HP Remote Insight Lights-Out Edition II User Guide

Audience assumptions

This document is for the person who installs, administers, and troubleshoots servers and storage systems. HP assumes you are qualified in the servicing of computer equipment and trained in recognizing hazards in products with hazardous energy levels.

Contents

Contents   5

Operational overview

In this section

New in this release

Added support for:

- Schema-free active directory ("Setup for Schema-free directory integration" on page 77)
- Two-factor authentication (on page 63)
- Terminal Services pass-through option (on page 41)

Updated the following:

- RIBCL ("Remote Insight command language" on page 138)
- Systems Insight Manager integration (on page 70)

RILOE II kit contents
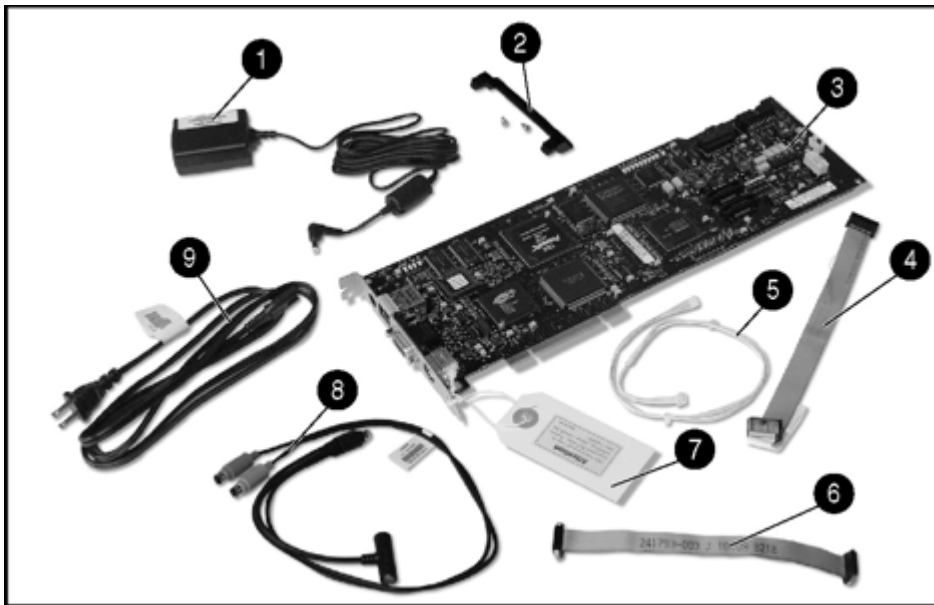
Item	Description
1	AC power adapter
2	PCI extender bracket
3	RILOE II board
4	Remote Insight cable (16-pin)

Item	Description
5	Virtual Power Button cable (4-pin)
6	Remote Insight cable (30-pin)
7	Network settings tag
8	Keyboard/mouse adapter cable
9	Power cord
	System documentation and support software CDs (not shown)

Installing the RILOE II

In this section

Preparing to install RILOE II

⚠ **WARNING: Some ProLiant servers are capable of producing energy levels that are considered hazardous. Do not remove enclosures or bypass the interlocks provided to protect against these hazardous conditions. Installation of accessories and options in areas other than front hot-plug bays should be performed by individuals who are both qualified in the servicing of computer equipment and trained in the hazards associated with products capable of producing hazardous energy levels. Refer to the documentation provided with the server for additional information on installing options in the server.**

1. Locate the documentation provided with the server for server-specific slot information.

2. Use the PCI slot matrix ("Server PCI Slot and Cable Matrix" on page 174) to select an unused PCI slot, appropriate cables, and video switch settings and to determine supported features for the server.

3. Be sure the server has the latest system ROM revision. For instructions on updating the system ROM of your server, refer to the server documentation. To download the latest server ROM upgrade for your server, go to the HP website (http://www.hp.com/servers/lights-out).

Remote Insight cable configuration

For servers that use the Remote Insight cable, RILOE II connects to the host server, peripheral devices, power source, and LAN.
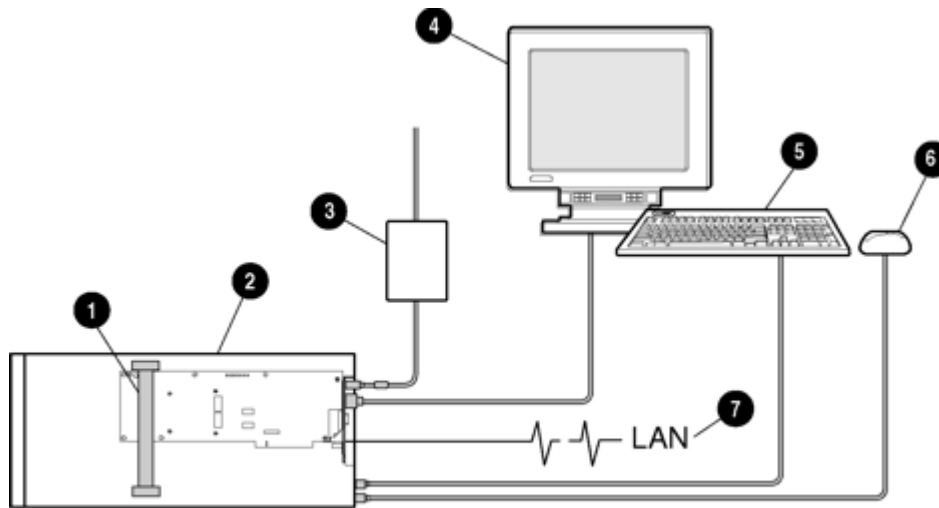
Item	Description
1	Remote Insight cable
2	RILOE II installed in a server
3	AC power adapter connected to RILOE II
4	Monitor connected to RILOE II
5	Keyboard connected to the server
6	Mouse connected to the server
7	LAN connected to RILOE II

Keyboard/mouse adapter cable configuration

△ **CAUTION:** Using the external mouse/keyboard cables with the internal cables causes conflicts with mouse and keyboard functions.

For servers that use the keyboard/mouse adapter cable, RILOE II connects to the host server, peripheral devices, power source, and LAN.
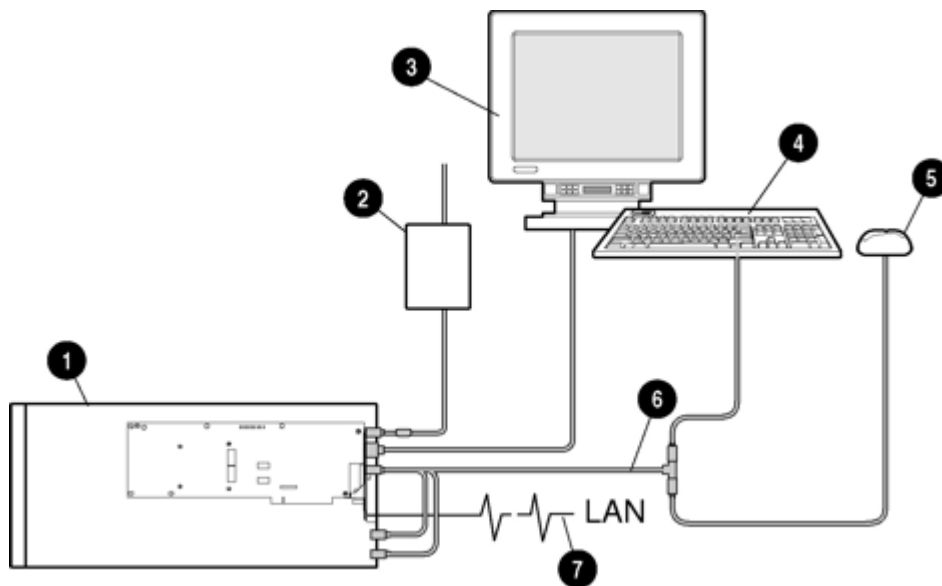
Item	Description
1	RILOE II installed in a server
2	AC power adapter connected to RILOE II
3	Monitor connected to RILOE II
4	Keyboard connected to RILOE II keyboard/mouse adapter cable
5	Mouse connected to the RILOE II keyboard/mouse adapter cable
6	Keyboard/mouse adapter cable
7	LAN connected to RILOE II

Installing RILOE II in the server

△ **CAUTION:** To prevent damage to electrical components, properly ground the server before beginning any installation procedure. Improper grounding can cause electrostatic discharge.

1. If you are installing RILOE II in a shared EISA/PCI slot, attach the PCI extender bracket to the board before installing the board in the server. The PCI extender bracket is not needed when installing the board in PCI-only slots.

⚠ **CAUTION:** The screws shown are self-tapping, and some amount of force is required for installation. Use caution when installing the screws to prevent damage to the RILOE II.
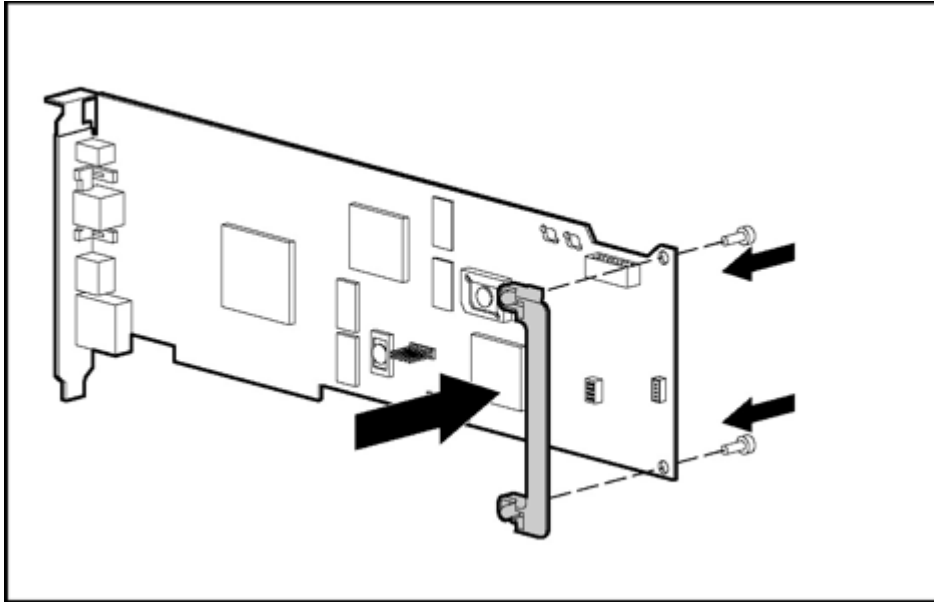
The extender should extend past the right edge of the board.

2. If you are installing RILOE II in a server that was previously configured with a RILOE and the server is running a Windows®-based operating system, upgrade the systems management driver with the Advanced System Management Driver found on the HP website (http://www.hp.com/servers/lights-out). The systems management driver must be upgraded before installing RILOE II in the server.

3. Power down the server and disconnect all power cords to remove power from the server.

4. Disassemble the server.

📝 **NOTE:** Refer to the server documentation for instructions on disassembling the server to install an option board.

5. Select an appropriate PCI slot. See the "Server PCI Slot and Cable Matrix (on page 174)" for more information. **RILOE II can be server-slot specific.**

6. Loosen the retaining screw and remove the slot cover. If RILOE II is being installed in a hot-plug slot, release the slot lever and remove the slot cover.

7. Press the RILOE II board firmly into the slot.

8. Secure the board in place with the retaining screw, or close the hot-plug slot lever, as appropriate.

9. Disable the onboard video, if required for the server. See the "Server PCI Slot and Cable Matrix (on page 174)" for more information.

Installing Internal Cables

⚠ **CAUTION:** Using the external mouse/keyboard cables with the internal cables causes conflicts with mouse and keyboard functions.

The following describes:

- installing a Virtual Power button cable (4-pin) (on page 14)
- installing a Remote Insight cable (16-pin) (on page 14)
- installing a Remote Insight cable (30-pin) (on page 14)

Installing a Virtual Power Button cable (4-pin)

To enable the Virtual Power Button feature of the RILOE II on servers that use a four-pin connector on the server system board, install the Virtual Power Button cable (4-pin) (PN 160011-001):

1. Power down the server and disconnect all power cords to remove power from the server.
2. Connect the four-pin connector on the cable to the Virtual Power Button cable connector, located on the rear of the RILOE II.
3. Connect the four-pin connector on the other end of the cable into the four-pin connector on the server system board.

IMPORTANT: Be sure that you do not connect the Virtual Power Button cable to the speaker connection on the server system board.

NOTE: For detailed instructions on the location of the connector on the server system board, refer to the documentation provided with the server.

4. Refer to the server documentation to reassemble the server.

Installing a Remote Insight cable (16-pin)

To install the Remote Insight cable (16-pin) (P/N 177634-001):

1. Power down the server and disconnect all power cords to remove power from the server.
2. Connect the 16-pin connector on the Remote Insight internal cable to the Remote Insight connector (16-pin), located on the edge of the board.
3. Connect the 16-pin connector on the other end of the Remote Insight internal cable to the 16-pin Remote Insight connector on the server system board.

NOTE: For detailed instructions on the location of the connector on the server system board, refer to the documentation provided with the server.

4. Refer to the server documentation to reassemble the server.

Installing a Remote Insight cable (30-pin)

To install the Remote Insight cable (30-pin) (P/N 241793-010):

1. Power down the server and disconnect all power cords to remove power from the server.
2. Connect the 30-pin connector on the Remote Insight cable to the Remote Insight connector (30-pin), located on the edge of the board.
3. Connect the 30-pin connector on the other end of the Remote Insight cable to the 30-pin Remote Insight connector on the server system board.

NOTE: For detailed instructions on the location of the connector on the server system board, refer to the documentation provided with the server.

