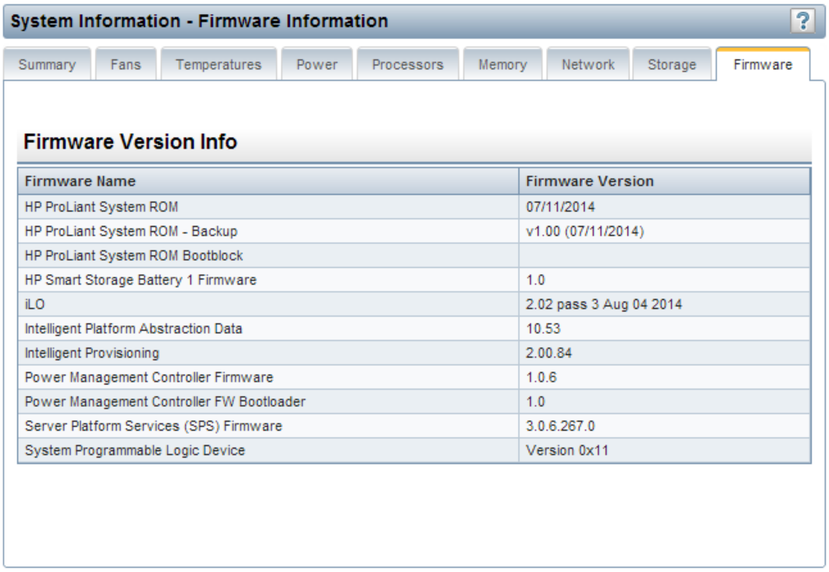
- Physical drive port, box, and bay numbers
- Physical drive status
- Physical drive serial number
- Physical drive model number
- Physical drive capacity
- Physical drive location
- Physical drive firmware version
- Physical drive configuration
- Encryption status

Viewing firmware information

The **Firmware Information** page displays firmware information for various server components.

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

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



System Information - Firmware Information

Firmware Version Info

Firmware Name	Firmware Version
HP ProLiant System ROM	07/11/2014
HP ProLiant System ROM - Backup	v1.00 (07/11/2014)
HP ProLiant System ROM Bootblock	
HP Smart Storage Battery 1 Firmware	1.0
iLO	2.02 pass 3 Aug 04 2014
Intelligent Platform Abstraction Data	10.53
Intelligent Provisioning	2.00.84
Power Management Controller Firmware	1.0.6
Power Management Controller FW Bootloader	1.0
Server Platform Services (SPS) Firmware	3.0.6.267.0
System Programmable Logic Device	Version 0x11

The following information is displayed:

- **Firmware Name**—The name of the firmware.

  The firmware types listed on this page vary based on the server model and configuration.

  For most servers, the HP ProLiant System ROM and the iLO firmware are listed. Other possible firmware options include the Power Management Controller, Server Platform Services, HP Smart Array, Intelligent Provisioning, Intelligent Platform Abstraction Data (Gen9 servers only), HP Smart Storage Battery (Gen9 servers only), and networking adapters.

  NOTE: To view firmware information for hard drives, navigate to the **System Information→Storage** page.

- **Firmware Version**—The version of the firmware.

Using the iLO Event Log

The iLO Event Log provides a record of significant events detected by iLO.

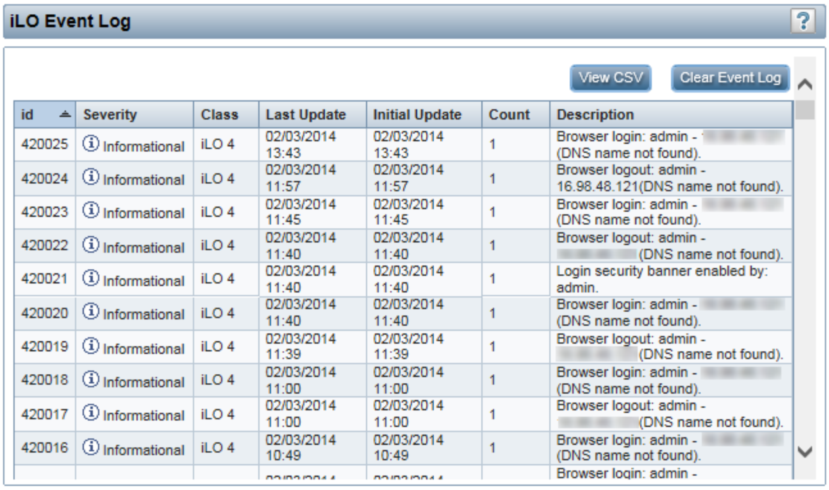
Logged events include major server events such as a server power outage or a server reset, and iLO events such as unauthorized login attempts. Other logged events include successful or unsuccessful browser and Remote Console logins, virtual power and power-cycle events, clearing the log, and some configuration changes, such as creating or deleting a user and registering for remote support.

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 the 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.



id	Severity	Class	Last Update	Initial Update	Count	Description
420025	ⓘ Informational	iLO 4	02/03/2014 13:43	02/03/2014 13:43	1	Browser login: admin - [redacted] (DNS name not found).
420024	ⓘ Informational	iLO 4	02/03/2014 11:57	02/03/2014 11:57	1	Browser logout: admin - 16.98.48.121(DNS name not found).
420023	ⓘ Informational	iLO 4	02/03/2014 11:45	02/03/2014 11:45	1	Browser login: admin - [redacted] (DNS name not found).
420022	ⓘ Informational	iLO 4	02/03/2014 11:40	02/03/2014 11:40	1	Browser logout: admin - [redacted](DNS name not found).
420021	ⓘ Informational	iLO 4	02/03/2014 11:40	02/03/2014 11:40	1	Login security banner enabled by: admin.
420020	ⓘ Informational	iLO 4	02/03/2014 11:40	02/03/2014 11:40	1	Browser login: admin - [redacted] (DNS name not found).
420019	ⓘ Informational	iLO 4	02/03/2014 11:39	02/03/2014 11:39	1	Browser logout: admin - [redacted](DNS name not found).
420018	ⓘ Informational	iLO 4	02/03/2014 11:00	02/03/2014 11:00	1	Browser login: admin - [redacted] (DNS name not found).
420017	ⓘ Informational	iLO 4	02/03/2014 11:00	02/03/2014 11:00	1	Browser logout: admin - [redacted](DNS name not found).
420016	ⓘ Informational	iLO 4	02/03/2014 10:49	02/03/2014 10:49	1	Browser login: admin - [redacted] (DNS name not found).
						Browser login: admin -

The log displays the following information:

- **id**—The event ID number. Events are numbered in the order in which they are generated.

  By default, the iLO Event Log is sorted by the ID, with the most recent event at the top.

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

  Possible values follow:

  ◦ **Critical**—The event indicates a service loss or imminent service loss. Immediate attention is needed.

  ◦ **Caution**—The event is significant but does not indicate performance degradation.

  ◦ **Informational**—The event provides background information.

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

  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 (server blades only)

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

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

  If the iLO firmware 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, important 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.

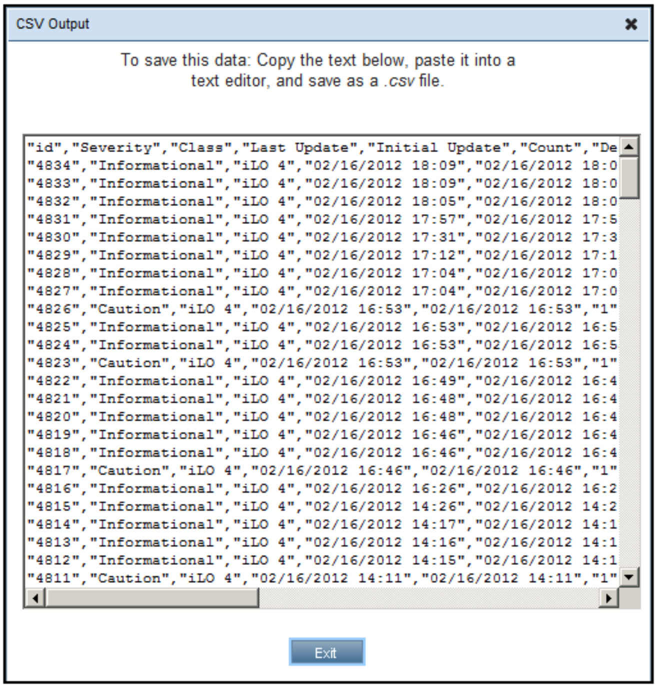
  If the iLO firmware is rolled back to an earlier version, the description `UNKNOWN EVENT TYPE` might be displayed for events recorded by the newer firmware. You can resolve this issue by updating the firmware to the latest supported version, or by clearing the event log.

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.



CSV Output

To save this data: Copy the text below, paste it into a text editor, and save as a *.csv* file.

```
"id","Severity","Class","Last Update","Initial Update","Count","De
"4834","Informational","iLO 4","02/16/2012 18:09","02/16/2012 18:0
"4833","Informational","iLO 4","02/16/2012 18:09","02/16/2012 18:0
"4832","Informational","iLO 4","02/16/2012 18:05","02/16/2012 18:0
"4831","Informational","iLO 4","02/16/2012 17:57","02/16/2012 17:5
"4830","Informational","iLO 4","02/16/2012 17:31","02/16/2012 17:3
"4829","Informational","iLO 4","02/16/2012 17:12","02/16/2012 17:1
"4828","Informational","iLO 4","02/16/2012 17:04","02/16/2012 17:0
"4827","Informational","iLO 4","02/16/2012 17:04","02/16/2012 17:0
"4826","Caution","iLO 4","02/16/2012 16:53","02/16/2012 16:53","1"
"4825","Informational","iLO 4","02/16/2012 16:53","02/16/2012 16:5
"4824","Informational","iLO 4","02/16/2012 16:53","02/16/2012 16:5
"4823","Caution","iLO 4","02/16/2012 16:53","02/16/2012 16:53","1"
"4822","Informational","iLO 4","02/16/2012 16:49","02/16/2012 16:4
"4821","Informational","iLO 4","02/16/2012 16:48","02/16/2012 16:4
"4820","Informational","iLO 4","02/16/2012 16:48","02/16/2012 16:4
"4819","Informational","iLO 4","02/16/2012 16:46","02/16/2012 16:4
"4818","Informational","iLO 4","02/16/2012 16:46","02/16/2012 16:4
"4817","Caution","iLO 4","02/16/2012 16:46","02/16/2012 16:46","1"
"4816","Informational","iLO 4","02/16/2012 16:26","02/16/2012 16:2
"4815","Informational","iLO 4","02/16/2012 14:26","02/16/2012 14:2
"4814","Informational","iLO 4","02/16/2012 14:17","02/16/2012 14:1
"4813","Informational","iLO 4","02/16/2012 14:16","02/16/2012 14:1
"4812","Informational","iLO 4","02/16/2012 14:15","02/16/2012 14:1
"4811","Caution","iLO 4","02/16/2012 14:11","02/16/2012 14:11","1"
```

2. Copy the text displayed in the **iLO Event Log CSV** 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 Integrated Management Log 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.

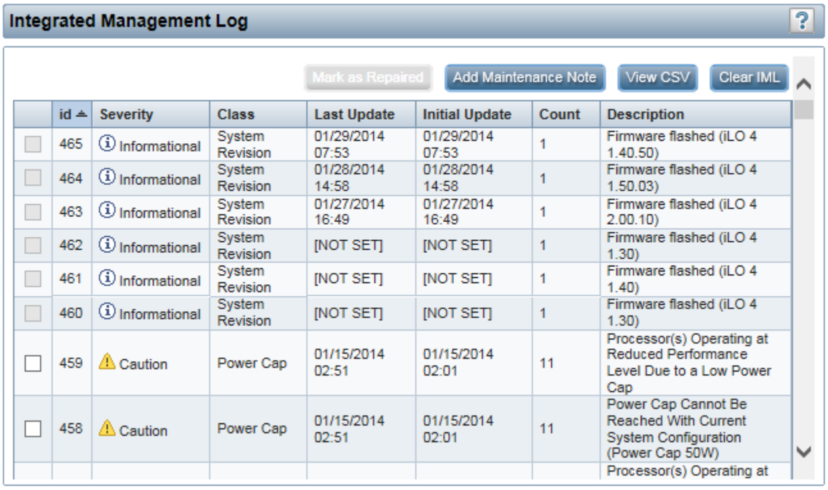
iLO manages the IML, which you can access through a supported browser, even when the server is off. The ability to view the log when the server is off can be helpful when troubleshooting remote host server issues.

Examples of the types of information recorded 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.



	id ▲	Severity	Class	Last Update	Initial Update	Count	Description
□	465	ⓘ Informational	System Revision	01/29/2014 07:53	01/29/2014 07:53	1	Firmware flashed (iLO 4 1.40.50)
□	464	ⓘ Informational	System Revision	01/28/2014 14:58	01/28/2014 14:58	1	Firmware flashed (iLO 4 1.50.03)
□	463	ⓘ Informational	System Revision	01/27/2014 16:49	01/27/2014 16:49	1	Firmware flashed (iLO 4 2.00.10)
□	462	ⓘ Informational	System Revision	[NOT SET]	[NOT SET]	1	Firmware flashed (iLO 4 1.30)
□	461	ⓘ Informational	System Revision	[NOT SET]	[NOT SET]	1	Firmware flashed (iLO 4 1.40)
□	460	ⓘ Informational	System Revision	[NOT SET]	[NOT SET]	1	Firmware flashed (iLO 4 1.30)
□	459	⚠ Caution	Power Cap	01/15/2014 02:51	01/15/2014 02:01	11	Processor(s) Operating at Reduced Performance Level Due to a Low Power Cap
□	458	⚠ Caution	Power Cap	01/15/2014 02:51	01/15/2014 02:01	11	Power Cap Cannot Be Reached With Current System Configuration (Power Cap 50W)
							Processor(s) Operating at

The IML displays the following information:

- 🔧 This column includes a check box next to each event with Critical or Caution status. Use this check box to select an event to mark as repaired.

  For more information about marking events as repaired, see "Marking a log entry as repaired" (page 176).

- **id**—The event ID number. Events are numbered in the order in which they are generated.

  By default, the IML is sorted by the ID, with the most recent event at the top. A factory reset will reset the counter.

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

  Possible values follow:

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

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

  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 (server blades 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 when the first event of this type occurred. This value is based on the date and time stored by the iLO firmware.

  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.

   To select an IML entry, click the check box next to the entry in the first column of the IML table. If a check box is not displayed next to an IML entry, that entry cannot be marked as repaired.

4. Click **Mark as Repaired**.

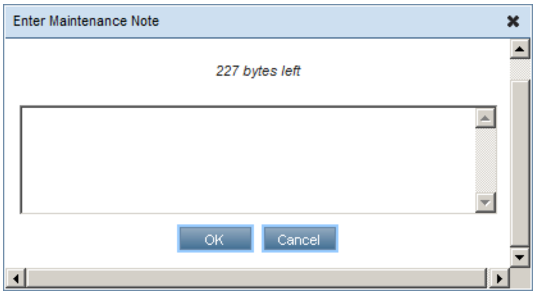
   The iLO web interface refreshes, and the selected log entry status changes to **Repaired**.

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.

   227 bytes left

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 the HP Active Health System

The HP Active Health System monitors and records changes in the server hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur. HP Active Health System does not collect information about your operations, finances, customers, employees, partners, or data center (for example, IP addresses, host names, user names, and passwords).

By downloading and sending Active Health System data to HP, you agree to have HP use the data for analysis, technical resolution, and quality improvements. The data that is collected is managed according to the HP Privacy Statement, available at http://www.hp.com/go/privacy.

Examples of data that is collected follow:

- Server model
- Serial number
- Processor model and speed
- Storage capacity and speed
- Memory capacity and speed
- Firmware/BIOS

NOTE: The HP Active Health System does not parse or change operating system data from third-party error event log activities (for example, content created or passed through the operating system).

When the Active Health System Log is full, new data overwrites the oldest data in the log.

You can download the Active Health System Log manually and send it to HP. To download the log, use iLO, Intelligent Provisioning, `curl`, or the Active Health System download CLI tool. For more information, see the following:

- "Downloading the Active Health System Log for a date range" (page 178)
- "Extracting the Active Health System log by using curl" (page 179)
- *HP Intelligent Provisioning User Guide for HP ProLiant Gen8 Servers*
- *HP Intelligent Provisioning User Guide for HP ProLiant Gen9 Servers*

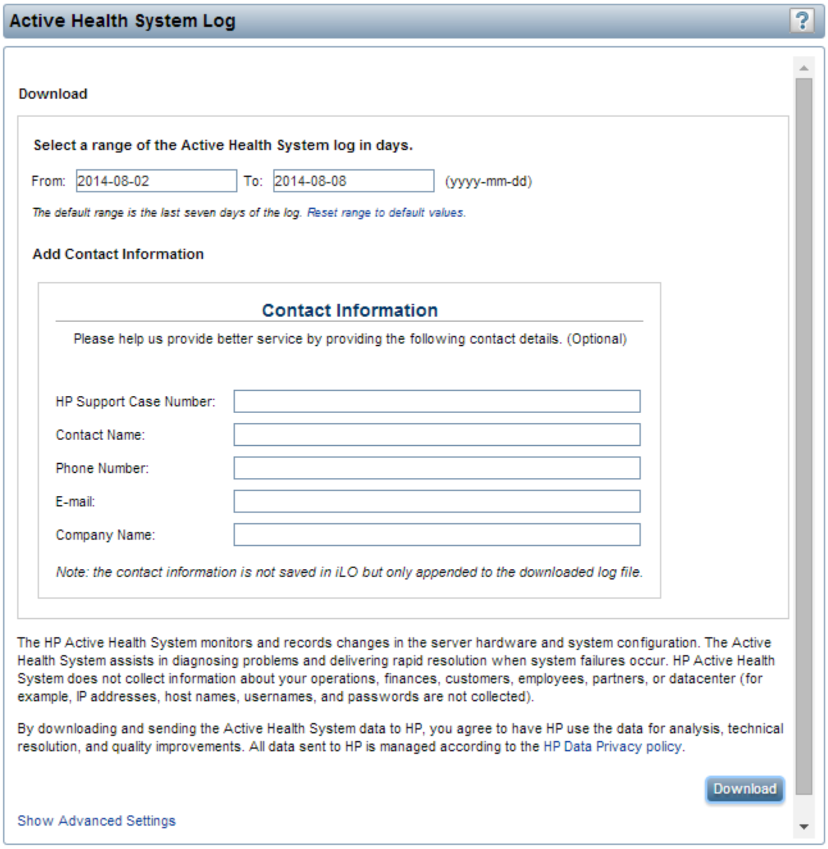
- *HP ProLiant Gen8 Troubleshooting Guide, Volume I: Troubleshooting*
- *HP ProLiant Gen9 Troubleshooting Guide, Volume I: Troubleshooting*

Any user can download the Active Health System Log. The Configure iLO Settings privilege is required to modify the Active Health System settings or to clear the log.

Downloading the Active Health System Log for a date range

Use the following procedure to download the Active Health System Log for a date range.

1. Navigate to the **Information→Active Health System Log** page.



Active Health System Log

Download

Select a range of the Active Health System log in days.

From: 2014-08-02 To: 2014-08-08 (yyyy-mm-dd)

The default range is the last seven days of the log. Reset range to default values.

Add Contact Information

Contact Information

Please help us provide better service by providing the following contact details. (Optional)

HP Support Case Number:

Contact Name:

Phone Number:

E-mail:

Company Name:

Note: the contact information is not saved in iLO but only appended to the downloaded log file.

The HP Active Health System monitors and records changes in the server hardware and system configuration. The Active Health System assists in diagnosing problems and delivering rapid resolution when system failures occur. HP Active Health System does not collect information about your operations, finances, customers, employees, partners, or datacenter (for example, IP addresses, host names, usernames, and passwords are not collected).

By downloading and sending the Active Health System data to HP, you agree to have HP use the data for analysis, technical resolution, and quality improvements. All data sent to HP is managed according to the HP Data Privacy policy.

2. Enter the range of days to include in the log.

   The default setting is to include log information for the last 7 days. Click **Reset range to default values** to reset the dates.

   a. Click the **From** box.

      A calendar is displayed.

   b. Select the range start date on the calendar.

   c. Click the **To** box.

      A calendar is displayed.

   d. Select the range end date on the calendar.

3. Optional: Enter the contact information to include in the downloaded file.

   - **HP Support Case Number**
   - **Contact Name**
   - **Phone Number**

- **E-mail**
- **Company Name**

  The contact information you provide will be treated in accordance with the HP Data Privacy Policy, available at http://www.hp.com/go/privacy. This information is not written to the log data stored on the server.

4. Click **Download**.
5. Save the file.

   The default file name is `HP_<server_serial_number>_<date>.ahs`.
6. If you have an open case with HP Support, you can email the log file to **HPSupport_Global@hp.com**.

   Use the following convention for the email subject: CASE: <HP support case number>.

   NOTE: Files that are larger than 15 MB must be compressed and uploaded to an FTP site. If needed, contact HP Support for FTP site information.

Downloading the entire Active Health System Log

Use the following procedure to download the entire Active Health System Log.

It might take a long time to download the entire Active Health System Log. If you must upload the Active Health System Log for a technical issue, HP recommends downloading the log for the specific range of dates in which the problem occurred. For instructions, see "Downloading the Active Health System Log for a date range" (page 178).

1. Navigate to the **Information→Active Health System Log** page.
2. Click **Show Advanced Settings**.
3. Optional: Enter the contact information to include in the downloaded file.
   - **HP Support Case Number**
   - **Contact Name**
   - **Phone Number**
   - **E-mail**
   - **Company Name**

   The contact information that you provide will be treated in accordance with the HP Data Privacy Policy, available at http://www.hp.com/go/privacy. This information is not written to the log data stored on the server.
4. Click **Download Entire Log**.
5. Save the file.
6. If you have an open case with HP Support, you can email the log file to **HPSupport_Global@hp.com**.

   Use the following convention for the email subject: CASE: <HP support case number>.

   NOTE: Files that are larger than 15 MB must be compressed and uploaded to an FTP site. If needed, contact HP Support for FTP site information.

Extracting the Active Health System log by using curl

iLO 4 1.30 and later supports extracting the Active Health System log with the `curl` command line tool.

You can download `curl` from the following website: http://curl.haxx.se/.

To download the Active Health System log by using `curl`:

1. Install `curl`.
2. Open a command window.
3. Enter the following command to download the Active Health System log for a range of dates:

   ```
   curl "https://<iLO IP address>/ahsdata/ahs.ahs?from=<yyyy-mm-dd>&to=
   <yyyy-mm-dd>" -k -v -u <username>:<password> -o <filename>.ahs
   ```

   Where:

   - `<iLO IP address>` is the iLO IP address.
   - `from=<yyyy-mm-dd>&to=<yyyy-mm-dd>` represents the start and end date of the range of dates to include in the log. Enter dates in the format `year-month-day`, for example, 2013-07-29 for July 29, 2013.
   - `–k` specifies that HTTPS warnings will be ignored.
   - `–v` specifies verbose output.
   - `-u <username>:<password>` specifies your iLO user account credentials.
   - `–o <filename>` specifies the output file name and path.

   NOTE: To download the entire log, omit the `from` and `to` parameters and use the following command: `curl "https://<iLO IP address>/ahsdata/ahs.ahs" -k -v -u <username>:<password> -o <filename>.ahs`

   The file is saved to the path you specified.
4. Close the command window.

Clearing the Active Health System Log

If the log file is corrupted, or if you want to clear and restart logging, use the following procedure to clear the Active Health System Log. You must have the Configure iLO Settings privilege to perform this procedure.

1. Navigate to the **Information→Active Health System Log** page.
2. Click **Show Advanced Settings**.
3. Scroll to the **Clear Log** section, and then click the **Clear** button.

   The following message appears:

   ```
   Are you sure that you want to clear the entire Active Health System
   log? This action cannot be undone.
   ```
4. Click **OK**.

   iLO notifies you that the log is being cleared.
5. Reset iLO.

   For instructions, see “Using iLO diagnostics” (page 180).

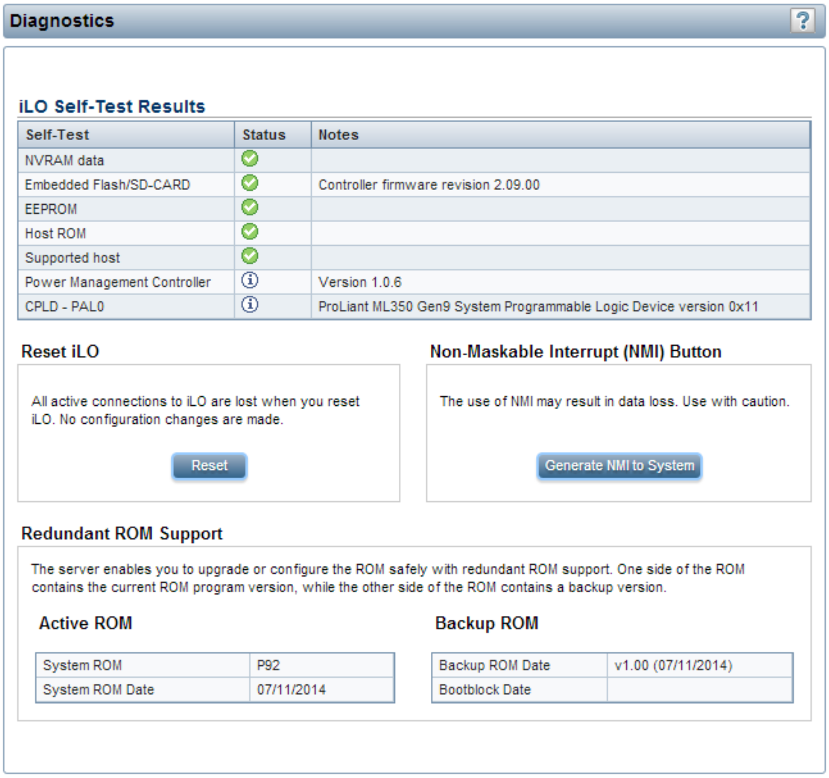
   Resetting iLO after clearing the Active Health System Log is required because some Active Health System data is recorded to the log only during iLO startup. Performing this step ensures that a complete set of data is available in the log.
6. Reboot the server.

   Rebooting the server after clearing the Active Health System Log is required because some information, such as the operating system name and version, is logged at server startup. Performing this step ensures that a complete set of data is available in the log.

Using iLO diagnostics

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

To view iLO diagnostics information, navigate to the **Information→Diagnostics** page.



Diagnostics

iLO Self-Test Results

Self-Test	Status	Notes
NVRAM data	✓	
Embedded Flash/SD-CARD	✓	Controller firmware revision 2.09.00
EEPROM	✓	
Host ROM	✓	
Supported host	✓	
Power Management Controller	ⓘ	Version 1.0.6
CPLD - PAL0	ⓘ	ProLiant ML350 Gen9 System Programmable Logic Device version 0x11

Reset iLO

All active connections to iLO are lost when you reset iLO. No configuration changes are made.

Non-Maskable Interrupt (NMI) Button

The use of NMI may result in data loss. Use with caution.

Redundant ROM Support

The server enables you to upgrade or configure the ROM safely with redundant ROM support. One side of the ROM contains the current ROM program version, while the other side of the ROM contains a backup version.

Active ROM

System ROM	P92
System ROM Date	07/11/2014

Backup ROM

Backup ROM Date	v1.00 (07/11/2014)
Bootblock Date	

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 displays the versions of other system programmable logic, such as the System Board PAL or the Power Management Controller.
  - The following information is displayed in the **Embedded Flash/SD-CARD** test results:
    - Firmware revision
    - SD-CARD size
    - SD-CARD slot
    - SD-CARD write counter

      The write counter counts data in 512-byte blocks. If the write counter is at zero, no write counter text is displayed in the iLO web interface.

      Write counter information is displayed only when a recognized “Genuine HP” SD-Card is installed with a retail version of iLO.
- **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.

- **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 server.
  - 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.

  For HP ProLiant Gen8 servers only: Click the **Swap ROM** button to swap the active ROM and the backup ROM. The change will take effect after the next system reboot. This feature is not supported on HP ProLiant Gen9 servers.

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 "Rebooting (Resetting) iLO" (page 309).

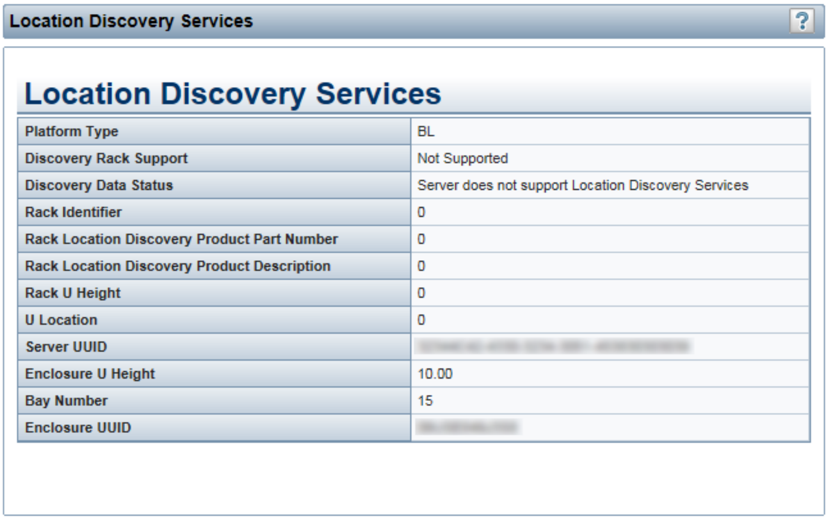
Using Location Discovery Services

Location Discovery Services is a component of HP Discovery Services. Location Discovery Services automatically reports server locations to HP SIM and Insight Control, eliminating this manual task for server administrators. Administrators can use the location information and system data with HP Asset Manager to obtain more precise and complete asset data.

Location Discovery Services is a rack U location discovery solution for G3 and later racks. It enables HP iLO, BL Onboard Administrator, and SL Chassis firmware to report and display the rack ID and the server U position in the rack. Supported racks are programmed with unique U values in 7U and/or 8U modules, and are installed with the tag version number, rack identifier, part number, product name, rack height, and U position. Location Discovery Services supports 14U, 22U, 36U, 42U, and 47U racks.

The rack device reads the rack U location tag each time iLO receives AC power or iLO is reset. The U position value denotes the U position read by the device. The contact position offset is a fixed value for each model that indicates the position of the contact relative to the bottom U position of the device. It is normally 0, but can be a positive value if the contact cannot be placed at the bottom U position of the device. The bottom-most U position occupied by the device is calculated by subtracting the U offset from the U position.

To view Location Discovery Services information, navigate to the **Information**→**Location Discovery Services** page.



Location Discovery Services

Location Discovery Services

Platform Type	BL
Discovery Rack Support	Not Supported
Discovery Data Status	Server does not support Location Discovery Services
Rack Identifier	0
Rack Location Discovery Product Part Number	0
Rack Location Discovery Product Description	0
Rack U Height	0
U Location	0
Server UUID	[redacted]
Enclosure U Height	10.00
Bay Number	15
Enclosure UUID	[redacted]

The **Location Discovery Services** page lists the following information:

- **Platform Type**—The server type.
- **Discovery Rack Support**—Whether the rack supports Location Discovery Services.
- **Discovery Data Status**—Whether there was an error during discovery.
- **Rack Identifier**—The rack identifier. If data is not available, the value **0** is displayed.
- **Rack Location Discovery Product Part Number**—The rack part number. If data is not available, the value **0** is displayed.
- **Rack Location Discovery Product Description**—The rack product name. If data is not available, the value **0** is displayed.
- **Rack U Height**—The rack height, in U rack units. Possible values are between 0 and 50. If data is not available, the value **0** is displayed.
- **U Location**—The side of the rack where the device is installed. Possible values are **Back**, **Front** (default), **Left**, and **Right**. If data is not available, the value **0** is displayed.
- **Server UUID—**The universally unique identifier of the server.

Additional information is listed, depending on the server type.

DL and ML server-specific data:

- **Server U Height**—The server height, in U rack units. Possible values are between 1.00 and 50.00.
- **Server Rack U Position**—The rack U position that aligns with the base of the server. Possible values are between 1 and 50.

Blade enclosures and BL server-specific data:

- **Bay Number**—The server bay in the enclosure.
- **Enclosure UUID**—The enclosure universally unique identifier.
- **Enclosure U Height**—The enclosure height, in U rack units. Possible values are between 1.00 and 50.00.
- **Enclosure Rack U Position**—The rack U position that aligns with the base of the enclosure. Possible values are between 1 and 50.

SL server-specific data:

- **Bay Number**—The server bay in the enclosure.
- **SL Chassis UUID**—The SL chassis universally unique identifier.

- **Chassis U Height**—The chassis height, in U rack units. Possible values are between 1.00 and 50.00.
- **Chassis Rack U Position**—The rack U position that aligns with the base of the SL chassis. Possible values are between 1 and 50.

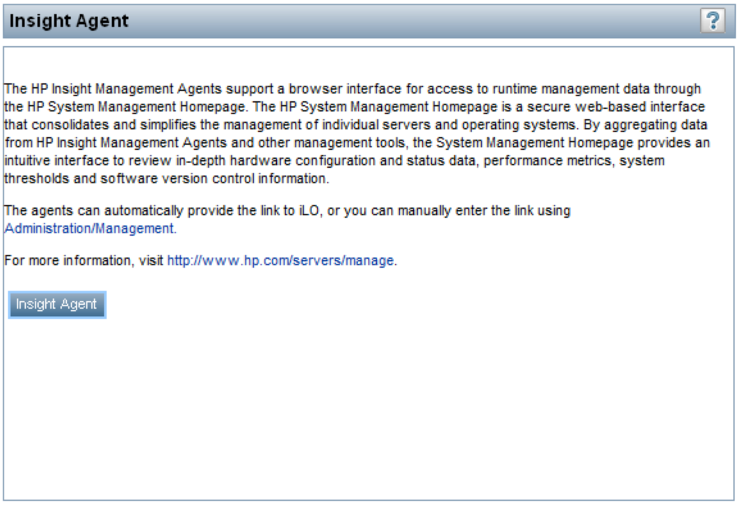
Using the HP Insight Management Agents

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.



The HP Insight Management Agents support a browser interface for access to runtime 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 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 using Administration/Management.

For more information, visit http://www.hp.com/servers/manage.

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

Using iLO Federation

iLO Federation enables you to manage multiple servers from one system running the iLO web interface.

HP iLO 4 firmware version 1.40 and later supports the following features:

- Group health status
- Group Virtual Media
- Group power control
- Automatic Group Power Capping
- Group firmware update

HP iLO 4 firmware version 2.00 and later supports the following features:

- Group license installation
- Group configuration

ⓘ **IMPORTANT:** iLO systems in the same iLO Federation group must use the same version of the iLO 4 firmware.

Any user can view information on iLO Federation pages, but some features require a license. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.

Configuring iLO Federation

You can use the iLO web interface or RIBCL scripts to configure iLO Federation.

- To configure iLO Federation with the iLO web interface, see "Configuring iLO Federation" (page 52).
- To configure iLO Federation with RIBCL scripts, see the *HP iLO 4 Scripting and Command Line Guide*.

Using the Selected Group list

When you select a group from the **Selected Group** list on an iLO Federation page:

- The servers that will be affected by a change on the **Group Virtual Media**, **Group Power**, **Group Firmware Update**, **Group Licensing**, and **Group Configuration** pages are listed in the **Affected Systems** table.
- The information displayed on iLO Federation pages applies to all of the servers in the selected group.
- The changes you make on iLO Federation pages apply to all of the servers in the selected group.
- The selected group is saved in a cookie and remains persistent, even when you log out of iLO.

After you select a group, you can filter the servers in the list in order to view server information or perform actions on a subset of the servers in the group.

Filtering the Selected Group list

When you filter the list of servers:

- The information displayed on iLO Federation pages applies to all of the servers in the selected group that meet the filter criteria.
- The changes you make on iLO Federation pages apply to all of the servers in the selected group that meet the filter criteria.
- The filter settings are saved in a cookie and remain persistent, even when you log out of iLO.

You can use the following criteria to filter the servers in a group:

- **Health status**—Click a health status link to select servers with a specific health status.
- **Model**—Click a server model number link to select servers matching the selected model.
- **Server name**—Click a server name to filter by an individual server.
- **Firmware Information**—Click a firmware version or flash status to select servers matching the selected firmware version or status.

- **Option ROM Measuring**—Click an Option ROM Measuring value to select servers based on their TPM status.

  If you have one or more servers with a TPM, use this filter to exclude servers with Option ROM Measuring enabled.

△ **CAUTION:** If you attempt to perform a system ROM or option ROM update on a server with Option ROM Measuring enabled, iLO prompts you to cancel the update, verify that you have a recovery key, and suspend BitLocker before the update. Failure to follow these instructions might result in losing access to your data.

- **License usage**—If an error message related to a license is displayed, click the license key to select servers that use that license key.
- **License Information**—Click a license type or status to select servers matching the selected license type or status.

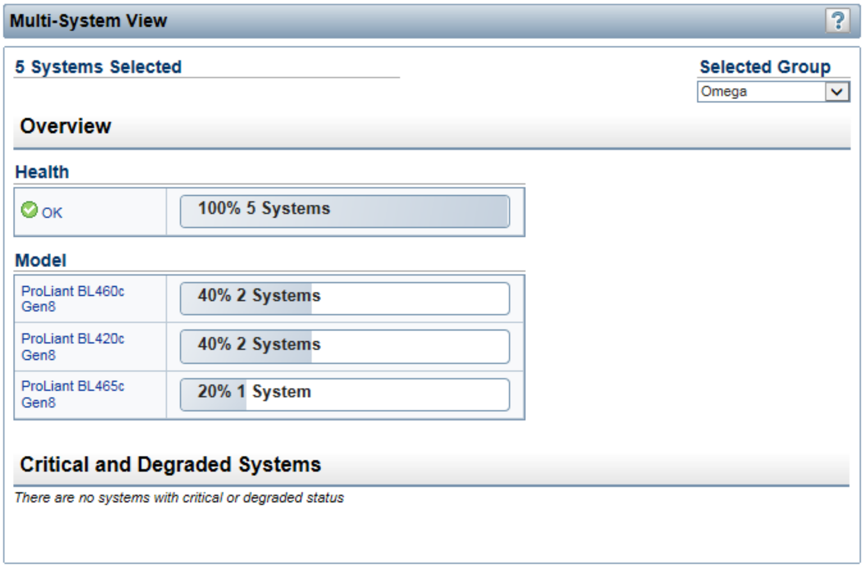
Using the iLO Federation multi-system view

The **Multi-System View** page provides a summary of the server models, server health, and critical and degraded systems in an iLO Federation group.

Viewing server health and model information

To view summary information for a group of servers:

1. Navigate to the **iLO Federation**→**Multi-System View** page.



Multi-System View

5 Systems Selected

Selected Group: Omega

Overview

Health

OK	100% 5 Systems

Model

ProLiant BL460c Gen8	40% 2 Systems
ProLiant BL420c Gen8	40% 2 Systems
ProLiant BL465c Gen8	20% 1 System

Critical and Degraded Systems

There are no systems with critical or degraded status

2. Select a group from the **Selected Group** menu.

3. Optional: To filter the list of servers, click a health status, server model, or server name link.

   The following information is displayed for the servers in the selected group that meet the filter criteria (if filters are used):

   - **Health**—The number of servers in each listed health status. The percentage of the total number of servers in each listed health status is also displayed.

     For a list of the possible health status values, see "Viewing health summary information" (page 151).
   - **Model**—The list of servers, grouped by model number. The percentage of the total number of servers for each model number is also displayed.
   - **Critical and Degraded Systems**—The list of servers in the critical or degraded state. For more information, see "Viewing critical and degraded servers" (page 187).