4. Refer to the server documentation to reassemble the server.

Connecting external cables to RILOE II

After installing RILOE II in your server, connect the external cables. During normal operation, the RILOE II passes the keyboard and mouse signals to the server and functions as the primary video controller. This configuration allows the following operations to occur:

- Transparent substitution of a remote keyboard and mouse for the server keyboard and mouse

- Saving of video captures of reset sequences and failure sequences in the RILOE II memory for later replay
- Simultaneous transmission of video to the server monitor and to a Remote Console monitor
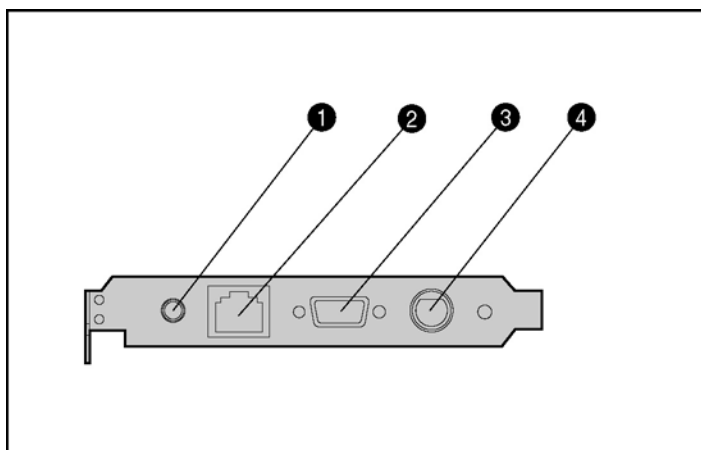
Item	Description
1	AC power adapter connector
2	LAN connector
3	Video connector
4	Keyboard/mouse connector

Keyboard/mouse adapter cable connection

The keyboard and mouse signals must pass through RILOE II. For more information, See the "Keyboard/Mouse Adapter cable configuration (on page 11)" section.

Some servers use a Remote Insight cable for the keyboard and mouse and do not require you to use the keyboard/mouse adapter cable. See the "Server PCI Slot and Cable Matrix (on page 174)" section to see if your server requires the keyboard/mouse cable.
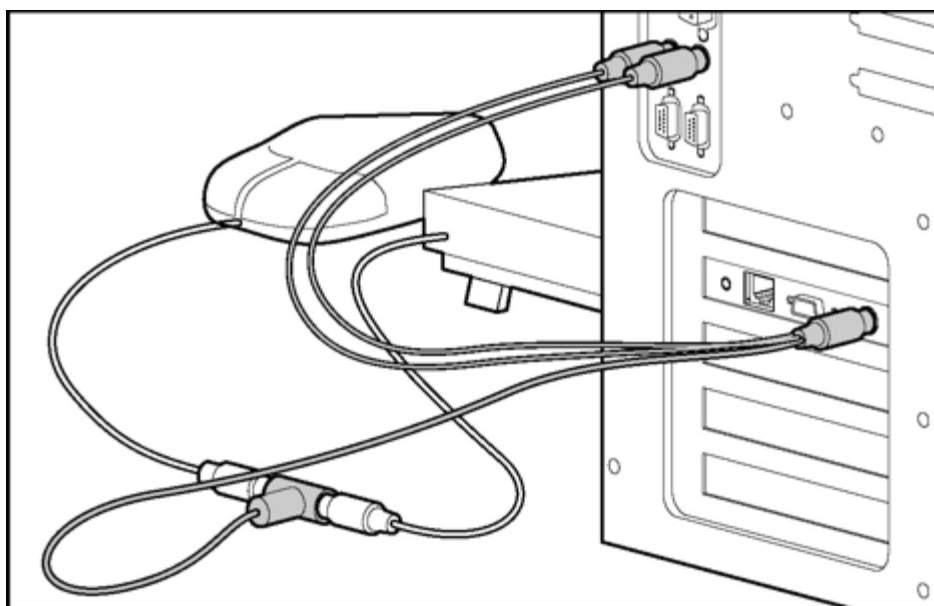
To connect the keyboard/mouse cable:

1. Disconnect the keyboard and mouse cables from the server.

2. Connect the keyboard and mouse cables to the color-coded T-shaped keyboard/mouse connector of the RILOE II keyboard/mouse adapter cable, as shown.

3. Connect the color-coded plugs of the keyboard mouse adapter cable to the keyboard and mouse connectors of the server.

4. Connect the black plug of the keyboard/mouse adapter cable to the RILOE II keyboard/mouse connector.

Headless server deployment

For headless server deployment, you do not have to connect the physical keyboard or mouse device to the server. However, to have remote keyboard and mouse capabilities, you must use the keyboard/mouse adapter cable provided with the RILOE II, the Remote Insight cable (16-pin), or Remote Insight cable (30-pin).

Monitor cable connection

To use a monitor with a server that has RILOE II installed, connect the monitor to the RILOE II video connector.

RILOE II incorporates the ATI RAGE XL video controller to ensure that a compatible controller is available for Remote Console operation. Adding RILOE II to a Windows® server replaces the embedded video controller of the server with the ATI RAGE XL video controller. Windows® loads a generic video driver to support the RILOE II video controller. The generic video driver works but lacks support for the ATI RAGE XL features.

For headless server deployment, do not connect a monitor to the server or to the RILOE II video connector.
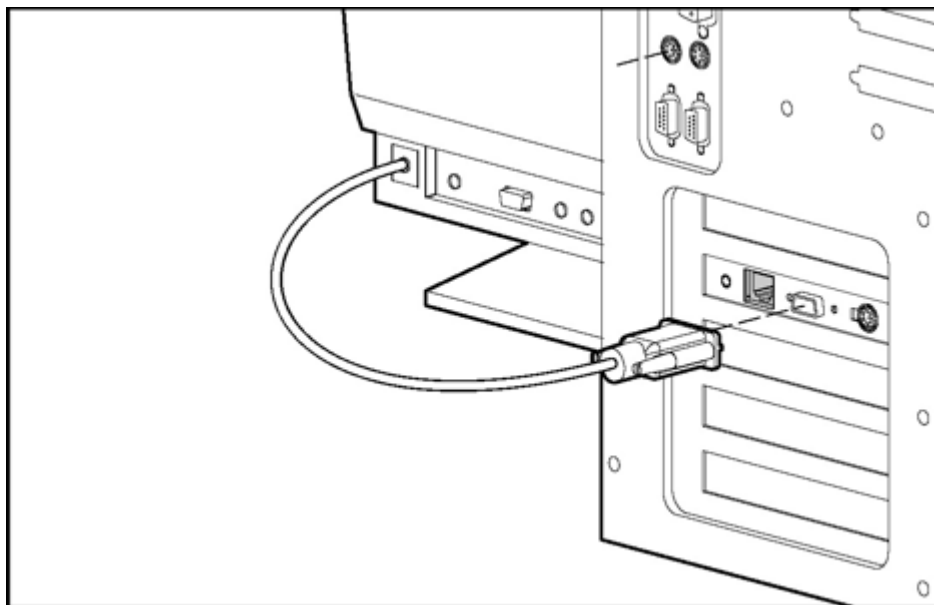
To connect the monitor signal cable:

1. Disconnect the monitor signal cable from the server monitor connector.

2. Connect the monitor signal cable to the RILOE II video connector.

3. If you are installing RILOE II in a server running Microsoft® Windows NT® 4.0, install the latest ATI RAGE XL driver from the PSP for Microsoft® Windows NT® 4.0 located on the SmartStart CD.

For RILOE II to perform correctly, some servers require disabling the server onboard video. See the slot matrix ("Server PCI Slot and Cable Matrix" on page 174) for a list of servers that require disabling the

server onboard video. For instructions on disabling the server onboard video, See the documentation provided with the server.

LAN cable connection

To access RILOE II using TCP/IP across a 10-MB or 100-MB Ethernet network, connect one end of the LAN cable to the LAN connector on RILOE II to an active network jack.
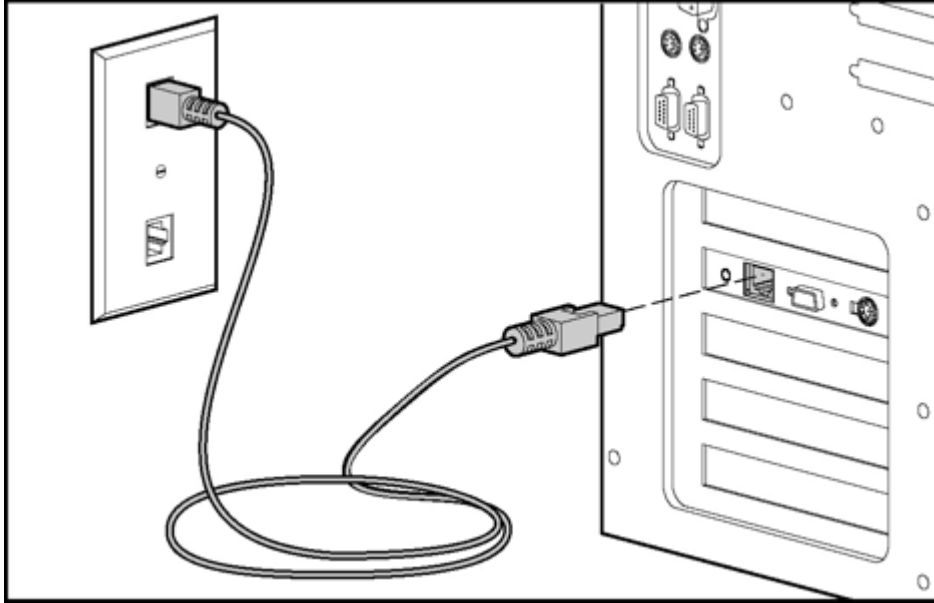
The green LED indicator that is located close to the AC power adapter connector indicates the speed of the connection. If the LED indicator is on, then the connection is 100-MB. If the LED is off, then the connection is 10-MB.

The green LED indicator that is located close to the video connector indicates a link. If the LED is on, then a connection is established.

AC power adapter connection

When the AC power adapter is connected, RILOE II has access to power that is independent of the main server power. To increase server manageability, HP recommends connecting the AC power adapter to a power circuit that is separate from that of the server.

HP ProLiant CL, DL, and ML servers that use the Remote Insight cable (16- or 30-pin) do not require the use of the AC power adapter.

The HP ProLiant ML330, ProLiant ML330e, and ProLiant DL760 servers require the installation of the power adapter included in RILOE II kit. For detailed information, See the documentation provided with the server. For a complete list of servers that require the AC power adapter, See the HP website (http://www.hp.com/servers/lights-out).

Connect the AC power adapter cable as shown.
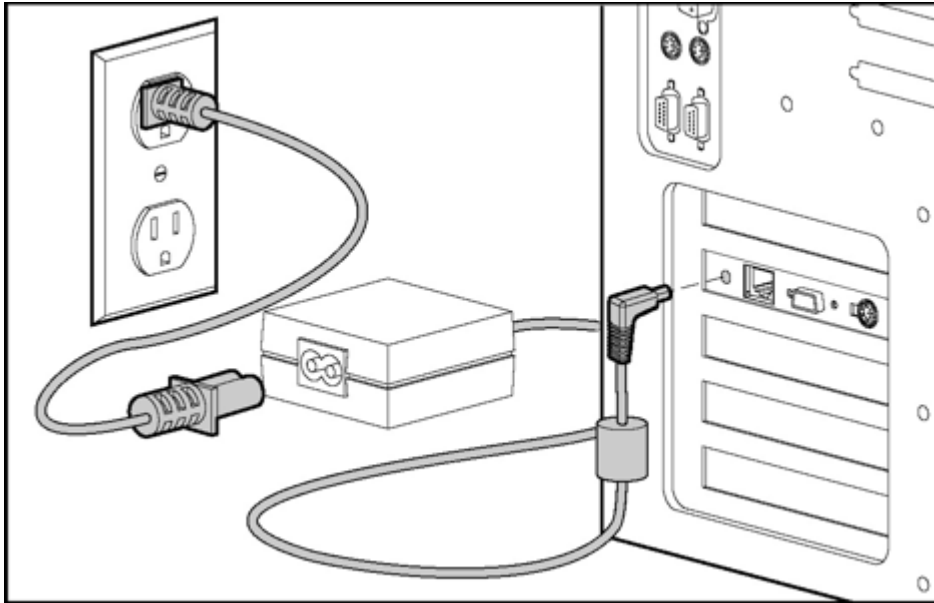
Powering up the server

1. Plug the AC main power cord into the server and then into a grounded AC outlet.

⚠ **WARNING: To reduce the risk of electric shock or damage to the equipment:**
- **Disconnect power from the system by unplugging all power cords from the power supplies.**
- **Do not disable the power cord grounding plug. The grounding plug is an important safety feature.**
- **Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.**

2. Turn on any peripheral devices attached to the server.
3. Turn on the server.

Configuring the RILOE II

In this section

Configuration options

After you have installed RILOE II in the server and completed all necessary peripheral connections, configure RILOE II.

RILOE II offers two configuration options:

- Remote setup allows you to configure RILOE II from the Remote Console through a browser interface.
- The ROM-based setup utility F8 (RBSU F8) allows you to configure RILOE II during server boot-up. RBSU F8 is useful for configuring servers that do not use DNS/DHCP. RBSU F8 is available every time the server is booted. RBSU F8 cannot run remotely.

Regardless of the configuration method you use, familiarize yourself with all the configuration parameters. Use the user guide to determine what parameters are required to set up RILOE II. Leave parameters set to default values unless you know the parameter should be changed for your environment. Before starting RBSU F8, record any required values for your installation.

Some servers contain DIP switches on the system board to control certain security settings. Before beginning configuration, if the server is equipped with a Configuration Lock Switch, set this switch to off (unlocked). See the documentation or hood labels that shipped with the server for more information about the Configuration Lock Switch. When configuration is complete, return the switch to the on (locked) position.

Remote setup

Remote setup allows you to configure the RILOE II from the Remote Console.

1. Using a standard Web browser, access the RILOE II from a remote network client and provide the default DNS name, user name, and password on the network settings tag supplied with the board.
2. When you successfully log on to the RILOE II, you will be able to change the default values of the network and user settings through the Web browser interface of the RILOE II. You will also be able to install operating system drivers and Insight Manager agents on the remote host server using the graphical Remote Console.

ROM-Based Setup Utility F8

RBSU F8 allows you to set up the RILOE II during server boot up. However, RBSU is **not** accessible through the RILOE II Remote Console. It can only be accessed locally at the server.

1. Restart or power up the server.
2. Press the **F8** key to enter RBSU when the cursor flashes and the RILOE II prompt displays on the screen.

3. Make and save any necessary changes to the RILOE II.
4. Exit the RBSU.

SmartStart setup of RILOE II

Use RBSU F8 during SmartStart to configure the RILOE II. Configuring the RILOE II using SmartStart is not an option.

Installing RILOE II device drivers

The RILOE II Management Interface Driver enables system software, such as SNMP Insight Agents and the Terminal Services pass-through service, to communicate with RILOE II.

The device drivers required to support RILOE II are part of the PSP located on the SmartStart CD or the, Management CD, or on the HP website (http://www.hp.com/servers/lights-out).