Viewing critical and degraded servers

To view details about the servers in a group that are in the critical or degraded state:

1. Navigate to the **iLO Federation→Multi-System View** page.
2. Select a group from the **Selected Group** menu.
3. Optional: To filter the list of servers, click a health status, server model, or server name link.

   The following information is displayed for the critical and degraded servers in the selected group that meet the filter criteria (if filters are used):

   - **Server Name**—The server name defined by the host operating system.
   - **System Health**—The server health status.
   - **Server Power**—The server power status (**ON** or **OFF**).
   - **UID Indicator**—The state of the server UID LED. The UID LED helps you identify and locate a server, especially in high-density rack environments. The possible states are **UID ON**, **UID OFF**, and **UID BLINK**.
   - **System ROM**—The installed HP ProLiant System ROM.
   - **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. Click the link in the **iLO Hostname** column to open the iLO web interface for the server.
   - **IP Address**—The network IP address of the iLO subsystem. Click the link in the **IP Address** column to open the iLO web interface for the server.
4. Click **Next** or **Previous** to view more servers in the list.

Viewing the iLO Federation Multi-System Map

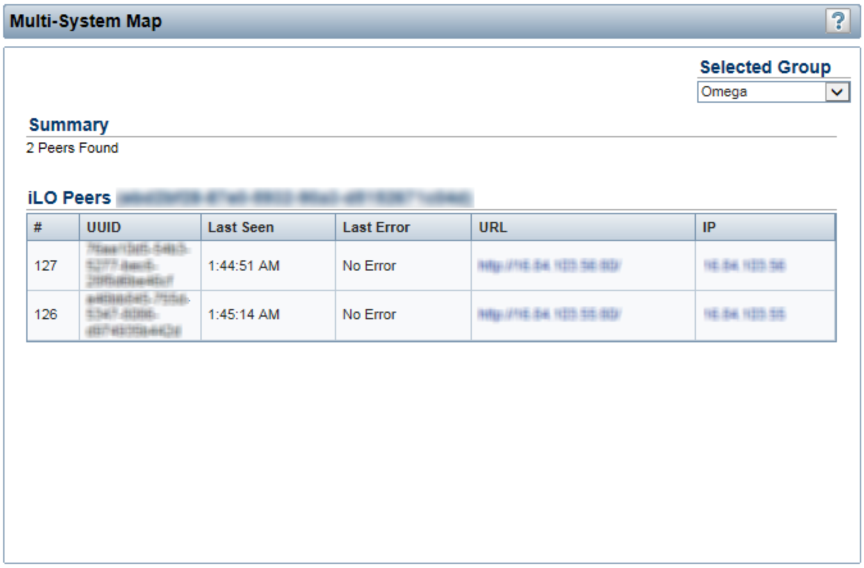
The **Multi-System Map** page displays information about the peers of the local iLO system. The local iLO system identifies its peers through multicast discovery.

When data is loaded on an iLO Federation page, a request for data is sent from the iLO system running the web interface to the iLO system's peers, and from those peers to other peers until all of the data for the selected iLO Federation group is retrieved.

For more information about multicast discovery and peer-to-peer communication, see "Configuring iLO Federation" (page 52).

To view the Multi-System Map:

1. Navigate to the **iLO Federation→Multi-System Map** page.



Multi-System Map

Selected Group: Omega

Summary

2 Peers Found

iLO Peers [redacted]

#	UUID	Last Seen	Last Error	URL	IP
127	[redacted]	1:44:51 AM	No Error	[redacted]	[redacted]
126	[redacted]	1:45:14 AM	No Error	[redacted]	[redacted]

2. Select a group from the **Selected Group** menu.

   The following information is displayed for each iLO peer:

   - **#**—The peer number.
   - **UUID**—The server UUID.
   - **Last Seen**—The time stamp of the last communication from the server.
   - **Last Error**—A description of the most recent communication error between the listed peer and the local iLO system.
   - **URL**—The URL for starting the iLO web interface for the listed peer.
   - **IP**—The peer IP address.

Using the iLO Federation Group Virtual Media feature

The Group Virtual Media feature enables you to connect scripted media for access by the servers in an iLO Federation group.

A license is required if you want to make changes on the **Group Virtual Media** page. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.

When you use Group Virtual Media, note the following:

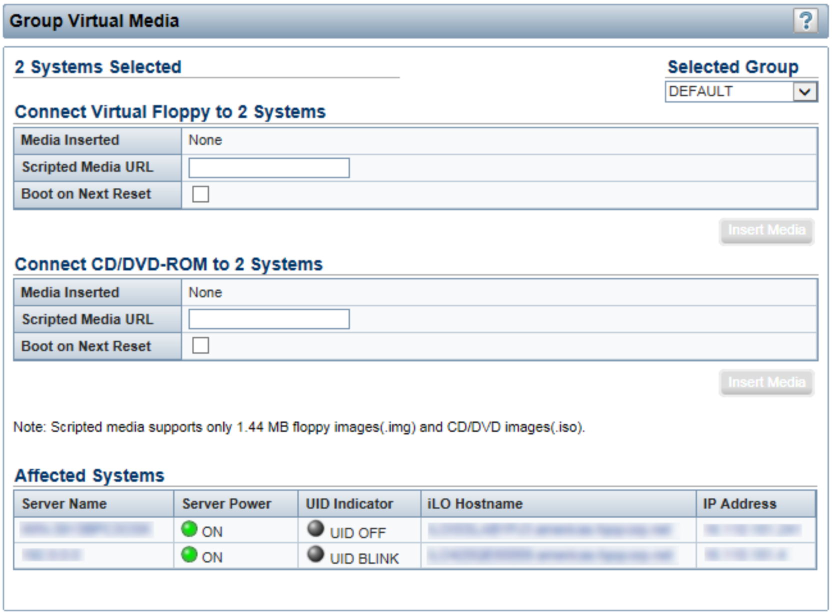
- You can connect scripted media to the iLO systems in an iLO Federation group. Scripted media only supports 1.44 MB floppy disk images (`.img`) and CD/DVD-ROM images (`.iso`). The image must be located on a web server on the same network as the iLO systems.
- If you want to use the Group Virtual Media feature with an iLO Federation group, ensure that each member of the group has granted the Virtual Media privilege to the group. For more information about privileges, see “Configuring iLO Federation” (page 52).
- Only one of each type of media can be connected to a group at the same time.
- You can view, connect, eject, or boot from scripted media. When you use scripted media, you save a floppy disk or CD/DVD-ROM disk image to a web server and connect to the disk image by using a URL. iLO accepts URLs in HTTP or HTTPS format. iLO does not support FTP.

NOTE: Using a floppy disk image to boot a remote host server is supported on Gen8 servers only. It is not supported on Gen9 servers.

- Before you use the iLO Virtual Media feature, review the operating system considerations in "Virtual Media operating system information" (page 225).

Connecting scripted media for groups

1. Navigate to the **iLO Federation→Group Virtual Media** page.



Group Virtual Media

2 Systems Selected

Selected Group: DEFAULT

Connect Virtual Floppy to 2 Systems

Media Inserted	None
Scripted Media URL	
Boot on Next Reset	□

Insert Media

Connect CD/DVD-ROM to 2 Systems

Media Inserted	None
Scripted Media URL	
Boot on Next Reset	□

Insert Media

Note: Scripted media supports only 1.44 MB floppy images(.img) and CD/DVD images(.iso).

Affected Systems

Server Name	Server Power	UID Indicator	iLO Hostname	IP Address
[redacted]	● ON	● UID OFF	[redacted]	[redacted]
[redacted]	● ON	● UID BLINK	[redacted]	[redacted]

2. Select a group from the **Selected Group** menu.

   All of the systems in the selected group will be affected by the changes you make on this page.

3. Enter the URL for the scripted media in the **Scripted Media URL** box in the **Connect Virtual Floppy** section (`.img` files) or **Connect CD/DVD-ROM** section (`.iso` files).

4. Select the **Boot on Next Reset** check box if the servers in the group 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 servers do not boot to this image twice.

   If this check box is not selected, the image will remain connected until it is ejected manually, and the servers will boot to it on all subsequent server resets, if the system boot options are configured accordingly.

   NOTE: Using a floppy disk image to boot a remote host server is supported on Gen8 servers only. It is not supported on Gen9 servers.

5. Click **Insert Media**.

Viewing and ejecting scripted media for groups

When scripted media is connected to the systems in an iLO Federation group, the following details are listed in the **Virtual Floppy Status** section and **Virtual CD/DVD-ROM Status** section:

- **Media 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.

NOTE: The **Virtual Floppy Status** and **Virtual CD/DVD-ROM Status** sections are displayed only when media is connected.

To eject scripted media devices:

1. Navigate to the **iLO Federation→Group Virtual Media** page.
2. Select a group from the **Selected Group** menu.

   All of the systems in the selected group will be affected by the changes you make on this page.
3. Click the **Eject Media** button in the **Virtual Floppy Status** section or **Virtual CD/DVD-ROM Status** section.

Viewing servers affected by a Group Virtual Media action

The **Affected Systems** section provides the following details about the servers that will be affected by changes you make on the **Group Virtual Media** page:

- **Server Name**—The server name defined by the host operating system.
- **Server Power**—The server power state (**ON** or **OFF**).
- **UID Indicator**—The state of the UID LED. The UID LED helps you identify and locate a server, especially in high-density rack environments. The possible states are **UID ON**, **UID OFF**, and **UID BLINK**.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. Click the link in the **iLO Hostname** column to open the iLO web interface for the server.
- **IP Address**—The network IP address of the iLO subsystem. Click the link in the **IP Address** column to open the iLO web interface for the server.

Using the iLO Federation Group Power feature

The Group Power feature enables you to manage the power of multiple servers from a system running the iLO web interface. Use this feature to do the following:

- Power off, reset, or power-cycle a group of servers that are in the **ON** or **Reset** state. For more information, see “Changing the power state for a group of servers” (page 191).
- Power on a group of servers that are in the **OFF** state. For more information, see “Changing the power state for a group of servers” (page 191).
- View the list of servers that will be affected when you click a button in the **Virtual Power Button** section of the **Group Power** page. For more information, see “Viewing servers affected by the Virtual Power Button” (page 192).

A license is required if you want to make changes on the **Group Power** page. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.

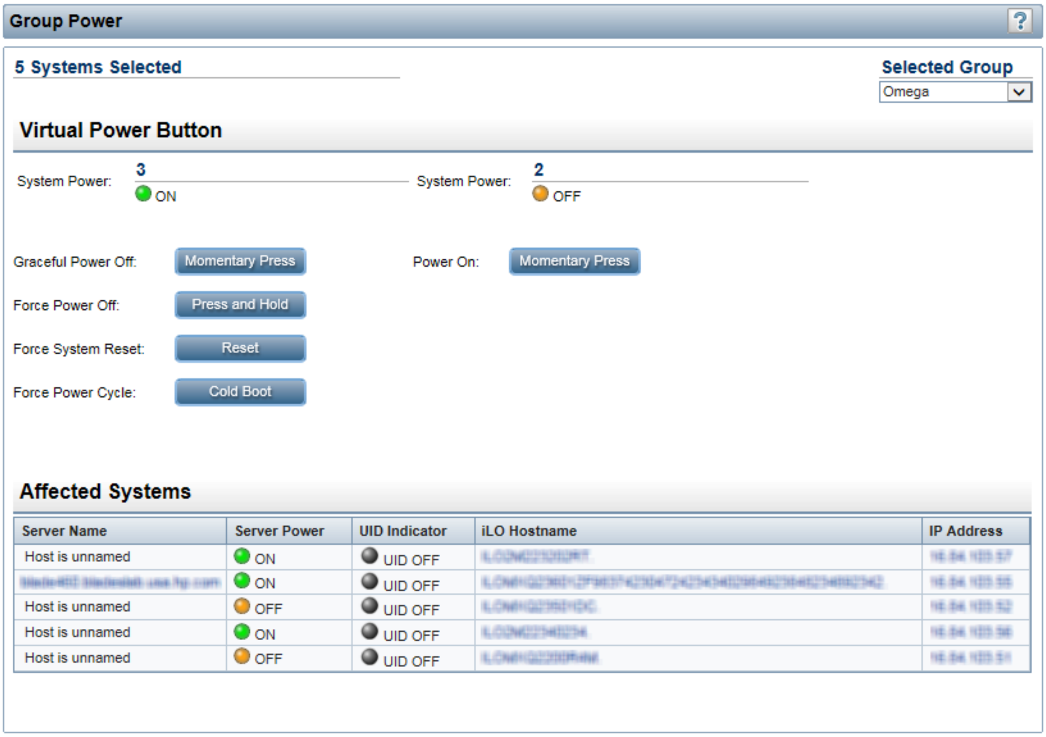
If you want to use the Group Power feature with an iLO Federation group, ensure that each member of the group has granted the Virtual Power and Reset privilege to the group. For more information about privileges, see “Configuring iLO Federation” (page 52).

Changing the power state for a group of servers

The **Virtual Power Button** section on the **Group Power** page displays a summary of the current power state of the grouped servers, including the total number of servers that are in the **ON**, **OFF**, or **Reset** state. The **System Power** summary indicates the state of the server power when the page is first opened. Use the browser refresh feature to update the **System Power** information.

To change the power state for a group of servers:

1. Navigate to the **iLO Federation**→**Group Power** page.


Group Power
?
Graceful Power Off: Momentary Press
Force Power Off: Press and Hold
Force System Reset: Reset
Force Power Cycle: Cold Boot
Power On: Momentary Press

5 Systems Selected

Selected Group: Omega

Virtual Power Button

System Power: 3 ● ON

System Power: 2 ● OFF

Affected Systems

Server Name	Server Power	UID Indicator	iLO Hostname	IP Address
Host is unnamed	● ON	● UID OFF	[redacted]	[redacted]
[redacted]	● ON	● UID OFF	[redacted]	[redacted]
Host is unnamed	● OFF	● UID OFF	[redacted]	[redacted]
Host is unnamed	● ON	● UID OFF	[redacted]	[redacted]
Host is unnamed	● OFF	● UID OFF	[redacted]	[redacted]

2. Select a group from the **Selected Group** menu.

   The grouped servers are listed by power state with a counter that shows the total number of servers in each state.

   All of the servers in the selected group will be affected by the changes you make on this page.

3. Do one of the following:

   - To change the power state for servers that are in the **ON** or **Reset** state, click one of the following buttons on the left side of the page:

     - **Momentary Press**—The same as pressing the physical power button.

       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 servers in the selected group are powered off as a result of this operation. Using this option might circumvent a graceful operating system shutdown.

       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 servers in the selected group to warm-boot: CPUs and I/O resources are reset. Using this option circumvents a graceful operating system shutdown.
    - **Cold Boot**—Immediately removes power from the servers in the selected group. Processors, memory, and I/O resources lose main power. The servers will restart after approximately 6 seconds. Using this option circumvents a graceful operating system shutdown.
  - To change the power state for servers that are in the **OFF** state, click the **Momentary Press** button on the right side of the page.

  NOTE: The **Press and Hold**, **Reset**, and **Cold Boot** options are not available for servers that are in the **OFF** state.

  A confirmation dialog box opens.

4. Click **OK** to continue.

   iLO displays a progress bar while the grouped servers respond to the Virtual Power Button push. The progress bar indicates the number of servers that successfully processed the command.

   The **Command Results** section displays the command status and results, including error messages related to the power state change.

Viewing servers affected by the Virtual Power Button

The **Affected Systems** table provides the following details about the servers that will be affected by the Virtual Power Button action:

- **Server Name**—The server name defined by the host operating system.
- **Server Power**—The server power state (**ON** or **OFF**).
- **UID Indicator**—The state of the UID LED. The UID LED helps you identify and locate a server, especially in high-density rack environments. The possible states are **UID ON**, **UID OFF**, and **UID BLINK**.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. Click the link in the **iLO Hostname** column to open the iLO web interface for the server.
- **IP Address**—The network IP address of the iLO subsystem. Click the link in the **IP Address** column to open the iLO web interface for the server.

Click **Next** or **Previous** to view more servers in the list.

Configuring iLO Federation group power settings

The Group Power Settings feature enables you to set dynamic power caps for the grouped servers.

When using the Automatic Group Power Capping feature, note the following:

- When a group power cap is set, the grouped servers share power in order to stay below the power cap. More power is allocated to busy servers and less power is allocated to servers that are idle.
- The power caps that you set for a group operate concurrently with the power caps that you can set on the **Power Settings** page for an individual server.
- When a power cap is set, the average power reading of the grouped servers must be at or below the power cap value.
- If you want to configure power capping settings for an iLO Federation group, ensure that each member of the group has granted the Configure iLO Settings privilege to the group. For more information about privileges, see “Configuring iLO Federation” (page 52).

- When a group power cap is set, you might see an unexpected session (with the IP address 127.0.0.1) in the **Active Sessions** list on the **iLO Overview** page and in the iLO Event Log. This temporary session is created by the Automatic Group Power Capping feature when it obtains the data that is required to maintain the power cap. You can ignore this session. It will be removed from the **Active Sessions** list within a minute.
- A license is required if you want to make changes on the **Group Power Settings** page. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.
- You cannot use the iLO web interface to configure group power capping settings for SL servers. Use one of the following tools to configure the power capping settings for SL servers:
  - **HP ProLiant Power Interface Control Utility**—This utility is available at the following website: http://www.hp.com/go/hpsc.
  - **HP ProLiant SL Advanced Power Manager**—For more information, see the *HP ProLiant SL Advanced Power Manager User Guide*.

The **HP Automatic Group 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 total power supply capacity for all servers in a group.
  - **Peak Observed Power**—The maximum observed power for all servers in a group.
  - **Minimum Observed Power**—The minimum observed power for all servers in a group.

  During POST, the ROM runs two power tests that determine the peak and minimum observed power values.
- Use the **Power Cap Thresholds** as guidelines for configuring the power cap value.
  - **Maximum Power Cap**—The maximum power available for the servers in a group. The servers in a group must not exceed this value.
  - **Minimum High-Performance Cap**—The maximum power that the servers in a group use in their current configuration. A power cap set to this value does not affect server performance.
  - **Minimum Power Cap**—The minimum power that the servers in a group use. A power cap set to this value reduces the server power usage to the minimum, which results in server performance degradation.
- The **Power Cap Value** section allows you to configure the power capping settings. For instructions, see "Configuring Automatic Group Power Capping settings" (page 194).

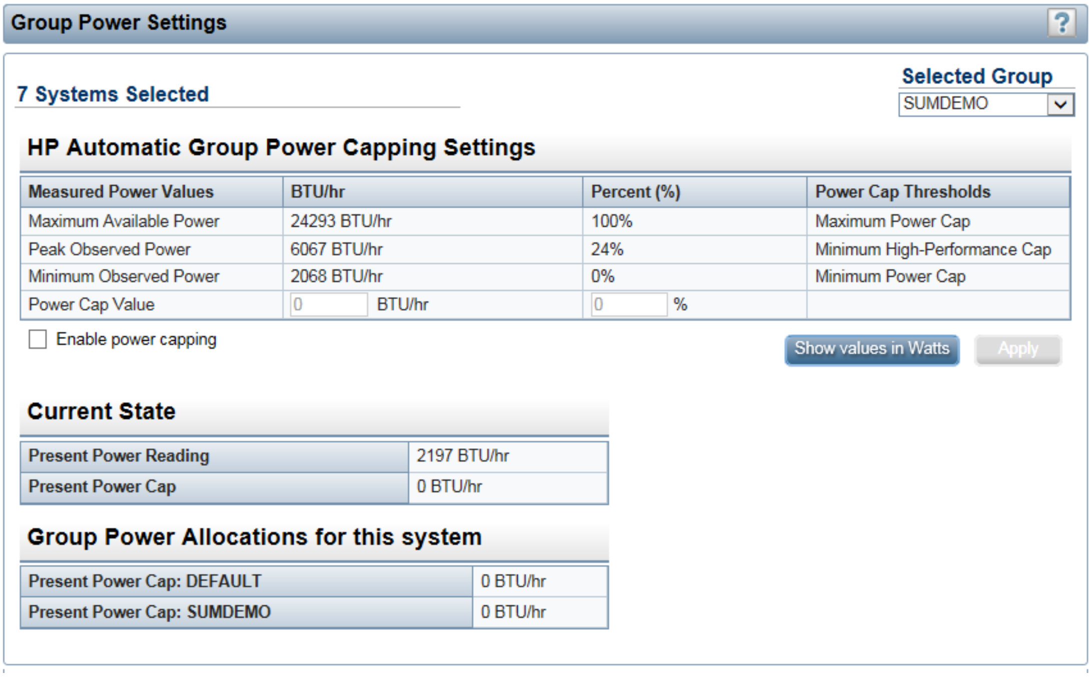
The **Current State** section shows the current power consumption for all servers in the selected iLO Federation group.

- **Present Power Reading**—The current power reading for all servers in a group.
- **Present Power Cap**—The current power cap value for all servers in a group. This value is 0 if a power cap is not configured.

The **Group Power Allocations for this system** section lists the group memberships of the local iLO system, and the power cap values configured by each listed group.

Configuring Automatic Group Power Capping settings

1. Navigate to the **iLO Federation→Group Power Settings** page.



Group Power Settings

7 Systems Selected

Selected Group: SUMDEMO

HP Automatic Group Power Capping Settings

Measured Power Values	BTU/hr	Percent (%)	Power Cap Thresholds
Maximum Available Power	24293 BTU/hr	100%	Maximum Power Cap
Peak Observed Power	6067 BTU/hr	24%	Minimum High-Performance Cap
Minimum Observed Power	2068 BTU/hr	0%	Minimum Power Cap
Power Cap Value	0 BTU/hr	0 %	

□ Enable power capping

Current State

Present Power Reading	2197 BTU/hr
Present Power Cap	0 BTU/hr

Group Power Allocations for this system

Present Power Cap: DEFAULT	0 BTU/hr
Present Power Cap: SUMDEMO	0 BTU/hr

2. Select a group from the **Selected Group** menu.

   All of the systems in the selected group will be affected by the changes you make on this page.
3. Select the **Enable power capping** check box.
4. 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.
5. Click **Apply**.

Using the iLO Federation Group Firmware Update feature

The Group Firmware Update feature enables you to update the firmware of multiple servers from a system running the iLO web interface.

A license is required if you want to make changes on the **Group Firmware Update** page. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.

This feature allows you to do the following:

- View the number of servers with each supported firmware version. The percentage of the total number of servers with the listed firmware version is also displayed.
- View the flash status for the grouped servers. The percentage of the total number of servers with the listed flash status is also displayed.
- View the TPM status for the grouped servers in the **Option ROM Measuring** section. The percentage of the total number of servers with the listed TPM status is also displayed.

- Update the firmware. The following firmware types are supported:
    - iLO firmware
    - HP ProLiant System ROM (BIOS)
    - SL Chassis Firmware (Power Management)
    - Power Management Controller
    - System Programmable Logic Device (CPLD)
- View the list of servers that will be affected by a firmware update. For more information, see "Viewing servers affected by a Group Firmware Update" (page 198).

Obtaining the iLO firmware image file

The `.bin` file from the iLO Online ROM Flash Component is required for updating the iLO firmware on the **Group Firmware Update** page.

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

1. Navigate to the HP Support Center website: http://www.hp.com/go/hpsc.
2. In the **Enter a product name or number** box, enter the server model number, and then click **Go**.
3. The HP Support Center page for the server opens.
4. Click the **Drivers, Software & Firmware** link.

   A list of operating systems is displayed.
5. Click the link for the server operating system.
6. Follow the onscreen instructions to download the iLO Online ROM Flash Component file.
7. Double-click the downloaded file, and then click the **Extract** button.
8. Select a location for the extracted files, and then click **OK**.

   The name of the iLO firmware image file is similar to `ilo4_<yyy>.bin`, where `<yyy>` represents the firmware version.

   The URL to enter for the iLO firmware image file is similar to http://<server.example.com>/<subdir>/ilo4_150.bin.

Obtaining supported server firmware image files

To obtain the system ROM, Power Management Controller, and SL Chassis Manager firmware image files:

1. Navigate to the HP Support Center website: http://www.hp.com/go/hpsc.
2. In the **Enter a product name or number** box, enter the server model number, and then click **Go**.
3. The HP Support Center page for the server opens.
4. Click the **drivers, software & firmware** link.

   A list of operating systems is displayed.
5. Click the link for the server operating system.
6. Follow the onscreen instructions to download an Online ROM Flash Component file.
7. Double-click the downloaded file, and then click the **Extract** button.

8. Select a location for the extracted files, and then click **OK**.
    - When you update the system ROM, you must use a signed image or the signed ROMPAQ image:
        - **Signed image example**:

          http://<server.example.com:8080>/<wwwroot>/P79_1.00_10_25_2013.signed.flash
        - **Signed ROMPAQ image example**:

          http://<server.example.com>/<wwwroot>/CPQPJ0612.A48
    - The Power Management Controller and SL Chassis Manager firmware files use the file extension `.hex`. For example, the file name might be similar to `ABCD5S95.hex`.
    - The System Programmable Logic Device (CPLD) firmware file uses the file extension `.vme`.

Updating the firmware for multiple servers

To update the firmware of servers in an iLO Federation group:

1. Download the supported firmware from the HP Support Center website: http://www.hp.com/go/hpsc.

   For more information about obtaining supported firmware files, see "Obtaining the iLO firmware image file" (page 195) and "Obtaining supported server firmware image files" (page 195).
2. Save the firmware file to a web server.
3. Navigate to the **iLO Federation→Group Firmware Update** page.
4. Select a group from the **Selected Group** menu.

   All of the systems in the selected group will be affected by the changes you make on this page.
5. Optional: Click a firmware version, flash status, or Option ROM Measuring status link to filter the list of affected systems.

6. In the **Firmware Update** section, enter the URL to the firmware file on your web server, and then click the **Update Firmware** button.

   Each selected system downloads the firmware image and attempts to flash it.

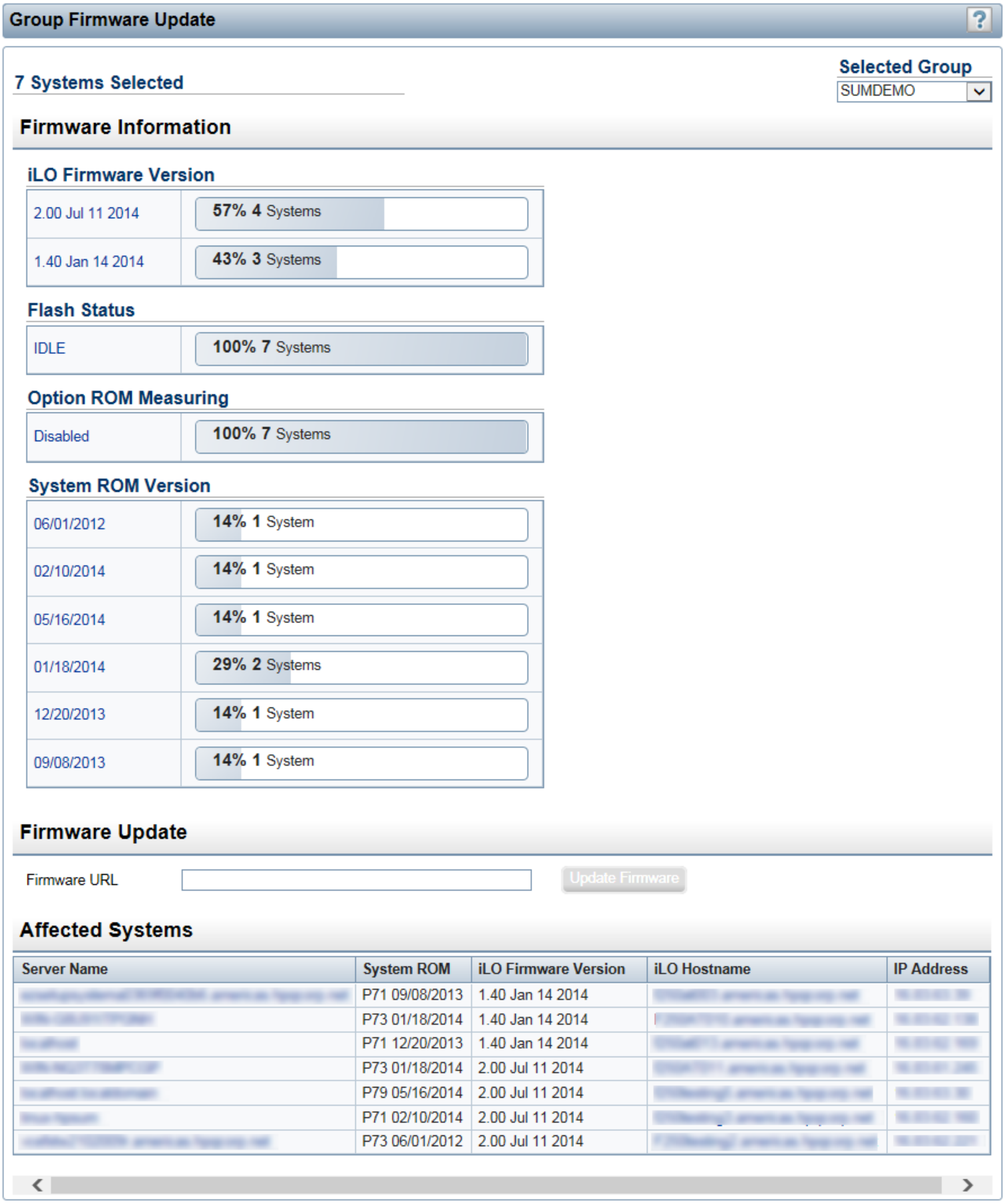
   The **Flash Status** section is updated and a message similar to the following appears:

   ```
   Flashing Firmware Image, please wait...
   ```

   This message and the **% Complete** value apply to all of the affected systems.

   When the update is complete, the **Firmware Information** section is updated.

   If a firmware image is not valid for a system or has a bad/missing signature, iLO rejects the image and the **Flash Status** section shows an error for the affected system.



Group Firmware Update

7 Systems Selected

Selected Group: SUMDEMO

Firmware Information

iLO Firmware Version

2.00 Jul 11 2014	57% 4 Systems
1.40 Jan 14 2014	43% 3 Systems

Flash Status

IDLE	100% 7 Systems

Option ROM Measuring

Disabled	100% 7 Systems

System ROM Version

06/01/2012	14% 1 System
02/10/2014	14% 1 System
05/16/2014	14% 1 System
01/18/2014	29% 2 Systems
12/20/2013	14% 1 System
09/08/2013	14% 1 System

Firmware Update

Firmware URL:

Affected Systems

Server Name	System ROM	iLO Firmware Version	iLO Hostname	IP Address
[redacted]	P71 09/08/2013	1.40 Jan 14 2014	[redacted]	[redacted]
[redacted]	P73 01/18/2014	1.40 Jan 14 2014	[redacted]	[redacted]
[redacted]	P71 12/20/2013	1.40 Jan 14 2014	[redacted]	[redacted]
[redacted]	P73 01/18/2014	2.00 Jul 11 2014	[redacted]	[redacted]
[redacted]	P79 05/16/2014	2.00 Jul 11 2014	[redacted]	[redacted]
[redacted]	P71 02/10/2014	2.00 Jul 11 2014	[redacted]	[redacted]
[redacted]	P73 06/01/2012	2.00 Jul 11 2014	[redacted]	[redacted]

   Some firmware update types might require an iLO reset, a system reset, or a server reboot for the new firmware to take effect.

Viewing servers affected by a Group Firmware Update

The **Affected Systems** table provides the following details about the servers that will be affected by a firmware update:

- **Server Name**—The server name defined by the host operating system.
- **System ROM**—The installed HP ProLiant System ROM.
- **iLO Firmware Version**—The installed iLO firmware version.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. Click the link in the **iLO Hostname** column to open the iLO web interface for the server.
- **IP Address**—The network IP address of the iLO subsystem. Click the link in the **IP Address** column to open the iLO web interface for the server.

Using iLO Federation group licensing

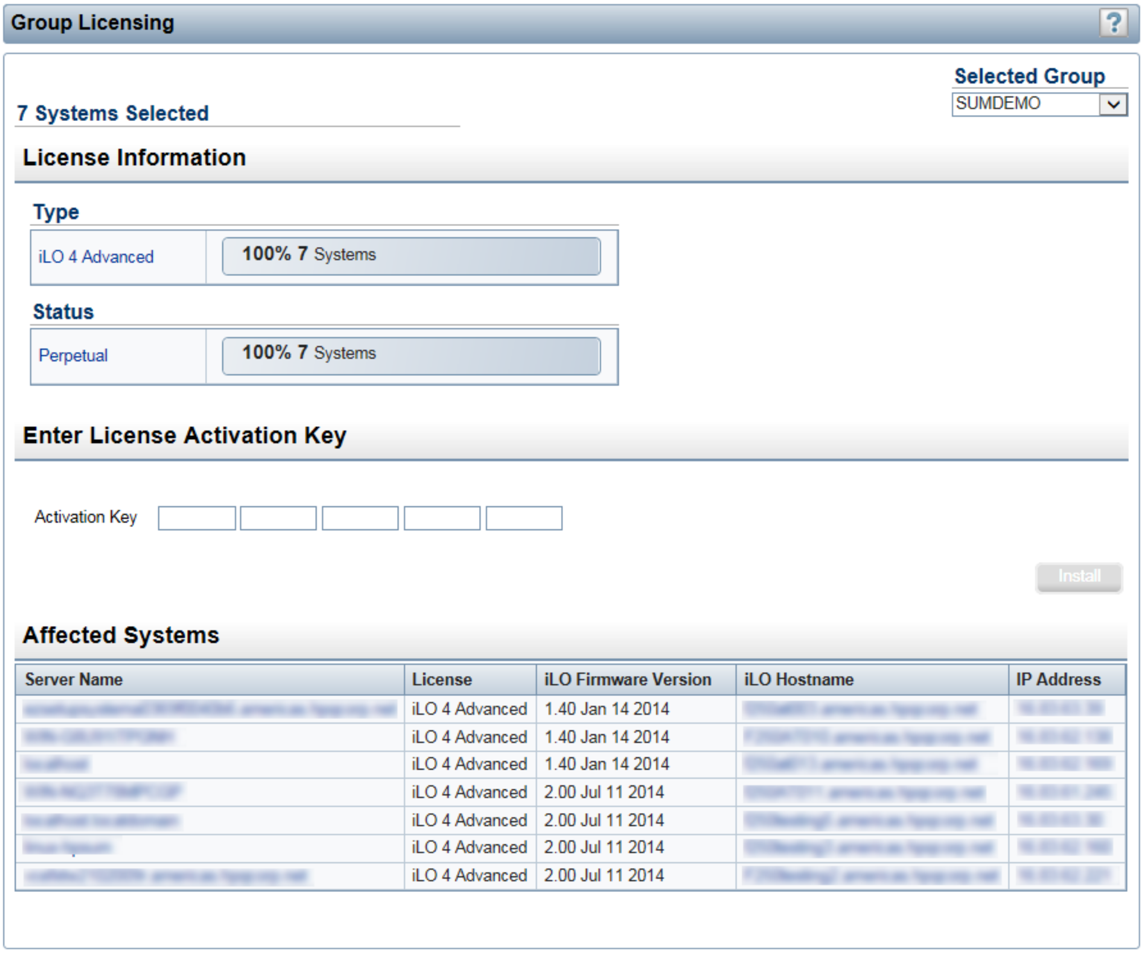
The **Group Licensing** page displays the license status for members of a selected iLO Federation group. Use this page to enter an optional key to activate iLO licensed features.

For an overview of iLO licensing, see "iLO licensing" (page 44).

Viewing license information

To view license information for a group of servers:

1. Navigate to the **iLO Federation**→**Group Licensing** page.



Selected Group: SUMDEMO

7 Systems Selected

License Information

Type

iLO 4 Advanced	100% 7 Systems

Status

Perpetual	100% 7 Systems

Enter License Activation Key

Activation Key

Affected Systems

Server Name	License	iLO Firmware Version	iLO Hostname	IP Address
[redacted]	iLO 4 Advanced	1.40 Jan 14 2014	[redacted]	[redacted]
[redacted]	iLO 4 Advanced	1.40 Jan 14 2014	[redacted]	[redacted]
[redacted]	iLO 4 Advanced	1.40 Jan 14 2014	[redacted]	[redacted]
[redacted]	iLO 4 Advanced	2.00 Jul 11 2014	[redacted]	[redacted]
[redacted]	iLO 4 Advanced	2.00 Jul 11 2014	[redacted]	[redacted]
[redacted]	iLO 4 Advanced	2.00 Jul 11 2014	[redacted]	[redacted]
[redacted]	iLO 4 Advanced	2.00 Jul 11 2014	[redacted]	[redacted]

2. Select a group from the **Selected Group** menu.

3. Optional: To filter the list of servers, click a license type or status link in the **License Information** section.

   The following information is displayed for the servers in the selected group that meet the filter criteria (if filters are used):

   - **Type**—The number of servers with each listed license type. The percentage of the total number of servers with each listed license type is also displayed.

     For more information about iLO license types, see the following website: http://www.hp.com/go/ilo/licensing.

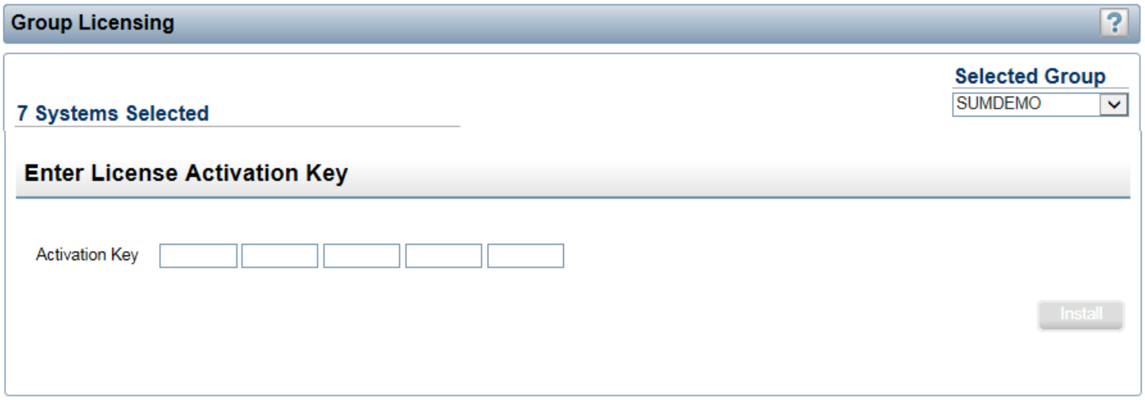
   - **Status**—The number of servers with each listed license status. The percentage of the total number of servers with each license status is also displayed. The possible status values follow:

     - **Evaluation**—A valid evaluation license is installed.
     - **Expired**—An expired evaluation license is installed.
     - **Perpetual**—A valid iLO Advanced, iLO Advanced for BladeSystem, iLO Essentials, or iLO Scale-Out license is installed. This license does not have an expiration date.
     - **Unlicensed**—The factory default license is installed (iLO Standard or iLO Standard for BladeSystem).

Installing license keys

To install a license key on the servers in an iLO Federation group:

1. Navigate to the **iLO Federation**→**Group Licensing** page in the iLO web interface.
2. Review the license agreement provided with your HP License Pack option kit.
3. Optional: Click a license type or status link to filter the list of affected systems.
4. Enter the license key in the **Activation Key** box.



Group Licensing

7 Systems Selected

Selected Group: SUMDEMO

Enter License Activation Key

Activation Key

   Press the **Tab** key or click inside a segment of the **Activation Key** box to move between segments. The cursor advances automatically when you enter data into the segments of the **Activation Key** box.

5. Click **Install**.

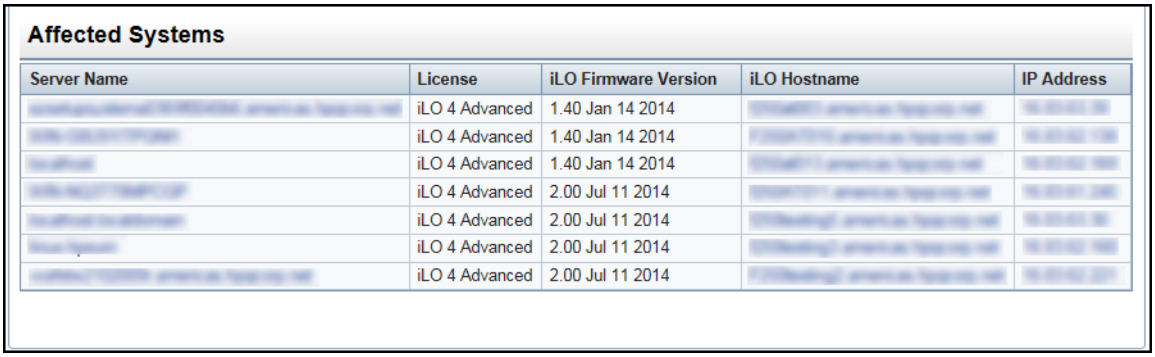
   The EULA confirmation dialog box opens. The EULA details are available in the HP License Pack option kit.

6. Click **OK**.

   The **License Information** section is updated to show the new license details for the selected group.

Viewing servers affected by a license installation

The **Affected Systems** section provides the following details about the servers that will be affected when you install a license key.



Affected Systems

Server Name	License	iLO Firmware Version	iLO Hostname	IP Address
[redacted]	iLO 4 Advanced	1.40 Jan 14 2014	[redacted]	[redacted]
[redacted]	iLO 4 Advanced	1.40 Jan 14 2014	[redacted]	[redacted]
[redacted]	iLO 4 Advanced	1.40 Jan 14 2014	[redacted]	[redacted]
[redacted]	iLO 4 Advanced	2.00 Jul 11 2014	[redacted]	[redacted]
[redacted]	iLO 4 Advanced	2.00 Jul 11 2014	[redacted]	[redacted]
[redacted]	iLO 4 Advanced	2.00 Jul 11 2014	[redacted]	[redacted]
[redacted]	iLO 4 Advanced	2.00 Jul 11 2014	[redacted]	[redacted]

The following information is displayed:

- **Server Name**—The server name defined by the host operating system.
- **License**—The installed license type.
- **iLO Firmware Version**—The installed iLO firmware version.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. Click the link in the **iLO Hostname** column to open the iLO web interface for the server.
- **IP Address**—The network IP address of the iLO subsystem. Click the link in the **IP Address** column to open the iLO web interface for the server.

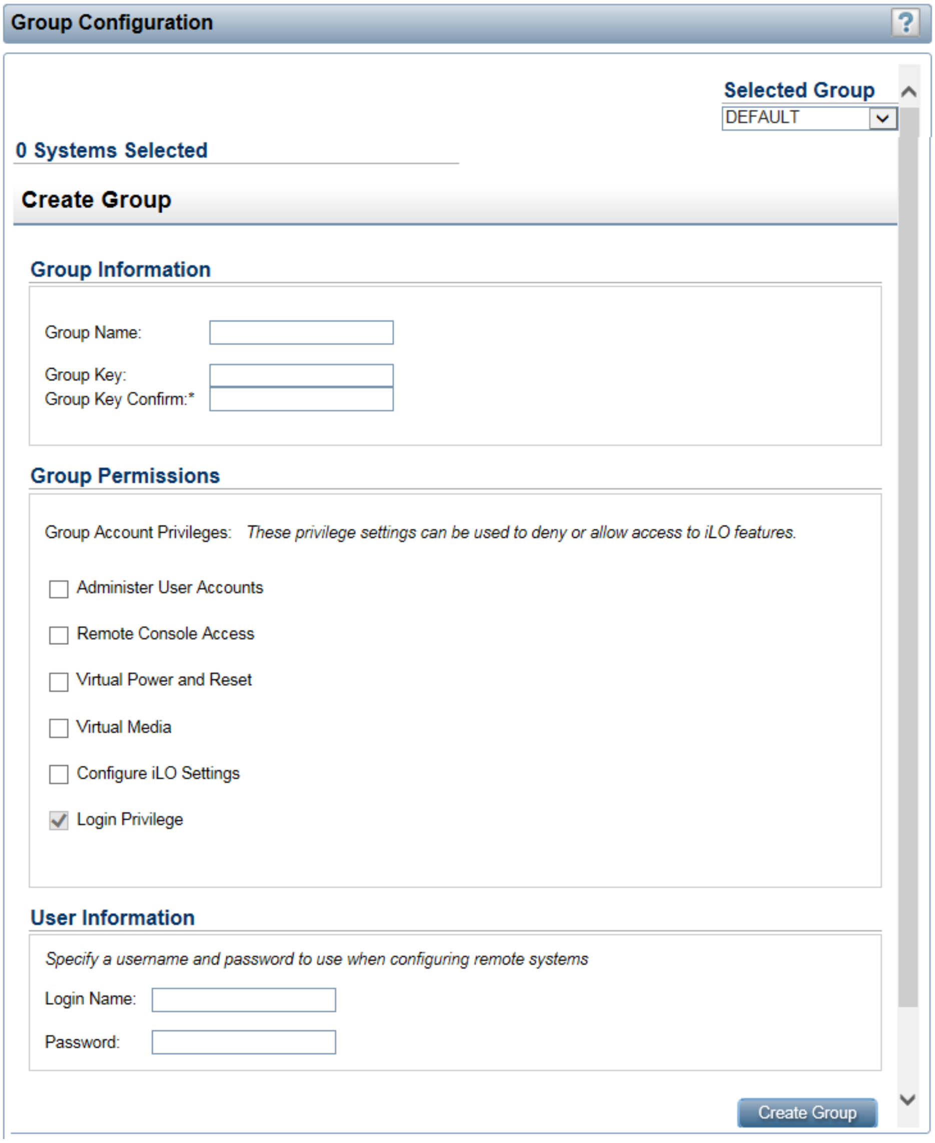
Configuring group memberships for an iLO Federation group

You can configure group memberships for the local iLO system, or you can configure them for the members of a selected iLO Federation group. This topic describes the procedure for working with iLO Federation groups. For information about managing groups for an individual iLO system, see "Managing iLO Federation group memberships for the local iLO system" (page 55).

For more information about iLO Federation groups, see "Understanding iLO Federation groups" (page 54).

To configure group memberships for an iLO Federation group:

1. Navigate to the **iLO Federation→Group Configuration** page.



Group Configuration

Selected Group: DEFAULT

0 Systems Selected

Create Group

Group Information

Group Name:

Group Key:

Group Key Confirm:*

Group Permissions

Group Account Privileges: *These privilege settings can be used to deny or allow access to iLO features.*

□ Administer User Accounts

□ Remote Console Access

□ Virtual Power and Reset

□ Virtual Media

□ Configure iLO Settings

☑ Login Privilege

User Information

Specify a username and password to use when configuring remote systems

Login Name:

Password:

2. Select a group from the **Selected Group** menu.

   All of the systems in the selected group will be affected by the changes you make on this page.

3. Enter the following information:
   - **Group Name**—The group name, which can be 1 to 31 characters long.
   - **Group Key**—The group password, which can be 3 to 39 characters long.
   - **Group Key Confirm**—Confirm the group password.

4. Select from the following permissions:
   - **Administer User Accounts**
   - **Remote Console Access**
   - **Virtual Power and Reset**
   - **Virtual Media**
   - **Configure iLO Settings**
   - **Login Privilege**

The permissions granted to the group by each group member control the tasks that users of other iLO systems in the group can perform on them.

For a description of these permissions, see "Viewing iLO Federation group memberships" (page 54).

5. Optional: Enter the **Login Name** and **Password** for a user account on the remote system(s) you want to manage.

   This is required if the local iLO system does not have permission to configure groups for a remote system.

TIP: If you need to enter credentials for multiple remote systems, create a user account with the same login name and password on each system.

6. Click **Create Group** to save the configuration.

Viewing servers affected by a group membership change

The **Affected Systems** section provides the following details about the servers that will be affected by a group membership change:

- **Server Name**—The server name defined by the host operating system.
- **Server Power**—The server power state (**ON** or **OFF**).
- **UID Indicator**—The state of the UID LED. The UID LED helps you identify and locate a server, especially in high-density rack environments. The possible states are **UID ON**, **UID OFF**, and **UID BLINK**.
- **iLO Hostname**—The fully qualified network name assigned to the iLO subsystem. Click the link in the **iLO Hostname** column to open the iLO web interface for the server.
- **IP Address**—The network IP address of the iLO subsystem. Click the link in the **IP Address** column to open the iLO web interface for the server.

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 146).

.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 89).

- Mozilla Firefox requires an add-on to launch .NET applications. 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 .NET applications.

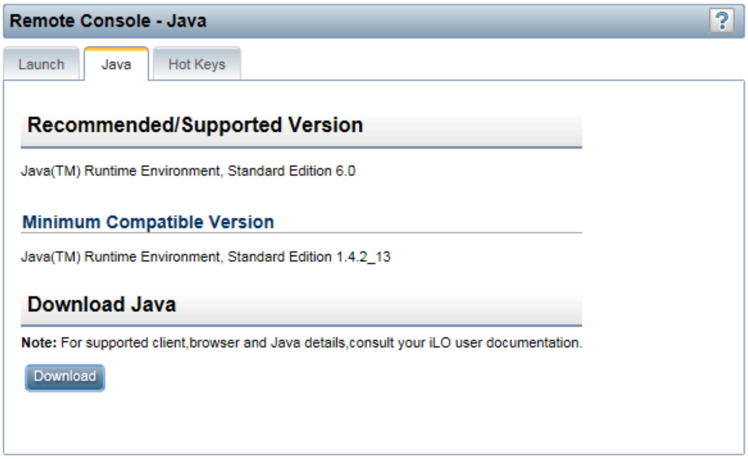
  As a workaround, use one of the following:

  - The .NET IRC with a different browser.
  - The standalone .NET IRC.
  - The Java IRC.
  - The iLO mobile app.

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.



Recommended/Supported Version

Java(TM) Runtime Environment, Standard Edition 6.0

Minimum Compatible Version

Java(TM) Runtime Environment, Standard Edition 1.4.2_13

Download Java

Note: For supported client,browser and Java details,consult your iLO user documentation.

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.

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.

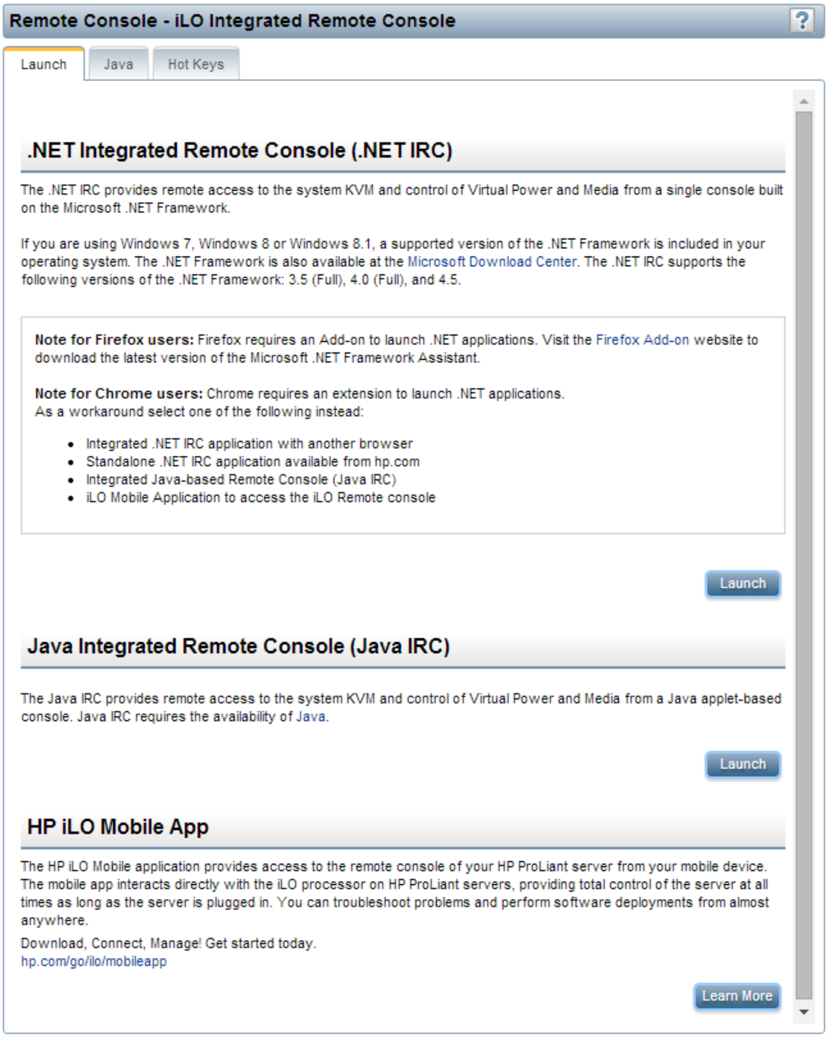
When you use the Remote Console, note the following:

- 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.

     For instructions, see "Using iLO diagnostics" (page 180).
  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 a browser.
- The Java IRC is a Java applet-based console that is launched from the iLO web interface. When you refresh or close the iLO web interface window, the Remote Console connection is closed, and you will lose access to Virtual Media devices that were connected through the Java IRC, except for devices that were connected by URL (using scripted media).
- 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 finish using the Remote Console, close the window or click the **Close** button to exit the .NET IRC or Java IRC.

To start the Remote Console:

1. Navigate to the **Remote Console→Remote Console** page.



Remote Console - iLO Integrated Remote Console

.NET Integrated Remote Console (.NET IRC)

The .NET IRC provides remote access to the system KVM and control of Virtual Power and Media from a single console built on the Microsoft .NET Framework.

If you are using Windows 7, Windows 8 or Windows 8.1, a supported version of the .NET Framework is included in your operating system. The .NET Framework is also available at the Microsoft Download Center. The .NET IRC supports the following versions of the .NET Framework: 3.5 (Full), 4.0 (Full), and 4.5.

Note for Firefox users: Firefox requires an Add-on to launch .NET applications. Visit the Firefox Add-on website to download the latest version of the Microsoft .NET Framework Assistant.

Note for Chrome users: Chrome requires an extension to launch .NET applications. As a workaround select one of the following instead:

- Integrated .NET IRC application with another browser
- Standalone .NET IRC application available from hp.com
- Integrated Java-based Remote Console (Java IRC)
- iLO Mobile Application to access the iLO Remote console

Java Integrated Remote Console (Java IRC)

The Java IRC provides remote access to the system KVM and control of Virtual Power and Media from a Java applet-based console. Java IRC requires the availability of Java.

HP iLO Mobile App

The HP iLO Mobile application 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. You can troubleshoot problems and perform software deployments from almost anywhere.

Download, Connect, Manage! Get started today.
hp.com/go/ilo/mobileapp

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.

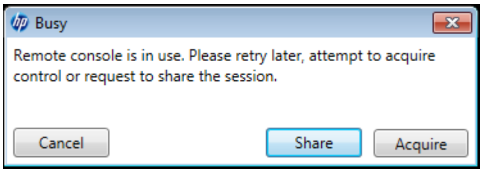
   If you attempt to open the Remote Console while it is in use, a warning message indicates that another user is using it. To view the Remote Console session that is in progress, follow the instructions in "Using Shared Remote Console (.NET IRC only)" (page 207). To take control of the session, follow the instructions in "Acquiring the Remote Console" (page 206).

Acquiring the Remote Console

If another user is working in the Remote Console, you can acquire it from that user.

1. Navigate to the **Remote Console→Remote Console** page.
2. Click the **Launch** button for the Remote Console that you want to use.

   The system notifies you that another user is working in the Remote Console.

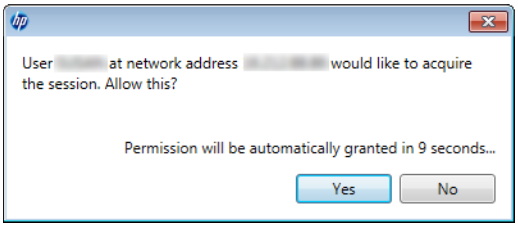


Busy

Remote console is in use. Please retry later, attempt to acquire control or request to share the session.

3. Click the **Acquire** button.

   The other user is prompted to approve or deny permission to acquire the Remote Console.

   User [redacted] at network address [redacted] would like to acquire the session. Allow this?

   Permission will be automatically granted in 9 seconds...

   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 Remote Console **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 off.

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 229).

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.

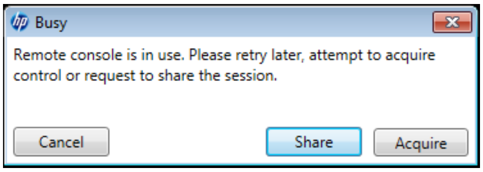
During a Shared Remote Console session, the session leader has access to all Remote Console features, whereas all other users can access only the keyboard and mouse. Satellite clients cannot control Virtual Power or Virtual Media.

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.

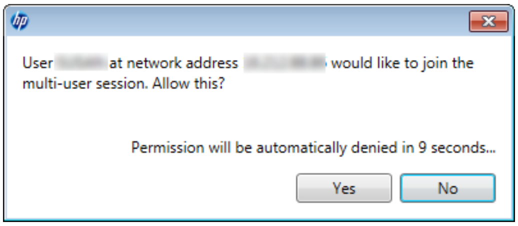
   

   Busy

   Remote console is in use. Please retry later, attempt to acquire control or request to share the session.

3. Click **Share**.

   The session leader receives your request to join the .NET IRC session.

   User [redacted] at network address [redacted] would like to join the multi-user session. Allow this?

   Permission will be automatically denied in 9 seconds...

   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.

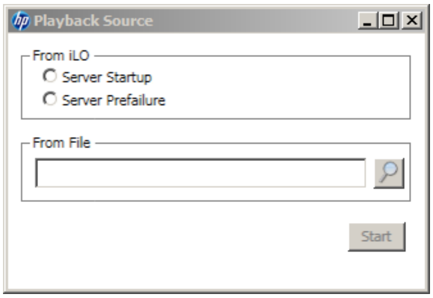
  The following playback controls are available:

  - ⏮ **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.

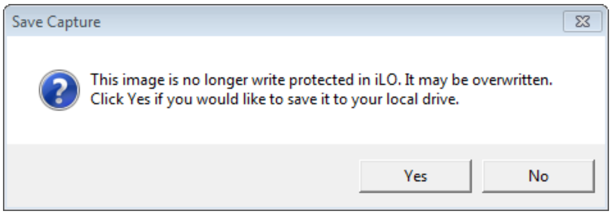


3. Select **Server Startup** or **Server Prefailure**.
4. Click **Start**.

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.



This image is no longer write protected in iLO. It may be overwritten.
Click Yes if you would like to save it to your local drive.

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.
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 the .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).

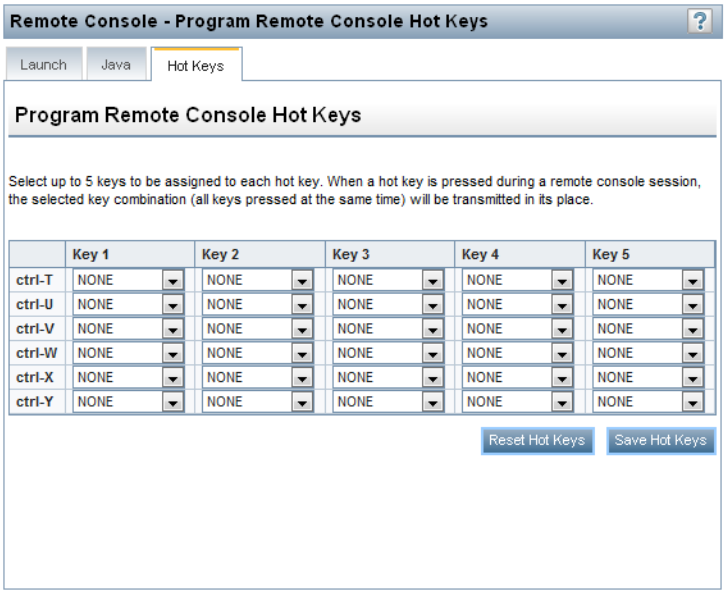
Example 1: If you want to send **Alt+F4** to the remote server, but pressing that key combination closes your browser, you can configure the hot key **Ctrl+X** to send the **Alt+F4** key combination to the remote server. After you configure the hot key, press **Ctrl+X** in the Remote Console window whenever you want to send **Alt+F4** to 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.



Remote Console - Program Remote Console Hot Keys

Program Remote Console Hot Keys

Select up to 5 keys to be assigned to each hot key. When a hot key is pressed during a remote console session, the selected key combination (all keys pressed at the same time) will be transmitted in its place.

	Key 1	Key 2	Key 3	Key 4	Key 5
ctrl-T	NONE	NONE	NONE	NONE	NONE
ctrl-U	NONE	NONE	NONE	NONE	NONE
ctrl-V	NONE	NONE	NONE	NONE	NONE
ctrl-W	NONE	NONE	NONE	NONE	NONE
ctrl-X	NONE	NONE	NONE	NONE	NONE
ctrl-Y	NONE	NONE	NONE	NONE	NONE

2. For each hot key that you want to create, 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 6 (page 211) lists the keys you can use when you configure hot keys.

Table 6 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
BACKSPACE	.	d	y

Table 6 Keys for configuring hot keys *(continued)*

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.
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 212)
- “Using the Text-based Remote Console (Textcons)” (page 222)

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**.

To start the UEFI System Utilities during a Virtual Serial Port session, enter the key combination **ESC+9**.

- 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 219).
- 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 220).

Configuring the iLO Virtual Serial Port in the host system RBSU

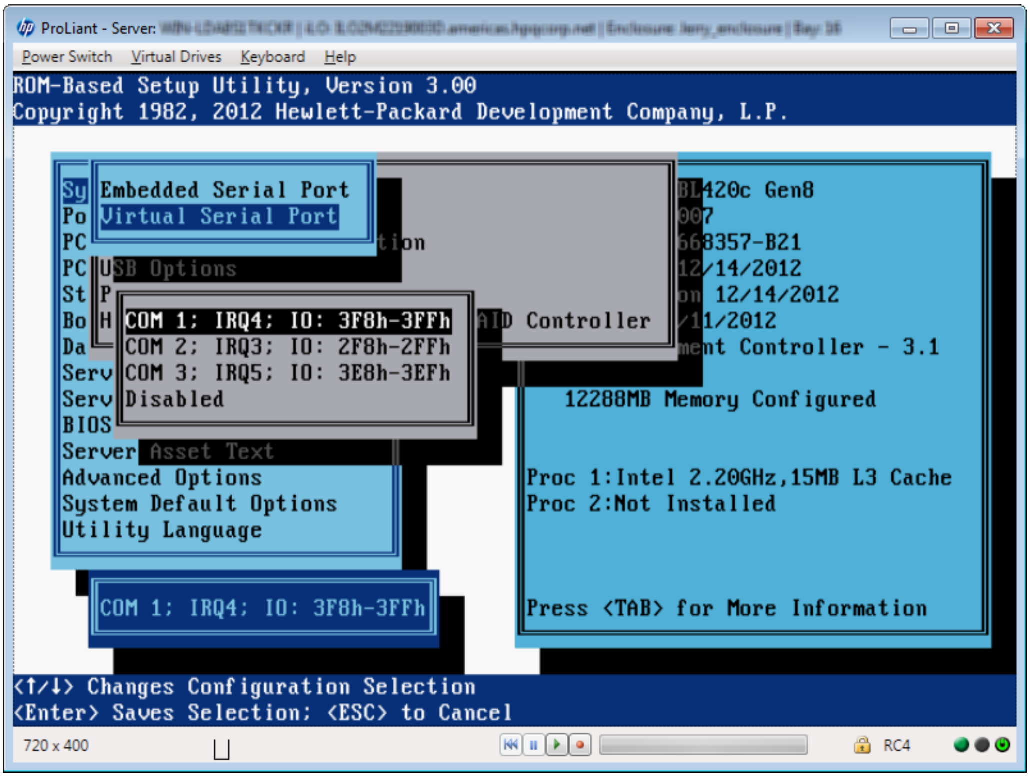
The following procedure describes the settings you must configure before you can use the iLO Virtual Serial Port. This procedure is required for both Windows and Linux systems.

This procedure is for systems that support the legacy system RBSU. For systems that support the UEFI System Utilities, see "Configuring the iLO Virtual Serial Port in the UEFI System Utilities" (page 216).

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**.

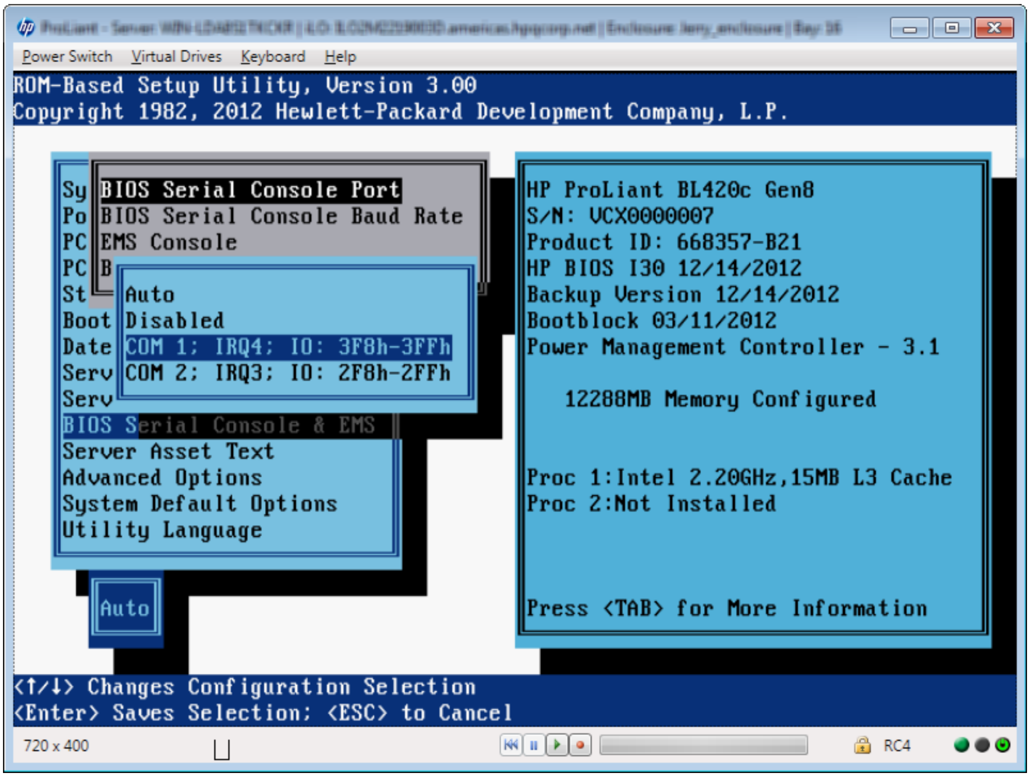


```
ROM-Based Setup Utility, Version 3.00
Copyright 1982, 2012 Hewlett-Packard Development Company, L.P.

Sy  Embedded Serial Port                     BL420c Gen8
Po  Virtual Serial Port                      007
PC                         tion              668357-B21
PC  USB Options                              12/14/2012
St  P                                        on  12/14/2012
Bo  H COM 1; IRQ4; IO: 3F8h-3FFh  AID Controller  /11/2012
Da    COM 2; IRQ3; IO: 2F8h-2FFh             ment Controller - 3.1
Serv  COM 3; IRQ5; IO: 3E8h-3EFh
Serv  Disabled                                  12288MB Memory Configured
BIOS
Server Asset Text
Advanced Options                             Proc 1:Intel 2.20GHz,15MB L3 Cache
System Default Options                       Proc 2:Not Installed
Utility Language

    COM 1; IRQ4; IO: 3F8h-3FFh               Press <TAB> for More Information

<↑/↓> Changes Configuration Selection
<Enter> Saves Selection; <ESC> to Cancel
```

8. Press **ESC** twice to return to the main menu.
9. Select **BIOS Serial Console & EMS**, and then press **Enter**.

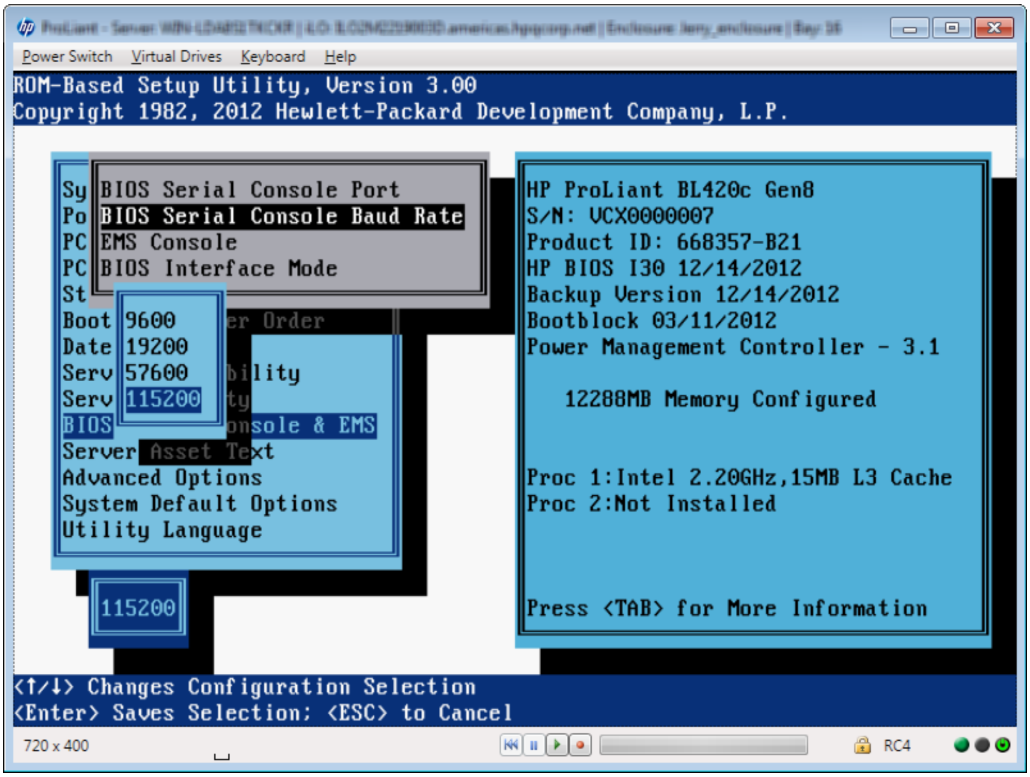
   NOTE: EMS is for Windows only.

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**.



```
ROM-Based Setup Utility, Version 3.00
Copyright 1982, 2012 Hewlett-Packard Development Company, L.P.

Sy   BIOS Serial Console Port                HP ProLiant BL420c Gen8
Po   BIOS Serial Console Baud Rate           S/N: VCX0000007
PC   EMS Console                             Product ID: 668357-B21
PC   B                                       HP BIOS I30 12/14/2012
St     Auto                                  Backup Version 12/14/2012
Boot   Disabled                              Bootblock 03/11/2012
Date   COM 1; IRQ4; IO: 3F8h-3FFh            Power Management Controller - 3.1
Serv   COM 2; IRQ3; IO: 2F8h-2FFh
Serv                                            12288MB Memory Configured
BIOS Serial Console & EMS
Server Asset Text
Advanced Options                             Proc 1:Intel 2.20GHz,15MB L3 Cache
System Default Options                       Proc 2:Not Installed
Utility Language

    Auto                                     Press <TAB> for More Information

<↑/↓> Changes Configuration Selection
<Enter> Saves Selection; <ESC> to Cancel
```

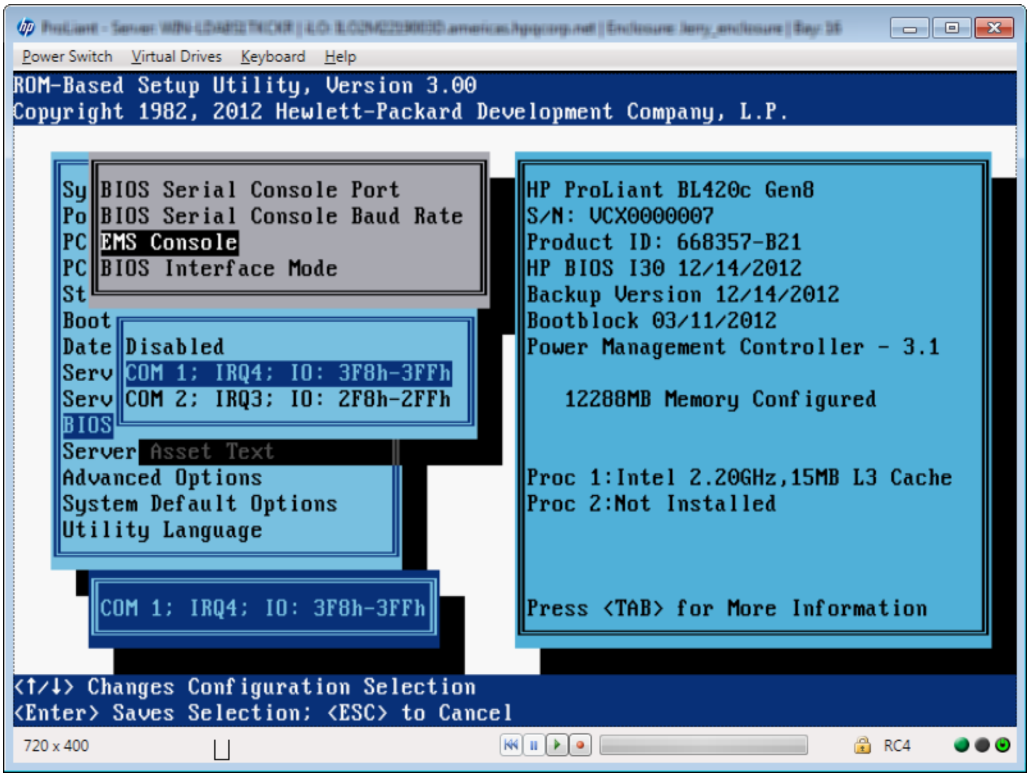
12. Select **BIOS Serial Console Baud Rate**, and then press **Enter**.
13. Select **115200**, and then press **Enter**.



```
ROM-Based Setup Utility, Version 3.00
Copyright 1982, 2012 Hewlett-Packard Development Company, L.P.

Sy BIOS Serial Console Port                 HP ProLiant BL420c Gen8
Po BIOS Serial Console Baud Rate            S/N: VCX0000007
PC EMS Console                              Product ID: 668357-B21
PC BIOS Interface Mode                      HP BIOS I30 12/14/2012
St                                          Backup Version 12/14/2012
Boot 9600    er Order                       Bootblock 03/11/2012
Date 19200                                  Power Management Controller - 3.1
Serv 57600   bility
Serv 115200  ty                                12288MB Memory Configured
BIOS         onsole & EMS
Server Asset Text
Advanced Options                            Proc 1:Intel 2.20GHz,15MB L3 Cache
System Default Options                      Proc 2:Not Installed
Utility Language

  115200                                    Press <TAB> for More Information

<↑/↓> Changes Configuration Selection
<Enter> Saves Selection; <ESC> to Cancel
```

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**.



```
ROM-Based Setup Utility, Version 3.00
Copyright 1982, 2012 Hewlett-Packard Development Company, L.P.

Sy BIOS Serial Console Port           HP ProLiant BL420c Gen8
Po BIOS Serial Console Baud Rate      S/N: VCX0000007
PC EMS Console                        Product ID: 668357-B21
PC BIOS Interface Mode                HP BIOS I30 12/14/2012
St                                    Backup Version 12/14/2012
Boot                                  Bootblock 03/11/2012
Date Disabled                         Power Management Controller - 3.1
Serv COM 1; IRQ4; IO: 3F8h-3FFh
Serv COM 2; IRQ3; IO: 2F8h-2FFh          12288MB Memory Configured
BIOS
Server Asset Text
Advanced Options                      Proc 1:Intel 2.20GHz,15MB L3 Cache
System Default Options                Proc 2:Not Installed
Utility Language

   COM 1; IRQ4; IO: 3F8h-3FFh         Press <TAB> for More Information

<↑/↓> Changes Configuration Selection
<Enter> Saves Selection; <ESC> to Cancel
```

16. Exit the system RBSU.

Configuring the iLO Virtual Serial Port in the UEFI System Utilities

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.

This procedure is for systems that support the UEFI System Utilities. For systems that support the legacy system RBSU, see "Configuring the iLO Virtual Serial Port in the host system RBSU" (page 213).

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

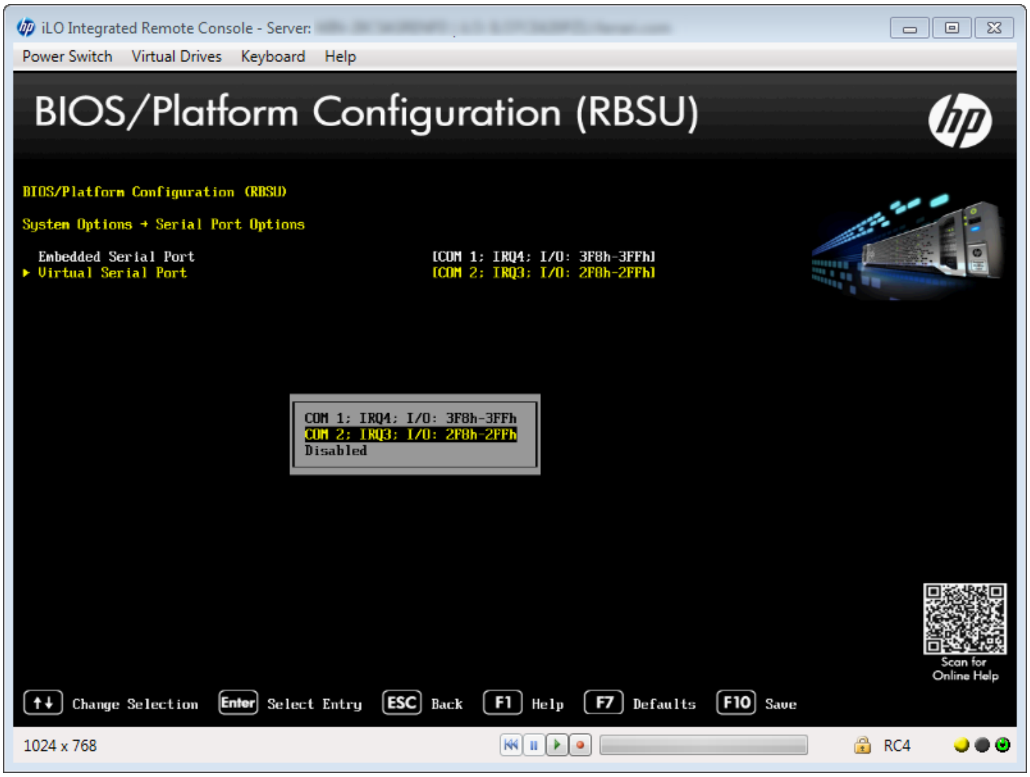
   You can use the .NET IRC or Java IRC.