All the support drivers for your server and RILOE II can be downloaded from the HP website (http://www.hp.com/servers/lights-out).

To download the device drivers:
1. Click the RILOE II graphic.
2. Select **Software and Drivers.**

Microsoft device driver support

The device drivers that support the RILOE II are part of the PSP that is located on the HP website (http://www.hp.com/support) or on the SmartStart CD. Before you install the Windows® drivers, obtain the Windows® documentation and the latest Windows® Service Pack.

RILOE II prerequisite files:
- CPQCIDRV.SYS provides the RILOE II Management Interface Driver support.
- CPQASM2.SYS, SYSMGMT.SYS, and SYSDOWN.SYS provide the RILOE II Advanced Server Management Controller Driver support.

PSP for Microsoft® Windows® products includes an installer that analyzes system requirements and installs all drivers. The PSP is available on the HP website (http://www.hp.com/support) or on the SmartStart CD.

To install the drivers in the PSP:
1. Download the PSP from the HP website (http://www.hp.com/support).
2. Run the SETUP.EXE file included in the download, and follow the installation instructions.

For additional information about the PSP installation, read the text file included in the PSP download.

Novell NetWare device driver support

The device drivers required to support RILOE II are part of the PSP that is located on the SmartStart CD and the HP website (http://www.hp.com/support).The PSP for Novell NetWare includes an installer that analyzes system requirements and installs all drivers.

RILOE II prerequisite files:
- The CPQHLTH.NLM file provides the Health Driver for Novell NetWare.
- The CPQCI.NLM file provides RILOE II Management Interface Driver support.

When updating RILOE II drivers, be sure RILOE II is running the latest version of RILOE II firmware. You can obtain the latest version as a Smart Component from the HP website (http://www.hp.com/servers/lights-out).

To install the drivers download the PSP from the HP website (http://www.hp.com/support) to a NetWare server. After downloading the PSP follow the Novell NetWare component installation instructions to complete the installation. For additional information about the PSP installation, read the text file included in the PSP download.

When using Novell NetWare 6.X, use the RAGE-XL video driver that is provided by the operating system for best results.

Linux device driver support

You can download the PSP files containing the RILOE II driver, the foundation agents, and health agents from the HP website (http://www.hp.com/support). The instructions on how to install or update the RILOE II driver are available on the website. The HP Management Agents for Linux are:

- ASM package (hpasm) which combines the health driver, IML viewer, foundation agents, health agent, and standard equipment agent into one package.
- RSM package (hprsm) which combines the RIB driver, rack daemon, RIB agent, and rack agent into one package.

To load the health and RILOE II driver packages, use the following commands:

```
rpm –ivh hpasm-d.vv.v-pp.Linux_version.i386.rpm
rpm –ivh hprsm-d.vv.v-pp.Linux_version.i386.rpm
```

where *d* is the Linux distribution and version and

vv.v-pp are version numbers.

For additional information, refer to the Software and Drivers website (http://www.hp.com/support).

To remove the health and RILOE II drivers, use the following commands:

```
rpm –e hprsm
rpm –e hpasm
```

For additional information, refer to the Software and Drivers website (http://www.hp.com/support).

Disabling DNS/DHCP

HP recommends using DNS/DHCP with the RILOE II to simplify installation. In the event that DNS/DHCP cannot be used, use the following procedure to disable DNS/DHCP and configure the network settings:

1. Restart or power up the server.
2. Press the **F8** key to enter the RBSU when the cursor flashes and the RILOE II prompt displays on the screen.

📝 **NOTE:** Use the arrow keys to highlight selections.

3. Select **Network**, **DNS/DHCP**, and press the **Enter** key. The **Network Autoconfiguration** screen displays.
4. Select **DHCP Enable** and press the space bar to turn off DHCP. Be sure that **DHCP Enable** is set to off and press the **F10** key to save the changes.

📝 **NOTE:** It will take a few minutes for the board to save the network changes and to reset.

5. Select **Network, NIC,** and **TCP/IP,** and press the **Enter** key. The **Network Configuration** screen displays.

6. Configure your network settings.

7. Press the **F10** key to save the changes.

NOTE: It will take a few minutes for the board to save the network changes and to reset.

8. Exit the RBSU.

Using the RILOE II

In this section

Accessing RILOE II for the first time

RILOE II is preconfigured with a default user name, password, and DNS name. A network-settings tag that shows the default values is attached to the board. Use these values to access the board remotely from a network client using a standard browser. For security reasons, HP recommends that you change these default settings after accessing RILOE II for the first time.

Default values:

- User name: Administrator
- Password: The last eight digits of the serial number
- DNS name: RIB*XXXXXXXXXXXX*, where the 12 *X*s are the MAC address of RILOE II

NOTE: User names and passwords are case sensitive.

1. Enter RILOE II IP address or DNS name in the address bar of the browser. A Security Alert page appears.
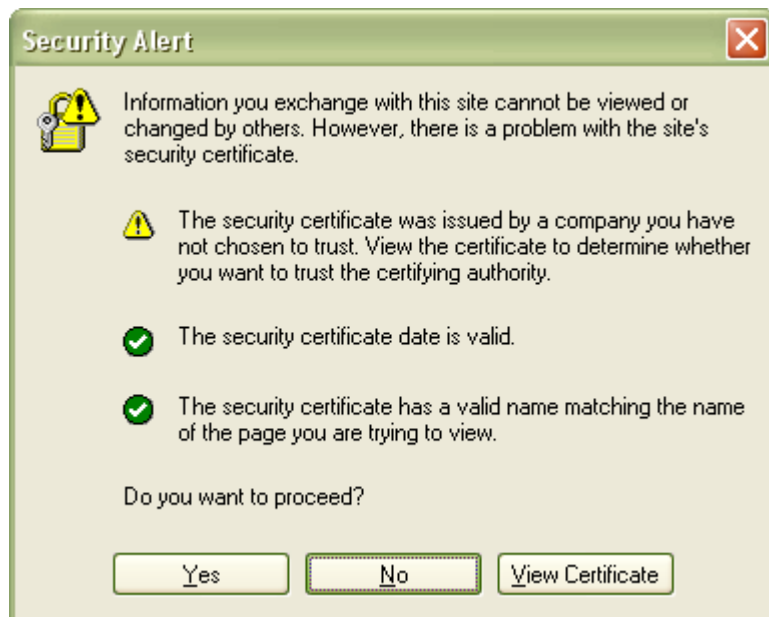
2. Perform one of the following actions:
   - Click **Yes** to continue to the login page of RILOE II.
   - Click **No** to return to the Welcome page of RILOE II.
   - Click **View Certificate** to view the certificate information. Installing the certificate to your browser prevents the security alert message from displaying in the future. However, security alert messages reappear when the certificate is removed from your browser, the firmware is upgraded, the board is rebooted, or the name of RILOE II board is changed.
3. To install the certificate, proceed to step 4. If you do not want to install the certificate, proceed to step 5.

NOTE: The Group Administration function, access to the RILOE II Web interface, and keystroke access to the Remote Console are encrypted with SSL security using a 128-bit RC4 cipher.

4. To install the certificate to your browser:
   a. Click **Install Certificate.** The Certificate Manager Import Wizard starts.
   b. Click **Next.**
   c. Click **Next** to allow the browser to automatically select the certificate store when the Certificate Store page appears.
   d. Click **Finish** when the Completing the Certificate Manager Import Manager Wizard appears.
   e. Click **Yes** to confirm the installation of the certificate when the confirmation page appears.
5. At the login page, use the default user name and password from the network settings tag and click **OK.**

NOTE: On the RILOE II login page, the maximum length of the **Login Name** is 40 characters for local users. For Directory Services users, the maximum length of the **Login Name** is 256 characters.

After the default user name and password are verified, the Remote Insight Status Summary page appears.

The Remote Insight Status Summary page provides general information about the RILOE II, such as the user currently logged on, server name and status, Remote Insight IP address and name, and latest log entry data. The summary home page also shows whether RILOE II has been configured to use HP web-based Management and Insight Management Web agents.

Features of the RILOE II

The RILOE II screen displays the following tabs:

- **System Status**

  This section provides information about the server and the RILOE II. The information includes server status, RILOE II status, survey information, the Remote Insight Event Log, and the Integrated Management Log.

- **Remote Console**

  This section gives you access to the Remote Console and enables you to define keystroke sequences that are transmitted to the remote host server at the press of a hot key. It also provides reset sequence playback and Windows® 2003 EMS access.

- **Virtual Devices**

  This section provides remote Virtual Power Button, power cycle capabilities, remote reset capabilities, Virtual Floppy Drive, Virtual Floppy Drive USB, and Virtual CD Drive USB.

- **Administration**

  This section allows you to manage individualized settings for users, SNMP alerts, the network environment, global security, certificates, and directory services settings. This section also includes an option that enables you to upgrade the RILOE II firmware.

Managing the user and configuration settings of the RILOE II

The options available in the **Administration** section allow you to manage user settings, SNMP alerting through integration with Insight Manager, security settings, and network environment settings. This section also provides a firmware upgrade option that allows you to keep the RILOE II current.

User configurations and settings

In User Settings of the Administration section, you can add new users or modify a user's profile. A user with administrator status can remotely add, delete, and modify the configurations of other Remote Insight users.

Parameter	Default value	Definition
User Name	Administrator	This parameter is the user's real name as it appears in the user list and event log. It is not the name used to log in. The maximum length of the user name is 40 characters.
Login Name	Administrator	This is a case-sensitive name that the user must provide to log in to RILOE II.
Password	A random, eight-character alphanumeric string that is factory assigned	This is a case-sensitive password that the user must provide to log in to RILOE II. In Security Options, the minimum password length can be assigned. The minimum password can be from 0 to 40 characters. The default minimum password length is eight characters.
Enforced client IP Address	None	This parameter specifies a specific IP address, an IP address range, or a DNS name. Client login attempts that do not meet the specified requirements are rejected.

Parameter	Default value	Definition
Administer User Access	Yes	This privilege allows a user to add, modify, and delete user accounts. It also allows the user to alter privileges for all users, including granting all permissions to a user.
Configure RILOE Access	No	This privilege enables a user to make changes to RILOE II settings, such as network settings and global settings, and to clear the event log.
Login Access	Yes	This setting grants or denies the user login access. Login access can be used to create a user who is a service provider and who receives alerts from the board but does not have login access to RILOE II.
Remote Console Access	Yes	This privilege allows a user to remotely manage the Remote Console of a managed system, including video, keyboard, and mouse controls.
Remote Server Reset and Power Button Sccess	Yes	This privilege allows a user to power-cycle or reset the host platform.
Virtual media	Yes	This privilege allows a user to use virtual media on the host platform.

Adding authorized users

You can assign a different access level to each user. A user can have the administer access privilege, which grants the ability to create, modify, or delete other users. Conversely, a user can be denied the administer access privilege, as well as access to other features of the RILOE II.

The RILOE II supports up to 25 users. Login attempts are tracked and login failures are logged. You have the option of generating alerts on a remote management system running Systems Insight Manager when login attempts fail. The RILOE II supports all LAN-oriented security features and dynamic password encryption.

To add a new user to the RILOE II:

1. Log in to the RILOE II using an account with administrator privileges.
2. Click **User Settings** on the **Administration** tab.
3. Click **Add** and complete the fields with the necessary information for the user being added.
4. When the user profile is complete, click **Save User Information** to return to the **User Settings** screen.

📝 **NOTE:** To clear the user profile form while entering a new user or to recover the user's original information, click **Restore User Information.**

Modifying an existing user's profile

To modify an existing user's information:

1. Log in to the RILOE II using an account with administrator privileges.
2. Click **User Settings** on the **Administration** tab.
3. Select the user that you want to modify and click **Modify.**
4. Change the user information in the fields that require modification. Click **Save User Information** to return to the **User Settings** screen.

NOTE: To clear the user profile form while entering a new user or to recover the user's original information, click **Restore User Information.**

Network settings

The Network Settings option on the Administration tab enables you to view and modify the NIC IP address, subnet mask, TCP/IP-related settings, and specify IP address or DNS name for web-based management agents. You can enable or disable DHCP and, for servers not using DHCP, you can configure a static IP address.

To change network settings for RILOE II:

1. Log in to the RILOE II using an account with administrator privileges.
2. Click **Network Settings** in the **Administration** tab.
3. Change the network settings as needed by typing in the fields. After completing parameter changes, click **Apply** to save the changes.

When you click **Apply,** RILOE II restarts. During the restart process, the connection from the browser to the board is terminated. To reestablish a connection, wait 60 seconds before launching another browser session and logging in to RILOE II.

Parameter	Default value	Definition
Transceiver Speed Autoselect	Yes	Autoselect detects the interface speed and sets the interface to operate at 10 Mb/s or 100 Mb/s and at half or full duplex. If necessary, you can set this parameter to No so you can manually adjust the speed and duplex settings.
Speed	Autoselect	Use this parameter to assign 10-Mb/s or 100-Mb/s connection speeds if Transceiver Speed Autoselect is not enabled.
Duplex	Autoselect	Use this parameter to assign half or full duplex to the NIC if Transceiver Speed Autoselect is not enabled.
Enable DHCP	Yes	This parameter enables you to select a static IP disables (No) or enables the use of a DHCP server (Yes) to obtain an IP address for the RILOE II subsystem. You cannot set the RILOE II IP address and subnet mask if DHCP is enabled. Enabling DHCP allows you to configure the following DHCP options: • Use DHCP Supplied Gateway • Use DHCP Supplied DNS Servers • Use DHCP Supplied WINS Servers • Use DHCP Supplied Static Routes • Use DHCP Supplied Domain Name
Use DHCP Supplied gateway	Yes	This parameter controls whether RILOE II uses the DHCP server-supplied gateway. If not, enter one in the Gateway IP Address box.
Use DHCP Supplied DNS servers	Yes	This parameter controls whether RILOE II uses the DHCP server-supplied DNS server list. If not, enter one in the Primary/Secondary/Tertiary DNS Server boxes.
Use DHCP Supplied WINS servers	Yes	This parameter controls whether RILOE II will use the DHCP server-supplied WINS server list. If not, enter one in the Primary/Secondary WINS Server boxes.
Use DHCP Supplied Static Routes	Yes	Toggles whether RILOE II will use the DHCP server-supplied static route. If not, enter one in the Static Route #1, #2, #3 boxes.
Register with WINS Server	Yes	RILOE II automatically registers with a WINS server. By default, WINS server addresses are assigned by DHCP.
IP Address	N/A	Use this parameter to assign a static IP address to RILOE II on your network. By default, the IP address is assigned by DHCP.
Subnet Mask	N/A	Use this parameter to assign the subnet mask for the default gateway. By default, the subnet mask is assigned by DHCP.
Gateway IP Address	N/A	Use this parameter to assign the IP address of the network router that connects RILOE II subnet to another subnet where the management console resides. By default, the gateway is assigned by DHCP.
RILOE II Board Name	N/A	Use this parameter to assign a unique name to RILOE II. This name can be used, if DHCP and DNS are configured as the address to connect to RILOE II instead of the IP address.
Domain Name	N/A	Enter the name of the domain in which RILOE II will participate. By default, the domain name is assigned by DHCP.
DHCP server	N/A	This parameter is automatically detected if Enable DHCP is set to Yes. You cannot change this parameter.