2. Restart or power on the server.
3. Press **F9** in the HP ProLiant POST screen.

   The **System Configuration** screen appears.

4. Use the up or down arrow keys and the **Enter** key to navigate to the **ROM-Based Setup Utility (RBSU)**→**System Options**→**Serial Port Options** screen.
5. Select **Virtual Serial Port**, and then press **Enter**.

6. Select the COM port you want to use, and then press **Enter**.

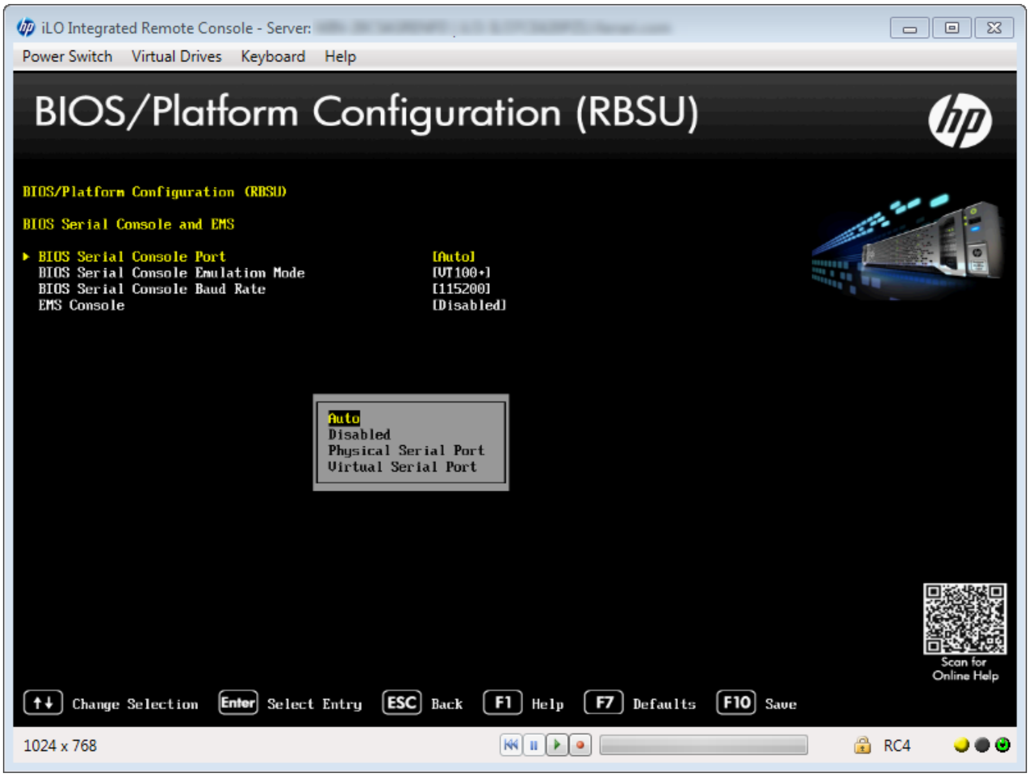

iLO Integrated Remote Console - Server: [redacted]
Power Switch
Virtual Drives
Keyboard
Help
BIOS/Platform Configuration (RBSU)
Scan for Online Help
1024 x 768
RC4

```
BIOS/Platform Configuration (RBSU)

System Options → Serial Port Options

  Embedded Serial Port                       [COM 1; IRQ4; I/O: 3F8h-3FFh]
▸ Virtual Serial Port                        [COM 2; IRQ3; I/O: 2F8h-2FFh]

                    COM 1; IRQ4; I/O: 3F8h-3FFh
                    COM 2; IRQ3; I/O: 2F8h-2FFh
                    Disabled

↑↓ Change Selection   Enter Select Entry   ESC Back   F1 Help   F7 Defaults   F10 Save
```

7. Press **ESC** twice to return to the main menu.
8. Select **BIOS Serial Console and EMS**, and then press **Enter**.

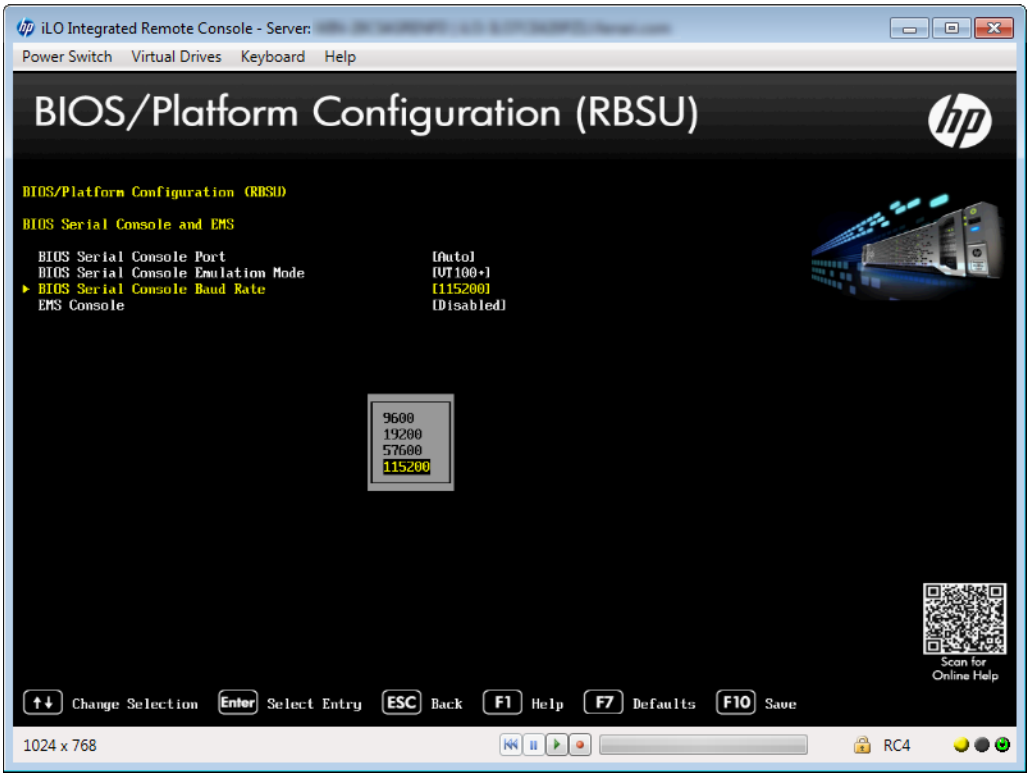
NOTE: EMS is for Windows only.

9. Select **BIOS Serial Console Port**, and then press **Enter**.
10. Select the COM port that matches the value selected in step 6, and then press **Enter**.



```
BIOS/Platform Configuration (RBSU)

BIOS Serial Console and EMS

▸ BIOS Serial Console Port                        [Auto]
  BIOS Serial Console Emulation Mode              [VT100+]
  BIOS Serial Console Baud Rate                   [115200]
  EMS Console                                     [Disabled]

                   Auto
                   Disabled
                   Physical Serial Port
                   Virtual Serial Port
```

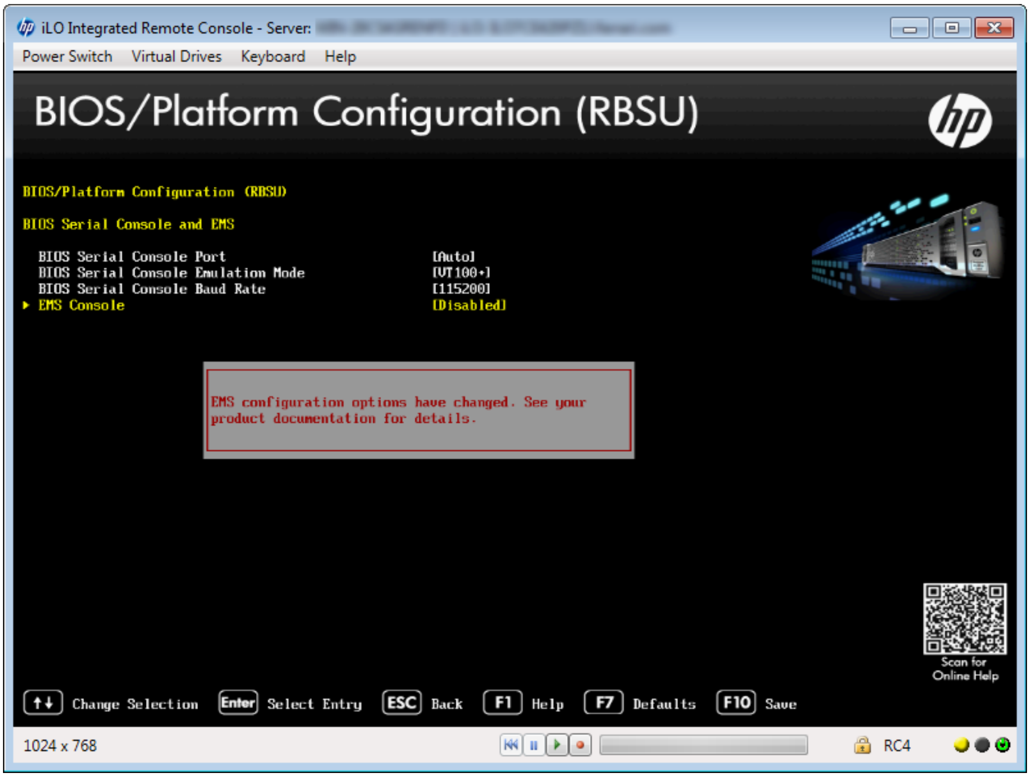
11. Press **ESC** to return to the main menu.
12. Select **BIOS Serial Console Baud Rate**, and then press **Enter**.
13. Select **115200**, and then press **Enter**.



```
BIOS/Platform Configuration (RBSU)

BIOS Serial Console and EMS

  BIOS Serial Console Port                        [Auto]
  BIOS Serial Console Emulation Mode              [VT100+]
▸ BIOS Serial Console Baud Rate                   [115200]
  EMS Console                                     [Disabled]

                        9600
                        19200
                        57600
                        115200
```

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. Press **ESC** to return to the main menu.
15. Select **EMS Console**, and then press **Enter**.
16. Select the COM port that matches the value selected in step 6, and then press **Enter**.



iLO Integrated Remote Console - Server: [redacted]

BIOS/Platform Configuration (RBSU)

```
BIOS/Platform Configuration (RBSU)

BIOS Serial Console and EMS

  BIOS Serial Console Port                    [Auto]
  BIOS Serial Console Emulation Mode          [VT100+]
  BIOS Serial Console Baud Rate               [115200]
▸ EMS Console                                 [Disabled]
```

```
EMS configuration options have changed. See your
product documentation for details.
```

17. Press **F10** to save the changes.

    The iLO 4 Configuration Utility prompts you to confirm that you want to save all pending configuration changes.

18. Press **Enter**.

    The iLO 4 Configuration Utility notifies you that iLO must be reset in order for the changes to take effect.

19. Press **Enter**.

    iLO resets, and the remote console session is automatically ended. You can reconnect in approximately 30 seconds.

20. Resume the normal boot process:
    a. Start the iLO remote console.

       The iLO 4 Configuration Utility is still open from the previous session.

    b. Press **ESC** several times to navigate to the **System Configuration** page.
    c. Press **ESC** to exit the System Utilities and resume the normal boot process.

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 or the UEFI System Utilities. 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 213) or "Configuring the iLO Virtual Serial Port in the UEFI System Utilities" (page 216).

- 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.

Starting an iLO Virtual Serial Port session

1. Verify that the iLO Virtual Serial Port settings are configured in the iLO RBSU or UEFI System Utilities.

   For more information, see "Configuring the iLO Virtual Serial Port in the host system RBSU" (page 213) or "Configuring the iLO Virtual Serial Port in the UEFI System Utilities" (page 216).

2. Verify that the Windows or Linux operating system is configured for use with the iLO Virtual Serial Port.

   For more information, see "Configuring the iLO Virtual Serial Port for the Windows EMS Console" (page 220) or "Configuring the iLO Virtual Serial Port for Linux" (page 219).

3. Start an SSH session.

   For example, you could enter **`ssh Administrator@<iLO IP address>`** or connect through port 22 with `putty.exe`.

4. When prompted, enter your iLO account credentials.
5. At the `</>hpiLO->` prompt, enter **`VSP`**,and press **Enter**.
6. For Windows systems only: At the `<SAC>` prompt, enter **`cmd`** to create a command prompt channel.
7. For Windows systems only: Enter **`ch - si <#>`** to switch to the channel specified by the channel number.
8. When prompted, enter the OS login credentials.

Viewing the iLO Virtual Serial Port log

If the iLO Virtual Serial Port log is enabled, you can view iLO Virtual Serial Port activity by using the `vsp log` command.

1. Verify that an iLO Advanced or iLO Scale-Out license is installed.
2. Enable **Secure Shell (SSH) Access** and **Virtual Serial Port Log** on the **Access Settings** page.

   For instructions, see "Configuring iLO access settings" (page 57).

3. Connect to the CLI through SSH.
4. Use the **`vsp`** command to view iLO Virtual Serial Port activity.
5. Enter **`ESC (`** to exit.
6. Enter **`vsp log`** to view the iLO Virtual Serial Port log.

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.

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 7 (page 223) lists the supported equivalents.

Table 7 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 device that 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 use Virtual Media, note the following:

- An iLO license key is required to use some forms of Virtual Media. For 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 virtual media can be connected at a time.

- The iLO Virtual Media feature supports ISO images of up to 8 TB. However, the maximum ISO image file size also depends on other factors such as the single file size limit for the file system where the ISO image is stored and the SCSI commands the server OS supports.
- In an operating system, an iLO Virtual Floppy/USB key or Virtual CD/DVD-ROM behaves like any other drive. When you use 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.

  NOTE: Using the iLO Virtual Floppy to boot a remote host server is supported only on Gen8 servers. It is not supported on Gen9 servers.

- 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 a 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 225).

- You can also access the Virtual Media feature by 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 try to 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**—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**—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 226).

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 this value 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.

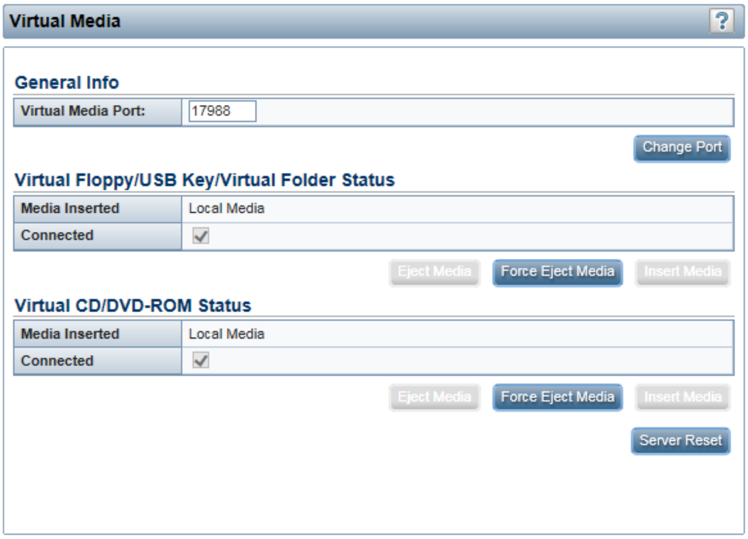
Viewing and modifying the Virtual Media port

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.



Virtual Media

General Info

Virtual Media Port:	17988

Virtual Floppy/USB Key/Virtual Folder Status

Media Inserted	Local Media
Connected	☑

Virtual CD/DVD-ROM Status

Media Inserted	Local Media
Connected	☑

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**
  - **Media 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**
  - **Media 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** or **Virtual CD/DVD-ROM Status** section.

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. The **Virtual Media** page supports the connection of 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.
2. Enter the URL for the scripted media in the **Scripted Media URL** box in the **Connect Virtual Floppy** (`.img` files) or **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.

   NOTE: Using the iLO Virtual Floppy to boot a remote host server is supported only on Gen8 servers. It is not supported on Gen9 servers.
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 details are listed in the **Virtual Floppy/Virtual Folder Status** or **Virtual CD/DVD-ROM Status** section:

- **Media 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** or **Virtual CD/DVD-ROM Status** section.

NOTE: For server blades 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.

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 will show virtual drive activity.

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 will show virtual drive activity.

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 does not show drive activity for URL-mounted virtual media.

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.

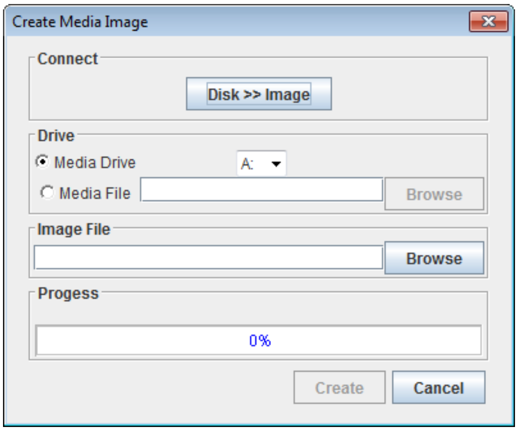
Creating an iLO disk image file

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.



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.
3. Click the **Disk>>Image** button to change 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.

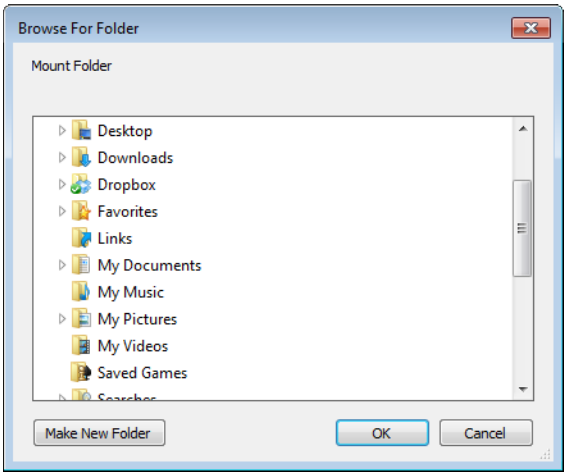
This feature and many others are part of an iLO licensing package. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.

The Virtual Folder is nonbootable and read-only; the mounted folder is static. Changes to the client folder 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.



3. Select the folder 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

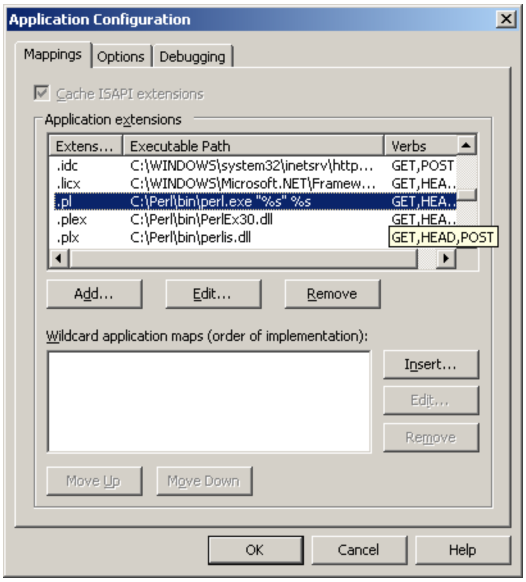
1. Install Perl (for example, ActivePerl).
2. Customize the Virtual Media helper application as needed.

   For a sample helper application, see “Sample Virtual Media helper application” (page 233).
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 5 (page 232).

Figure 5 Perl configuration example



☑ Cache ISAPI extensions

Application extensions

Extens...	Executable Path	Verbs
.idc	C:\WINDOWS\system32\inetsrv\http...	GET,POST
.licx	C:\WINDOWS\Microsoft.NET\Framew...	GET,HEA..
.pl	C:\Perl\bin\perl.exe "%s" %s	GET,HEA..
.plex	C:\Perl\bin\PerlEx30.dll	GET,HEA..
.plx	C:\Perl\bin\perlis.dll	GET,HEAD,POST

Wildcard application maps (order of implementation):

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 233).

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 4 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.

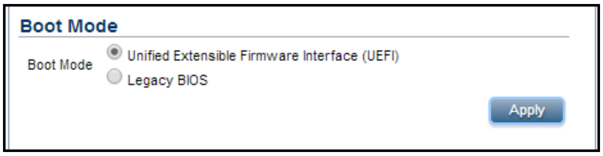
NOTE: Changes made to the boot mode, boot order, or one-time boot status might require a server reset. iLO notifies you when a reset is required.

Changing the server boot mode

HP ProLiant servers that support the Unified Extensible Firmware Interface include the HP UEFI System Utilities software, which is embedded in the system ROM. On servers that support this feature, the iLO web interface **Boot Order** page includes the **Boot Mode** section. Use the **Boot Mode** setting to define how the server looks for OS boot firmware. You can select UEFI or the Legacy BIOS.

To change the server boot mode:

1. Navigate to the **Virtual Media→Boot Order** page.
2. Select **Unified Extensible Firmware Interface (UEFI)** or **Legacy BIOS**.



Boot Mode

Boot Mode ● Unified Extensible Firmware Interface (UEFI)
○ Legacy BIOS

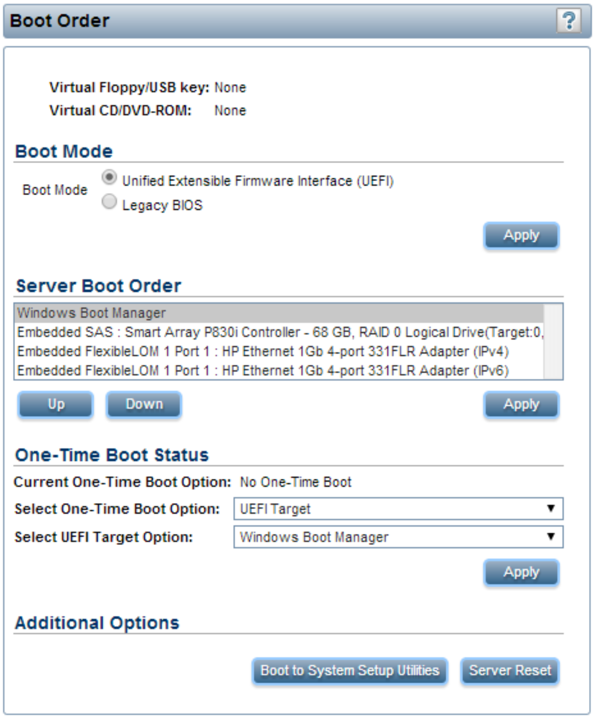
3. Click **Apply**.

   iLO prompts you to confirm the change. When you change this setting, you cannot make additional changes on the **Boot Order** page until you reset the server.
4. Click **OK** to confirm the change.
5. Click **Server Reset** to reset the server.

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.



Boot Order

Virtual Floppy/USB key: None
Virtual CD/DVD-ROM: None

Boot Mode

Boot Mode ● Unified Extensible Firmware Interface (UEFI) ○ Legacy BIOS

Server Boot Order

Windows Boot Manager
Embedded SAS : Smart Array P830i Controller - 68 GB, RAID 0 Logical Drive(Target:0,
Embedded FlexibleLOM 1 Port 1 : HP Ethernet 1Gb 4-port 331FLR Adapter (IPv4)
Embedded FlexibleLOM 1 Port 1 : HP Ethernet 1Gb 4-port 331FLR Adapter (IPv6)

One-Time Boot Status

Current One-Time Boot Option: No One-Time Boot
Select One-Time Boot Option: UEFI Target
Select UEFI Target Option: Windows Boot Manager

Additional Options

When Virtual Media is connected, the iLO web interface displays the Virtual Media type next to the **Virtual Floppy/USB key** and **Virtual CD/DVD-ROM** text at the top of the 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.

   In Legacy BIOS mode, select from the following devices:

   - **CD/DVD Drive**
   - **Floppy Drive (Gen8 only)**
   - **USB Storage Device**
   - **Hard Disk Drive**
   - **Network Device <number>**, where the server Ethernet card and additional NIC/FlexibleLOM cards are Network Device 1, Network Device 2, Network Device 3, and so on.

   In UEFI mode, select from the following devices:

   - **CD/DVD Drive**
   - **Floppy Drive (Gen8 only)**
   - **USB Storage Device**
   - **Hard Disk Drive**
   - **<Network Device>**—On servers that support the UEFI System Utilities, the **Server Boot Order** list shows a device-specific name instead of the generic term that describes the device type. For example, instead of **Network Device**, you might see **Embedded FlexibleLOM 1 Port 1 : Broadcom NetXtreme Gigabit Ethernet (BCM5719) (IPv4)**.

3. Click **Apply**.

   The following message appears:

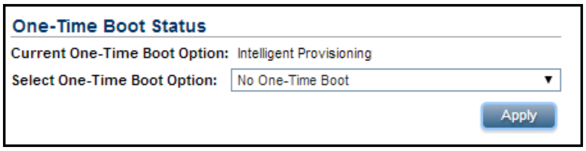
   ```
   Successfully set boot order.
   ```

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:

Changing the one-time boot status in Legacy BIOS mode

1. Navigate to the **Virtual Media**→**Boot Order** page.
2. Select an option from the **Select One-Time Boot Option** list.



One-Time Boot Status

Current One-Time Boot Option: Intelligent Provisioning

Select One-Time Boot Option: No One-Time Boot

The following options are available:

- **No One-Time Boot**
- **CD/DVD Drive**
- **Floppy Drive (Gen8 only)**
- **USB Storage Device**
- **Hard Disk Drive**
- **Network Device <number>**, where the server Ethernet card is Network Device 1, and additional NIC/FlexibleLOM cards are Network Device 2, Network Device 3, and so on.
- **Intelligent Provisioning**

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.

Changing the one-time boot status in UEFI mode

1. Navigate to the **Virtual Media**→**Boot Order** page.
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 (Gen8 only)**
- **USB Storage Device**
- **Hard Disk Drive**
- **Network Device <number>**, where the server Ethernet card is Network Device 1, and additional NIC/FlexibleLOM cards are Network Device 2, Network Device 3, and so on.
- **Intelligent Provisioning**

- **UEFI Target**—When you select this option, you can select from the list of available boot devices in the **Select UEFI Target Option** list.
- **Embedded UEFI Shell**—When you select this option, the server boots to an embedded shell environment that is separate from the UEFI System Utilities. For more information, see the *HP UEFI Shell User Guide*.

3. If you selected **UEFI Target** in the **Select One-Time Boot Option** list, select a boot device from the **Select UEFI Target Option** list. For example, you might have a hard drive that contains two bootable partitions, and you can use this option to select the bootable partition to use on the next server reset.
4. 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.

- Depending on whether your system supports the legacy system RBSU or the UEFI System Utilities, click **Boot to System RBSU** or **Boot to System Setup Utilities** to load the ROM-based setup utility 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

Powering on the server

Before the introduction of the HP ProLiant Gen8 servers, some HP ProLiant servers (particularly ML and DL) could be powered on through the power button within a few seconds after AC power was connected. If an AC power loss occurs on HP ProLiant Gen8 or Gen9 servers with iLO 4, approximately 30 seconds must elapse before the servers can power on again. The power button will blink, indicating a pending request, if it is pressed during that time.

This delay is a result of the iLO firmware loading, authenticating, and booting. iLO processes pending power-button requests when initialization is complete. If the server does not lose power, there is no delay. A 30-second delay occurs only during an iLO reset. The power button is disabled until iLO is ready to manage power.

A power-button watchdog allows the user to power on the system using the power button when iLO does not boot successfully.

The iLO firmware monitors and configures power thresholds to support managed-power systems (for example, using HP power capping technology). Multiple system brownout, blackout, and thermal overloads might result when systems are allowed to boot before iLO can manage power. The managed-power state is lost because of AC power loss, so iLO must first boot to a restore state and allow power-on.

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 **Auto-Power On** is set to **Always Remain**

Off. 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 34).

The Thermal Shutdown option in the system RBSU or UEFI System Utilities allows you to disable the automatic shutdown feature. This configuration allows the disabling of automatic shutdown except in the most extreme conditions when physical damage might result.

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 or UEFI System Utilities. You cannot modify these settings through iLO. For more information, see the *HP ROM-Based Setup Utility User Guide* or the *HP UEFI System Utilities 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**.

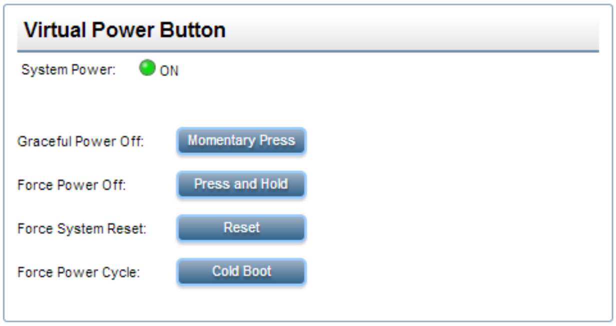
Managing the server power

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 power state 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.

Use the following procedure to change the server power state. You must have the Virtual Power and Reset privilege to use this feature.

1. Navigate to the **Power Management**→**Server Power** page.



Virtual Power Button

System Power: ● ON

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.

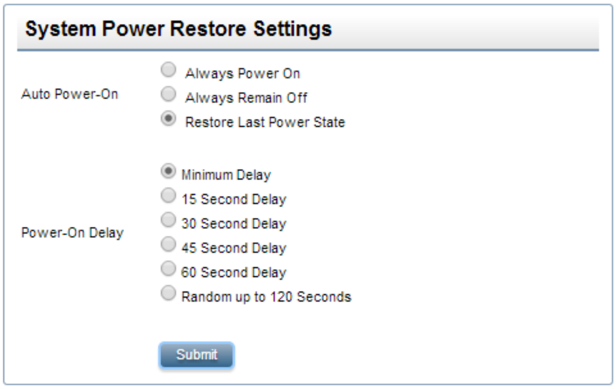
NOTE: The **Press and Hold**, **Reset**, and **Cold Boot** options are not available when the server is powered down.

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 or UEFI System Utilities 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.



System Power Restore Settings

Auto Power-On
○ Always Power On
○ Always Remain Off
● Restore Last Power State

Power-On Delay
● Minimum Delay
○ 15 Second Delay
○ 30 Second Delay
○ 45 Second Delay
○ 60 Second Delay
○ Random up to 120 Seconds

2. Select an **Auto Power-On** value.

   This setting determines how iLO behaves after power is restored—for example, when the server is plugged in or when a UPS is activated after a power outage. This setting is not supported with micro-UPS systems.

   The following options are available:

   - **Always Power On**—Power on the server after the power-on delay (default for BL servers).
   - **Always Remain Off**—The server remains off until directed to power on.
   - **Restore Last Power State**—Returns the server to the power state when power was lost. If the server was on, it powers on; if the server was off, it remains off. This option is the default setting for ML, DL, and SL servers. It is not available on BL servers.

   NOTE: Changes to the **Auto Power On** value might not take place until after the next server reboot.

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. This setting is not supported with micro-UPS systems.

   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.

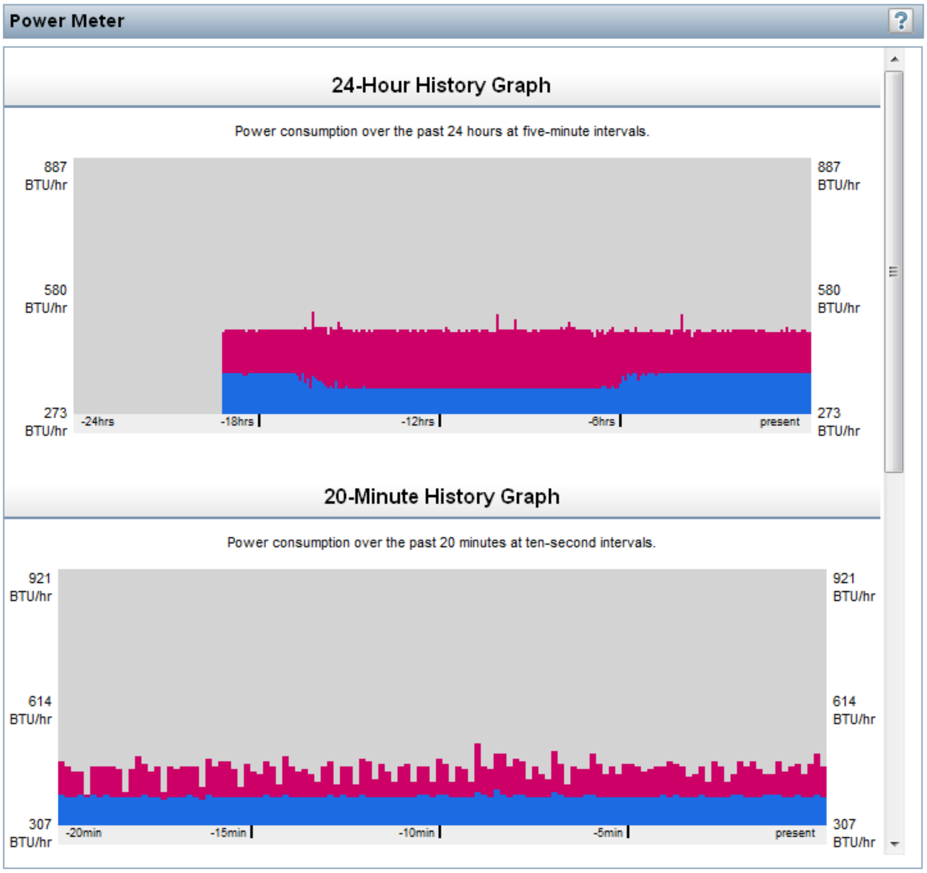
4. Click **Submit**.

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.

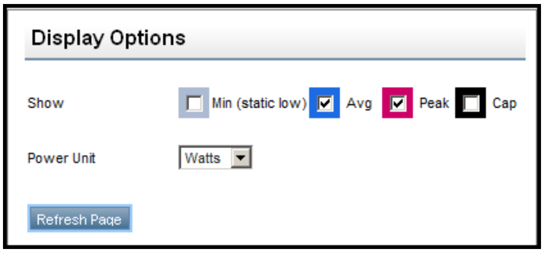


The power-meter graphs display recent server power usage. The graph data is reset when iLO or the server is reset. The iLO firmware periodically samples peak power, average power, and power cap. The following graphs are displayed:

- **24-Hour History Graph**—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**—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 view the power-meter graphs, use the **Display Options** to control the displayed information. You can view minimum, average, peak, and cap power information.


Display Options

Show □ Min (static low) ☑ Avg ☑ Peak □ Cap

Power Unit Watts

Select one or more of the following check boxes, and then click **Refresh Page** to update the graphs.

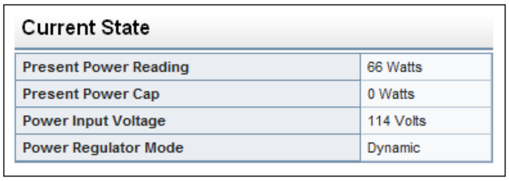
- **Min (static low)**—The minimum value observed during a measurement period. Typically, the 20-minute graph measures a minimum value every 10 seconds, which matches the average value. The 24-hour graph can capture minimum values lower than the 5-minute average value.
- **Avg**—The mean power reading 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, the **Cap** option is not available.
    - 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 might 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 from the **Power Unit** list to change the power reading display to 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. Scroll to the **Current State** section.



Current State

Present Power Reading	66 Watts
Present Power Cap	0 Watts
Power Input Voltage	114 Volts
Power Regulator Mode	Dynamic

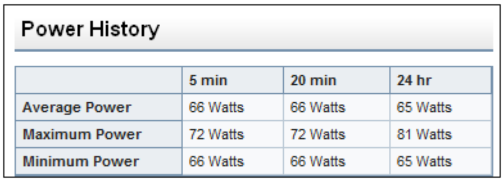
The values displayed in the **Current State** table vary depending on the server type:

- **Present Power Reading**—The current power reading from the server. This value is displayed for all HP ProLiant servers.
- **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 and DL servers, and server blades.
- **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 servers. For information about the possible settings, see "Configuring power settings" (page 243).

- **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. Scroll to the **Power History** section.



Power History

	5 min	20 min	24 hr
Average Power	66 Watts	66 Watts	65 Watts
Maximum Power	72 Watts	72 Watts	81 Watts
Minimum Power	66 Watts	66 Watts	65 Watts

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

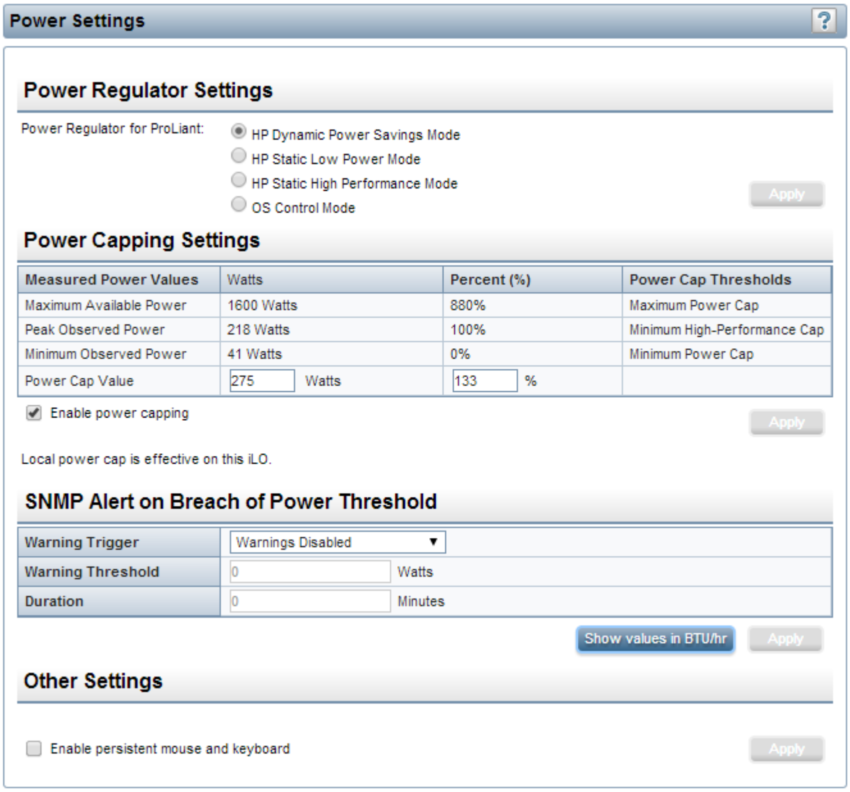
The **Power Settings** page enables you to view and control the power management features of the server. The power management features on this page vary based on the server configuration. You must have the Configure iLO Settings privilege to change the values on this page.

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.



Power Settings

Power Regulator Settings

Power Regulator for ProLiant:
● HP Dynamic Power Savings Mode
○ HP Static Low Power Mode
○ HP Static High Performance Mode
○ OS Control Mode

Power Capping Settings

Measured Power Values	Watts	Percent (%)	Power Cap Thresholds
Maximum Available Power	1600 Watts	880%	Maximum Power Cap
Peak Observed Power	218 Watts	100%	Minimum High-Performance Cap
Minimum Observed Power	41 Watts	0%	Minimum Power Cap
Power Cap Value	275 Watts	133 %	

☑ Enable power capping

Local power cap is effective on this iLO.

SNMP Alert on Breach of Power Threshold

Warning Trigger	Warnings Disabled ▾
Warning Threshold	0 Watts
Duration	0 Minutes

Other Settings

□ Enable persistent mouse and keyboard

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 server blade.
  - **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 capping 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 Control Power Management.
- 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.
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.
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. If you selected **Peak Power Consumption** or **Average Power Consumption** in the **Warning Trigger** list, enter the following:
   - **Warning Threshold**—Sets the power consumption threshold, in watts. If power consumption exceeds this value for the specified time duration, an SNMP alert is triggered.
   - **Duration**—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.
4. 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 disabled by default.

To change the persistent mouse and keyboard setting:

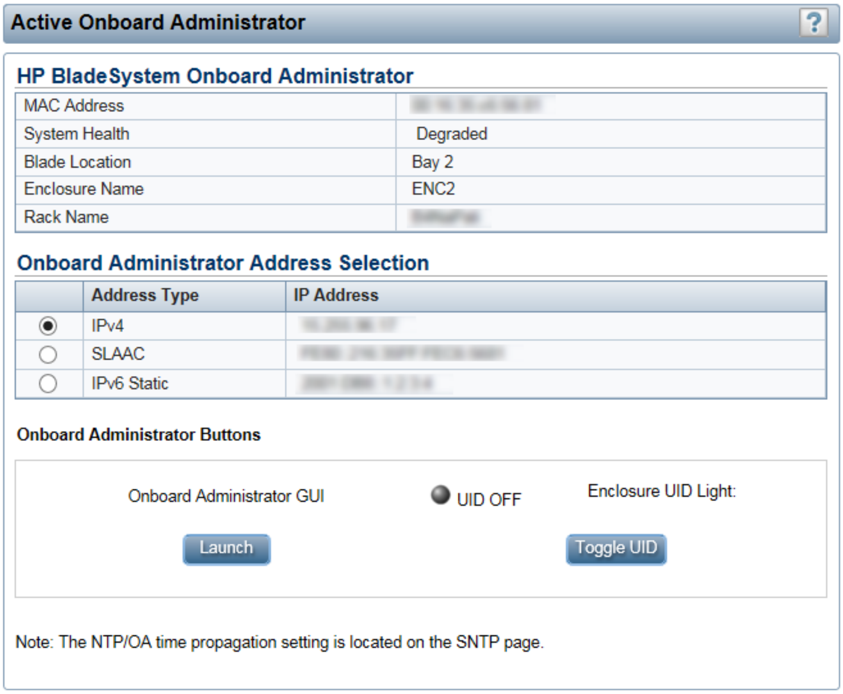
1. Navigate to the **Power Management→Power Settings** page.
2. Select or clear the **Enable persistent mouse and keyboard** check box.
3. Click **Apply** to save the configuration.

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.



Active Onboard Administrator

HP BladeSystem Onboard Administrator

MAC Address	[redacted]
System Health	Degraded
Blade Location	Bay 2
Enclosure Name	ENC2
Rack Name	[redacted]

Onboard Administrator Address Selection

	Address Type	IP Address
●	IPv4	[redacted]
○	SLAAC	[redacted]
○	IPv6 Static	[redacted]

Onboard Administrator Buttons

Onboard Administrator GUI

● UID OFF

Enclosure UID Light:

Note: The NTP/OA time propagation setting is located on the SNTP page.

The displayed information and options follow:

- **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

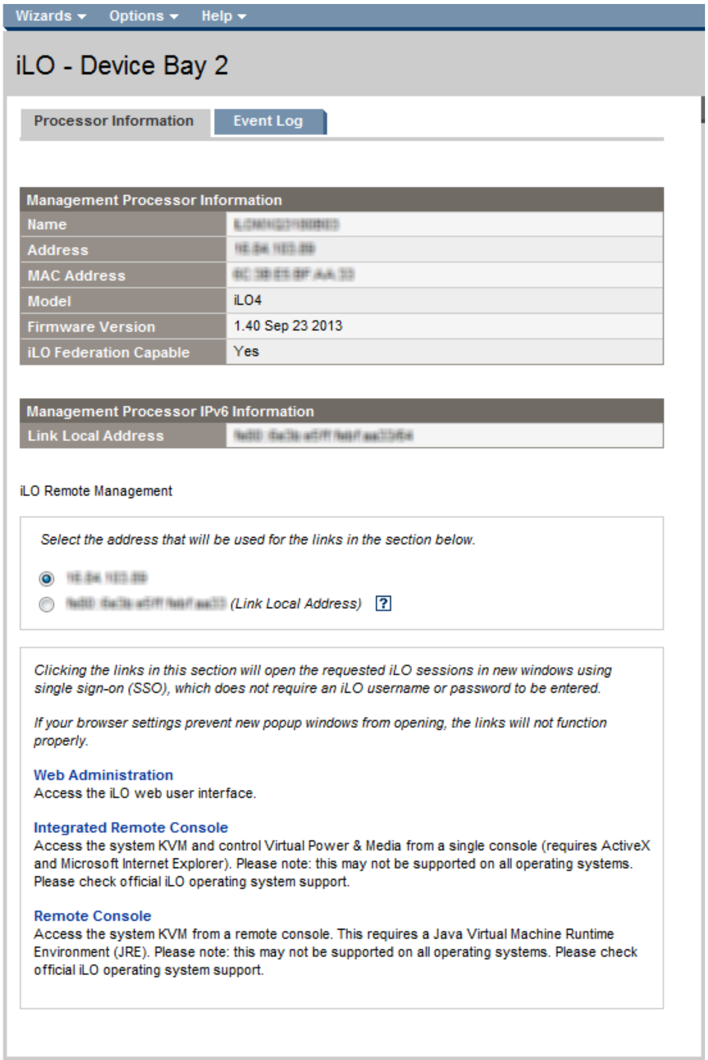
In c-Class blade servers, OA controls the enclosure fans (also called virtual fans). The iLO firmware cannot detect these enclosure fans. Instead, the iLO firmware monitors an ambient temperature sensor located on the blade server. This information is displayed on the iLO web interface, and is retrieved 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 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.



iLO - Device Bay 2

Management Processor Information	
Name	[redacted]
Address	[redacted]
MAC Address	[redacted]
Model	iLO4
Firmware Version	1.40 Sep 23 2013
iLO Federation Capable	Yes

Management Processor IPv6 Information	
Link Local Address	[redacted]

iLO Remote Management

Select the address that will be used for the links in the section below.

● [redacted]
○ [redacted] *(Link Local Address)* ?

Clicking the links in this section will open the requested iLO sessions in new windows using single sign-on (SSO), which does not require an iLO username or password to be entered.

If your browser settings prevent new popup windows from opening, the links will not function properly.

Web Administration
Access the iLO web user interface.

Integrated Remote Console
Access the system KVM and control Virtual Power & Media from a single console (requires ActiveX and Microsoft Internet Explorer). Please note: this may not be supported on all operating systems. Please check official iLO operating system support.

Remote Console
Access the system KVM from a remote console. This requires a Java Virtual Machine Runtime Environment (JRE). Please note: this may not be supported on all operating systems. Please check official iLO operating system support.

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 provisioning

HP Insight Control server provisioning 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 provisioning, see the documentation on the HP Insight Control website at http://www.hp.com/go/insightcontrol.

Using HP Enterprise Secure Key Manager with iLO

The **Key Manager** page enables you to connect to an operational key manager, change redundancy settings, view the key manager connection settings, test the connection, and view key management events.

iLO 4 1.40 and later supports the HP Enterprise Secure Key Manager 3.1 and later, which can be used in conjunction with HP Secure Encryption.

- HP Secure Encryption supports HP Smart Array Controllers and provides data-at-rest encryption for direct-attached HDD or SSD storage connected to HP ProLiant servers. It provides an integrated solution to encrypting HDD or SSD volumes by using 256-bit XTS-AES algorithms.
- HP Enterprise Secure Key Manager generates, stores, serves, controls and audits access to data encryption keys. It enables you to protect and preserve access to business-critical, sensitive, data-at-rest encryption keys.
- HP iLO manages the key exchange between the ESKM and the Smart Array Controller. iLO uses a unique user account based on its own MAC address for communicating with the ESKM. For the initial creation of this account, iLO uses a deployment user account that pre-exists on the ESKM with administrator privileges. For more information about the deployment user account, see the *HP Secure Encryption Installation and User Guide*

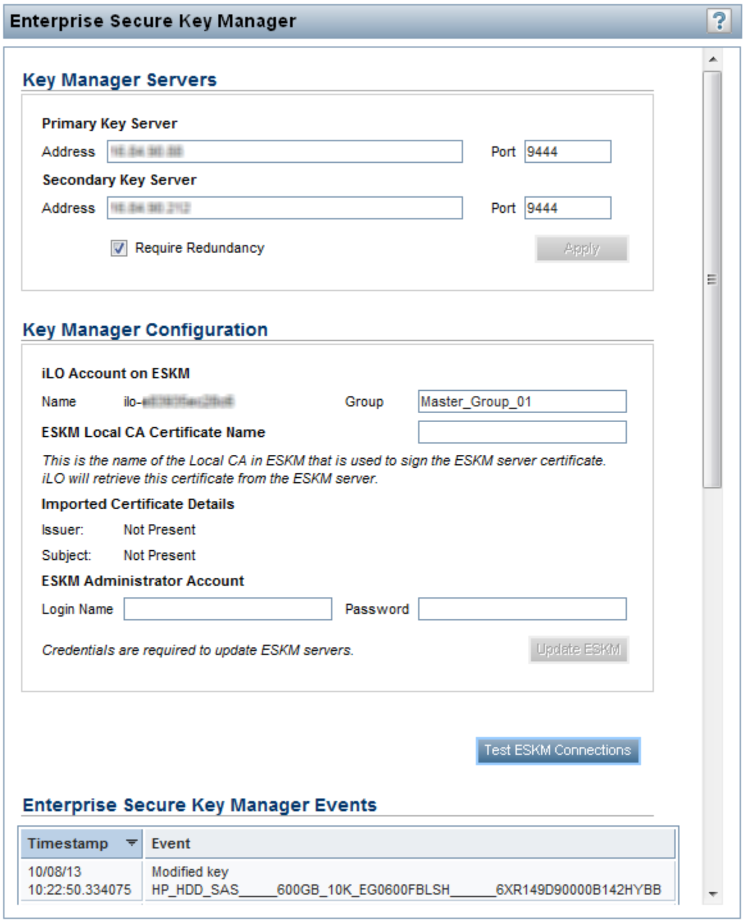
This feature and many others are part of an iLO licensing package. For more information about iLO licensing, see the following website: http://www.hp.com/go/ilo/licensing.

For information about HP Secure Encryption and ESKM, see the *HP Secure Encryption Installation and User Guide*

Configuring key manager servers

To configure key manager servers in iLO:

1. Navigate to the **Administration→Key Manager** page.



Enterprise Secure Key Manager

Key Manager Servers

Primary Key Server

Address [redacted] Port 9444

Secondary Key Server

Address [redacted] Port 9444

☑ Require Redundancy

Key Manager Configuration

iLO Account on ESKM

Name ilo-[redacted] Group Master_Group_01

ESKM Local CA Certificate Name

This is the name of the Local CA in ESKM that is used to sign the ESKM server certificate. iLO will retrieve this certificate from the ESKM server.

Imported Certificate Details

Issuer: Not Present

Subject: Not Present

ESKM Administrator Account

Login Name Password

Credentials are required to update ESKM servers.

Enterprise Secure Key Manager Events

Timestamp	Event
10/08/13 10:22:50.334075	Modified key HP_HDD_SAS_____600GB_10K_EG0600FBLSH______6XR149D90000B142HYBB

2. Enter the following information:
   - **Primary Key Server**—The primary key server IP address or FQDN and port.
   - **Secondary Key Server**—The secondary key server IP address or FQDN and port.
3. Optional: For configurations with a primary and secondary key server, select the **Require Redundancy** check box to check for server redundancy.

   HP recommends enabling this option. When this option is disabled, iLO will not verify that encryption keys are copied to both of the configured Key Servers.
4. Click **Apply**.

Adding key manager configuration details

1. Navigate to the **Administration→Key Manager** page.

   The listed **iLO Account on ESKM** account name is **ilo-<iLO MAC address>**. The account name is read-only and is used when iLO communicates with the ESKM.
2. Enter the following information in the **Key Manager Configuration** section:
   - **Group**—The Local Group created on the ESKM for use with iLO user accounts and the keys iLO imports into the ESKM. When keys are imported, they are automatically accessible to all devices assigned to the same group.
   - **ESKM Local CA Certificate Name** (optional)—To ensure that iLO is communicating with a trusted ESKM server, enter the name of the local certificate authority certificate in ESKM.

It is typically named **Local CA** and is listed in ESKM under Local CAs. iLO will retrieve the certificate and use it to authenticate the ESKM server(s) for all transactions going forward.

- **Login Name**—The Local User name with administrator permissions that is configured on the ESKM. This is the ESKM *deployment user*.

  The deployment user account must be created before you add key manager configuration details in iLO.

- **Password**—The password for the Local User name with administrator permissions that is configured on the ESKM.

3. Click **Update ESKM**.

   iLO verifies that an iLO account named **ilo-<iLO MAC address>** exists on the ESKM.

   If the account exists, iLO verifies that the account password is correct. If the password is incorrect, iLO updates the password. This password is automatically generated by iLO and might have been changed if iLO was restored to the factory default settings. If the account does not exist, iLO creates it.

   If iLO is not a member of an ESKM Local Group, it will try to create a group with the requested name. If iLO is already a member of an ESKM Local Group, it will ignore the group entered in Step 2, and will use the existing group assignment that is present on the ESKM. Attempted group changes in iLO do not affect current key group permissions that are set on the ESKM. If a new group assignment is needed, you must make the changes on the ESKM before updating the iLO settings.

   If you entered the **ESKM Local CA Certificate Name** in Step 2, certificate information is listed in the **Imported Certificate Details** section of the Enterprise Secure Key Manager page.

See the *HP Secure Encryption Installation and User Guide* for more information about groups and their use with key management.

Testing the ESKM configuration

After the key manager configuration is complete in iLO, you can use the **Test ESKM Connections** feature to verify the configuration settings. The tests confirm that iLO and the ESKM servers are set up to provide key management services for HP Secure Encryption. During the test, iLO attempts the following tasks:

- Connects to the primary ESKM server (and secondary ESKM server, if configured) by using SSL.
- Tries to authenticate to the ESKM by using the configured credentials and account.
- Confirms that the version of the ESKM software is compatible with iLO.

To test the ESKM configuration:

1. Navigate to the **Administration**→**Key Manager** page.
2. Click **Test ESKM Connections**.

   The test results are displayed in the **Enterprise Secure Key Manager Events** table.

Viewing Enterprise Secure Key Manager events

1. Navigate to the **Administration**→**Key Manager** page.
2. Scroll to the Enterprise Secure Key Manager Events section.

   Each event is listed with a time stamp and description.

Viewing remote management tool information

iLO 4 1.30 and later allows remote management through supported tools such as HP OneView.

The association between iLO 4 and a remote management tool is configured by using the remote management tool. For instructions, see your remote management tool documentation.

When iLO is under the control of a remote management tool, the iLO GUI includes the following enhancements:

- A message similar to the following is displayed on the iLO login page:

  ```
  Warning! Some iLO settings are managed by <Remote Management Tool Name>.
  ```

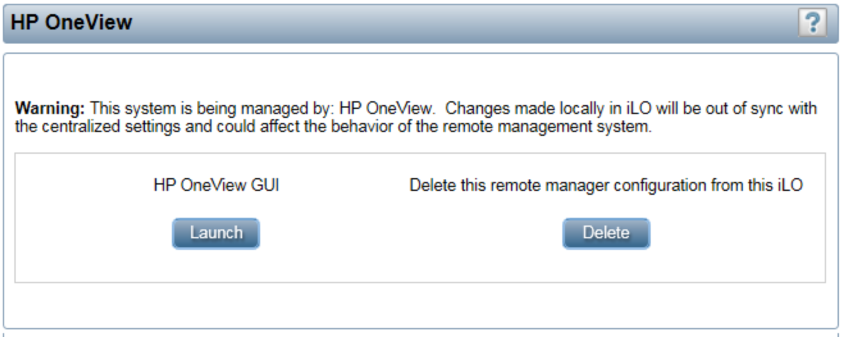
  ```
  Changes made directly in iLO will be out of sync with the centralized settings.
  ```

- A page called **<Remote Management Tool Name>** is added to the iLO navigation tree.

Starting a remote management tool

When iLO is under the control of a remote management tool, use the following procedure to start the remote manager GUI from iLO.

1. Navigate to the **<Remote Management Tool Name>** page.



HP OneView

Warning: This system is being managed by: HP OneView. Changes made locally in iLO will be out of sync with the centralized settings and could affect the behavior of the remote management system.

2. Click **Launch**.

   The remote management tool starts in a separate browser window.

Deleting a remote manager configuration

If you discontinue the use of a remote management tool in your network, you can remove the association between the tool and iLO.

IMPORTANT: HP recommends that you remove the server from the remote management tool before you delete the remote manager configuration in iLO. Do not delete the remote manager configuration for a tool that is still in use on the network and is managing the server that contains the current iLO system.

1. Navigate to the **<Remote Management Tool Name>** page.
2. Click the **Delete** button in the **Delete this remote manager configuration from this iLO** section.

   A warning message similar to the following appears:

   ```
   Proceed with this deletion only if this iLO is no longer under the control of <Remote Management Tool Name>.
   ```

3. Click **OK**.

   The **<Remote Management Tool Name>** page is removed from the iLO navigation tree.

Using iLO with HP OneView

HP OneView interacts with an iLO management processor to configure, monitor, and manage an HP ProLiant server. HP OneView configures seamless access to the iLO graphical remote console, enabling you to launch the iLO remote console from the HP OneView user interface in a single click. Your iLO privileges are determined by the role assigned to your HP OneView appliance account.

HP OneView manages the following iLO settings:

- The remote management tool
- SNMP v1 trap destination
- SNMP v1 read community
- HP SSO certificate—HP OneView adds a trusted certificate to the **Administration→Security→HP SSO** page.
- NTP (time server) configuration
- User Account—HP OneView adds an administrative user account to iLO with the name **_HPOneViewAdmin**.
- Firmware version—When you add a server to HP OneView, if a supported version of the iLO firmware is not installed, HP OneView updates the firmware.

ⓘ **IMPORTANT:** For best performance when using HP OneView with HP iLO 4, HP recommends that you do not delete or change these settings by using the iLO web interface.

For more information about HP OneView, see http://www.hp.com/go/oneview/docs.

Using the Embedded User Partition

HP iLO 4 stores files such as Active Health System data and the Intelligent Provisioning software in non-volatile flash memory that is embedded on the system board. This flash memory is called the iLO NAND. HP ProLiant Gen9 servers with a 4 GB iLO NAND allow you to use a 1 GB non-volatile flash memory partition as if it was an SD-card attached to the server. When the Embedded User Partition is enabled, you can access it through the server operating system.

The Embedded User Partition is accessible through the server OS for read and write access when the server is configured for Legacy BIOS or UEFI boot mode.

To determine whether your server includes a 4 GB iLO NAND, see the server QuickSpecs at http://www.hp.com/go/qs.

You can use the Embedded User Partition for tasks such as:

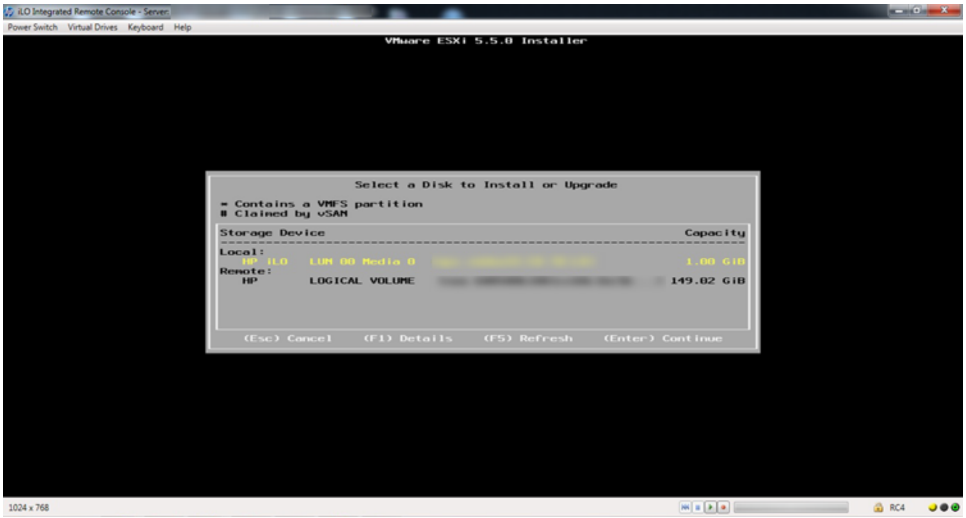
- Storing UEFI shell scripts and test tools. UEFI scripts can be run automatically when the server boots to the embedded UEFI shell. To use this feature, place a `startup.nsh` shell script file in the root directory of the Embedded User Partition.

  This feature is supported only when the server is configured for the UEFI boot mode.

  For more information, see the *HP UEFI Shell User Guide for HP ProLiant Gen9 Servers* on the HP website: http://www.hp.com/go/ProLiantUEFI/docs.

- Installing and booting from VMware ESXi (UEFI mode only)

  To select the Embedded User Partition for an OS or hypervisor installation, select the volume **HP iLO LUN <number>.**



```
VMware ESXi 5.5.0 Installer

              Select a Disk to Install or Upgrade

* Contains a VMFS partition
# Claimed by vSAN

Storage Device                                                Capacity
----------------------------------------------------------------------
Local:
   HP iLO    LUN 00 Media 0   [redacted]                      1.00 GiB
Remote:
   HP        LOGICAL VOLUME   [redacted]                    149.02 GiB

   (Esc) Cancel    (F1) Details    (F5) Refresh    (Enter) Continue
```

- Storing iLO scripts
- Storing iLO language packs

For information about configuring access to the Embedded User Partition, see "Configuring the Embedded User Partition" (page 255).

Configuring the Embedded User Partition

You can use the UEFI System Utilities, UEFI Shell, and HP RESTful Interface tool to configure the Embedded User Partition.

Configuring the Embedded User Partition (UEFI System Utilities)

Use the following procedure to enable or disable the Embedded User Partition by using the UEFI System Utilities.

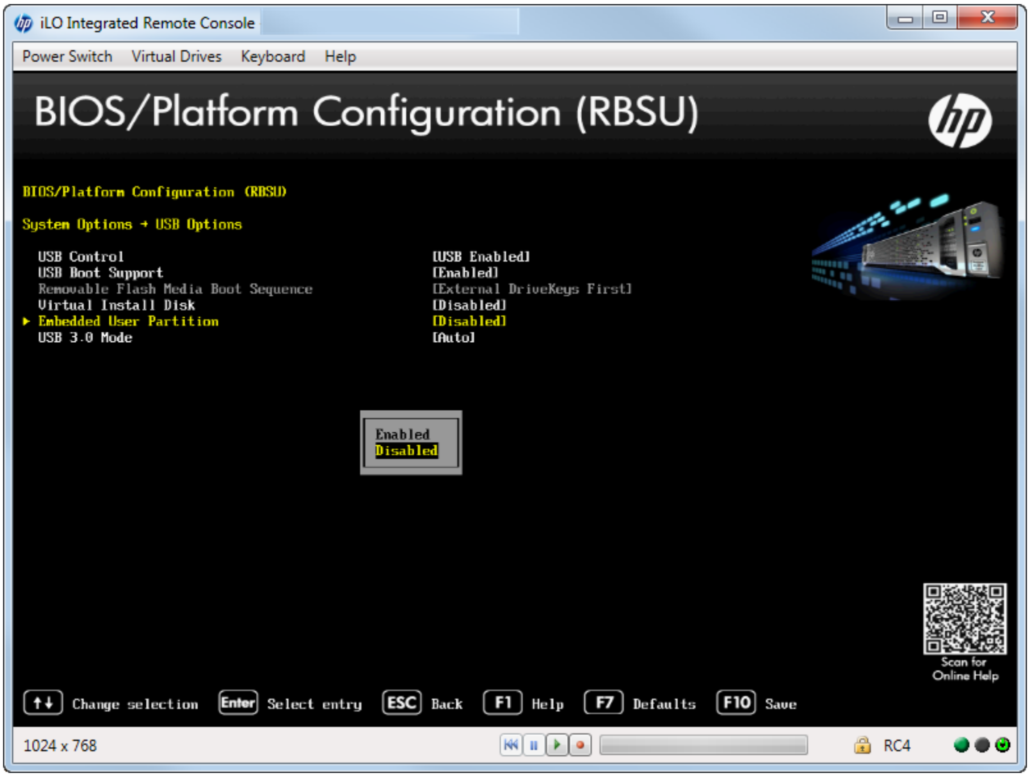
1. Optional: If you access the server remotely, start an iLO remote console session.

   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 Utilities** screen appears.

4. From the **System Utilities** screen, select **System Configuration**→**BIOS/Platform Configuration (RBSU)**→**System Options**→**USB Options**→**Embedded User Partition** and press **Enter**.
5. Select one of the following options:
   - **Enabled**
   - **Disabled** (default)



```
BIOS/Platform Configuration (RBSU)

System Options → USB Options

  USB Control                                 [USB Enabled]
  USB Boot Support                            [Enabled]
  Removable Flash Media Boot Sequence         [External DriveKeys First]
  Virtual Install Disk                        [Disabled]
▶ Embedded User Partition                     [Disabled]
  USB 3.0 Mode                                [Auto]

                     Enabled
                     Disabled
```

6. Press **F10** to save your selection.
7. Restart the server.
8. After you enable the Embedded User Partition, format it by using the server operating system software.

   Once the partition is formatted, it can be accessed for read and write access from the server operating system.

Configuring the Embedded User Partition (UEFI Shell)

Use the following procedure to configure the Embedded User Partition by using the UEFI Shell.

1. Boot to the UEFI Shell. For instructions, see the *HP UEFI Shell User Guide for HP ProLiant Gen9 Servers*.
2. Use the following command to enable the Embedded User Partition:

   ```
   sysconfig -s embeddeduserpartition=Enabled
   ```
3. Restart the server.
4. After you enable the Embedded User Partition, format it by using the server operating system software.

   Once the partition is formatted, it can be accessed for read and write access from the server operating system.

Configuring the Embedded User Partition (HP RESTful Interface Tool)

1. Enable or disable the Embedded User Partition.

   For information about configuring the Embedded User Partition with the HP RESTful Interface Tool, see the RESTful Interface Tool documentation at the following website: http://www.hp.com/go/restfulinterface/docs.
2. After you enable the Embedded User Partition, format it by using the server operating system software.

   Once the partition is formatted, it can be accessed for read and write access from the server operating system.

Configuring the Embedded User Partition boot settings

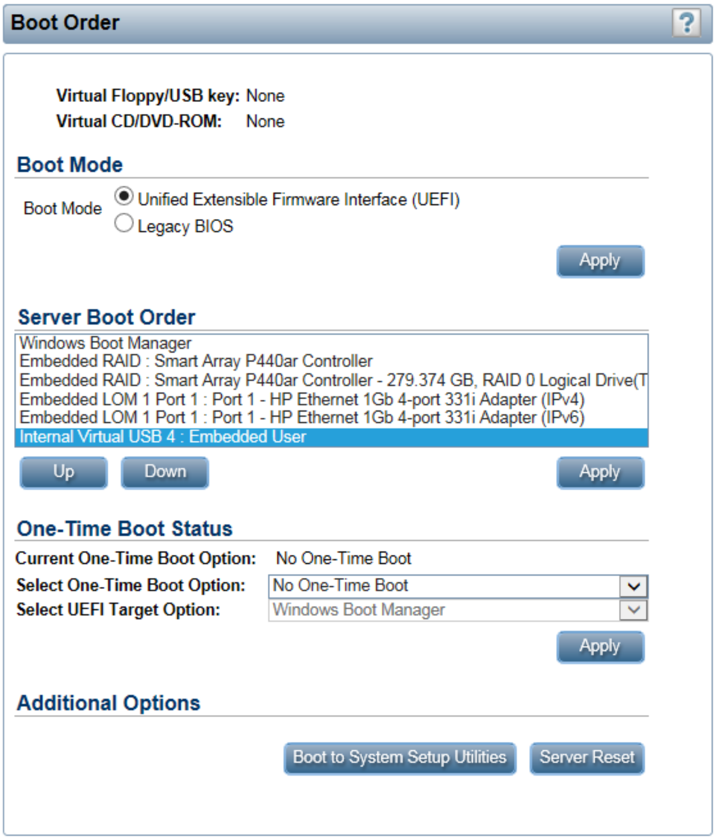
You can use the UEFI System Utilities, UEFI Shell, HP RESTful Interface tool, or iLO web interface to configure the Embedded User Partition boot settings.

Configuring the Embedded User Partition boot order setting (iLO web interface)

Use the following procedure to change the position of the Embedded User Partition in the **Server Boot Order** list.

NOTE: This feature is not available when the **Legacy BIOS** boot mode is selected.

1. Navigate to the **Virtual Media→Boot Order** page.



Boot Order

Virtual Floppy/USB key: None
Virtual CD/DVD-ROM: None

Boot Mode

Boot Mode ● Unified Extensible Firmware Interface (UEFI)
○ Legacy BIOS

Server Boot Order

Windows Boot Manager
Embedded RAID : Smart Array P440ar Controller
Embedded RAID : Smart Array P440ar Controller - 279.374 GB, RAID 0 Logical Drive(T
Embedded LOM 1 Port 1 : Port 1 - HP Ethernet 1Gb 4-port 331i Adapter (IPv4)
Embedded LOM 1 Port 1 : Port 1 - HP Ethernet 1Gb 4-port 331i Adapter (IPv6)
Internal Virtual USB 4 : Embedded User

One-Time Boot Status

Current One-Time Boot Option: No One-Time Boot
Select One-Time Boot Option: No One-Time Boot
Select UEFI Target Option: Windows Boot Manager

Additional Options

2. Select the Embedded User Partition device in the **Server Boot Order** list, and click **Up** or **Down** to move it up or down in the boot order.

   The Embedded User Partition is listed with a name similar to the following:

   ```
   Internal Virtual USB 4 : Embedded User.
   ```

3. Click **Apply**.

   The following message appears:

   ```
   Successfully set boot order.
   ```

Configuring the Embedded User Partition for one-time boot (iLO web interface)

Use the following procedure to set the position of the Embedded User Partition in the **Server Boot Order** list.

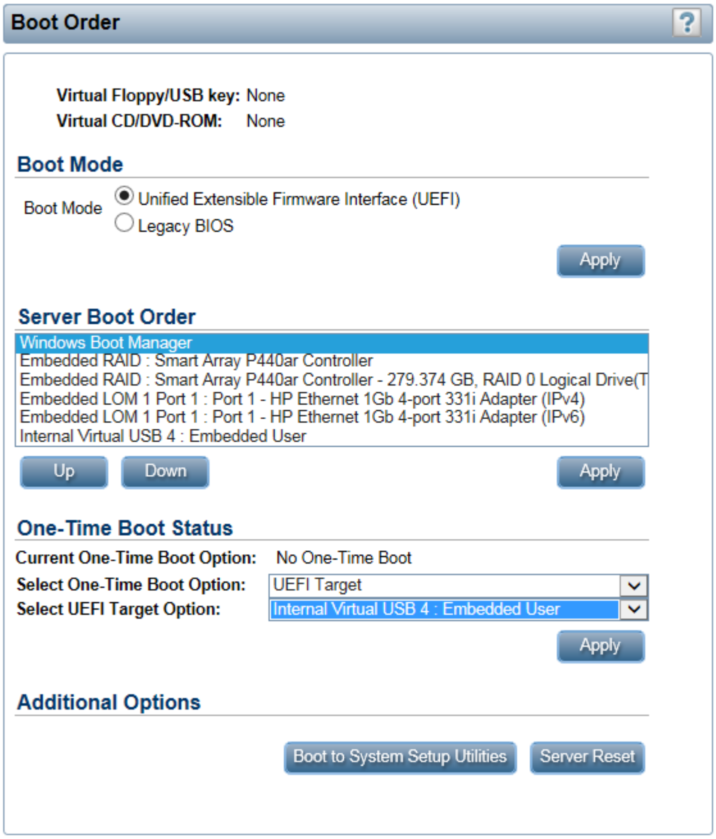
NOTE: This feature is not available when the **Legacy BIOS** boot mode is selected.

1. Navigate to the **Virtual Media→Boot Order** page.

2. Select **UEFI Target** in the **Select One-Time Boot Option** list.
3. Select the Embedded User Partition from the **Select UEFI Target Option** list.

   The Embedded User Partition is listed with a name similar to the following:

   ```
   Internal Virtual USB 4 : Embedded User.
   ```



Boot Order

Virtual Floppy/USB key: None
Virtual CD/DVD-ROM: None

Boot Mode

Boot Mode ● Unified Extensible Firmware Interface (UEFI)
○ Legacy BIOS

Server Boot Order

Windows Boot Manager
Embedded RAID : Smart Array P440ar Controller
Embedded RAID : Smart Array P440ar Controller - 279.374 GB, RAID 0 Logical Drive(T
Embedded LOM 1 Port 1 : Port 1 - HP Ethernet 1Gb 4-port 331i Adapter (IPv4)
Embedded LOM 1 Port 1 : Port 1 - HP Ethernet 1Gb 4-port 331i Adapter (IPv6)
Internal Virtual USB 4 : Embedded User

One-Time Boot Status

Current One-Time Boot Option: No One-Time Boot
Select One-Time Boot Option: UEFI Target
Select UEFI Target Option: Internal Virtual USB 4 : Embedded User

Additional Options

4. 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.

Configuring the Embedded User Partition boot order setting (UEFI System Utilities)

Use the following procedure to change the position of the Embedded User Partition in the **UEFI Boot Order** list.

NOTE: This feature is not available when the **Legacy BIOS** boot mode is selected.

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.

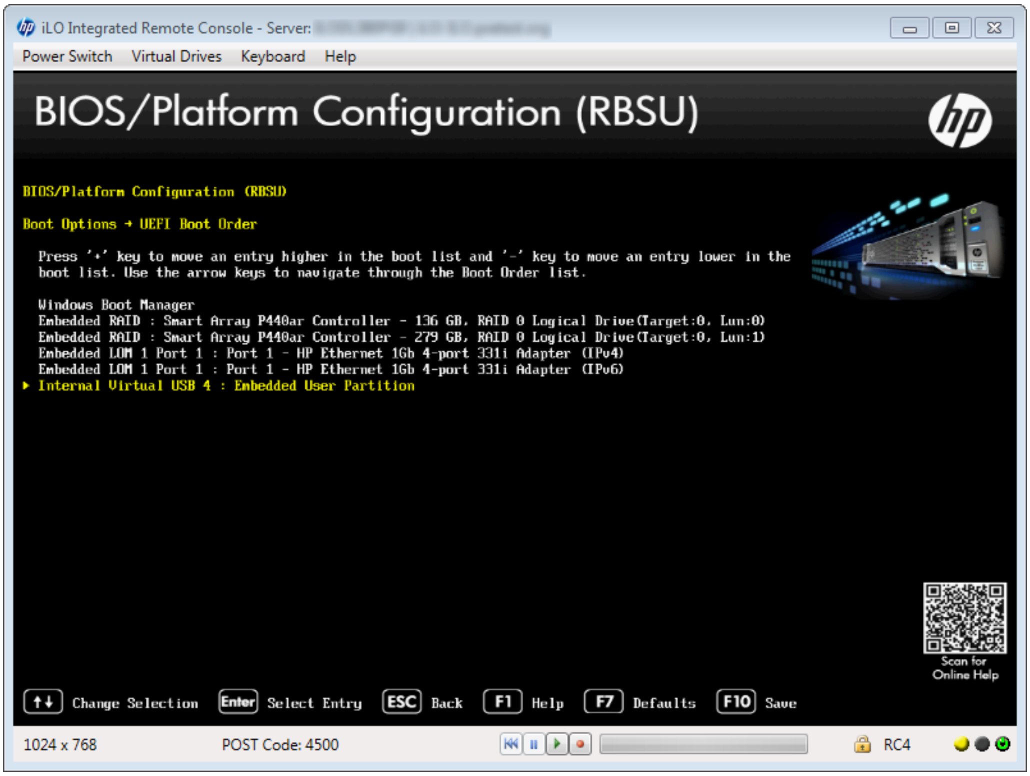
   The **System Utilities** screen appears.
4. From the **System Utilities** screen, select **System Configuration→BIOS/Platform Configuration (RBSU)→Boot Options→UEFI Boot Order** and press **Enter**.

   The UEFI Boot Order screen appears.

5. Press **Enter** to open the **UEFI Boot Order** list.

   The Embedded User Partition is listed with a name similar to the following:

   `Internal Virtual USB 4 : Embedded User Partition.`



```
BIOS/Platform Configuration (RBSU)

Boot Options → UEFI Boot Order

  Press '+' key to move an entry higher in the boot list and '-' key to move an entry lower in the
  boot list. Use the arrow keys to navigate through the Boot Order list.

  Windows Boot Manager
  Embedded RAID : Smart Array P440ar Controller - 136 GB, RAID 0 Logical Drive(Target:0, Lun:0)
  Embedded RAID : Smart Array P440ar Controller - 279 GB, RAID 0 Logical Drive(Target:0, Lun:1)
  Embedded LOM 1 Port 1 : Port 1 - HP Ethernet 1Gb 4-port 331i Adapter (IPv4)
  Embedded LOM 1 Port 1 : Port 1 - HP Ethernet 1Gb 4-port 331i Adapter (IPv6)
▶ Internal Virtual USB 4 : Embedded User Partition
```

6. Update the position of the Embedded User Partition in the boot order list, as needed.
   - Use the arrow keys to navigate within the boot order list.
   - Press the + key (plus) to move an entry higher in the boot list.
   - Press the - key (minus) to move an entry lower in the list.
7. Press **F10** to save your selection.
8. From the System Utilities screen, select **Exit and Resume Boot**.

For more information about the UEFI Boot Order list, see the *HP UEFI System Utilities User Guide for HP ProLiant Gen9 Servers*.

Configuring the Embedded User Partition for one-time boot (UEFI System Utilities)

Use the following procedure to set the position of the Embedded User Partition in the **One Time Boot Menu**.

NOTE: This feature is not available when the **Legacy BIOS** boot mode is selected.

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.

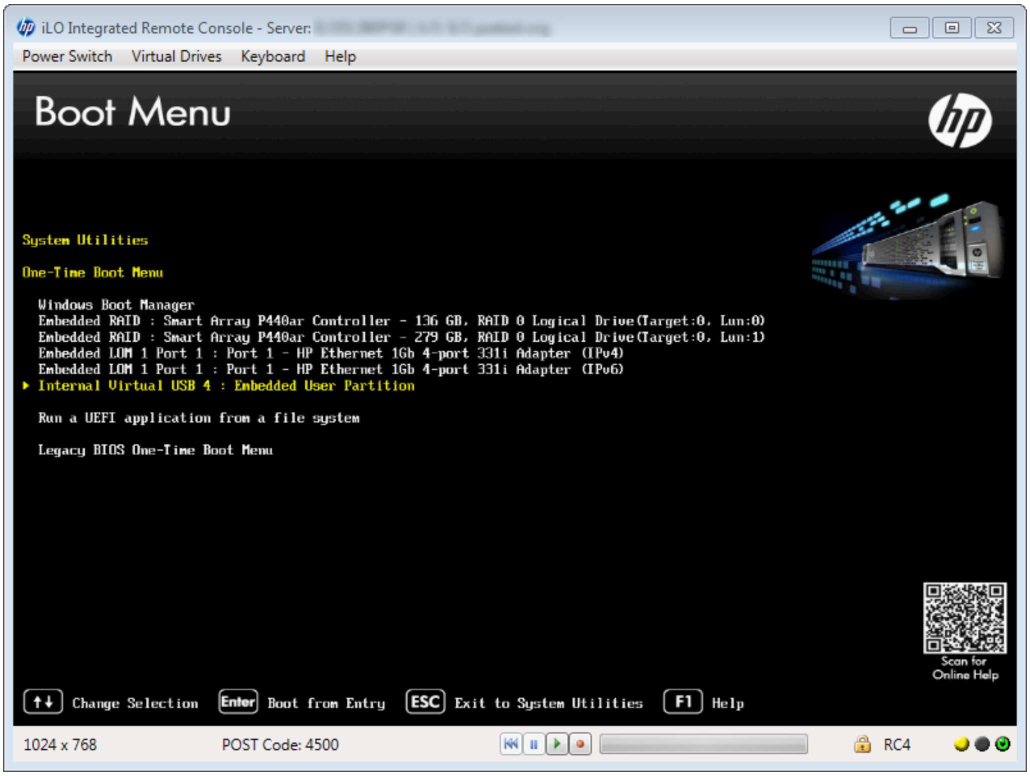
   The **System Utilities** screen appears.
4. From the **System Utilities** screen, select **One Time Boot Menu**, and then press **Enter**.