Parameter	Default value	Definition
Primary, secondary, and tertiary DNS server	N/A	Use this parameter to assign a unique DNS server IP address on the network. By default, the primary, secondary, and tertiary DNS servers are assigned by DHCP.
Primary and secondary WINS server	N/A	Use this parameter to assign a unique WINS server IP address on the network. By default, the primary and secondary WINS servers are assigned by DHCP.
Static routes #1, #2, #3	N/A for both the destination and gateway address	Use this parameter to assign a unique static route destination and gateway IP address pair on the network. You can assign up to three static route pairs. By default, the static routes are assigned by DHCP.
Insight Manager Web Agent Address http://	N/A	Use this parameter to assign the IP address of the host server. Port number 2301 is automatically appended to the IP address to allow access to the HP web-enabled Systems Management Agents from within RILOE II user interface.

Global settings

The Global Settings option enables you to view and modify security settings for RILOE II. The Global Settings page enables you to configure the Remote Console time-out and RILOE II ports to be used for the RILOE II web server, Remote Console, and Virtual Media. These settings are applied globally, regardless of the individual user settings.

To change global settings for RILOE II:

1. Log in to RILOE II using an account that has the Configure RILOE II Settings privilege. Click **Administration.**
2. Click **Global Settings.**
3. Change the global settings as needed by entering your selections in the fields.

After completing any parameter changes, click **Apply** to save the changes.

Parameter	Default value	Definition
Session Timeout (minutes)	30 minutes	This parameter specifies how many minutes a session can remain inactive before RILOE II the user is required to log in again.
ROM configuration utility (F8)	Enabled	This parameter enables or disables the use of the F8 key, during POST, to access the Remote Insight ROM Configuration Utility.
Emergency Management Services	Enabled	This parameter enables or disables the use of the Windows .NET EMS through RILOE II.
Bypass Reporting Of External Power Cable	Disabled	This parameter determines if RILOE II reports whether or not the external power cable is connected to the operating system agent. If this settings is Enabled and there are no other status problems, Insight Manager reports a green status. If this parameter is Disabled, RILOE II reports the true status of the external power connector to the operating system agent. Insight Manager reports RILOE II status as degraded if the external connector is disconnected.
Remote Console Port Configuration	Enabled	This parameter determines how the Remote Console port is configured. There are three options: • Enabled allows administrators to specify the Remote Console port. • Disabled prevents administrators from designating a Remote Console port. • Automatic uses the default port.
Remote Access with Pocket PC	Enabled	This parameter enables or disables access to RILOE II through a Pocket PC client.
Remote Console Data Encryption	Enabled	This parameter determines if data communication with the Remote Console is encrypted. Encryption (enabled) helps keep your remote console session private on the network. If you intend to use a standard telnet client to access a RILOE II, this parameter must be disabled.
SSL Encryption Strength	128-bit	This parameter displays the current cipher strength setting. The most secure is 128-bit (High).
Current Cipher	N/A	This parameter displays the encryption algorithm currently being used to protect data during transmission between the browser and RILOE II. The algorithm is negotiated by RILOE II and the browser.
Remote Insight HTTP Port	80	The embedded web server in RILOE II is configured by default to use port 80 for unencrypted communications.
Remote Insight HTTPS Port	443	The embedded web server in RILOE II is configured by default to use port 443 for encrypted communications.
Remote Insight console Port	23	RILOE II Remote Console is configured by default to use port 23 for Remote Console communications.
Host Keyboard Model	US	This parameter enables you to specify the language model of the keyboard during a Remote Console session.

Parameter	Default value	Definition
Level of Data Returned	Medium	This parameter configures how much data is returned to Insight Manager. • None returns no data. • Low returns the current board status and the board type (RILOE II). • Medium returns the board status, the board type, and the serial number. • High returns the board status, the board type, the serial number and several other pieces of information.
View XML Reply	N/A	This parameter displays the XML reply sent to Insight Manager. This parameter only displays when you use Internet Explorer.

SNMP alerts and settings

In the Administration>SNMP Settings section, you can enable, disable, and test SNMP alerts. SNMP alerts are forwarded from the host server and RILOE II to an Insight Manager console. The two types of alerts are:

- **Host OS Generated SNMP Traps**—The Insight Management agents provided for each supported network operating system generate these alerts. These agents must be installed on the host server to receive these alerts. Alerts are sent to Insight Manager clients on the network and forwarded asynchronously by RILOE II to users that have been configured to receive them.
- **Remote Insight Board Alerts**—These alerts are generated when RILOE II detects conditions that are independent of the host server operating system. These alerts can be Insight Manager SNMP traps or pager alerts. Alerts include major events, such as a host server power outage or host server reset, and RILOE II events, such as a disconnected keyboard cable or an unauthorized login attempt.
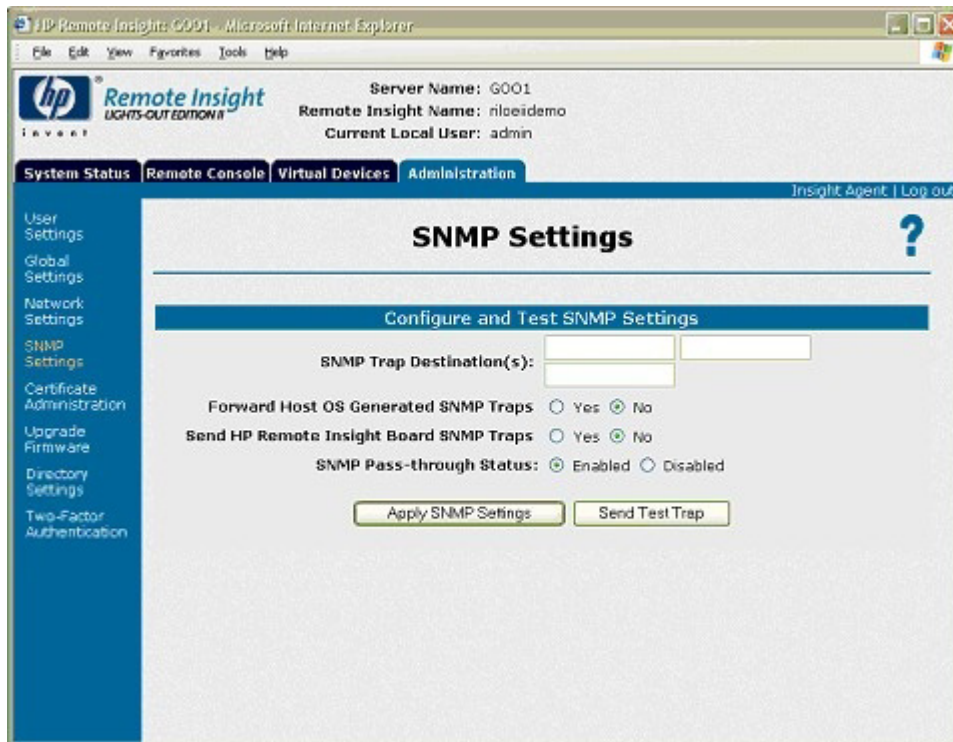
To enable alerts:

1. Log in to the RILOE II using an account with administrator privileges.
2. Click **SNMP Settings** on the Administration tab.
3. Click **Yes** for the alert types that you want to receive.
4. Enter the IP addresses to send the alerts to in the SNMP Trap Destinations field.
5. Click **Apply SNMP Settings.**

Parameter	Default Value	Definition
SNMP Trap Alert Destination(s)	N/A	Enter the IP address of the remote management PC that will receive SNMP trap alerts from RILOE II. Up to three IP addresses can be designated to receive SNMP alerts. The maximum value for each address is 50 characters.
Forward Host OS Generated SNMP Alerts	No	This parameter enables or disables forwarding of host operating system generated SNMP traps.
Send HP Remote Insight Board SNMP traps	No	This parameter enables or disables sending of RIB SNMP trap information.
Enable SNMP Pass-through Status	Enabled	This parameter enables the system to pass SNMP packets from the Insight Management Agent. When set to No, all SNMP traffic is stopped and will not pass-through RILOE II.

SNMP Pass-through Status

When the SNMP Pass-through Status feature is enabled, RILOE II will accept SNMP packets from a management station and pass them to the Insight Management Agents running on the server. The agents on the server processes these SNMP packets and send the response back to RILOE II, which in turn transmits these packets back to the management station. This helps the management station gather information about the server even when the server network connection is not working.

When the SNMP Pass-through Status feature is disabled, RILOE II will not accept any SNMP packet from a management station and thus will not forward these packets to the agents. So, the management software can not get information or send commands to the agents running on the server if the server network connection is not working.

Generating Test Alerts

Test alerts are generated through the **Manage Alerts** option in the **Administration** section. These alerts include Systems Insight Manager SNMP traps and are used to verify the network connectivity of the RILOE II in Systems Insight Manager.

To send out a test alert:
1. Click **SNMP Settings** on the Administration tab.
2. Click **Send Test Trap.** If a trap destination is not provided, an error message displays.
3. After generating the alert, a confirmation screen appears.
4. If the alert system is working correctly, an alarm screen displays advising you that an alert has been received.

Disabling Alerts

1. Log in to the RILOE II using an account with administrator privileges.
2. Click **SNMP Settings** on the Administration tab.

3. Click **No** for the alert types that you want to disable.

4. Click **Apply SNMP Settings.**

Two-Factor Authentication Settings

The Two-Factor Authentication Settings page displays the configuration of two-factor authentication settings, the trusted CA certificate information, and provides a method of changing the configuration and importing or deleting a trusted CA certificate.
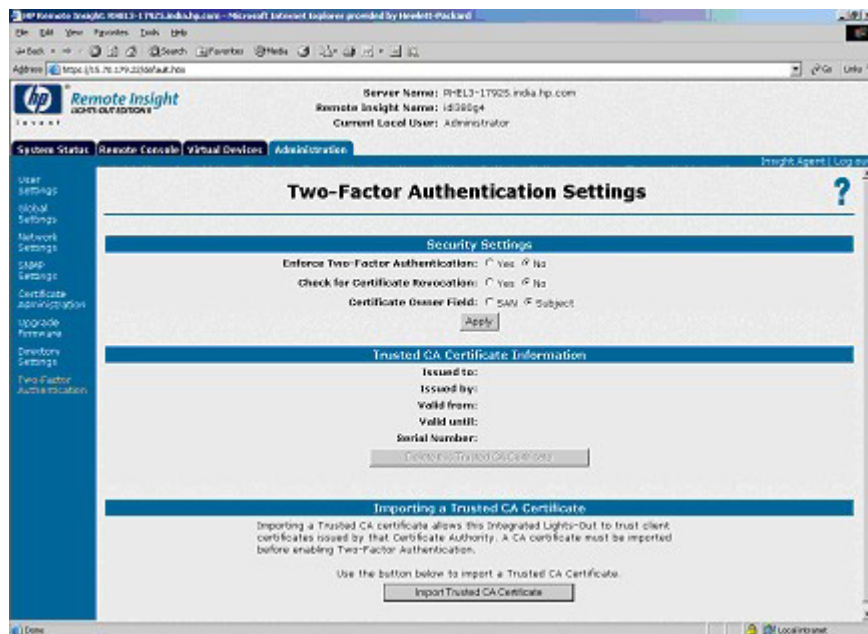
The Enforce Two-Factor Authentication setting controls whether two-factor authentication is used for user authentication during login. Selecting Yes for the Enforce Two-Factor Authentication setting will require two-factor authentication. The No value disables the feature and allows login with user name and password only. You cannot change the setting to Yes if a trusted CA certificate is not configured. Changing the setting resets RILOE II saving the changes. To provide the necessary security, the following configuration changes are made when two-factor authentication is enabled:

- Remote Console Data Encryption: Yes (Disables telnet access)
- Enable Secure Shell (SSH) Access: No
- Serial Command Line Interface Status: Disabled

If telnet, SSH, or Serial CLI access is required, re-enable these settings after two-factor authentication is enabled. However, because these access methods do not provide a means of two-factor authentication, only a single factor is required to access RILOE II with telnet, SSH or Serial CLI.

When two-factor authentication is enabled, access with the CPQLOCFG utility is disabled, because CPQLOCFG does not supply all authentication requirements. However, the HPONCFG utility is functional, because administrator privileges on the host system are required to execute the utility.

The Check for Certificate Revocation setting controls whether RILOE II uses the certificate CRL distribution points attribute to download the latest CRL and check for revocation of the client certificate. If the client certificate is contained in the CRL or if the CRL cannot be downloaded for any reason, access is denied. The CRL distribution point must be available and accessible to RILOE II when Check Certificate Revocation is set to Yes.

The Certificate Owner Field setting specifies which attribute of the client certificate to use when authenticating with the directory. If SAN is specified, RILOE II extracts the User Principle Name from the Subject Alternative Name attribute and then uses the User Principle Name when authenticating with the

directory, for example, username@domain.extension. If Subject is specified, RILOE II will derive the user's distinguished name from the subject name attribute. For example, if the subject name is `/DC=com/DC=domain/OU=organization/CN=user`, RILOE II will derive: `CN=user,OU=organization,DC=domain,DC=com.`

The Certificate Owner Field setting is only used if directory authentication is enabled. Configuration of the Configuration Owner Field depends on the version of directory support used, the directory configuration, and the certificate issuing policy of your organization.

A trusted CA certificate is required for two-factor authentication to function. You cannot change the Enforce Two-Factor Authentication setting to Yes if a trusted CA certificate has not been configured. Also, a client certificate must be mapped to a local user account if local user accounts are used. If RILOE II is using directory authentication, client certificate mapping to local user accounts is optional.

To change two-factor authentication settings for RILOE II:

1. Log in to RILOE II using an account that has the Configure RILOE II Settings privilege. Click **Administration.**
2. Click **Two-Factor Authentication Settings.**
3. Change the settings as needed by entering your selections in the fields.
4. After completing any parameter changes, click **Apply** to save the changes.

Security Settings

The **Security Settings** provided for the RILOE II include:

- **Session Timeout**—This option allows the Remote Console session on the network client to end automatically after the set amount of time selected.
- **ROM-Based Configuration Utility (F8)**—This option allows you to enable or disable the RBSU F8 setup.
- **Remote Access with Pocket PC**—This option allows you to enable or disable the remote access for pocket PCs.

To change the security settings:

1. Log in to the RILOE II using an account with administrator privileges.
2. Click **Global Settings** on the **Administration** tab.
3. Change the settings in the **Security Settings** section.
4. Click **Apply Settings.**

Another security feature is the progressive delays for failed browser login attempts. After a series of five failed login attempts by a user, the RILOE II imposes delays to subsequent logins. This scenario continues until a valid login is completed. This feature assists in defending against possible dictionary attacks against the browser login port.

RILOE II firmware updates

Firmware upgrades enhance the functionality of RILOE II. Firmware upgrades can be accomplished from any network client using a standard web browser. However, only users with the "configure RILOE settings" privilege can upgrade the firmware on RILOE II.

The most recent firmware is available on the HP website (http://www.hp.com/servers/lights-out) as a Smart Component.

To upgrade RILOE II firmware:

1. Log in to RILOE II using an account with "configure RILOE settings" privileges.
2. Click **Upgrade Firmware** on the **Administration** tab.

3. Follow the instructions on the firmware upgrade page. If you need additional assistance, click **?**.
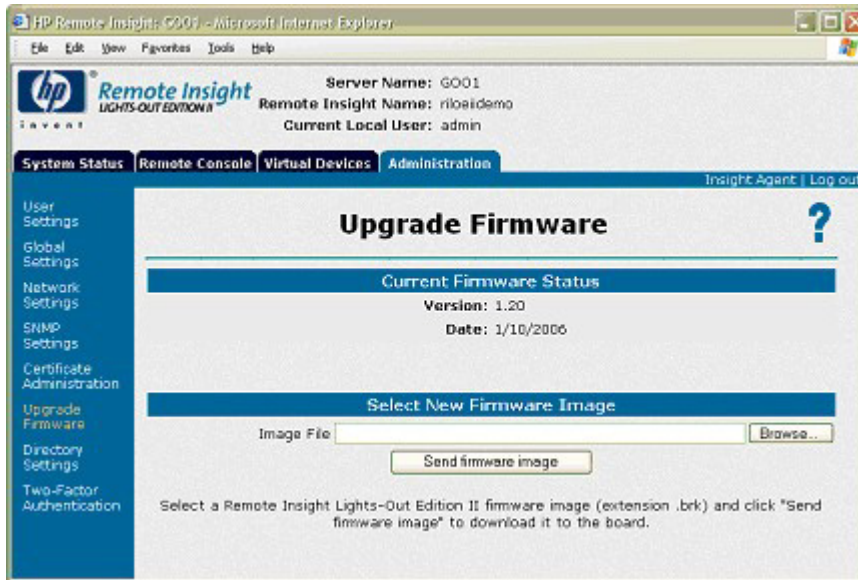
Using the Remote Console

The Remote Console tab provides access to different views of the Remote Console and enables you to define keystroke sequences that are transmitted to the remote host server by pressing a hot key. Standard RILOE II provides embedded hardware Remote Console capabilities on a text mode page. The operating system-independent console supports text modes that display remote host server activities, such as shutdown and startup operations.

The Remote Console option redirects the host server console to the network client browser, providing full text (standard) and graphical mode video, keyboard, and mouse access to the remote host server.

With the Remote Console, you have complete control over a remote host server as if you were in front of it. You can access the remote file system and the network drives. The Remote Console enables you to change hardware and software settings for the remote host server, install applications and drivers, change remote server screen resolution, and gracefully shut down the remote system.

With the Remote Console, you can observe POST boot messages as the remote host server restarts and initiate ROM-based setup routines to configure the hardware of the remote host server. When installing operating systems remotely, the graphical Remote Console enables you to view and control the host server page throughout the installation process.

For best performance, be sure to configure the host operating system display as described in "Optimizing performance for graphical Remote Console (on page 37)."

Remote Console Information Option

The Remote Console Information option displays information concerning the Remote Console options available, as well as a link to download an updated Java™ Runtime Environment, which is necessary for using Remote Console with the single cursor option.

Although up to 10 users are allowed to simultaneously log in to RILOE II, only one user at a time can access the Remote Console. A warning message displays indicating the Remote Console is already in use.

Remote Console will not be available if the remote console port configuration on the Global Settings tab is set to disabled.

Using Enhanced Features of the Remote Console

Local Cursor

Local (single) cursor mode presents a single mouse cursor during a Remote Console session. Synchronization of two cursors is eliminated, making navigation easier in the Remote Console window. Local cursor mode is the default setting.

The dual cursor mode uses two mouse cursors in the Remote Console window to represent the host server mouse cursor and the local client mouse cursor. The local client cursor is seen as a crosshair in the Remote Console window.

To switch to dual cursor mode, click **OFF** next to Local Cursor. To return to single cursor mode, click **ON** next to Local Cursor.

Refresh

Instances might occur when the Remote Console screen is not displaying the latest data. Click **Refresh** to force the RILOE II to repaint the screen.

Ctl+Alt+Del

Click **Ctl+Alt+Del** to log on to Windows NT®, Windows® 2000, and Windows® Server 2003.

Alt Lock

The ALT key on the local keyboard is not passed from the client to the host server. To simulate pressing the ALT key on the host server, select **ALT Lock**.

Character Set

Use this option to change the default character set used by the Remote Console and the type of operating system to which the Remote Console is connected. Modifying the Remote Console settings ensures proper operation of the Remote Console and correct display of colors and characters.

Optimizing performance for graphical Remote Console

HP recommends the following client and server settings based on the operating system used.

Recommended client settings

Ideally, the remote server operating system display resolution should be the same resolution, or smaller, than that of the browser computer. Higher server resolutions transmit more information, slowing the overall performance.

Use the following client and browser settings to optimize performance:

- **Display Properties**
  - Select an option greater than 256 colors.
  - Select a greater screen resolution than the screen resolution of the remote server.
  - Linux X Display Properties—On the X Preferences screen, set the font size to **12.**
- **Remote Console**
  - For Remote Console speed, HP recommends using a 700-MHz or faster client with 128 MB or more of memory.
  - For the Remote Console Java™ applet execution, HP recommends using a single processor client.
- **Mouse Properties**
  - Set the Mouse Pointer speed to the middle setting.
  - Set the Mouse Pointer Acceleration to low or disable the pointer acceleration.

Remote Console Linux settings

When using the RILOE II Remote Console to display text screens in Linux, border characters or other line drawing characters might not display correctly.

To properly configure the Remote Console text mode character set:

1. Click the **Character Set** dropdown menu from the Remote Console applet.
2. Select the **Lat1–16** character set.

Recommended server settings

The following is a list of recommended server settings based on the operating system used.

📝 **NOTE:** To display the entire host server screen on the client Remote Console applet, set the server display resolution less than or equal to that of the client.

Microsoft® Windows® 2000 settings

To optimize performance, set server **Display Propertie**s to a plain background (no wallpaper pattern).

Microsoft® Windows® Server 2003 settings

To optimize performance, set the server **Display Properties to** plain background (no wallpaper pattern) and set the Server **Mouse Properties** to **Disable Pointer Trails.**

Microsoft® Windows NT® 4.0 and Windows® 2000 settings

Use the following settings to optimize performance:

- Server **Display Properties**
  - Plain Background (no wallpaper pattern)
  - Display resolution of 800 x 600 or 1024 x 768 pixels
  - 256-color or 24-bit color mode
- Server **Mouse Properties**
  - Select **None** for mouse pointer Scheme.
  - Deselect **Enable Pointer Shadow.**
  - Select **Motion** or **Pointer Options** and set the pointer Speed slider to the middle position.
  - Set pointer Acceleration to **None.**

Red Hat Linux and SUSE Linux server settings

To optimize performance, set the server Mouse Properties>Pointer Acceleration to **1x.** For KDE, access the **Control Center,** select **Peripherals/Mouse,** then select the **Advanced** tab.

Novell NetWare settings

Use the following settings to optimize performance:

Server **Display Properties**

- 800 x 600 pixels or lower screen resolution
- 256 colors

Remote Console hot keys

The Remote Console hot keys feature enables you to define up to five multiple-key combinations for each hot key. When a hot key is pressed in the Remote Console, the defined key combination (all keys pressed at the same time) is transmitted in place of the hot key to the remote host server.

The Remote Console hot keys are active during a remote console session through the Remote Console applet and during a text remote console session through a telnet client.

To define a Remote Console hot key:

1. Click **Remote Console Hot Keys** in the Remote Console tab.
2. Select the hot key you want to define and use the list boxes to select the key sequence to be transmitted to the host server when you press the hot key.
3. Click **Save Hot Keys** when you have finished defining the key sequences.

The Remote Console Hot Keys page also contains a Reset Hot Keys option. The Reset Hot Keys option clears all entries in the hot key fields. Click **Save Hot Keys** to save the cleared fields.
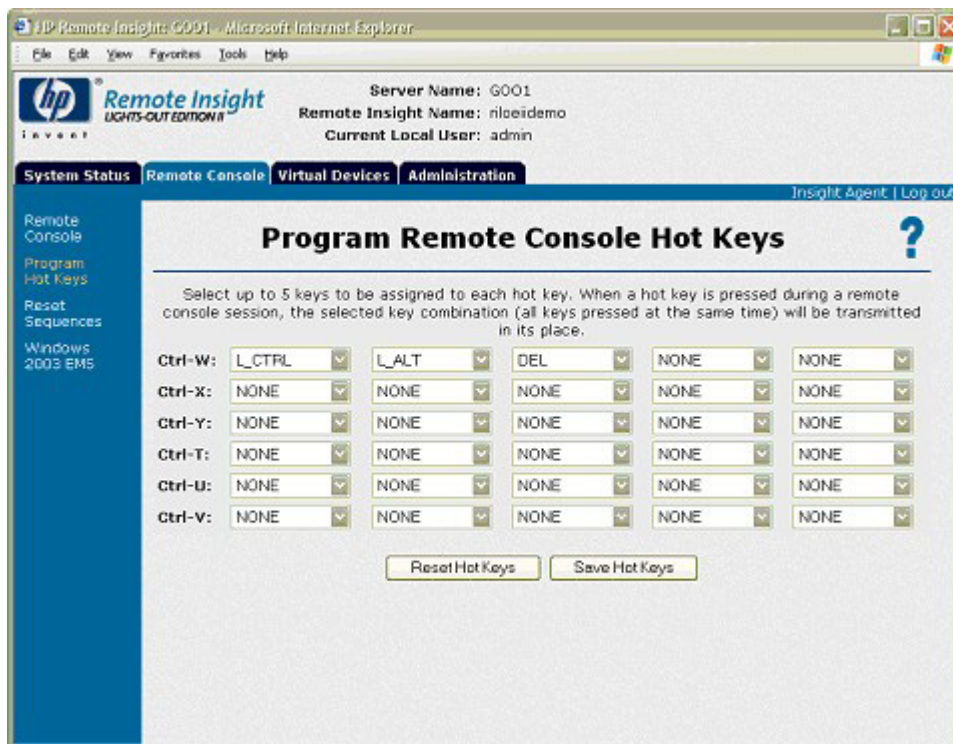
Supported hot keys

The Program Remote Console Hot Keys page allows you to define up to 6 different sets of hot keys for use during a Remote Console session. Each hot key represents a combination of up to 5 different keys which are sent to the host machine whenever the hot key is pressed during a Remote Console session. The selected key combination (all keys pressed at the same time) are transmitted in its place. For more information, refer to "Remote Console hot keys (on page 38)." The following table lists keys available to combine in a Remote Console hot key sequence.

ESC	F12	:	o
L_ALT	" " (Space)	<	p
R_ALT	!	>	q
L_SHIFT	#	=	r
R_SHIFT	$	?	s
INS	%	@	t
DEL	&	[	u
HOME	~	]	v
END	(	\	w
PG UP	)	^	x
PG DN	*	_	y
ENTER	+	a	z
TAB	-	b	{
BREAK	.	c	}

F1	/	d	|
F2	0	e	;
F3	1	f	'
F4	2	g	L_CTRL
F5	3	h	R_CTRL
F6	4	i	NUM PLUS
F7	5	j	NUM MINUS
F8	6	k	SCRL LCK
F9	7	l	BACKSPACE
F10	8	m	SYS RQ
F11	9	n	

Video replays of previous server Reset Sequences

The **Reset Sequences** option on the **Remote Console** tab provides video replay of server reset sequences. This option allows you to observe ROM-based POST messages and operating system load messages of previous host server resets, including any error messages displayed by the operating system before a server stops.

IMPORTANT: The reset sequences option requires the use of the Remote Console. You cannot access the Remote Console while replaying the reset sequences. A user cannot use Remote Console if another user is on one of the selected replay sequence pages. Only one user is permitted access to Remote Console at a time. If another user is viewing one of the previous, current, or failed sequence pages, you will receive the following message: "Another user is accessing the Remote Console feature of the RILOE II. Only one user is permitted access at a time. Remote Console will automatically start when Remote Console becomes available."

To access video replays of the host server reset sequences:

1. Click **Reset Sequences** on the **Remote Console** tab.
2. Select the desired sequence replay from the following options:
    - **Previous Reset Sequence Replay**—This option allows you to replay the video sequence prior to the most recent host server reset. The video replay displays ROM-based messages and operating system load messages that occurred while starting the remote host server.
    - **Current Reset Sequence Replay**—This option allows you to replay the video sequence of the most recent host server reset. The video replay displays ROM-based messages and operating system load messages that occurred while starting the remote host server.
    - **Failure Sequence Replay**—This option lets you replay the video sequence leading up to the most recent host server reset resulting from a system problem. This video replay includes any error information generated by the operating system prior to the host server problem and subsequent reset.