   The **One-Time Boot Menu** screen appears.

5. Select the Embedded User Partition option, and then press **Enter**.

   The Embedded User Partition is listed with a name similar to the following:

   `Internal Virtual USB 4 : Embedded User Partition.`



iLO Integrated Remote Console - Server: [redacted]

Boot Menu

```
System Utilities

One-Time Boot Menu

  Windows Boot Manager
  Embedded RAID : Smart Array P440ar Controller - 136 GB, RAID 0 Logical Drive(Target:0, Lun:0)
  Embedded RAID : Smart Array P440ar Controller - 279 GB, RAID 0 Logical Drive(Target:0, Lun:1)
  Embedded LOM 1 Port 1 : Port 1 - HP Ethernet 1Gb 4-port 331i Adapter (IPv4)
  Embedded LOM 1 Port 1 : Port 1 - HP Ethernet 1Gb 4-port 331i Adapter (IPv6)
▸ Internal Virtual USB 4 : Embedded User Partition

  Run a UEFI application from a file system

  Legacy BIOS One-Time Boot Menu
```

   The server resumes the boot process and boots from the Embedded User Partition.

For more information about the **One-Time Boot Menu**, see the *HP UEFI System Utilities User Guide for HP ProLiant Gen9 Servers*.

Configuring the Embedded User Partition boot order setting (UEFI Shell)

Use the following procedure to configure the Embedded User Partition by using the UEFI Shell.

1. Boot to the UEFI Shell. For instructions, see the *HP UEFI Shell User Guide for HP ProLiant Gen9 Servers*.
2. Use the following command to configure the Embedded User Partition boot order setting:

   ```
   sysconfig -s uefibootorder=settingvalue
   ```

   Where *`settingvalue`* is a UEFI boot order option.

   NOTE: For information about using this command, see the *HP UEFI Shell User Guide for HP ProLiant Gen9 Servers*.

Configuring the Embedded User Partition for one-time boot (UEFI Shell)

Use the following procedure to configure the Embedded User Partition by using the UEFI Shell.

1. Boot to the UEFI Shell. For instructions, see the *HP UEFI Shell User Guide for HP ProLiant Gen9 Servers*.

2. Use the following command to configure the Embedded User Partition for one-time boot:

   ```
   boot -n settingvalue
   ```

   Where `settingvalue` is the boot number of the device to use for one-time boot.

   NOTE: For information about using this command, see the *HP UEFI Shell User Guide for HP ProLiant Gen9 Servers*.

Configuring the Embedded User Partition boot order setting (HP RESTful Interface Tool)

For information about configuring the Embedded User Partition boot order setting with the HP RESTful Interface Tool, see the RESTful Interface Tool documentation at the following website: http://www.hp.com/go/restfulinterface/docs.

Configuring the Embedded User Partition for one-time boot (HP RESTful Interface Tool)

For information about configuring the Embedded User Partition one-time boot settings with the HP RESTful Interface Tool, see the RESTful Interface Tool documentation at the following website: http://www.hp.com/go/restfulinterface/docs.

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 or Agentless Management**—iLO, combined with Agentless Management or 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 “Using HP SSO” (page 83).

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 116).

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 106).

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 4,
,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.
- **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 271).
   - **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 271).
   - **Yes**—Use HP schema directory integration. For more information, see "Setting up HP extended schema directory integration" (page 275).

   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 265). "Directory-enabled remote management" (page 287) 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 93).

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 72).

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 46).

4. Navigate to the **Information→Overview** page to check the **Current iLO Date/Time**.

   For more information, see “Viewing iLO overview information” (page 148).

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 103).

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/ilo4. For more information, see the *HP iLO 4 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 4 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 269).

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.

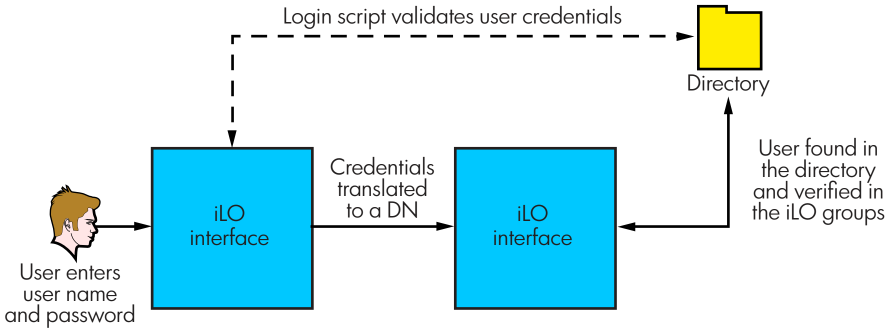
   If a prompt for credentials appears, Kerberos authentication has failed. Click **Cancel** to close the dialog box.

   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 6 (page 271).

Figure 6 Schema-free directory integration


Login script validates user credentials
Directory
User found in the directory and verified in the iLO groups
Credentials translated to a DN
iLO interface
iLO interface
User enters user name and password

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 272).

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.

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 274).
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 4 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 292).

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 273), "Schema-free setup using scripts" (page 273), and "Schema-free setup with HP Directories Support for ProLiant Management Processors" (page 273).

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 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 use HP schema directory integration, iLO supports Active Directory. This directory service requires 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 265).
   - Directory-enabled remote management. For more information, see "Directory-enabled remote management" (page 287).
   - Directory services schema. For more information, see "Directory services schema" (page 344).

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/ilo4.

   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 72).

   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 46).

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 287). Examples are available in "Directory services for Active Directory" (page 279).

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 292).

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 344).

Directory services support

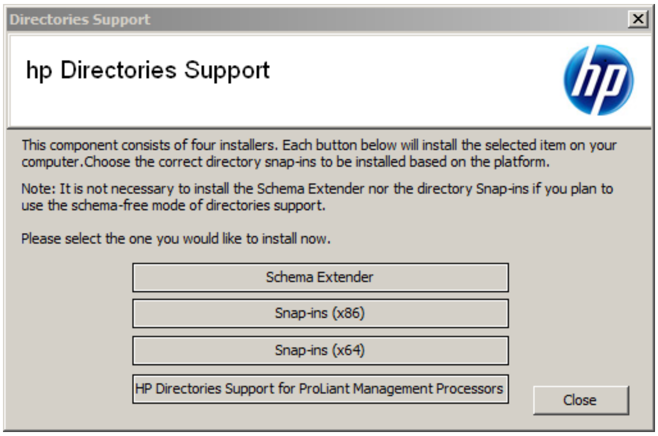
iLO software is designed to run with the Microsoft Active Directory Users and Computers snap-in, enabling you to manage user accounts through the directory.

iLO supports the following directory services for HP schema directory integration:

- Microsoft Active Directory
- Microsoft Windows Server Active Directory

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. You can download the software from http://www.hp.com/support/ilo4.



This component consists of four installers. Each button below will install the selected item on your computer.Choose the correct directory snap-ins to be installed based on the platform.

Note: It is not necessary to install the Schema Extender nor the directory Snap-ins if you plan to use the schema-free mode of directories support.

Please select the one you would like to install now.

You cannot run the schema installer on a domain controller that hosts Windows Server Core. For security and performance reasons, Windows Server 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

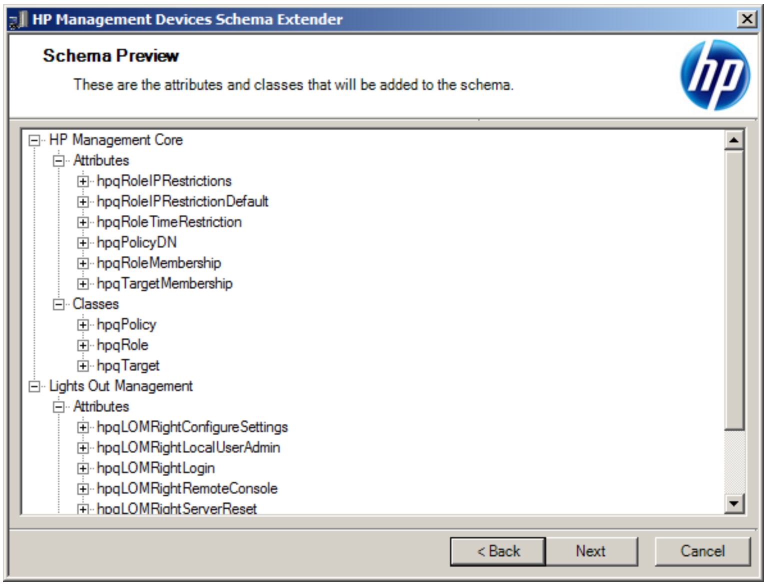
Several `.xml` files are bundled with the Schema Extender. These files contain the schemas that are added to the directory. Typically, one of these files contains a core schema that is common to all of the supported directory services. Additional files contain product-specific schemas. The schema installer requires the .NET Framework.

The Schema Extender installer includes three important windows:

- **Schema Preview**
- **Setup**
- **Results**

Schema Preview window

The **Schema Preview** window 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.



HP Management Devices Schema Extender

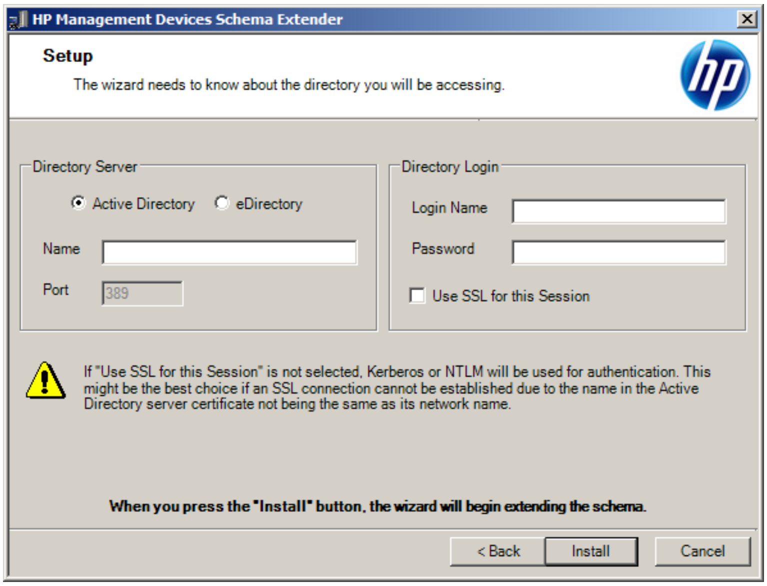
Schema Preview

These are the attributes and classes that will be added to the schema.

```
⊟ HP Management Core
   ⊟ Attributes
      ⊞ hpqRoleIPRestrictions
      ⊞ hpqRoleIPRestrictionDefault
      ⊞ hpqRoleTimeRestriction
      ⊞ hpqPolicyDN
      ⊞ hpqRoleMembership
      ⊞ hpqTargetMembership
   ⊟ Classes
      ⊞ hpqPolicy
      ⊞ hpqRole
      ⊞ hpqTarget
⊟ Lights Out Management
   ⊟ Attributes
      ⊞ hpqLOMRightConfigureSettings
      ⊞ hpqLOMRightLocalUserAdmin
      ⊞ hpqLOMRightLogin
      ⊞ hpqLOMRightRemoteConsole
      ⊞ hpqLOMRightServerReset
```

Setup window

You use the **Setup** window to enter the appropriate information before extending the schema.



HP Management Devices Schema Extender

Setup

The wizard needs to know about the directory you will be accessing.

Directory Server

● Active Directory ○ eDirectory

Name

Port 389

Directory Login

Login Name

Password

□ Use SSL for this Session

If "Use SSL for this Session" is not selected, Kerberos or NTLM will be used for authentication. This might be the best choice if an SSL connection cannot be established due to the name in the Active Directory server certificate not being the same as its network name.

When you press the "Install" button, the wizard will begin extending the schema.

The **Directory Server** section of the **Setup** window enables you to select Active Directory, and to set the computer name and the port to be used for LDAP communications.

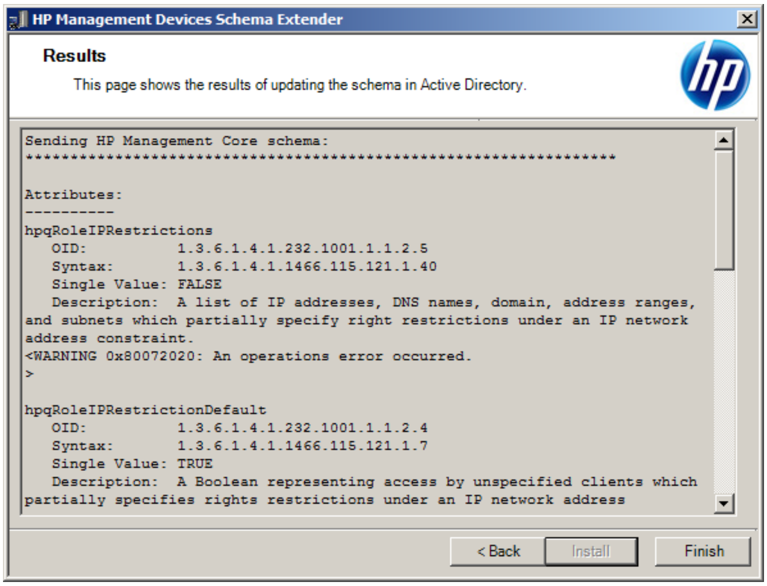
NOTE: When you are running the Schema Extender tool, you must use the `Administrator` login along with the domain name, for example, `Administrator@domain.com` or `domain\Administrator`.

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.

Results window

The **Results** window displays the results of the installation, including whether the schema could be extended and what attributes were changed.



This page shows the results of updating the schema in Active Directory.

```
Sending HP Management Core schema:
*******************************************************************

Attributes:
----------
hpqRoleIPRestrictions
   OID:          1.3.6.1.4.1.232.1001.1.1.2.5
   Syntax:       1.3.6.1.4.1.1466.115.121.1.40
   Single Value: FALSE
   Description:  A list of IP addresses, DNS names, domain, address ranges,
and subnets which partially specify right restrictions under an IP network
address constraint.
<WARNING 0x80072020: An operations error occurred.
>

hpqRoleIPRestrictionDefault
   OID:          1.3.6.1.4.1.232.1001.1.1.2.4
   Syntax:       1.3.6.1.4.1.1466.115.121.1.7
   Single Value: TRUE
   Description:  A Boolean representing access by unspecified clients which
partially specifies rights restrictions under an IP network address
```

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/ilo4.

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. Install Active Directory, DNS, and the root CA.
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 72).
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 46).
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 97).

For HP extended schema

1. Install Active Directory, DNS, and the root CA.
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/ilo4.
4. Extend the schema by using the Schema Extender.

   For more information, see "Schema required software" (page 276).
5. Install the HP LDAP component snap-ins.

   For more information, see "Schema required software" (page 276).
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 72).
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 "Managing the iLO network settings" (page 91).

NOTE: The LDAP component does not work with a Windows Server 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 282).

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 282).

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, 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 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

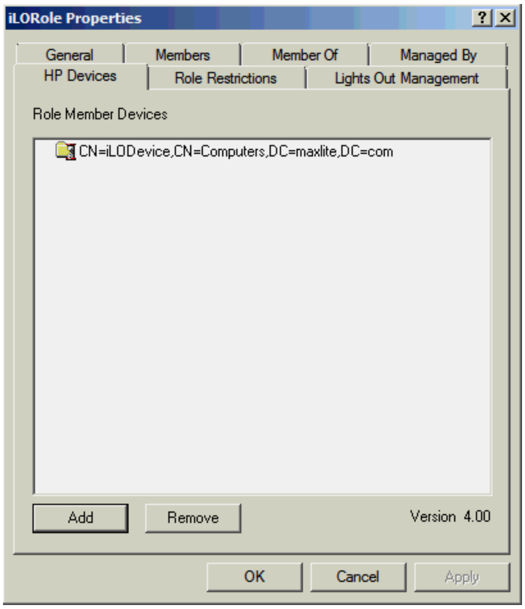
NOTE: After the snap-ins are installed, ConsoleOne and MMC must be restarted to show the new entries.

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 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.



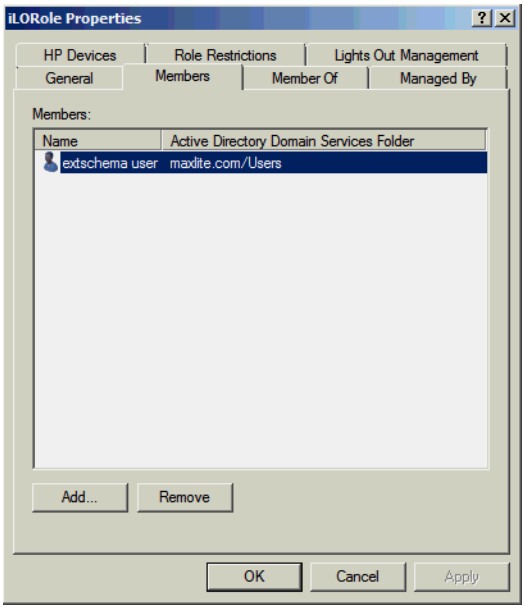
Role Member Devices

CN=iLODevice,CN=Computers,DC=maxlite,DC=com

Version 4.00

Members tab

After user objects are created, the **Members** tab 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.

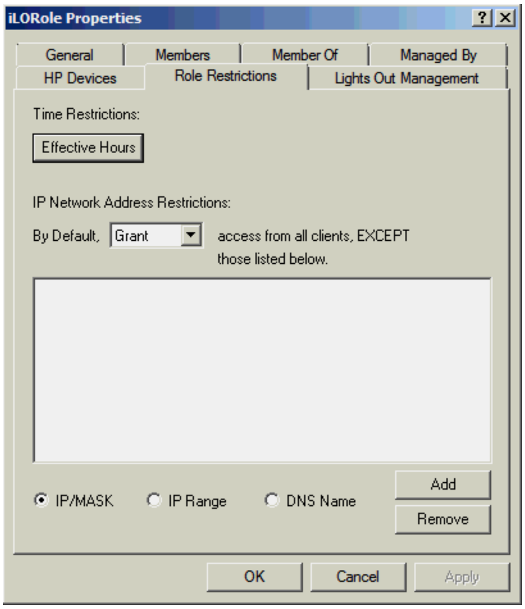


Members:

Name	Active Directory Domain Services Folder
extschema user	maxlite.com/Users

Role Restrictions tab

The **Role Restrictions** tab enables you to set restrictions for a role.



By Default, Grant access from all clients, EXCEPT those listed below.

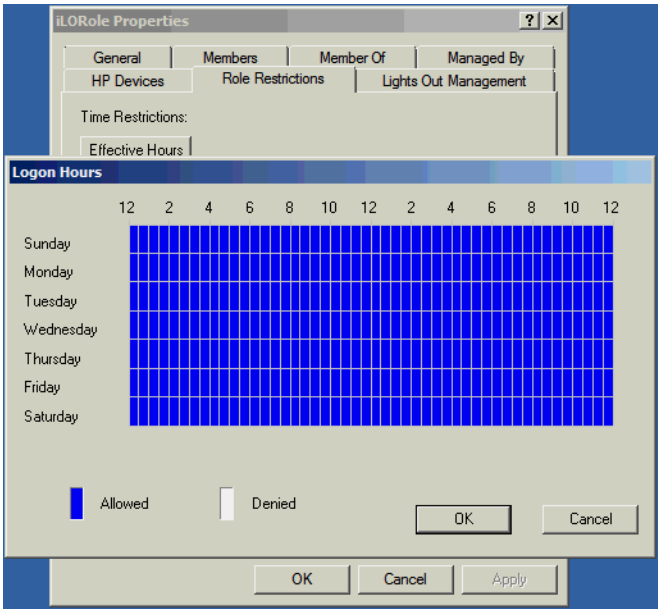
● IP/MASK ○ IP Range ○ DNS Name

The following restrictions can be configured:

- Time restrictions
- IP network address restrictions:
  - IP/mask
  - IP range
  - DNS name

Time restrictions

You can manage the hours available for logon by members of the role by clicking **Effective Hours** on the **Role Restrictions** tab.

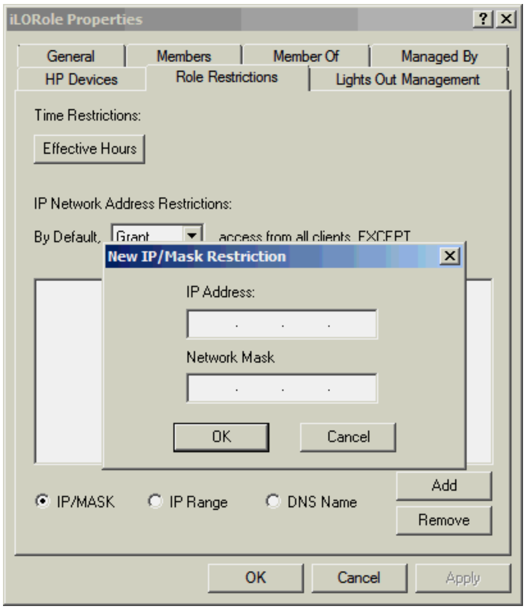


In the **Logon Hours** dialog box , you can select the times available for logon for each day of the week, in half-hour increments. You can change a single square by clicking it, or you can change a section of squares by clicking and holding the mouse button, dragging the cursor across the squares to be changed, and releasing the mouse button. The default setting is to allow access at all times.

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, enter the required information, and then click **OK**.

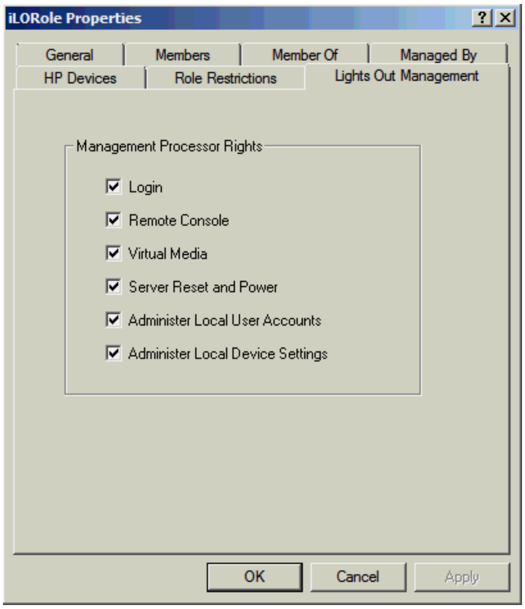


4. Click **OK** to save the changes and close the **Properties** dialog box.

To remove any of the entries, highlight the entry in the display list and click **Remove**.

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.



Management Processor Rights

☑ Login
☑ Remote Console
☑ Virtual Media
☑ Server Reset and Power
☑ Administer Local User Accounts
☑ Administer Local Device Settings

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 281), if a user is in both the `remoteAdmins` and `remoteMonitors` roles, they will have all available rights, because the `remoteAdmins` role has all rights.

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.

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

    Example: `HP\jsmith`
  - `username@domain` form

    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 about creating LOM device objects, see "Directory services" (page 265). 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 73). 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

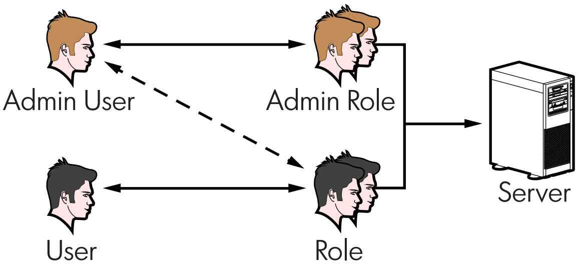
Most deployments do not require that the same user be in multiple roles managing the same device. However, these configurations are useful for building complex rights relationships. When users build multiple-role relationships, they receive all rights assigned by every applicable role. Roles can only 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.

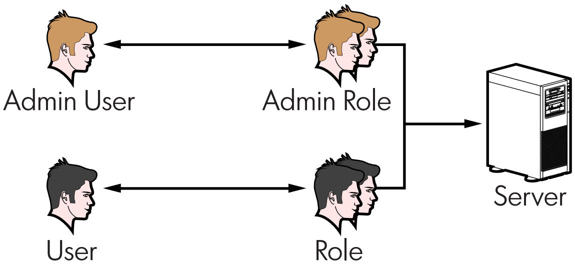
An Admin user gains the login right from the regular user role. Advanced rights are assigned through the Admin role, which assigns the advanced rights Server Reset and Remote Console (Figure 7).

Figure 7 Admin user



The Admin role assigns all Admin rights: Server Reset, Remote Console, and Login (Figure 8).

Figure 8 Admin role

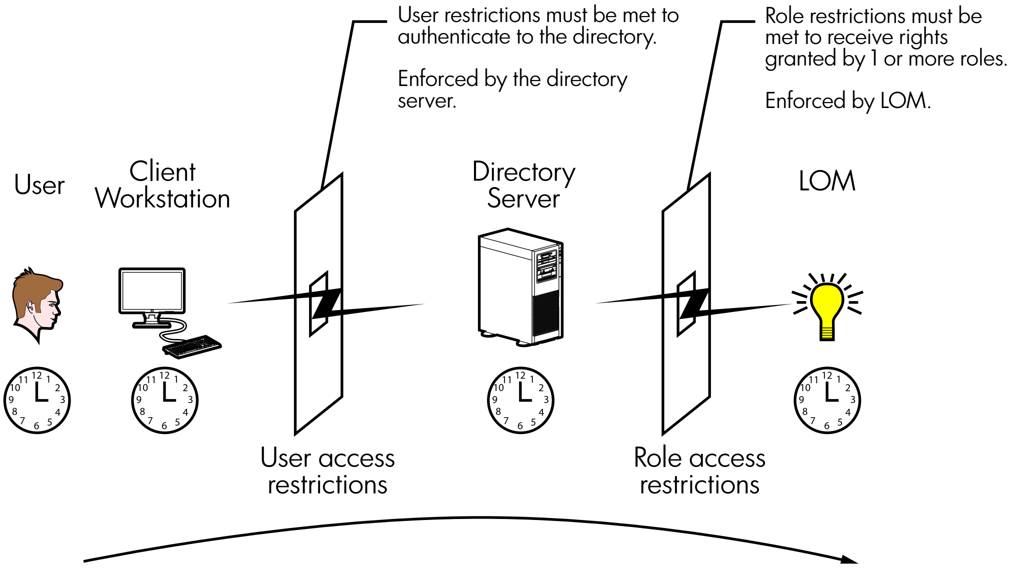


How directory login restrictions are enforced

Two sets of restrictions can limit a directory user's access to LOM devices (Figure 9).

- **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 9 Directory login restrictions


User restrictions must be met to authenticate to the directory.
Enforced by the directory server.
Role restrictions must be met to receive rights granted by 1 or more roles.
Enforced by LOM.
User
Client Workstation
Directory Server
LOM
User access restrictions
Role access 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 283).

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, 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.

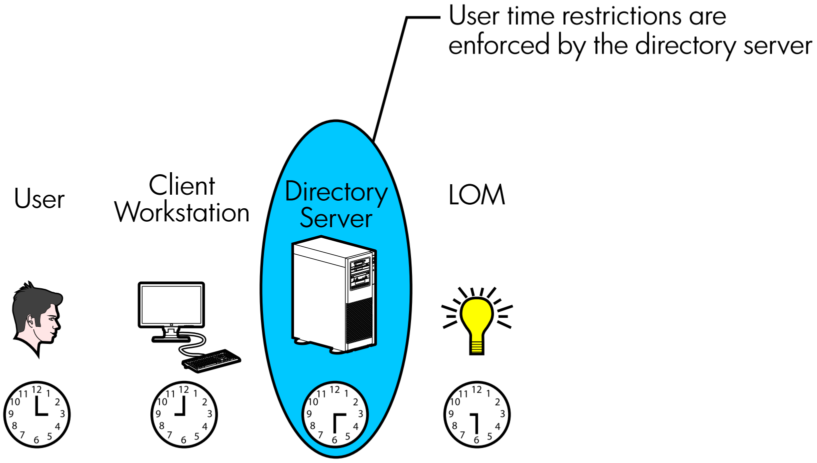
Using DNS-based restrictions can create security complications. Name service protocols are not secure. Any individual who has malicious intent and access to the network can place a rogue DNS service on the network and create a fake address restriction criterion. When implementing DNS-based address restrictions, be sure to take organizational security policies into consideration.

User time restrictions

Administrators can place a time restriction on directory user accounts (Figure 10). 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 10 User time restrictions



Creating multiple restrictions and roles

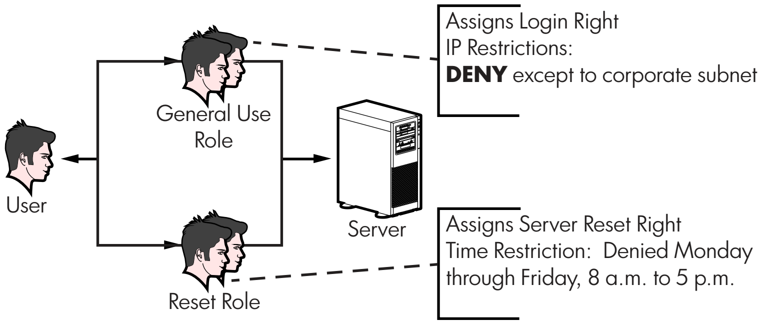
The most useful application of multiple roles is restricting one or more roles so that rights do not apply in all situations. Other roles provide different rights under different constraints. Using multiple restrictions and roles enables the administrator to create arbitrary, complex rights relationships 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 11 (page 291), security policy dictates that general use is restricted to clients in the corporate subnet, and server reset capability is restricted to after hours.

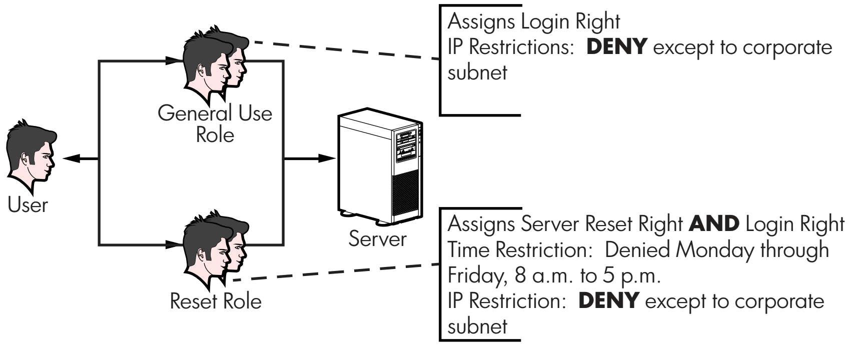
Figure 11 Creating restrictions and roles


Assigns Login Right
IP Restrictions:
DENY except to corporate subnet
General Use Role
User
Server
Assigns Server Reset Right
Time Restriction: Denied Monday through Friday, 8 a.m. to 5 p.m.
Reset Role

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 11) 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 12 (page 292).

Figure 12 Restricting the Reset and General Use roles



Assigns Login Right
IP Restrictions: **DENY** except to corporate subnet
General Use Role
User
Server
Assigns Server Reset Right **AND** Login Right
Time Restriction: Denied Monday through Friday, 8 a.m. to 5 p.m.
IP Restriction: **DENY** except to corporate subnet
Reset Role

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 294).

- **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 4 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 344).

HP Directories Support for ProLiant Management Processors utility

You can download this utility from http://www.hp.com/support/ilo4.

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

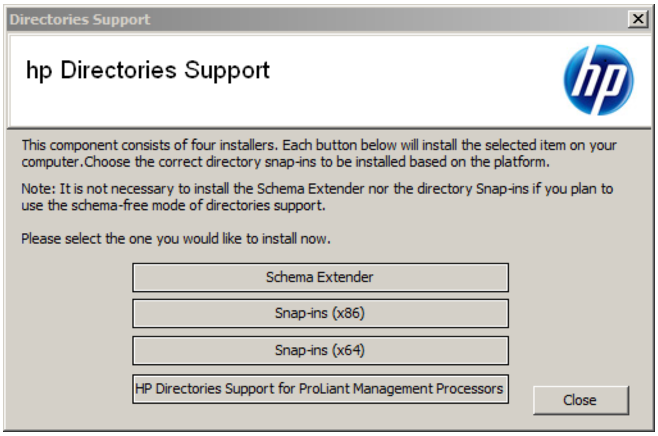
The HP Directories Support for ProLiant Management Processors utility operates on Microsoft Windows and requires the Microsoft .NET Framework. The utility supports the following operating systems:

- 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/ilo4. 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**.



This component consists of four installers. Each button below will install the selected item on your computer.Choose the correct directory snap-ins to be installed based on the platform.

Note: It is not necessary to install the Schema Extender nor the directory Snap-ins if you plan to use the schema-free mode of directories support.

Please select the one you would like to install now.

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.

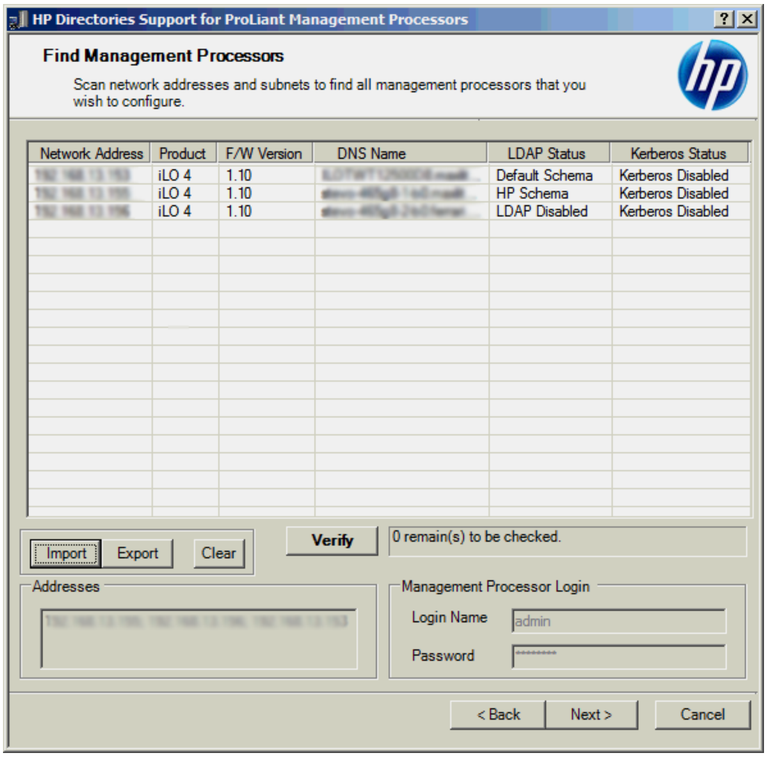
2. Click **Next**.

   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**.



HP Directories Support for ProLiant Management Processors

Find Management Processors

Scan network addresses and subnets to find all management processors that you wish to configure.

Network Address	Product	F/W Version	DNS Name	LDAP Status	Kerberos Status
[redacted]	iLO 4	1.10	[redacted]	Default Schema	Kerberos Disabled
[redacted]	iLO 4	1.10	[redacted]	HP Schema	Kerberos Disabled
[redacted]	iLO 4	1.10	[redacted]	LDAP Disabled	Kerberos Disabled

0 remain(s) to be checked.

Addresses: [redacted]

Management Processor Login

Login Name: admin

Password: ********

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**.

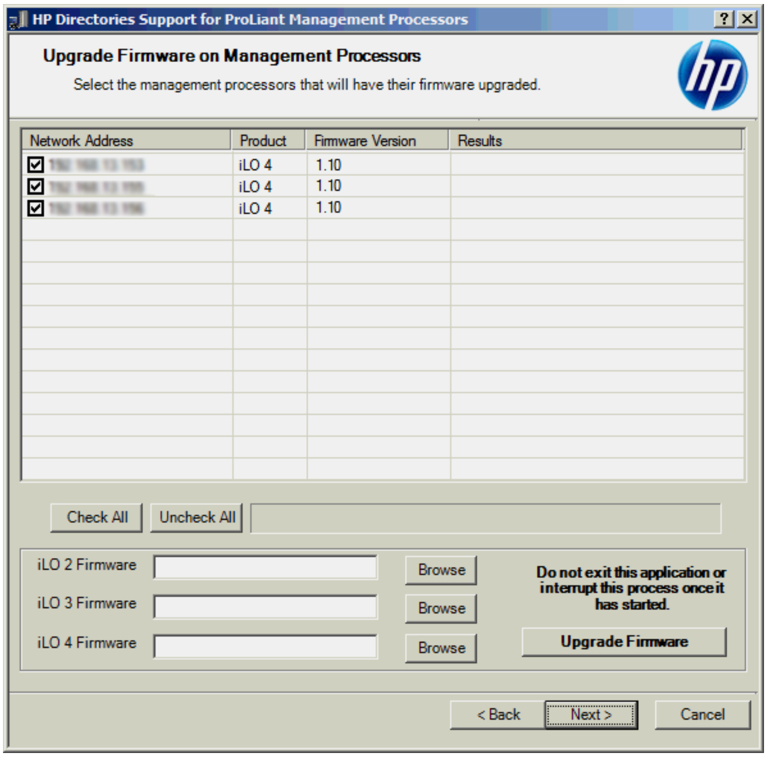
NOTE: Binary images of the firmware for the management processors must be accessible from the system that is running the migration utility. These binary images can be downloaded from http://www.hp.com/support/ilo4.

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.



HP Directories Support for ProLiant Management Processors

Upgrade Firmware on Management Processors

Select the management processors that will have their firmware upgraded.

Network Address	Product	Firmware Version	Results
☑ [redacted]	iLO 4	1.10	
☑ [redacted]	iLO 4	1.10	
☑ [redacted]	iLO 4	1.10	

Do not exit this application or interrupt this process once it has started.

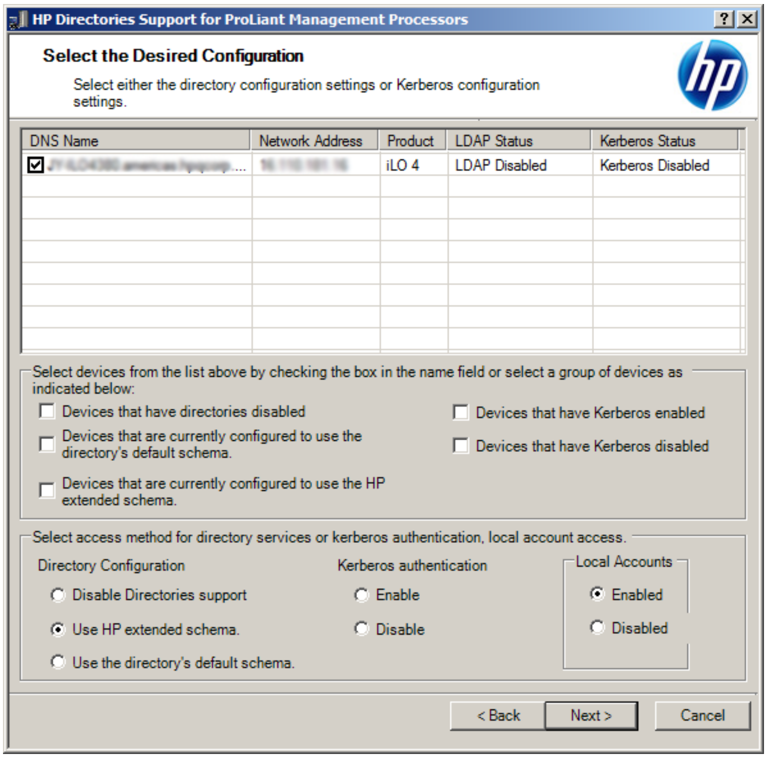
2. Select the management processors to upgrade.
3. For each discovered management processor type, enter the correct pathname to the firmware image or browse to the image.
4. Click **Upgrade Firmware**.