Windows® EMS console

A feature of Windows® Server 2003 is the EMS. The typical usage model for the EMS console is to physically connect a serial cable to the server. RILOE II, however, enables you to use EMS over the network through a Web browser. Microsoft® EMS gives you the ability to display running processes, change the priority of processes, and halt processes. The EMS console and the RILOE II Remote Console can be used at the same time.

The Windows® EMS Console, if enabled, provides the ability to perform EMS in cases where video, device drivers, or other operating system features have prevented normal operation and normal corrective actions from being performed.

The Windows® EMS serial port must be enabled through the host system RBSU. The configuration allows for the enabling or disabling of the EMS port, and the selection of the COM port. The RILOE II system will automatically detect whether the EMS port is enabled or disabled, and the selection of the COM port.

To obtain the `SAC>` prompt, typing `Enter` might be required after connecting through the Virtual Serial Port console.

For more information on using the EMS features, refer to the Windows® Server 2003 Server documentation.

Terminal Services pass-through option

Terminal Services is provided by the Microsoft® Windows® operating systems. The RILOE II Terminal Services pass-through option provides a connection between the Terminal Services server on the host system and the Terminal Services client on the client system. When the Terminal Services pass-through option is enabled, RILOE II firmware sets up a socket, listening by default on port 3389. All data received from the Terminal Services on this port is forwarded to the server and all data it receives from the server is forwarded back to the socket. The firmware assumes anything received on this port is in an RDP packet. RDP packets are exchanged between the RILOE II firmware and the server's Terminal Services (RDP) server through the localhost address on the server. A service is provided to facilitate communications between the RILOE II firmware and the RDP server, such that the RDP server believes that an external RDP connection has been established. For more information on RDP service, refer to the "Windows® RDP Pass-Through service (on page 42)" section.

A Terminal Services session provides a performance-enhanced view of the host system console. When the operating system is unavailable (or the Terminal Services server or client is unavailable), the traditional RILOE II remote console provides the view of the host system console. For more information on Remote Console and Terminal Services, refer to the "Remote Console and Terminal Services clients (on page 44)" section.

To configure the Terminal Services pass-through option, refer to "Terminal Services Client requirements (on page 41)" and "Terminal Services Pass Through installation ("Terminal Services pass-through installation" on page 42)."

Terminal Services Client requirements

The Terminal Services client is available on Microsoft® Windows® client machines running:

- Windows® 2000

  Microsoft® Windows® 2000 servers require the installation of Microsoft® .NET Framework to support the use of Terminal Services. After .NET Framework is installed, the Terminal Services client must be installed from diskettes created by the Terminal Services server. Consult your Windows® operating guides or help files for instructions. When installing the Terminal Services client on Windows® 2000, use the default installation location. The Terminal Services client in Windows® 2000 generates a dialog box asking for which target Terminal Services server to use.

- Windows® Server 2003

  On Windows® Server 2003 servers, the Terminal Services client and RDP connection is built in. The client is an integral part of the operating system and is activated using Remote Desktop sharing. To activate desktop sharing allow, select **My Computer>Properties>Remote>Remote Desktop.** The Terminal Services client in Windows® Server 2003 provides command line options and seamless launches from the Remote Console applet.

- Windows® XP

On Windows® XP servers, the Terminal Services client and RDP connection is built in. The client is an integral part of the operating system and is executed by selecting **Start>Programs>Accessories>Communications>Remote Desktop.** The Terminal Services client in Windows® XP provides command line options and seamless launches from the Remote Console applet.

Windows® RDP Pass-Through service

To use the RILOE II Terminal Services Pass-Through feature, a service must be installed on the host system. This service will show the name of RILOE II Proxy in the host's list of available services. The service utilizes the Microsoft® .NET framework's security and reliability. After the service has started, the service polls the RILOE II to find out if a an RDP connection with the client has been established. If an RDP connection with the client has been established, it then establishes a TCP connection with localhost and begins exchanging packets. The port used to communicate with localhost is read from the Windows® registry at

```
HKLM\SYSTEM\CurrentControlSet\Control\TerminalServer\Wds\rdpwd\Tds\tcp\P
ortNumber
```

This is typically port 3389.

Terminal Services pass-through installation

- Microsoft® Windows® 2000 and Windows® 2003 require Microsoft® .NET Framework to support the use of Terminal Services. The Terminal Services pass-through service and the RILOE II Management Interface Driver for Microsoft® Windows® 2000 and Microsoft® Windows Server™ 2003 must be installed on the server that has the RILOE II. The service and RILOE II driver are available as Smart Components on the HP website and on the HP SmartStart CD. They are also part of the ProLiant Support Pack for Microsoft® Windows® Server 2003 and Microsoft® Windows®.

  a. Install the RILOE II Management Interface driver.

  b. Install the service. To install the service, launch the component installer and follow the directions in the installation wizard.

     If the service is already installed, then it must be manually restarted or the server rebooted when the driver is installed.

  c. Install or activate the Terminal Services client.

     Microsoft® Windows® 2000 servers require the installation of Microsoft® .NET Framework to support the use of Terminal Services. After .NET Framework is installed, the Terminal Services client must be installed from diskettes created by the Terminal Services server or by downloading the client from the Microsoft® website and installed through the Control Panel using Add or Remove Programs. Consult your Windows® operating guides or help files for instructions. When installing the Terminal Services client on Windows® 2000, use the default installation location.

     On Microsoft® Windows Server™ 2003, you can activate Remote Desktop sharing by selecting the **Remote** tab under My Computer and Properties.

  If the RILOE II installation is complete and if Terminal Services Pass-through is set to automatic, then Terminal Services launches when the installation is complete.

- Microsoft® Windows® XP clients have the Remote Desktop Connection built in and no other installation is required.

Errors during installation and during execution of the pass-through service are logged in the server's Application Event Log. The pass-through service can be removed using Add or Remove Programs in the Control Panel.

Windows® 2000 Terminal Services port change

If the Terminal Services port is changed, Windows® 2000 client must manually configure the Terminal Services Client Connection Manager.

1. Start the Terminal Services Client Connection Manager, and create a new connection to the terminal server.
2. Highlight the icon created, and select **File>Export.** Rename the file with a .cns extension. For example: myilo.cns.
3. Edit the `myilo.cns` file by looking for the line Server Port=3389. Replace 3389 with your new port number and save the file.
4. From the Client Connection Manager, highlight the **New Connection** icon, and click **File>Import.**
5. Double-click the newly created icon to launch terminal server and connect to the new port.

Enabling the Terminal Services Pass-Through option

By default, the Terminal Services pass-through feature is disabled and must be enabled in Global Settings. Until the Terminal Services pass-through feature is enabled, the Remote Console has the Terminal Services button deactivated, and the console session error message `Remote Session already in use by another user` is misleading.

Use of the Terminal Services pass-through feature requires installation of the latest Lights-Out Management Interface Driver and Terminal Services pass-through Service for Microsoft® Windows® on the server. The interface driver must be installed before installing the service.

When the Terminal Services pass-through option is set to Enabled or Automatic on the Global Settings page and the Terminal Services Client is installed on the Windows® client (installs by default on Windows® XP), the Terminal Services button is enabled. When the Terminal Services button is clicked, the applet tries to launch the Terminal Services, even if the server is not running a Windows® operating system.

You must comply with Microsoft® license requirements which are the same as connecting through the server's NIC. For instance, when set for administrative access, Terminal Services does not allow more than two connections, regardless of whether the connections are through the server's NIC or RILOE II or both.

Terminal Services Pass-Through status

The RILOE II Status page displays the status of the Terminal Services pass-through feature, as follows:

- Server software not detected
- Available for use
- In use

The UID light flashes whenever a Terminal Services connection is active through the RILOE II. It flashes at the same frequency and duty cycle as when the Remote Console is active.

Terminal Services warning message

Terminals Services users operating on Windows® 2003 Server might notice the following when using the Terminal Services pass-through feature of RILOE II. If a Terminal Services session is established through RILOE II and a second Terminal Services session is established by a Windows® administrator (Console mode), the first Terminal Services session is disconnected. However, the first Terminal Services session does not receive the warning message indicating the disconnection until approximately one minute later. During this one-minute period, the first Terminal Services session is available or active. This is normal behavior, but it is different than the behavior observed when both Terminal Services sessions are established by Windows® administrators. In that case, the warning message is received by the first Terminal Services session immediately.

Terminal Services button display

RILOE II firmware does not accurately display through the Terminal Services button. Even if the operating system is not enabled (for example, the host operating system is Linux, which does not support Terminal Services operation), the Terminal Services button might not appear inactive and might inaccurately imply that Terminal Services operation is available.

Remote Console and Terminal Services clients

Using the management network connection to the RILOE II, an RILOE II Remote Console session can be used to display a Terminal Services session to the host. When the RILOE II Remote Console applet runs, it launches the Terminal Services client based on user preference. The Sun JVM must be installed to obtain full functionality of this feature. If the Sun JVM is not installed, then the dual-cursor Remote Console cannot automatically launch the Terminal Services client.

If Terminal Services pass-through is enabled, and the Terminal Services server is available, switching between RILOE II Remote Console and the Terminal Services client will be seamless as the server progresses from pre-OS environment to OS-running environment, to OS-not available environment. The seamless operation is available as long as the Terminal Services client is not started before Remote Console is available. If Remote Console is available, and the Terminal Services client is available, Remote Console will start the Terminal Services client when appropriate.

When using the Terminal Services pass-through option with Windows® 2000, there is approximately a one-minute delay after the CTRL-ALT-DEL dialog box appears before the Terminal Services client launches. On Windows® Server 2003, the delay is about 30 seconds. The 30 second delay represents how long it takes for the service to connect to the RDP client running on the server. If the server is rebooted from the Terminal Services client, the Remote Console screen turns grey or black for up to one minute while RILOE II determines that the Terminal Services server is no longer available.

If Terminal Services mode is set to `Enabled`, but you want to use the Remote Console, then the Terminal Services client should be launched directly from the Terminal Services client menu. Launching directly from the client menu allows simultaneous use of the Terminal Services client and the Remote Console.

Terminal Services can be disabled or enabled at any time. Changing the Terminal Services configuration causes the RILOE II firmware to reset. Resetting the RILOE II firmware interrupts any open connections to RILOE II.

When the Terminal Services client is launched by the Remote Console, Remote Console goes into a sleep mode to avoid consuming CPU bandwidth. Remote Console still listens to the Remote Console default port 23 for any commands from the RILOE II.

RILOE II passes-through only one Terminal Services connection at a time. Terminal Services has a limit of two concurrent sessions.

The Remote Console activates and becomes available if the Remote Console is in sleep mode and the Terminal Services client is interrupted by any of the following:

- The Terminal Services client is closed by the user.
- The Windows® operating system is shut down.
- The Windows® operating system locks-up.

Troubleshooting Terminal Services

If you are experiencing problems with RILOE II Terminal Services pass-through, check the following:

1. Verify that Terminal Services is enabled on the host by selecting **My Computer>Properties>Remote>Remote Desktop.**

2. Verify that the RILOE II pass-through configuration is enabled or set to automatic by checking the RILOE II Global Settings configuration.

3. Verify if the RILOE II Management Interface Driver is installed on the host by selecting **My Computer>Properties>Hardware>Device Manager>Multifunction Adapters.**

4. Verify if Terminal Services pass-through service and the RILOE II proxy is installed and running on the host by selecting **Control Panel>Administrative Tools>Services** and attempting to restart the Terminal Service.

5. Determine if the Application Event Log is full.

    The Terminal Services pass-through service might experience start-up problems when the operating system Application Event Log is full. To view the event log, select **Computer Management>System Tools>Event Viewer>Application.**

6. Verify that the Terminal Services port assignment is correct. Verify that the Terminal Services client, mstsc.exe, is located in \WINDOWS\SYSTEM32.

    If not, reconfigure the pass-through configuration to **Enabled** and manually activate the Terminal Services client.

Using virtual devices

With virtual devices, an administrator directs a host server to boot and use a diskette or CD-ROM on the client machine or use an image file from anywhere on the network. Virtual devices eliminate the need to visit a host server to insert and use a diskette or CD-ROM, enabling remote operating system installation and host server ROM updates from a CD or network drive.

Virtual devices allow you to carry out any of the following functions:

*   Running User Diagnostics by booting the host server from a diagnostic diskette

NOTE: HP recommends that you first delete the SYSMON2.TM file before using User Diagnostics with the Virtual Floppy Drive.

*   Applying ROM updates to remote host servers
*   Deploying an operating system or other software from a CD in a client machine to a host server
*   Performing disaster recovery of failed operating systems

NOTE: If the server operating system does not support ACPI, using the virtual power button feature of the RILOE II will shut down the server immediately and not permit a graceful shutdown.

Virtual power

The Virtual Power button enables control of the power state of the remote server and simulates pressing the physical power button on the server. If the remote host server is not responding, the Virtual Power button feature allows you to initiate a cold or warm reboot to bring the server back online.
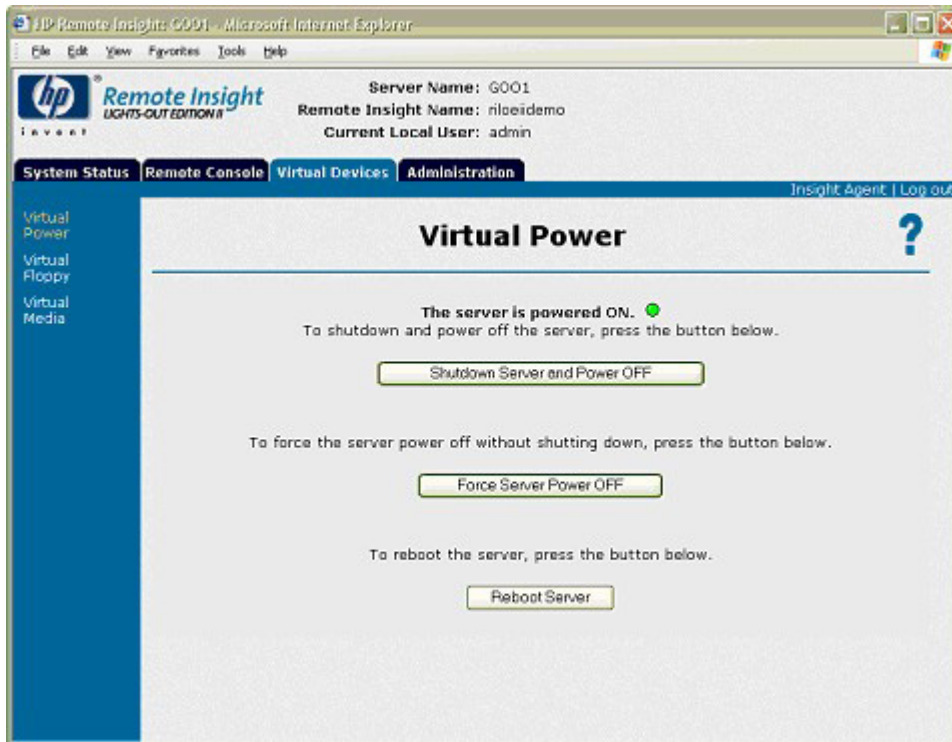
Some of the following power options do not gracefully shut down the operating system. To initiate a graceful shutdown, use the Remote Console before using the Virtual Power button.