   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.



HP Directories Support for ProLiant Management Processors

Select the Desired Configuration

Select either the directory configuration settings or Kerberos configuration settings.

DNS Name	Network Address	Product	LDAP Status	Kerberos Status
☑ [redacted]	[redacted]	iLO 4	LDAP Disabled	Kerberos Disabled

Select devices from the list above by checking the box in the name field or select a group of devices as indicated below:

- □ Devices that have directories disabled
- □ Devices that are currently configured to use the directory's default schema.
- □ Devices that are currently configured to use the HP extended schema.
- □ Devices that have Kerberos enabled
- □ Devices that have Kerberos disabled

Select access method for directory services or kerberos authentication, local account access.

Directory Configuration
- ○ Disable Directories support
- ● Use HP extended schema.
- ○ Use the directory's default schema.

Kerberos authentication
- ○ Enable
- ○ Disable

Local Accounts
- ● Enabled
- ○ Disabled

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**.

To configure the management processor for directory services, see "Configuring directories when HP extended schema is selected" (page 298). To configure the management processor for Schema-free (default schema) directories support, see "Configuring directories when schema-free integration is selected" (page 302).

Naming management processors

The **Name the management processors** window 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

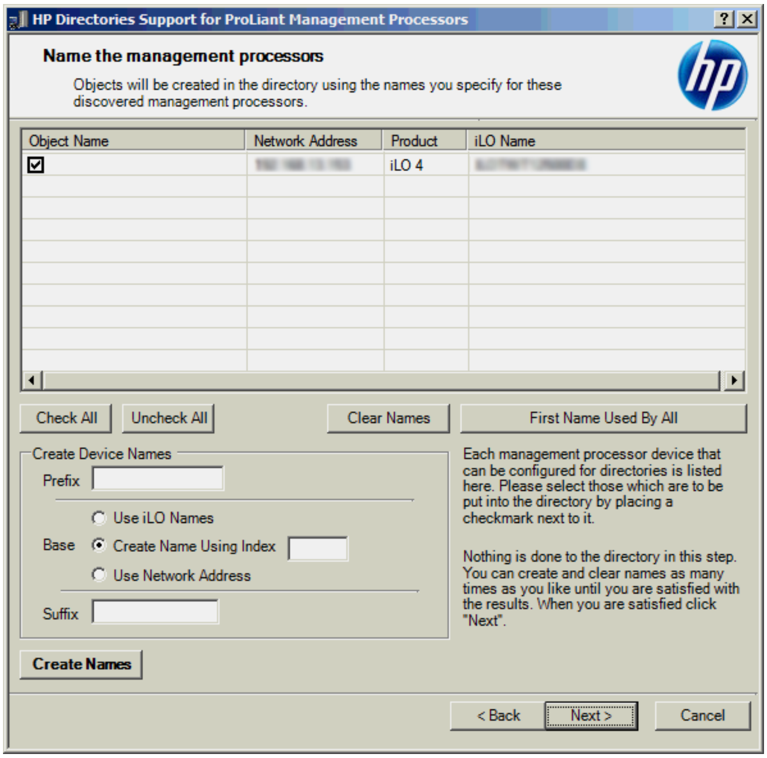
To name the management processors, click the **Object Name** column and enter the name, or do the following:

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**.



HP Directories Support for ProLiant Management Processors

Name the management processors

Objects will be created in the directory using the names you specify for these discovered management processors.

Object Name	Network Address	Product	iLO Name
☑	[redacted]	iLO 4	[redacted]

Create Device Names

Prefix

Base
○ Use iLO Names
● Create Name Using Index
○ Use Network Address

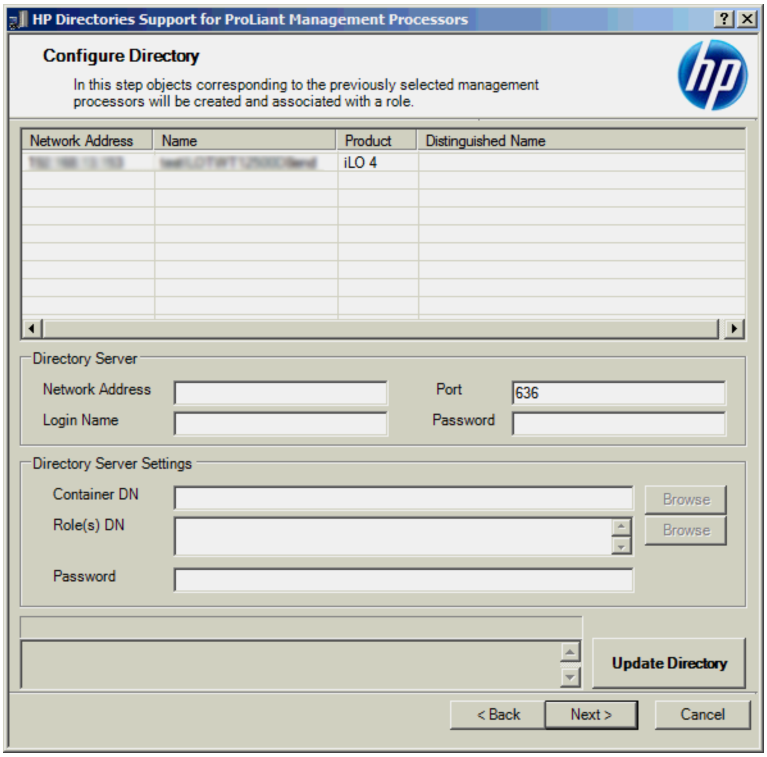
Suffix

Each management processor device that can be configured for directories is listed here. Please select those which are to be put into the directory by placing a checkmark next to it.

Nothing is done to the directory in this step. You can create and clear names as many times as you like until you are satisfied with the results. When you are satisfied click "Next".

Configuring directories when HP extended schema is selected

The **Configure Directory** window 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.



In this step objects corresponding to the previously selected management processors will be created and associated with a role.

Network Address	Name	Product	Distinguished Name
[redacted]	[redacted]	iLO 4	

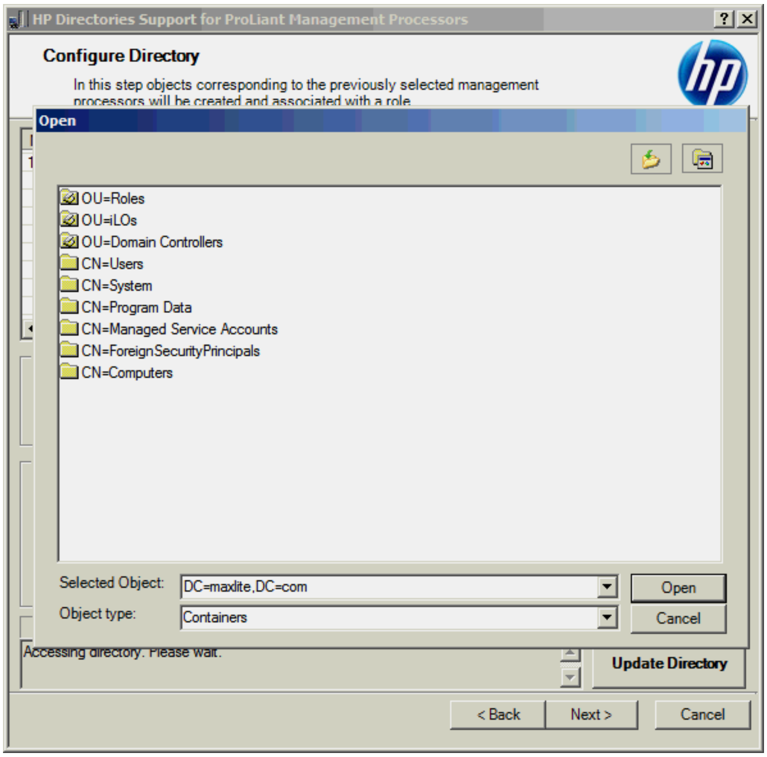
Port: 636

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(s) 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.

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** to select a container DN.



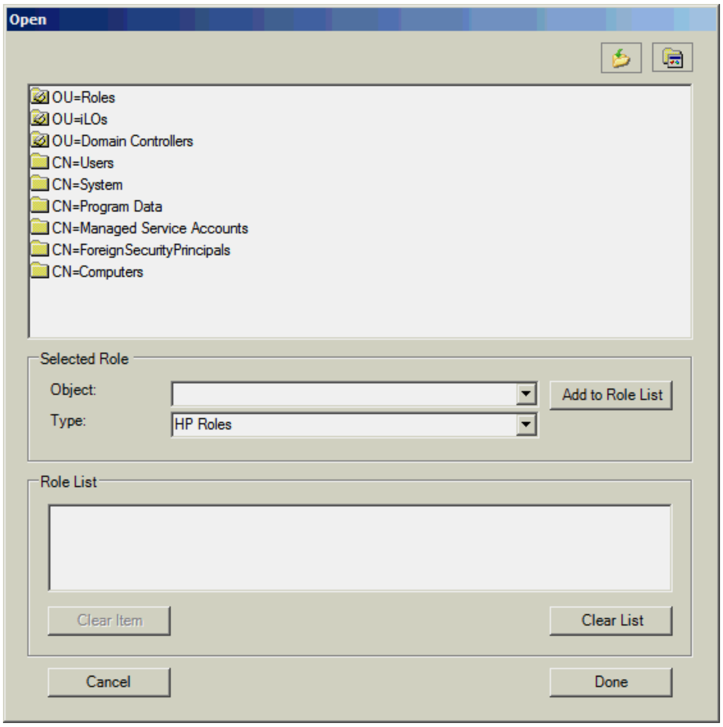
In this step objects corresponding to the previously selected management processors will be created and associated with a role.

Selected Object: DC=maxlite,DC=com

Object type: Containers

Accessing directory. Please wait.

3. Associate device objects with a member of a role by entering the role DN in the **Role(s) DN** box, or click **Browse** to select a role DN.



Object:

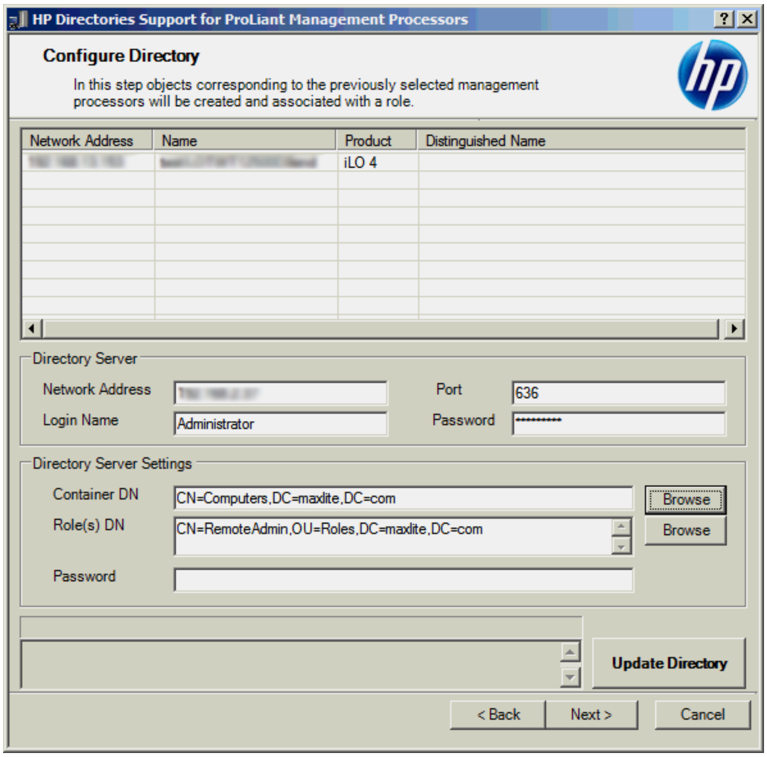
Type: HP Roles

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.



HP Directories Support for ProLiant Management Processors

Configure Directory

In this step objects corresponding to the previously selected management processors will be created and associated with a role.

Network Address	Name	Product	Distinguished Name
[redacted]	[redacted]	iLO 4	

Directory Server

Network Address: [redacted]

Port: 636

Login Name: Administrator

Password: *********

Directory Server Settings

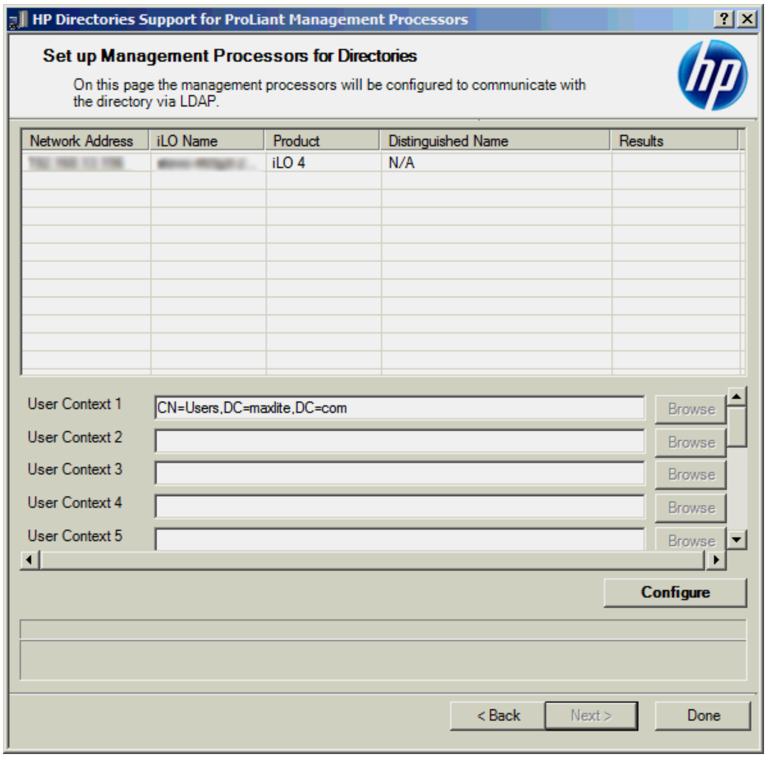
Container DN: CN=Computers,DC=maxlite,DC=com

Role(s) DN: CN=RemoteAdmin,OU=Roles,DC=maxlite,DC=com

Password:

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** to select user contexts.



HP Directories Support for ProLiant Management Processors

Set up Management Processors for Directories

On this page the management processors will be configured to communicate with the directory via LDAP.

Network Address	iLO Name	Product	Distinguished Name	Results
[redacted]	[redacted]	iLO 4	N/A	

User Context 1: CN=Users,DC=maxlite,DC=com

User Context 2:

User Context 3:

User Context 4:

User Context 5:

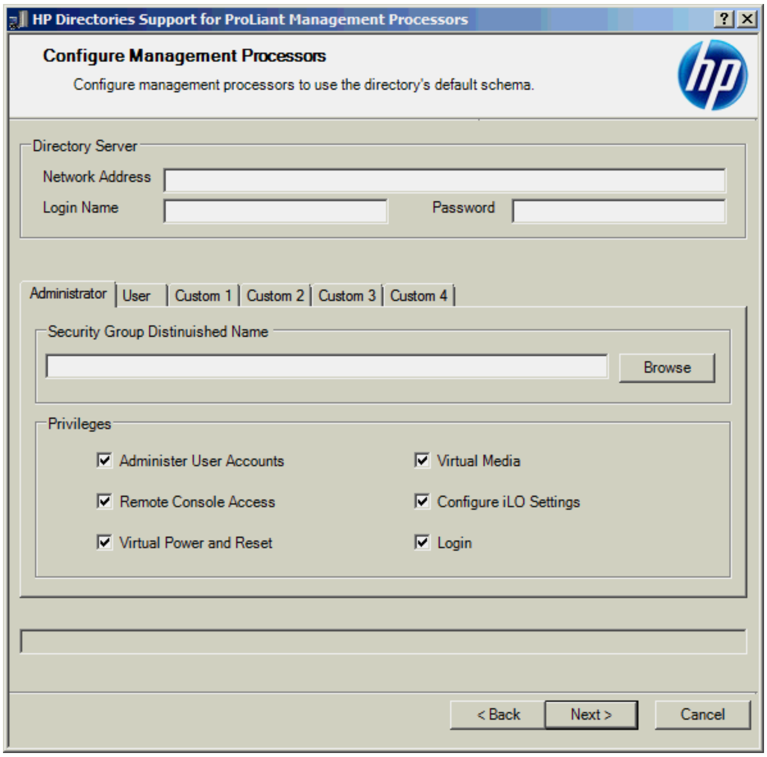
7. Click **Configure**, and then click **Done** when button is available.

Configuring directories when schema-free integration is selected

The boxes on the **Configure Management Processors** window 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.



HP Directories Support for ProLiant Management Processors

Configure Management Processors

Configure management processors to use the directory's default schema.

Directory Server

Network Address

Login Name

Password

Security Group Distinuished Name

Privileges

☑ Administer User Accounts

☑ Remote Console Access

☑ Virtual Power and Reset

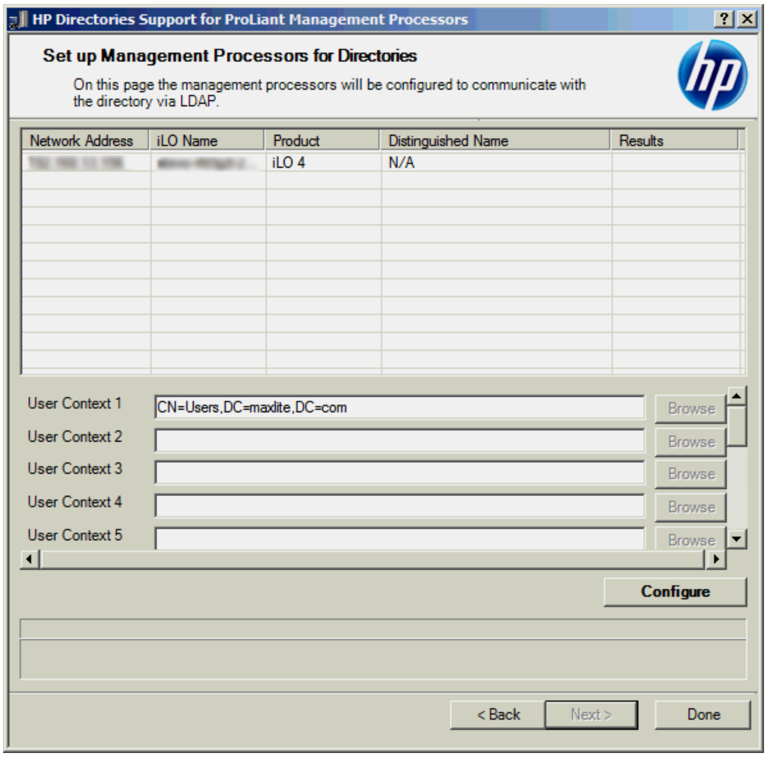
☑ Virtual Media

☑ Configure iLO Settings

☑ Login

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 enables you to create user contexts.



HP Directories Support for ProLiant Management Processors

Set up Management Processors for Directories

On this page the management processors will be configured to communicate with the directory via LDAP.

Network Address	iLO Name	Product	Distinguished Name	Results
[redacted]	[redacted]	iLO 4	N/A	

User Context 1: CN=Users,DC=maxlite,DC=com

User Context 2:

User Context 3:

User Context 4:

User Context 5:

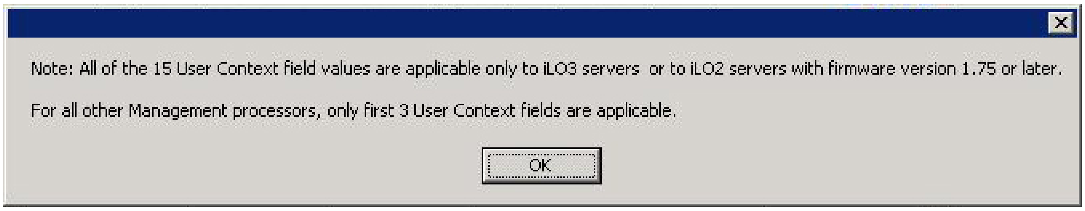
User contexts enable the user to use short names or user object names to log in, rather than the full DN. For example, having a user context such as `CN=Users,DC=iLOTEST2,DC=HP` enables user Elizabeth Bennett to log in using `Elizabeth Bennett` rather than `CN=Elizabeth Bennett,CN=Users, DC=iLOTEST2,DC=HP`. 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.

   When you click **Configure**, the utility might display a message similar to the following:



Note: All of the 15 User Context field values are applicable only to iLO3 servers or to iLO2 servers with firmware version 1.75 or later.

For all other Management processors, only first 3 User Context fields are applicable.

3. Click **OK** to continue.
4. When the process is complete, click **Done**.

7 Troubleshooting

This chapter provides troubleshooting solutions for HP iLO.

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 or UEFI System Utilities.
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 63) and "Administering SSH keys" (page 66).

   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.

General information

Using the HP ProLiant Pre-boot Health Summary

If an HP ProLiant Gen9 server will not start up, you can use iLO to display diagnostic information on an external monitor. This feature is supported on servers that support external video and have a UID button or an SUV connector. When the server is off and power is available, iLO runs on auxiliary power and can take control of the server video adapter to show the Pre-boot Health Summary.

To verify whether your server supports a UID button or an SUV connector, see your server *User Guide*.

To view the Pre-boot Health Summary:

1. Verify that the server is off and power is available.

2. Do one of the following:
   - Press the UID button on the server.

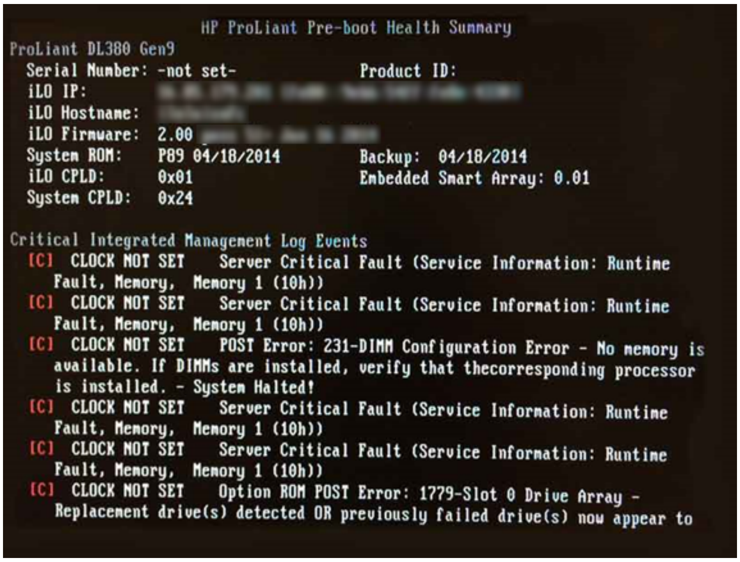
     △ **CAUTION:** To use this feature, press and release the UID button. Holding it down at any time for more than 5 seconds initiates a graceful iLO reboot or a hardware iLO reboot. Data loss or NVRAM corruption might occur during a hardware iLO reboot.

   - Log in to the iLO web interface, and change the UID state to **UID ON**.

     You can do this by clicking the UID icon at the bottom right corner of any iLO web interface window.

   - Plug in an SUV connector.

   The **HP ProLiant Pre-boot Health Summary** screen is displayed on the server monitor, and remains until the server is powered on, the UID state is changed to **UID OFF**, an SUV connector is removed, or an iLO reboot completes.



```
                   HP ProLiant Pre-boot Health Summary
ProLiant DL380 Gen9
  Serial Number: -not set-              Product ID:
  iLO IP:        [redacted]
  iLO Hostname:  [redacted]
  iLO Firmware:  2.00 [redacted]
  System ROM:    P89 04/18/2014         Backup:  04/18/2014
  iLO CPLD:      0x01                   Embedded Smart Array: 0.01
  System CPLD:   0x24

Critical Integrated Management Log Events
  [C]  CLOCK NOT SET    Server Critical Fault (Service Information: Runtime
     Fault, Memory,  Memory 1 (10h))
  [C]  CLOCK NOT SET    Server Critical Fault (Service Information: Runtime
     Fault, Memory,  Memory 1 (10h))
  [C]  CLOCK NOT SET    POST Error: 231-DIMM Configuration Error - No memory is
     available. If DIMMs are installed, verify that thecorresponding processor
     is installed. - System Halted!
  [C]  CLOCK NOT SET    Server Critical Fault (Service Information: Runtime
     Fault, Memory,  Memory 1 (10h))
  [C]  CLOCK NOT SET    Server Critical Fault (Service Information: Runtime
     Fault, Memory,  Memory 1 (10h))
  [C]  CLOCK NOT SET    Option ROM POST Error: 1779-Slot 0 Drive Array -
     Replacement drive(s) detected OR previously failed drive(s) now appear to
```

   The HP ProLiant Pre-boot Health Summary cannot be accessed when the UID is in the **BLINK** state, for example, if the remote console is in use, or a firmware update is in progress.

The following information is listed:

- Server model number
- Server serial number
- Product ID
- iLO IP address (IPv4 and IPv6)—This is displayed only if **Show iLO IP during POST** is set to **Enabled** on the **Administration**→**Access Settings** page in iLO.

  For more information, see "Configuring access options" (page 59).
- iLO Hostname
- iLO firmware version
- HP ProLiant System ROM version
- HP ProLiant System ROM – Backup version
- iLO CPLD version
- System CPLD version

- Embedded Smart Array version number—This value is displayed only if server POST has successfully completed since the last auxiliary power cycle.
- **Critical** events—The most recent **Critical** events from the IML are displayed, with the most recent event displayed first.

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.

Testing the SSL connection to a server

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 weblog, 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.

Rebooting (Resetting) iLO

In some cases, it might be necessary to reboot iLO; for example, if iLO is not responding to the browser.

Rebooting iLO does not make any configuration changes, but ends all active connections to iLO.

ⓘ **IMPORTANT:** The iLO web interface and the ROM-based setup utilities sometimes uses the term iLO reset to mean an iLO reboot.

To reboot 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 180).
- Use the CLI or HPONCFG. For instructions, see the *HP iLO 4 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.
- Use the iLO 4 Configuration Utility. The iLO 4 Configuration Utility is available only on servers that support UEFI. For instructions, see "Resetting iLO by using the iLO 4 Configuration Utility" (page 309).
- Use the UID button on supported HP ProLiant Gen9 servers. For instructions, see "Rebooting iLO with the server UID button" (page 311).

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 by using the iLO 4 Configuration Utility

If iLO is slow to respond, you can use the iLO 4 Configuration Utility **Reset iLO** menu to perform a reset.

Resetting iLO does not make any configuration changes, but it ends all active connections to iLO. You must have the Configure iLO Settings privilege to reset iLO using this method.

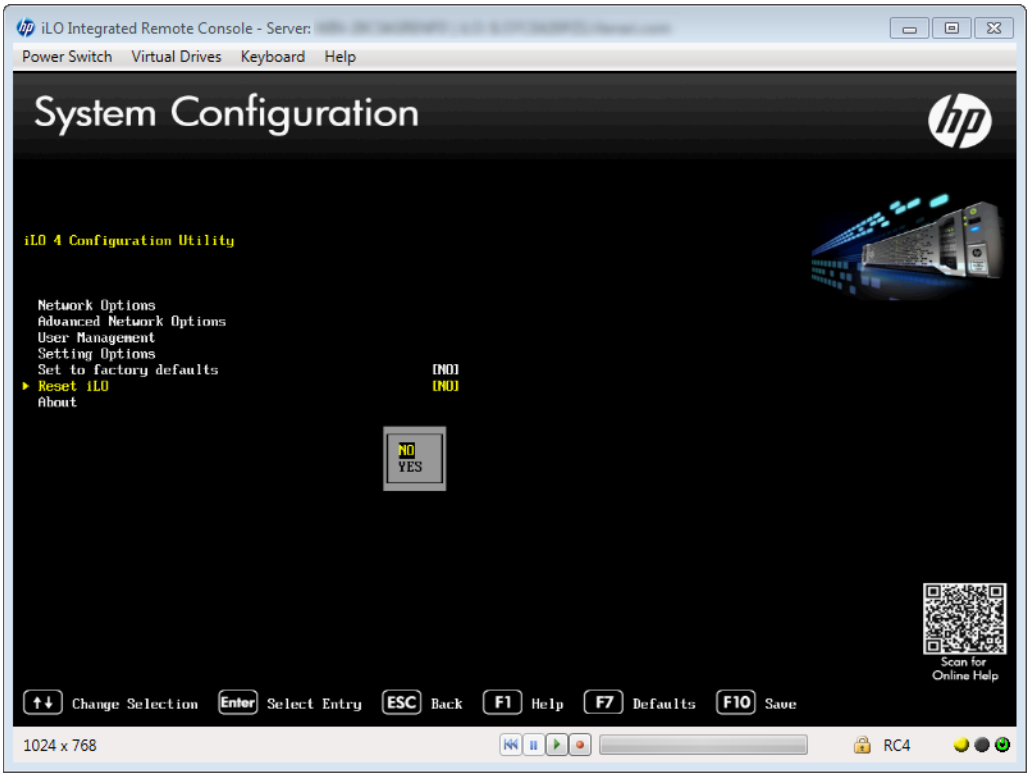
To reset iLO:

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 Utilities** screen appears.
4. From the **System Utilities** screen, select **System Configuration→iLO 4 Configuration Utility→Reset iLO**.

   The iLO 4 Configuration Utility prompts you to select **YES** or **NO**.



iLO Integrated Remote Console - Server: [redacted]

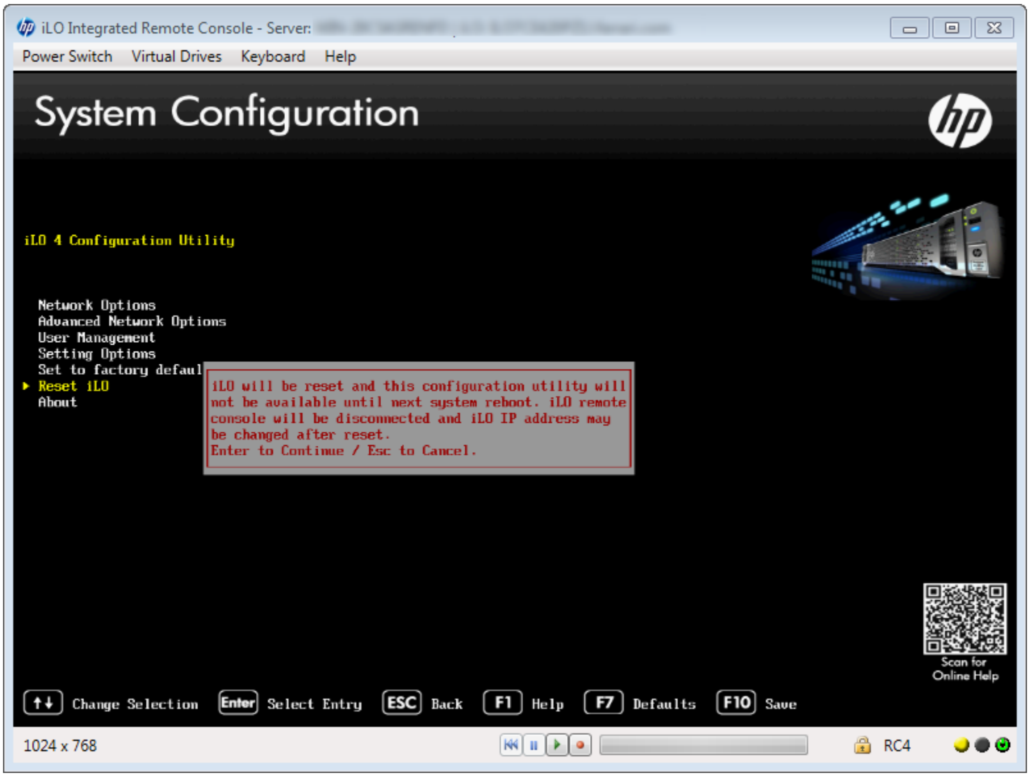
System Configuration

iLO 4 Configuration Utility

```
Network Options
Advanced Network Options
User Management
Setting Options
Set to factory defaults                    [NO]
▸ Reset iLO                                [NO]
About

                    NO
                    YES
```

5. Select **YES**, and then press **Enter**.

   The iLO 4 Configuration Utility prompts you to confirm the reset request.



iLO Integrated Remote Console - Server: [redacted]

System Configuration

iLO 4 Configuration Utility

```
Network Options
Advanced Network Options
User Management
Setting Options
Set to factory defaul
▸ Reset iLO
About
```

```
iLO will be reset and this configuration utility will
not be available until next system reboot. iLO remote
console will be disconnected and iLO IP address may
be changed after reset.
Enter to Continue / Esc to Cancel.
```

When you reset iLO, the iLO 4 Configuration Utility is not available again until the next reboot.

6. Press **Enter**.

   iLO resets. If you are managing iLO remotely, the remote console session is automatically ended.

7. Resume the boot process:
   a. Optional: If you are managing iLO remotely, wait for the iLO reset to finish, and then start the iLO remote console.

      The UEFI System Utilities are still open from the previous session.
   b. Press **Esc** until the main menu is displayed.
   c. Select **Exit and Resume Boot** in the main menu, and then press **Enter**.
   d. When prompted to confirm the request, press **Enter** to exit the utility and resume the normal boot process.

Rebooting iLO with the server UID button

The UID button on ProLiant Gen9 servers (if present) can be used to initiate a manual reboot of iLO.

There are two types of iLO reboots:

- **Graceful iLO reboot**—An iLO reboot is initiated by the iLO firmware. To use this feature, press and hold the UID button for 5 to 10 seconds.

  The UID button/LED flashes blue 4 Hz/cycle per second to indicate that a graceful iLO reboot is in progress.

  Initiating a graceful iLO reboot 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 reboot iLO until the process is finished.

- **Hardware iLO reboot**—An iLO reboot is initiated by the ProLiant hardware. To use this feature, press and hold the UID button for more than 10 seconds.

  The UID button/LED flashes blue 8 Hz/cycle per second to indicate that an iLO hardware reboot is in progress.

△ **CAUTION:** Initiating a hardware iLO reboot does not make any configuration changes, but ends all active connections to iLO. If a firmware flash is in progress, it is interrupted, which might cause data corruption on the flash device. If this happens, use the recovery method described in "iLO network Failed Flash Recovery" (page 334).

Data loss or NVRAM corruption might occur during a hardware iLO reboot.

Do not initiate a hardware reboot if other troubleshooting options are available.

For more information about the UID button, see the *User Guide* for your server at the following website: http://www.hp.com/support/proliantgen9/docs.

Resetting iLO to the factory default settings

In some cases, you might need to reset iLO to the factory default settings. For example, you must reset iLO to the default settings when you disable FIPS mode. You can use the iLO RBSU or the UEFI system utilities to perform this task.

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 4 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.

Resetting iLO to the factory default settings by using the iLO 4 Configuration Utility

You can use the iLO 4 Configuration Utility **Set to Factory Defaults** menu to reset iLO to the factory default settings.

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.

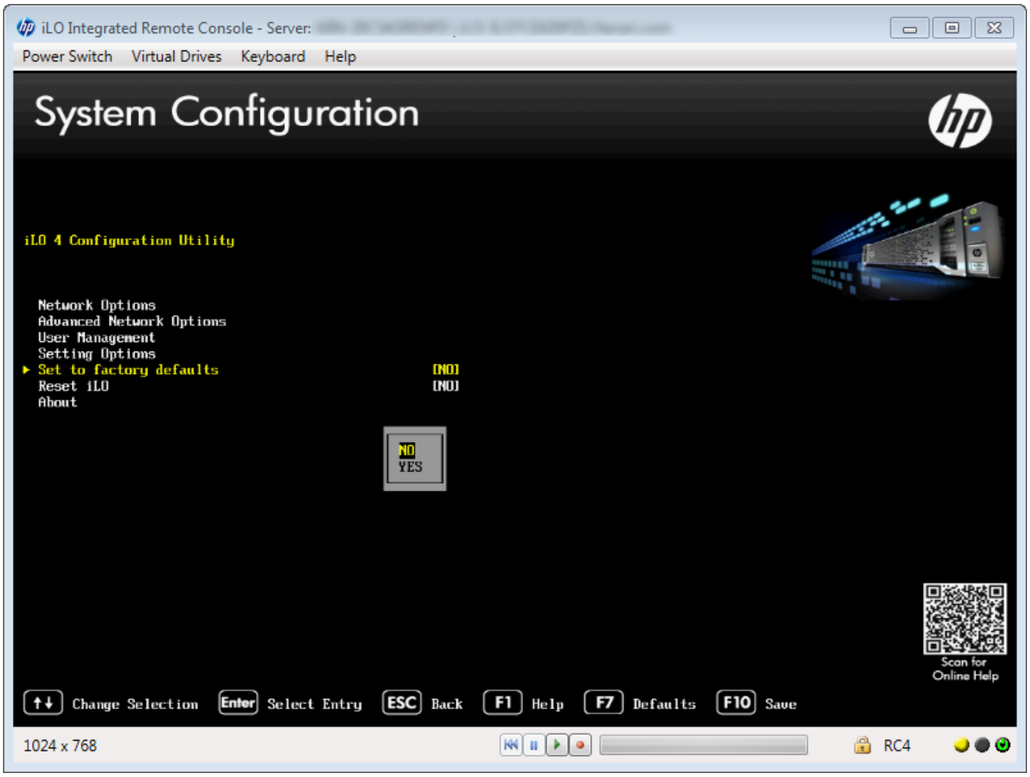
   You can use the .NET IRC or Java IRC.

2. Restart or power on the server.
3. Press **F9** in the HP ProLiant POST screen.

   The **System Utilities** screen appears.

4. From the **System Utilities** screen, select **System Configuration**→**iLO 4 Configuration Utility**→**Set to factory defaults**.

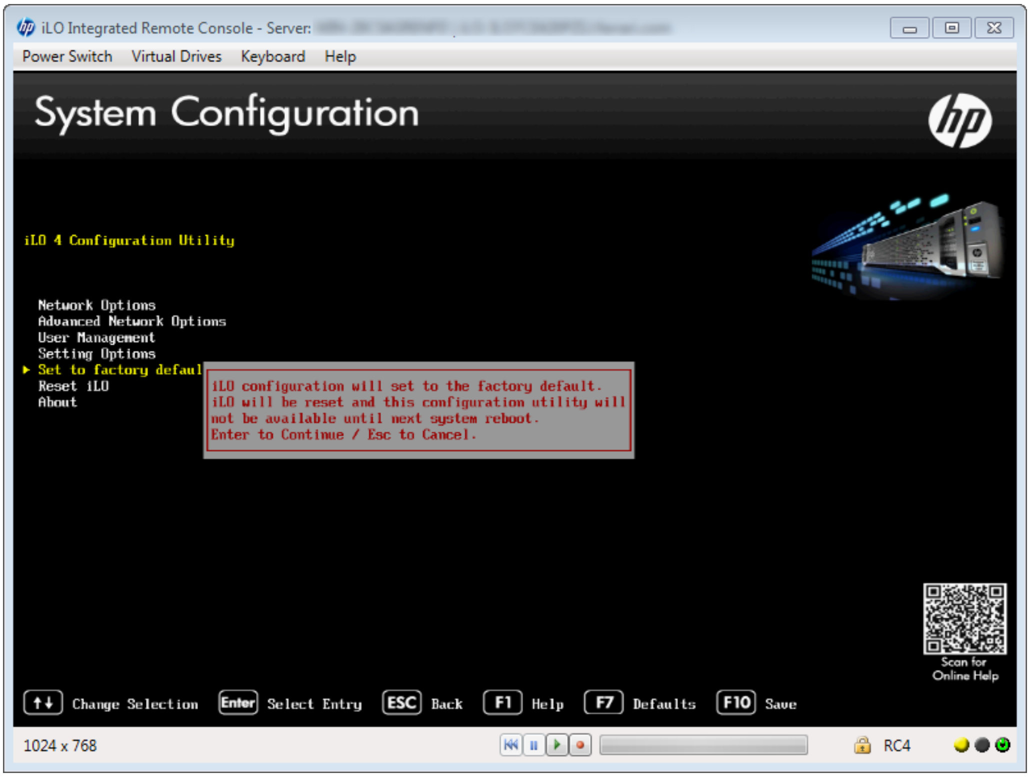
   The iLO 4 Configuration Utility prompts you to select **YES** or **NO**.



```
iLO 4 Configuration Utility

  Network Options
  Advanced Network Options
  User Management
  Setting Options
▸ Set to factory defaults                        [NO]
  Reset iLO                                      [NO]
  About

                         NO
                         YES
```

5. Select **YES**, and then press **Enter**.

   The iLO 4 Configuration Utility prompts you to confirm the reset request.



```
iLO 4 Configuration Utility

  Network Options
  Advanced Network Options
  User Management
  Setting Options
▸ Set to factory defaul
  Reset iLO
  About

iLO configuration will set to the factory default.
iLO will be reset and this configuration utility will
not be available until next system reboot.
Enter to Continue / Esc to Cancel.
```

The iLO system is reset, and you cannot access the iLO 4 Configuration Utility until after the next system reboot.

You can press **Enter** to confirm, or press **Esc** to cancel.

6. Press **Enter**.

   iLO resets to the factory default settings. If you are managing iLO remotely, the remote console session is automatically ended.

7. Resume the boot process:

   a. Optional: If you are managing iLO remotely, wait for the iLO reset to finish, and then start the iLO remote console.

      The iLO 4 Configuration Utility screen is still open from the previous session.

   b. Press **Esc** until the main menu is displayed.

   c. Select **Exit and Resume Boot** in the main menu, and then press **Enter**.

   d. When prompted to confirm the request, press **Enter** to exit the screen and resume the boot process.

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.

Event log entries

Table 8 (page 314) lists typical iLO event log entries.

Table 8 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.
`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.

Table 8 Event log entries *(continued)*

Event log entry	Description
`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.
`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.

Table 8 Event log entries *(continued)*

Event log entry	Description
`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 iLO 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.
`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.

Table 8 Event log entries *(continued)*

Event log entry	Description
`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 label 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, the iLO 4 Configuration Utility, or the iLO web interface. For more information, see "Setting up iLO by using iLO RBSU or the iLO 4 Configuration Utility" (page 21) or "Setting up iLO by using the iLO web interface" (page 33).

Login issues

Use the following information when attempting to resolve login issues:

- Try using the default account information, which is located on the serial label 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 4 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 46).

NOTE: The iLO RBSU or iLO 4 Configuration Utility can also be used to configure user accounts. For instructions, see “Adding user accounts” (page 26) or “Adding user accounts” (page 29).

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, the iLO 4 Configuration Utility, or iLO web interface. For more information, see “Setting up iLO by using iLO RBSU or the iLO 4 Configuration Utility” (page 21) or .

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 non-dynamic 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.

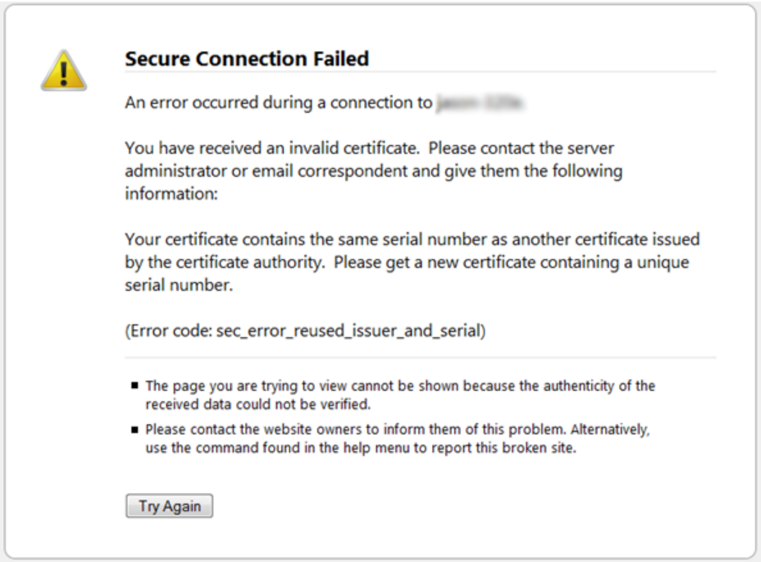
If the iLO processor is reset and the server is immediately reset, iLO firmware might not be fully initialized when the server performs its initialization and attempts to start the iLO RBSU. In this case, the iLO RBSU is unavailable, or the iLO option ROM code is skipped altogether.

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.



Secure Connection Failed

An error occurred during a connection to [redacted]

You have received an invalid certificate. Please contact the server administrator or email correspondent and give them the following information:

Your certificate contains the same serial number as another certificate issued by the certificate authority. Please get a new certificate containing a unique serial number.

(Error code: sec_error_reused_issuer_and_serial)

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem. Alternatively, use the command found in the help menu to report this broken site.

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 .

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 or the iLO 4 Configuration Utility 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 69).

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 57).

Troubleshooting alert and trap issues

Table 9 (page 321) lists the alerts and traps that might occur.

Table 9 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.

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 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 72).

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
```

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.

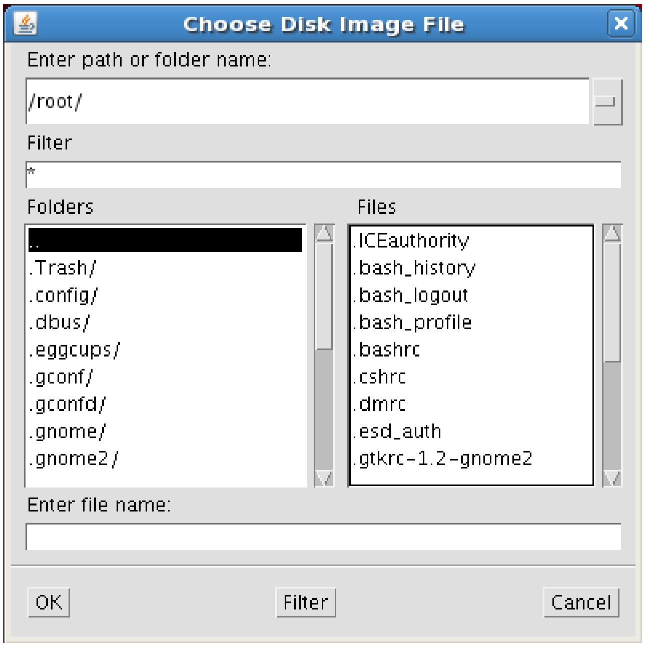
Java IRC does not display correct floppy and USB-key device

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.



Enter path or folder name: /root/

Filter: *

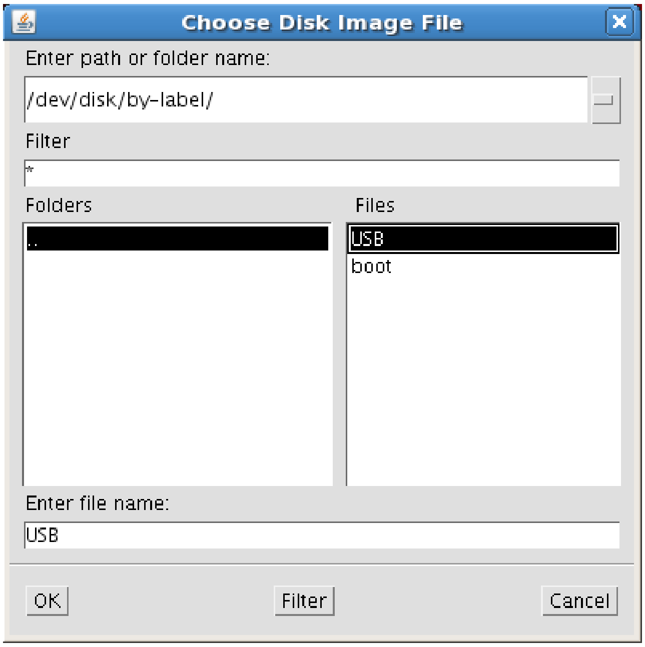
Folders:
..
.Trash/
.config/
.dbus/
.eggcups/
.gconf/
.gconfd/
.gnome/
.gnome2/

Files:
.ICEauthority
.bash_history
.bash_logout
.bash_profile
.bashrc
.cshrc
.dmrc
.esd_auth
.gtkrc-1.2-gnome2

Enter file name:

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.



Enter path or folder name: /dev/disk/by-label/

Filter: *

Folders:
..

Files:
USB
boot

Enter file name: USB

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 206).

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, or use the Remote Console Acquire feature. For more information, see "Acquiring the Remote Console" (page 206).

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.

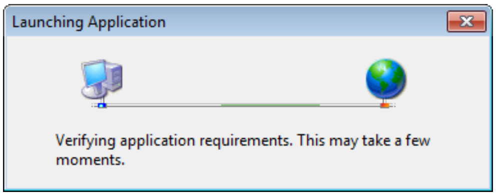
△ **CAUTION:** Do not use Windows Explorer to refresh the contents of the USB key.

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 **Launching Application** dialog box appears and remains on the screen for a long time.



Launching Application

Verifying application requirements. This may take a few moments.

Solution:

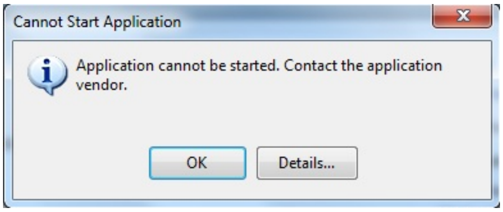
1. Open Internet Explorer.
2. Select **Tools**→**Internet Options**.

   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 **Cannot Start Application** dialog box appears.

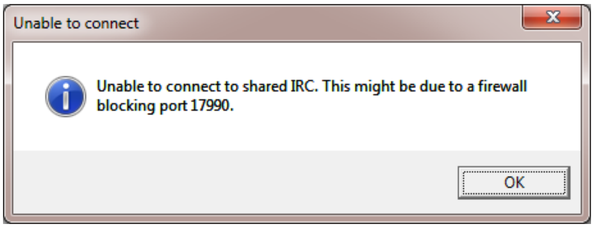

Cannot Start Application

Application cannot be started. Contact the application vendor.

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 **Unable to connect** dialog box appears.


Unable to connect

Unable to connect to shared IRC. This might be due to a firewall blocking port 17990.

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).

.NET IRC launch is blocked by Google Chrome

When you launch the .NET IRC in the Chrome browser, the application might fail to start.

If the iLO system is using the default iLO SSL certificate, which is not a trusted certificate that is signed by a certificate authority, the iLO web interface starts the .NET IRC by using HTTP instead of HTTPS. Since the iLO web interface uses HTTPS, and the web interface starts the IRC by using HTTP, the Chrome browser displays a warning.

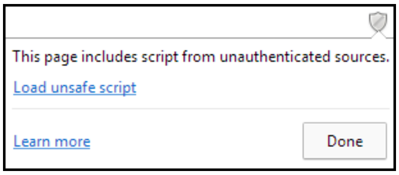
Solution: Do one of the following:

- **Solution 1 (most secure)**: Import an SSL certificate into iLO and enable the **IRC Requires a Trusted Certificate in iLO** setting on the **Administration**→**Security**→**Remote Console** page.

  For information about importing certificates, see "Administering SSL certificates" (page 69).

For information about changing the **IRC Requires a Trusted Certificate in iLO** setting, see "Configuring the Integrated Remote Console Trust setting (.NET IRC)" (page 89).

- **Solution 2**: Click the shield icon in the Chrome address bar, and then click the **Load unsafe script** link.



This page includes script from unauthenticated sources.

The warning might vary depending on your browser version.

- **Solution 3**: Use a different browser.
- **Solution 4 (least secure)**: Use the following command line flag to configure Chrome to stop checking for insecure content: `--allow-running-insecure-content`.

IMPORTANT: If you use this flag, insecure content will be allowed on all web pages. For more information, see the Chrome documentation.

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 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 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 Remote Support issues

SSL Bio Error during Insight RS registration

Issue: The following error occurs when you try to register an HP ProLiant server with Insight RS: `SSL Bio Error.`

Solution: Navigate to the **Information**→**Diagnostics** page in the iLO web interface, and then click **Reset iLO**. When the reset is finished, log in to the iLO web interface and retry the registration procedure.

Clicking **Reset iLO** does not make any configuration changes, but it terminates any active connections to iLO and completes any firmware updates in progress. You must have the Configure iLO Settings privilege to reset iLO on the **Diagnostics** page.

HP ProLiant Gen8 or Gen9 server identified in Insight Online as <product name>_<serial number> and in Insight RS as <serial number>

Issue: If a server is registered for Insight Remote Support before iLO discovers the server name, Insight Online assigns a server name in the format <product name>_<serial number>, and Insight RS identifies the server by its serial number.

Solution: Use the following procedure to display a user-friendly server name in Insight Online and the Insight RS Console:

1. Do one of the following:
   - Verify that AMS is enabled and the operating system is running.
   - Update the **Server Name** on the **Administration→Access Settings** page in the iLO web interface.
   - For Windows systems only, start the operating system. Insight Online and Insight RS will use the Windows computer name to identify the server.
2. For Insight Remote Support central connect only: Depending on your configuration, do one of the following:
   - For configurations with iLO firmware 1.30 or later, no additional action is required. iLO automatically detects the server name and forwards it to Insight RS and Insight Online for display.
   - HP ProLiant Gen8 servers only: For configurations with iLO firmware versions earlier than 1.30, the server name is updated automatically the next time data collection information is transmitted. Data collection occurs every 30 days and can be initiated immediately from the **Remote Support→Data Collections** page in the iLO web interface. For instructions, see "Sending data collection information" (page 131).
3. If you were logged in to Insight Online when you performed Step 1, click the refresh button (labeled **Devices**) to update the Insight Online view with the server information.

HP ProLiant Gen8 or Gen9 server operating system name and version not listed in Insight RS or Insight Online

Issue: If a server is registered for Remote Support when the operating system and AMS are not running (for example, during an Intelligent Provisioning registration), iLO is unable to determine which operating system is installed. To update the Insight RS and Insight Online operating system information, iLO must acquire the operating system information from AMS.

Solution: Use the following procedure:

1. Verify the following:
   - For HP ProLiant Gen8 servers: iLO firmware 1.20 or later (Insight Remote Support central connect) or 1.40 or later (Insight Online direct connect) is installed.
   - For HP ProLiant Gen9 servers: iLO firmware 2.00 or later is installed.
   - AMS is enabled and the operating system is running.
   - For Insight Remote Support central connect only: Verify that a supported version of Insight RS is installed on the Hosting Device. For more information, see http://h17007.www1.hp.com/us/en/enterprise/servers/supportmatrix/insight_rs.aspx.
   - For Insight Remote Support central connect only: Verify that the RIBCL credentials for the server have been entered in the Insight RS Console and are associated with the HP ProLiant server.

2. Initiate the data collection process from the **Remote Support→Data Collections** page in the iLO web interface. For instructions, see "Sending data collection information" (page 131). The operating system name and version are forwarded to Insight RS and Insight Online during the data collection process.
3. If you were logged in to Insight Online when you performed Step 2, click the refresh button (labeled **Devices**) to update the Insight Online view with the server information.

When using Insight Online, the operating system name and version are listed on the **Device Configuration Details** page if AMS is installed and the operating system was running during the most recent data collection transmission.

Connection error during iLO Insight Online direct connect registration

Issue: The following error occurs when you try to register an HP ProLiant server for Insight Online direct connect: `Cannot connect to remote host.`

Solution: Verify that DNS information is configured in iLO.

For instructions, see "Managing the iLO network settings" (page 91).

iLO session ends unexpectedly during iLO Insight Online direct connect registration

Issue: The iLO web interface session ends unexpectedly with the error `Session Expired` when you try to register an HP ProLiant server for Insight Online direct connect.

Solution: Verify that the DNS settings are configured correctly in iLO. Depending on your network configuration, you can view and change these settings on the following iLO web interface pages:

- **Network→iLO Dedicated Network Port→IPv4**
- **Network→iLO Dedicated Network Port→IPv6**
- **Network→Shared Network Port→IPv4**
- **Network→Shared Network Port→IPv6**

HP remote support registration fails on servers that use NIC teaming

Issue: An HP ProLiant Gen8 or Gen9 server that uses NIC teaming on Ethernet port 0 cannot be registered for HP remote support.

Cause: NIC teaming is not supported with the iLO 4 Embedded Remote Support feature.

Troubleshooting iLO Federation Management issues

Query errors occur on iLO Federation pages

Issue: When you open an iLO Federation page, iLO peers and associated data might be missing from the page, and the following error is displayed:

```
Errors occurred during query, returned data may be incomplete or
inconsistent.
```

This error might occur when a network communication error, configuration problem, or failed iLO system prevents the retrieval of data from all systems in an iLO Federation group.

Solution 1: Wait for twice the configured multicast interval, and then refresh the iLO Federation page. If an iLO system was reconfigured and can no longer communicate with the local iLO system, it will be dropped from its peer relationships after they expire. This should eliminate the query error.

Solution 2: Check the **Multi-System Map** page for errors. This page can help you identify communication problems between iLO peers. For more information, see "Viewing the iLO Federation Multi-System Map" (page 187), "A 502 error is displayed on the Multi-System Map page" (page

332), “A timeout error is displayed on the Multi-System Map page” (page 332), and “A 403 error is displayed on the Multi-System Map page” (page 332).

Solution 3: If you are using server blades in an enclosure, verify that **Enclosure iLO Federation Support** is configured on the **Enclosure Settings**→**Network Access**→**Protocols** page in the Onboard Administrator web interface. You must have Onboard Administrator 4.11 or later to configure this setting. This is required to allow peer-to-peer communication between the server blades in an enclosure. For more information, see “Configuring enclosure support for iLO Federation” (page 56).

Solution 4: Verify that the switches in the network are configured to allow communication between iLO peers. For more information, see “iLO Federation network requirements” (page 52).

Solution 5: If you recently changed the network routes, subnet mask, IP address, or HTTP port for an iLO peer, verify that the iLO peer has a communication path to the local iLO system.

For more information about iLO network settings, see .

For more information about the iLO HTTP port setting, see “Configuring iLO access settings” (page 57).

Solution 6: Ensure that communication between the local iLO system and the peer with the error is not blocked by an intermediate firewall or a change to the iLO network configuration and HTTP port setting.

A timeout error is displayed on the Multi-System Map page

Issue: The **Multi-System Map** page might display a `Timed Out` error for a peer of the local iLO system in the following situations:

- A peer of the local iLO system has a peer that has failed.
- An intermediate firewall is preventing communication between the local iLO system and a peer.
- Network configuration changes are preventing communication between the local iLO system and a peer.
- The enclosure that contains the peer is not configured for iLO Federation support.

Solution 1: Remove or repair the failed peer.

Solution 2: Verify that the network is configured to allow communication between the iLO peers.

Solution 3: Verify that the enclosure that contains an iLO server blade peer is configured for iLO Federation support on the **Enclosure Settings**→**Network Access**→**Protocols** page in the Onboard Administrator web interface. You must have Onboard Administrator 4.11 or later to configure this setting. This is required to allow peer-to-peer communication between the server blades in an enclosure. For more information, see “Configuring enclosure support for iLO Federation” (page 56).

A 502 error is displayed on the Multi-System Map page

Issue: The **Multi-System Map** page shows a 502 error.

This error indicates that the listed peer rejected a request from the local iLO system.

Solution: Ensure that communication between the local iLO system and the peer with the error is not blocked by an intermediate firewall or a change to the iLO network configuration and HTTP port setting.

A 403 error is displayed on the Multi-System Map page

Issue: The **Multi-System Map** page shows a 403 Forbidden/Authorization error.

This error occurs when the group key on the local iLO system does not match the group key on a peer iLO system.

Solution: Ensure that the group key matches for all iLO systems that are members of the selected group.

iLO peers are not displayed

Issue: iLO peers (systems in the same group as the local iLO system) are not displayed on iLO Federation pages.

Solution 1: Ensure that the group key matches for all iLO systems that are members of the selected group.

Solution 2: Wait for twice the configured multicast interval, and then refresh the iLO Federation page. If an iLO system was reconfigured and can no longer communicate with the local iLO system, it will be dropped from its peer relationships after they expire. This should eliminate the query error.

Solution 3: If you are using server blades in an enclosure, verify that **Enclosure iLO Federation Support** is configured on the **Enclosure Settings→Network Access→Protocols** page in the Onboard Administrator web interface. You must have Onboard Administrator 4.11 or later to configure this setting. This is required to allow peer-to-peer communication between the server blades in an enclosure. For more information, see "Configuring enclosure support for iLO Federation" (page 56).

Solution 4: Verify that the switches in the network are configured to allow communication between iLO peers. For more information, see "iLO Federation network requirements" (page 52).

Solution 5: Ensure that communication between the local iLO system and the peer with the error is not blocked by an intermediate firewall or a change to the iLO network configuration and HTTP port setting.

iLO peers are displayed with IPv6 addresses on IPv4 networks

Issue: iLO peers on an IPv4 network are displayed with IPv6 addresses on iLO Federation pages.

Solution: If the network is configured to use IPv4 only, verify that the **iLO Client Applications use IPv6 first** check box is not selected on the **Network→iLO Dedicated Network Port→IPv6** page.

Troubleshooting miscellaneous issues

The following sections discuss troubleshooting miscellaneous hardware or software issues.

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 34).

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 37).

iLO firmware update does not finish

Issue: An iLO firmware update remains at 1% complete and does not finish.

Solution: Reset iLO, and then retry the firmware update.

1. Install the HP Lights-Out Online Configuration Utility (HPONCFG) on the HP ProLiant server.

   You can download HPONCFG from the following website: http://www.hp.com/support/ilo4.

2. Open a command window.
3. Change to the directory that contains HPONCFG.
4. Enter the following command:
   - Windows: `hponcfg /reset`
   - Linux: `hponcfg -r`

   NOTE: The user credentials are not required when you use HPONCFG from the server operating system.

5. Retry the iLO firmware update.

TIP: For information about using HPONCFG, see the *HP iLO 4 Scripting and Command Line Guide*.

For information about other methods you can use to reset iLO, see the *HP iLO 4 User Guide* and the *HP iLO 4 Scripting and Command Line Guide*.

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:\ilo>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 iLO.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
```

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.
- Set iLO to the factory default settings by using iLO RBSU or the iLO 4 Configuration Utility.

  △ **CAUTION:** This procedure clears all iLO configuration information, not just the **Server Name**.

  For more information, see “Resetting iLO to the factory default settings by using iLO RBSU” (page 311) and “Resetting iLO to the factory default settings by using the iLO 4 Configuration Utility” (page 312).

- Change the server name on the **Administration**→**Access Settings**→**Access Options** page in the iLO web interface.

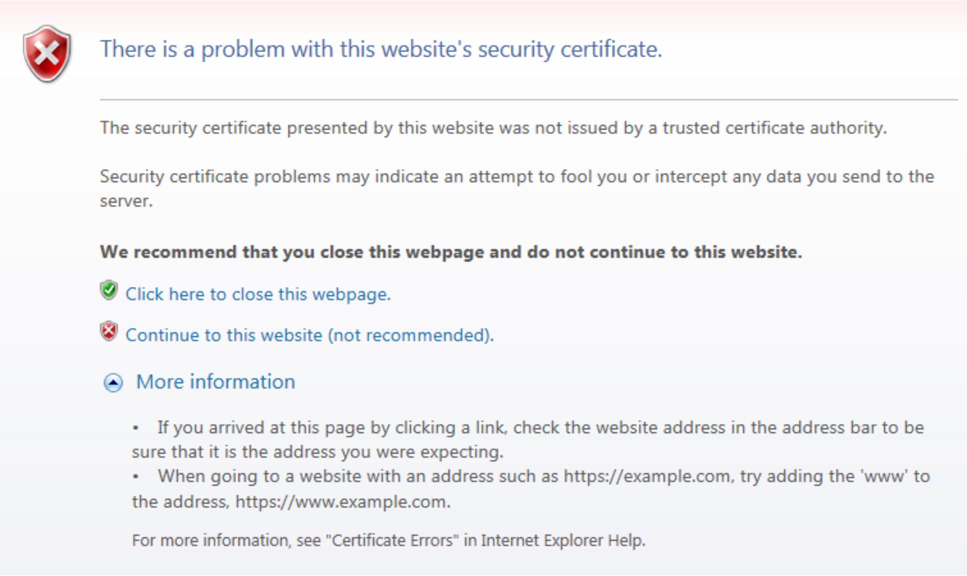
Certificate error when navigating to iLO web interface

Issue: When you navigate to the iLO web interface, a certificate error appears.

Solution: 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.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

- If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting.
- When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com.

For more information, see "Certificate Errors" in Internet Explorer Help.

2. Log in to the iLO web interface.
3. Navigate to the **Administration→Security→SSL Certificate** page.
4. Click **Customize Certificate**.

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

   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.

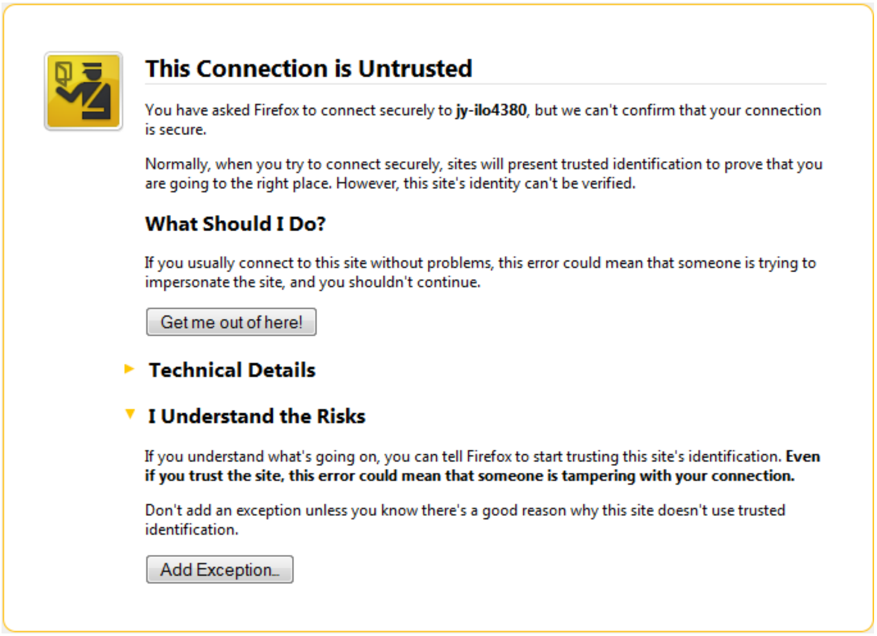
10. Follow the onscreen instructions and submit the CSR to the CA.

    The CA will generate a certificate in the PKCS #10 format.
11. After you obtain the certificate, verify 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.
    - The first and last lines are included in the certificate.
12. Return to the **SSL Certificate Customization** page in the iLO web interface.
13. Click **Import Certificate**.

    The **Import Certificate** window opens.
14. Paste the certificate into the text box, and then click **Import**.
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**.



This Connection is Untrusted

You have asked Firefox to connect securely to **jy-ilo4380**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

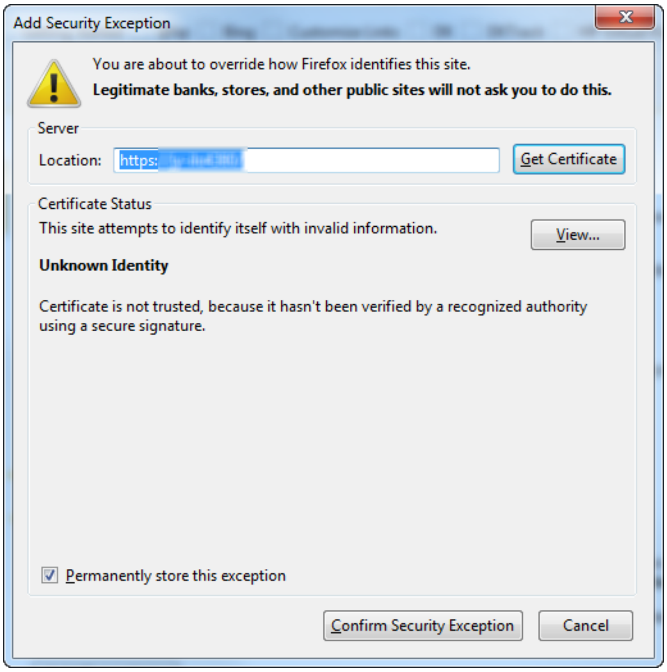
Technical Details

I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

2. In the **Add Security Exception** dialog box, enter `https://<iLO hostname or IP address>` in the **Location** box.



You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Location: https:[redacted]

This site attempts to identify itself with invalid information.

Unknown Identity

Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.

☑ Permanently store this exception

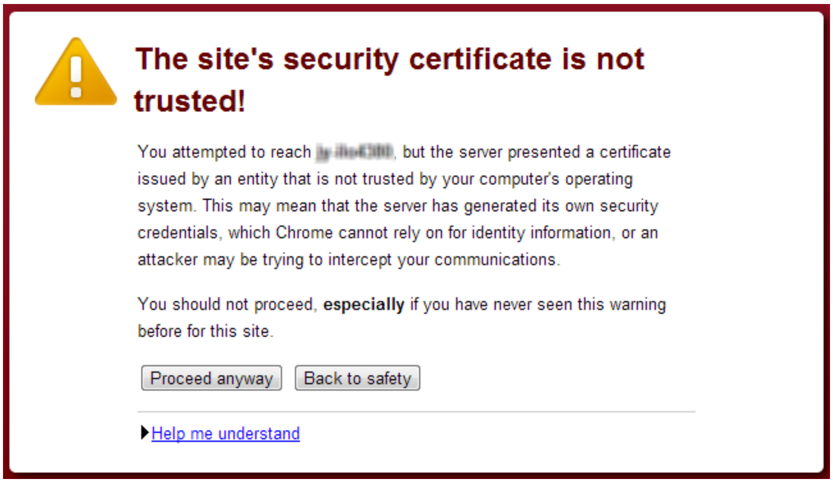
3. Click **Confirm Security Exception** to resolve the security warning.

   The security exception is saved and the iLO login screen appears.

4. Log in to iLO.

Resolving a browser certificate error: Chrome

1. When the security warning appears, click **Proceed anyway**.



The site's security certificate is not trusted!

You attempted to reach [redacted], but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

2. Log in to iLO.
3. Optional: To prevent the certificate warning from appearing in future iLO web interface sessions, install an SSL certificate.

   For instructions, perform Step 3 through Step 15 in "Resolving a browser certificate error: Internet Explorer" (page 336).

8 Support and other resources

Contacting HP

For worldwide technical support information, see the HP Support Center:

http://www.hp.com/go/hpsc

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

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 4 Scripting and Command Line Guide*
- *HP iLO 4 Release Notes*
- *HP ROM-Based Setup Utility User Guide*
- *HP UEFI System Utilities User Guide*
- *HP Intelligent Provisioning User Guide for HP ProLiant Gen8 Servers*
- *HP Intelligent Provisioning User Guide for HP ProLiant Gen9 Servers*
- *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 Systems Insight Manager User Guide*
- *HP BladeSystem Onboard Administrator User Guide*
- *HP ProLiant Gen8 Troubleshooting Guide, Volume I: Troubleshooting*
- *HP ProLiant Gen9 Troubleshooting Guide, Volume I: Troubleshooting*
- *HP Insight Remote Support Installation and Configuration Guide*
- *HP Insight Remote Support Monitored Devices Configuration Guide*
- *HP Insight Remote Support and Insight Online Setup Guide for HP ProLiant Servers and HP BladeSystem c-Class Enclosures*
- *HP iLO Federation Management User Guide*

Websites

- HP ProLiant Gen8 Server Management: http://www.hp.com/go/proliantgen8/docs
- HP ProLiant Gen9 Server Management: http://www.hp.com/support/proliantgen9/docs
- HP Intelligent Provisioning: http://www.hp.com/go/intelligentprovisioning/docs
- HP UEFI System Utilities: http://www.hp.com/go/ProLiantUEFI/docs
- HP Insight Remote Support: www.hp.com/go/insightremotesupport/docs
- HP RESTful API: http://www.hp.com/go/restfulinterface/docs
- HP SUM: http://www.hp.com/go/hpsum
- HP Service Pack for ProLiant: http://www.hp.com/go/spp/documentation
- HP iLO 4: http://www.hp.com/go/ilo/docs
- 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 10 (page 342) lists the features that are included with each iLO license.

Table 10 iLO 4 license options

Feature	iLO Standard	iLO Standard for BladeSystem	iLO Scale-Out[1]	iLO Essentials	iLO Advanced for BladeSystem	iLO Advanced
Platform Support	All (except BL)	BL	All HP ProLiant Gen8 and Gen9 SL and BL servers.	All HP ProLiant Gen8 e-series servers, Microservers, and Gen9 100 series and lower series.	BL	All (except BL)
Embedded Health System	X	X	X	X	X	X
Virtual Power Buttons	X	X	X	X	X	X
IPMI Over LAN/DCMI	X	X	X	X	X	X
Web-Based GUI	X	X	X	X	X	X
SSH Command Line Interface	X	X	X	X	X	X
RIBCL	X	X	X	X	X	X
Virtual Serial Port	X	X	X	X	X	X
IPv6	X	X	X	X	X	X
Active Health System	X	X	X	X	X	X
Embedded Remote Support	X	X	X	X	X	X
Agentless Management	X	X	X	X	X	X
Integrated Remote Console (IRC/Virtual KVM—Supports text and graphics)	Pre-OS only	X	Pre-OS only	X	X	X
iLO Federation Discovery	X	X	X	X	X	X
iLO Federation Group License Activation	X	X	X	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	X
Scripted Virtual Media					X	X
Text-based Remote Console via SSH (Textcons)			X		X	X
Directory Service Authentication					X	X
Kerberos Authentication					X	X

Table 10 iLO 4 license options *(continued)*

Feature	iLO Standard	iLO Standard for BladeSystem	iLO Scale-Out[1]	iLO Essentials	iLO Advanced for BladeSystem	iLO Advanced
Email-Based Alerting			X	X	X	X
Remote Syslog			X		X	X
Advanced Power Management (Power History Graphs, Dynamic Power Capping)			X		X	X
Virtual Serial Port Record and Playback			X		X	X
Discovery Services					X	X
HP Smart Array Secure Encryption			X		X	X
iLO Federation Management			X		X	X

[1] When an iLO Scale-Out license is applied to a blade server, it does not remove features that are available with the iLO Standard for BladeSystem license.

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.

Glossary

3DES Triple DES, the Data Encryption Standard cipher algorithm.

ABEND Abnormal end.

ACPI Advanced Configuration and Power Interface.

AES Advanced Encryption Standard.

ALOM Advanced Lights Out Manager.

AMP Advanced Memory Protection.

AMS Agentless Management Service.

API Application Programming Interface.

ARP Address Resolution Protocol.

ASR Automatic Server Recovery.

BIOS Basic Input/Output System.

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.

CSV Comma-separated values.

DCMI Data Center Manageability Interface.

DD A Unix program used to convert and copy a file.

DDNS Dynamic Domain Name System.

DDR Double data rate.

DER Distinguished Encoding Rules.

DHCP Dynamic Host Configuration Protocol.

DHE Diffie–Hellman key exchange.

DIMM Dual in-line memory module. A small circuit board holding memory chips.

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.

ESKM HP Enterprise Secure Key Manager is a pre-configured security server that provides a unified service for creating, protecting, and delivering cryptographic keys to data encryption devices and applications across the distributed enterprise IT infrastructure. You can use ESKM to configure HP Smart Array drive encryption.

FAT	File Allocation Table.
FIPS	Federal Information Processing Standard.
FQDN	Fully Qualified Domain Name.
FSMO	Flexible Single Master Operations.
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.
IDE	Integrated Drive Electronics.
IETF	Internet Engineering Task Force.
IIS	Internet Information Services.
iLO	Integrated Lights-Out.
IML	Integrated Management Log.
iPDU	HP Intelligent Power Distribution Unit.
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.
JSON	JavaScript Object Notation.
KCS	Keyboard Controller Style.
KDC	Key Distribution Center.
KDE	K Desktop Environment (for Linux).
KVM	Keyboard, video, and mouse.
LDAP	Lightweight Directory Access Protocol.
LDIFDE	A utility that allows you to import and export information to and from Active Directory.
LILO	Linux Loader.
LOM	Lights-Out Management.
MAC	Media Access Control.
MD5	Message-Digest algorithm 5.
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.
MLD	Multicast Listener Discovery.
MMC	Microsoft Management Console.
MSA	Mail Submission Agent.
MTA	Mail Transfer Agent.
NAND	A partition of non-volatile flash memory that is embedded on the system board of HP ProLiant servers. The NAND flash is used for files such as Active Health System data and the Intelligent Provisioning software.

NIC	Network interface card. A device that handles communication between a device and other devices on a network.
NMI	Non-maskable interrupt.
NTLM	NT LAN Manager.
NTP	Network Time Protocol.
OA	Onboard Administrator.
OU	Active Directory Organizational Units.
PAL	Programmable Array Logic.
PDS	HP Power Discovery Services.
PIM	Protocol-Independent Multicast.
PKCS	Public-key cryptography standards.
POST	Power-on self test.
PuTTY	A terminal emulator that can act as a client for the SSH, Telnet, rlogin, and raw TCP protocols and as a serial console client.
RBSU	ROM-Based Setup Utility.
RDRAM	Rambus Dynamic Random Access Memory.
REST	Representational State Transfer.
RIBCL	Remote Insight Board Command Language.
RIMM	Rambus In-line Memory Module.
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.
SLAAC	Stateless address autoconfiguration.
SLES	SUSE Linux Enterprise Server.
SMASH	Systems 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.
UEFI	Unified Extensible Firmware Interface

UHCI	Universal Host Controller Interface.
UID	Unit identification.
UPN	User principal name.
UPnP	Universal Plug and Play.
UPS	Uninterruptible Power Supply.
USB	Universal serial bus. A serial bus standard used to interface devices.
USM	User-based Security Model.
UTC	Coordinated Universal Time.
UTP	Unshielded twisted pair.
UUID	Universally unique identifier.
VSP	Virtual Serial Port.
WBEM	Web-Based Enterprise Management.
WINS	Windows Internet Name Service.

Index