Use the refresh feature of the browser to keep the status of the power indicator up to date.

To use the Virtual Power button, select the power option you want and click to initiate the power option.

The available power options are:

- Shutdown Server and Power OFF performs a graceful shutdown before initiating a power off to the host server. Shutdown Server and Power OFF is enabled on if RILOE II is attached to the server's power button using the correct cable.
- Turn Server Power ON turns the server on.
- Force Server Power Off forces the server power off and does not initiate a graceful shutdown. Force Server Power Off is available only if RILOE II is attached to the server's power button using the correct cable.
- Reboot Server initiates a reboot of the server and does not initiate a graceful shutdown before rebooting the server.

Virtual media

RILOE II Virtual Media option provides you with a Virtual Floppy disk drive and CD-ROM drive, which can direct a remote host server to boot and use standard media from anywhere on the network. Virtual Media devices are available when the host system is booting. RILOE II Virtual media devices connect to the host server using USB technology. Using USB also enables new capabilities for RILOE II Virtual Media devices when connected to USB-supported operating systems. Different operating systems provide varying levels of USB support.

- If the Virtual Floppy capability is enabled, the floppy drive normally cannot be accessed from the client operating system.
- If the Virtual CD-ROM capability is enabled, the CD-ROM drive cannot be accessed from the client operating system.

Under certain conditions, you can access the Virtual Floppy drive from the client operating system while it is connected. However, it is important that access to the Virtual Floppy drive from the client operating system not be attempted while it is connected as a virtual media device. Doing so could cause data loss on the floppy drive. Always disconnect virtual media before trying to access it from the client operating system.

You can access virtual media on a host server from a client through a graphical interface using a Java™ applet and through a script interface using an XML engine.

To access RILOE II Virtual Media devices using the graphical interface, select Virtual Media on the Virtual Devices tab. An applet loads in support of the Virtual Floppy or Virtual CD-ROM device.

RILOE II Virtual Floppy

RILOE II Virtual Floppy disk is available at server boot time for all operating systems. Booting from RILOE II Virtual Floppy enables you to upgrade the host system ROM, deploy an operating system from network drives, and perform disaster recovery of failed operating systems, among other tasks.

If the host server operating system supports USB mass storage devices, then RILOE II Virtual Floppy is also available after the host server operating system loads. You can use RILOE II Virtual Floppy when the host server operating system is running to upgrade device drivers, create an emergency repair diskette, and perform other tasks. Having the Virtual Floppy available when the server is running can be especially useful if you must diagnose and repair a problem with the NIC driver.

The Virtual Floppy can be the physical floppy drive on which you are running the web browser, or an image file stored on your local hard drive or network drive.

NOTE: For best performance use image files. HP recommends using local image files stored either on the hard drive of your client PC or on a network drive accessible through a high-speed network link.

To use a physical floppy in your client PC:

1. Select **Local Media Drive.**
2. Select the drive letter of the desired local floppy or USB key drive on your client PC from the dropdown menu. To ensure the source diskette or image file is not modified during use, select the **Force read-only access** option.
3. Click **Connect.**

The connected drive icon and LED changes state to reflect the current status of the Virtual Floppy Drive.
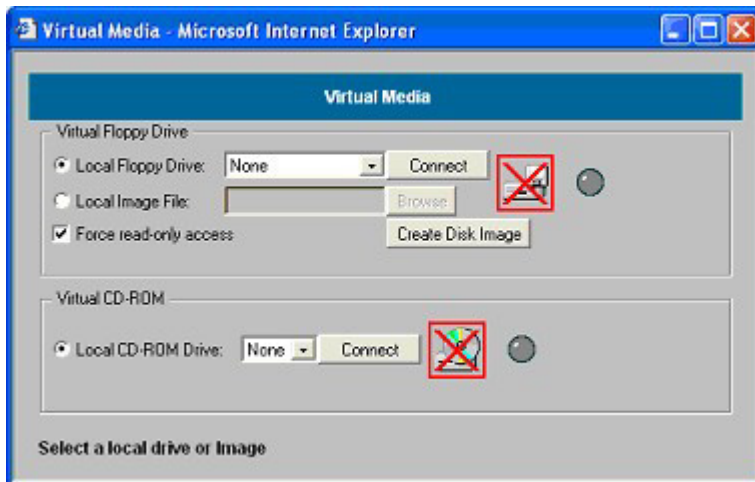
To use an image file:

1. Select **Local Image File** within the Virtual Floppy section of the Virtual Media applet.
2. Enter the path or file name of the image in the text box, or click **Browse** to locate the image file using the Choose Disk Image File dialog. To ensure the source diskette or image file is not modified during use, select the **Force read-only access** option.
3. Click **Connect.**

The connected drive icon and LED changes state to reflect the current status of the Virtual Floppy drive. When connected, the virtual devices are available to the host server until you close the Virtual Media applet. When you are finished using the Virtual Floppy, you can either select to disconnect the device from the host server or close the applet.

NOTE: The Virtual Media applet must remain open in your browser as long as you continue to use a Virtual Media Device.

RILOE II Virtual Floppy is available to the host server at run time if the operating system on the host server supports USB floppy drives. See "Operating System USB Support (on page 57)" for information on which operating systems support USB mass storage at the time of the publication of this manual.

RILOE II Virtual Floppy appears to your operating system just like any other drive. When using RILOE II for the first time, the host operating system might prompt you to complete a New Hardware Found wizard.

When you are finished using RILOE II Virtual Media and disconnect it, you might receive a warning message from the host operating system regarding unsafe removal of a device. This warning can be avoided by using the operating system-provided feature to stop the device before disconnecting it from the Virtual Media.

Virtual Floppy operating systems notes

- MS-DOS

  During boot and during an MS-DOS session, the Virtual Floppy device displays as a standard BIOS floppy drive. This device will display as drive A. An existing physically attached floppy drive is obscured and unavailable during this time. You cannot use a physical local floppy drive and the Virtual Floppy simultaneously.

- Windows® 2000 SP3 or later and Windows® Server 2003

  Virtual Floppy drives display automatically after Microsoft® Windows® has recognized the mounting of the USB device. Use it as you would a locally attached device.

  To use Virtual Floppy during a Windows® installation to provide a driver diskette, disable the integrated diskette drive in the host RBSU which forces the Virtual Floppy to appear as drive A.

- Red Hat and SLES Linux

  Linux supports the use of USB diskette drives. Refer to the "Mounting USB Virtual Floppy in Linux ("Mounting USB Virtual Media Floppy in Linux" on page 49)" section for step-by-step instructions.

Mounting USB Virtual Media Floppy in Linux

1. Access RILOE II through a browser.
2. Select **Virtual Media** in the Virtual Devices tab.
3. Select a diskette drive or diskette image and click **Connect.**
4. Load the USB drivers, using the following commands:

   ```
   modprobe usbcore
   modprobe usb-storage
   modprobe usb-ohci
   ```
5. Load the SCSI disk driver, using the following command:

   ```
   modprobe sd_mod
   ```
6. Mount the floppy drive, using the following command:

   ```
   mount /dev/sda  /mnt/floppy -t vfat
   ```

NOTE: Use the `man mount` command for additional file system types.

The floppy device can be used as a Linux file system, if formatted as such, with the `mount` command. However, 1.44-Mb diskettes are usually accessed utilizing the mtools utilities distributed with both Red Hat and SLES. The default mtools configuration does not recognize a USB-connected floppy. To enable the various m commands to access the Virtual Floppy device, modify the existing /etc/mtools.conf file and add the following line:

```
drive v: file="/dev/sda" exclusive
```

This modification enables the mtools suite to access the Virtual Floppy as v. For example:

```
mcopy /tmp/XXX.dat v:
mdir v:
mcopy v:foo.dat /tmp/XXX
```

Virtual Floppy screen

The **Virtual Floppy** screen provides the status of the Virtual Floppy, the ability to load a Virtual Floppy image, and the ability to change Virtual Floppy settings.

Uploading a diskette image to the remote server

The Insert Floppy Image option allows you to send a diskette image file to RILOE II on the remote host server. RILOE II treats the diskette image file as a standard diskette.

The external power of the 16- and 30-pin Remote Insight cables must be installed when booting to a Virtual Floppy, otherwise the image will be lost when the server is reset.

NOTE: Image files of diskettes are created and stored locally on the hard drive or on a network drive with the Diskette Image Utility (on page 51). This utility is available for download from the HP website (http://www.hp.com/servers/lights-out).
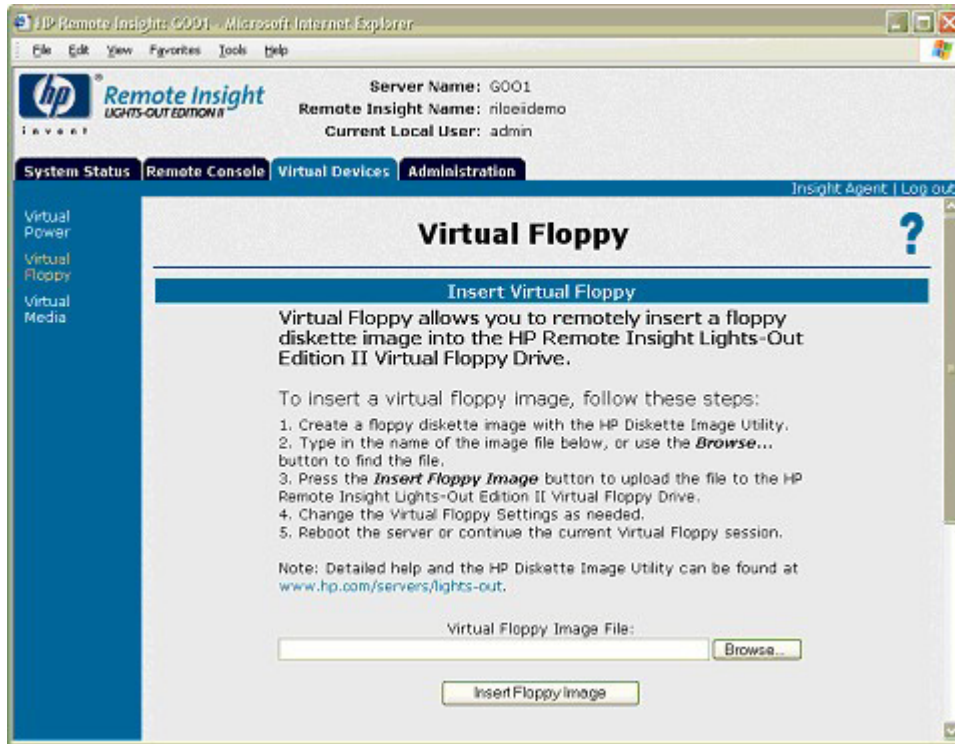
To upload a diskette image to RILOE II on the host server:

1. Click **Virtual Floppy** in the Virtual Devices tab.

2. Enter the location and name of the diskette image file, or click **Browse** and select the diskette image file you want to transfer to RILOE II.

3. When the full path and diskette image file name are in the text entry field, click **Insert Floppy Image** to upload the image file to RILOE II in the host server.

The Virtual Floppy Drive can hold only one diskette image file at a time. The uploaded diskette image file remains in the Virtual Floppy Drive until it is either replaced with another diskette image file or erased from the Virtual Floppy Drive by clicking Eject Virtual Floppy on the Virtual Floppy Status page. The diskette image file is erased if power to RILOE II is lost. Logging out of RILOE II does not erase the diskette image file from the Virtual Floppy Drive.

Changing Virtual Floppy drive settings

The **Virtual Floppy** screen allows you to view and change current settings for the Virtual Floppy Drive. Changes you make to the virtual diskette drive boot and write-protect options take effect when you click **Submit Changes.**

A host server can use files uploaded to a Virtual Floppy Drive only if the Virtual Floppy Drive is active. The Virtual Floppy Drive becomes active when the RILOE II restarts the host server using a diskette image file uploaded to the Virtual Floppy Drive. The Virtual Floppy Drive remains active until the remote host server is restarted with its own operating system.

NOTE: Although the Virtual Floppy Drive is active, the physical diskette drive of the host server is temporarily disabled. The diskette drive of the host server becomes re-enabled when the host server is restarted with its own operating system and the Virtual Floppy Drive is not active.

The Virtual Floppy Boot option has three settings:

- **Boot Always**—This setting instructs the RILOE II to always boot the host server from the diskette image file in the Virtual Floppy Drive. If this setting is checked, the **Virtual Floppy Status** screen shows the virtual drive as active after the server has restarted.

- **Boot Once**—This setting instructs the RILOE II to boot the host server one time from the diskette image file in the Virtual Floppy Drive. If this setting is checked, the **Virtual Floppy Status** screen shows the virtual drive as active after the server has restarted.

- **No Boot**—This is the default setting for the Virtual Floppy Drive. It instructs the RILOE II not to boot the host server from the diskette image file in the Virtual Floppy Drive. This setting has no effect on the Virtual Floppy Drive status.

Copying files on the host server to the Virtual Floppy drive

The **Write Protect Virtual Floppy** option on the **Virtual Floppy** screen specifies whether data on the host server can be copied to the Virtual Floppy Drive. If this option is selected, the Virtual Floppy Drive is write protected and no data from the host server can be copied to it.

To copy remote files to the Virtual Floppy Drive using standard operating system commands typed at the Remote Console, be sure that the **Write Protect Virtual Floppy** option is deselected. The **Virtual Floppy** option cannot be used to upgrade the RILOE II firmware.

Diskette Image Utility

The Diskette Image Utility has three functions:

- Creating an image file from a standard 1.44-MB diskette suitable for use with the Virtual Floppy Drive

- Creating a standard 1.44-MB diskette from an image file copied from the Virtual Floppy Drive

- Comparing a diskette image file with a standard 1.44-MB diskette

To create an image file from a diskette

1. Launch the Diskette Image Utility and click the **Create Image File** tab.
2. Insert the diskette you want to make an image of into the diskette drive.
3. Provide the path, the file name of the image, and an image file description. A page similar to the following appears.

📝 **NOTE:** The path can be a local or a network path. If you do not provide a path, the image file is saved on the Desktop.

4. Click **Create** to generate the image file in the specified location.
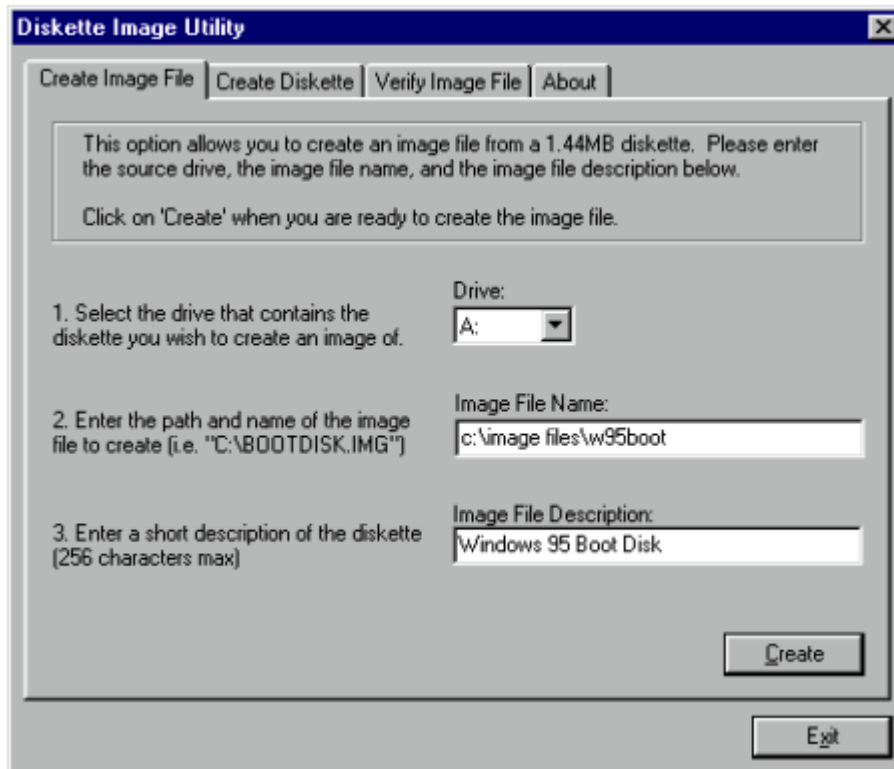
To create a diskette from an image file

1. Launch the Diskette Image Utility and click the **Create Diskette** tab.
2. Insert a blank diskette into the diskette drive.

⚠ **CAUTION:** If the diskette is not blank, all data on the diskette will be erased.

3. Enter the path and name of the image file and the target diskette drive.
4. To navigate to the location of the image file, click **Browse.** A page similar to the following appears.

5. Click **Create** to generate the diskette from the image file.
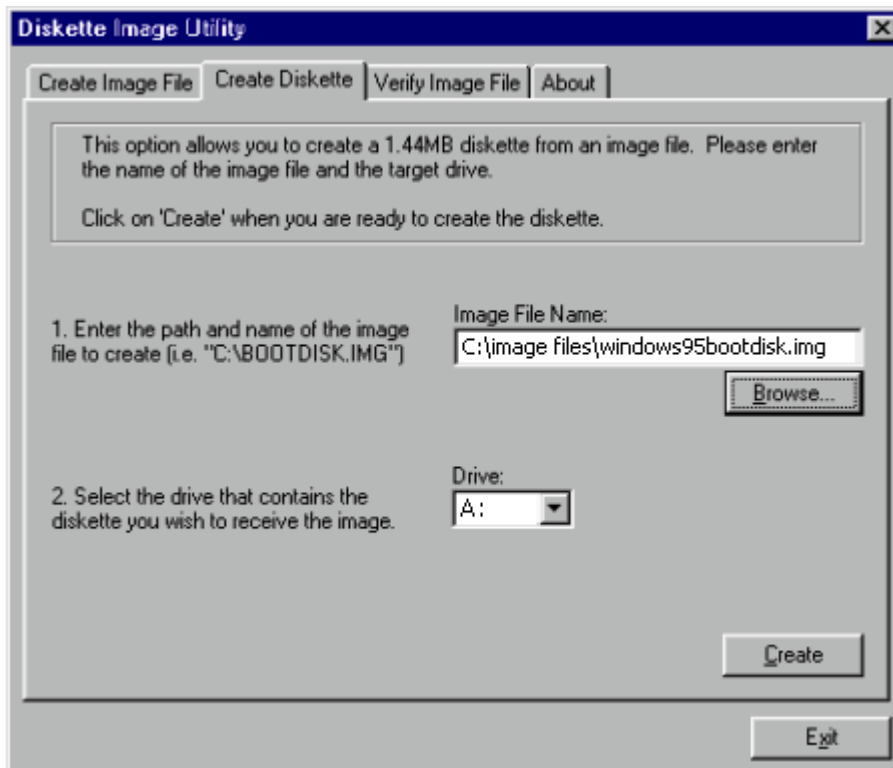
To compare an image file with a diskette

1. Launch the Diskette Image Utility and click the **Verify Image File** tab.
2. Insert the diskette you want to compare against an image file into the diskette drive.
3. Enter the path and name of the image file and the target diskette drive or navigate to the location of the image file by clicking **Browse.** A page similar to the following appears.

4. Click **Verify** to start comparing the image file with the diskette. When the verification is complete, the results appears.
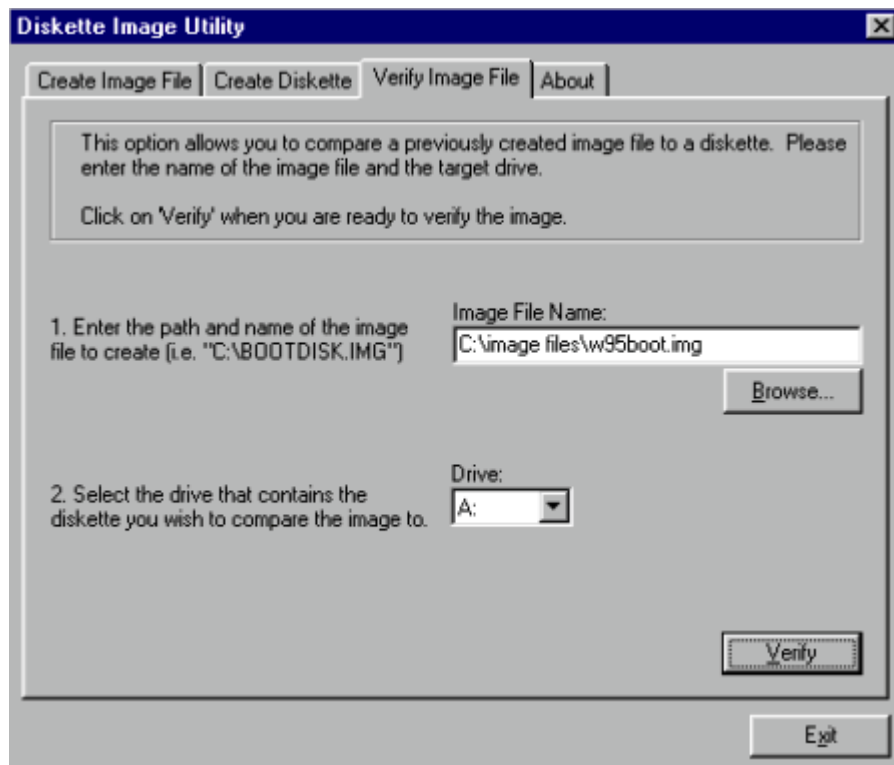
RILOE II Virtual CD-ROM

RILOE II Virtual CD-ROM is available at server boot time for operating systems specified in the "Operating system USB support (on page 57)" section. Booting from RILOE II Virtual CD-ROM enables you to deploy an operating system from network drives, and perform disaster recovery of failed operating systems, among other tasks.

If the host server operating system supports USB mass storage devices, then RILOE II Virtual CD-ROM is also available after the host server operating system loads. You can use RILOE II Virtual CD-ROM when the host server operating system is running to upgrade device drivers, install software, and perform other tasks. Having the Virtual CD-ROM available when the server is running can be especially useful if you must diagnose and repair a problem with the NIC driver.

The Virtual CD-ROM can be the physical CD-ROM drive on which you are running the web browser, or an image file stored on your local hard drive or network drive.

NOTE: For best performance use image files. HP recommends using local image files stored either on the hard drive of your client PC or on a network drive accessible through a high-speed network link.

To use a physical CD-ROM drive in your client PC:

1. Select **Local CD-ROM Drive.**

2. Select the drive letter of the desired physical CD-ROM drive on your client PC from the dropdown menu.

3. Click **Connect.**
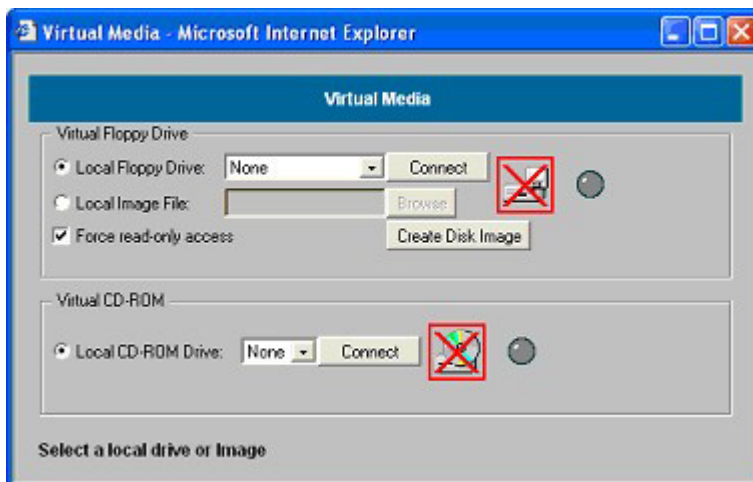
To use an image file:

1. Select **Local Image File** within the Virtual CD-ROM section of the Virtual Media applet.

2. Enter the path or file name of the image in the text box or click **Browse** to locate the image file using the Choose Disk Image File dialog.

3. Click **Connect.**

The connected drive icon and LED changes state to reflect the current status of the Virtual CD-ROM. When connected, virtual devices are available to the host server until you close the Virtual Media applet. When you are finished using the Virtual CD-ROM, you can choose to disconnect the device from the host server or close the applet. The Virtual Media applet must remain open when using a Virtual Media Device.

RILOE II Virtual Media CD-ROM will be available to the host server at run time if the operating system on the host server supports USB floppy drives. See "Operating system USB support (on page 57)" for information on which operating systems support USB mass storage at the time of the publication of this manual.

RILOE II Virtual Media CD-ROM appears to your operating system just like any other CD-ROM. When using RILOE II for the first time, the host operating system may prompt you to complete a New Hardware Found wizard.

When you are finished using RILOE II virtual media and disconnect it, you might receive a warning message from the host operating system regarding unsafe removal of a device. This warning can be avoided by using the operating system-provided feature to stop the device before disconnecting it from the Virtual Media.

Virtual Media CD-ROM operating system notes

- MS-DOS

  The virtual CD-ROM is not supported in MS-DOS.

- Windows® 2000 SP3 or later and Windows® Server 2003

  The virtual CD-ROM displays automatically after Windows® has recognized the mounting of the USB device. Use it as you would a locally attached CD-ROM device.

  On Windows® 2000 SP3 or later, My Computer on the host server displays an additional CD-ROM drive when the Virtual Media applet is connected. If the server operating system is up and running and you attempt to disconnect and reconnect within the Virtual Media applet, it can fail. The icon turns green, but the additional CD-ROM drive does not display in My Computer.

To resolve this problem, reboot the host server, and, after the operating system is available, the Virtual Media CD-ROM is ready for use. This problem only occurs on servers with no physical CD-ROM drive.

- Linux
  - Red Hat Linux

    On servers with a locally attached IDE CD-ROM, the virtual CD-ROM device is accessible at /dev/cdrom1. However, on servers without a locally attached CD-ROM, such as the BL-class blade systems, the virtual CD-ROM is the first CD-ROM accessible at /dev/cdrom.

    The virtual CD-ROM can be mounted as a normal CD-ROM device using:

    mount /mnt/cdrom1
  - SLES 9

    The SLES 9 operating system places USB-connected CD-ROMs in a different location and the virtual CD-ROM can be found at /dev/scd0, unless there is already a USB-connected local CD-ROM, in which case, it would be /dev/scd1.

    The virtual CD-ROM can be mounted as a normal CD-ROM device using:

    mount /dev/scd0 /media/cdrom11

Refer to "Mounting USB Virtual Media CD-ROM in Linux (on page 56)" for step-by-step instructions.

Mounting USB Virtual Media CD-ROM in Linux

1. Access RILOE II through a browser.
2. Select **Virtual Media** in the Virtual Devices tab.
3. Select a CD-ROM to be used and click **Connect.**
4. Mount the drive using the following command:

   ```
   mount /dev/cdrom1  /mnt/cdrom1
   ```

   For SLES 9:

   ```
   mount /dev/scd0  /media/cdrom11
   ```

Creating RILOE II disk image files

The RILOE II virtual media feature enables you to create diskette and CD-ROM image files within the same applet. Creation of DVD image files using the Virtual Media applet is not supported. The image files created from the applet are ISO-9660 file system images. The performance of RILOE II virtual media is faster when image files are used. The utility to create RILOE II Virtual Floppy and CD-ROM disk image files is integrated into the Virtual Media applet; however, images can also be created using industry-standard tools, such as DD.

To create an image file:

1. Click **Create Disk Image**.
2. Select the local media drive from the dropdown menu.
3. Enter the path or file name in the text box or click **Browse** to select an existing image file or to change the directory in which the image file will be created.

4. Click **Create.** The virtual media applet begins the process of creating the image file. The process is complete when the progress bar reaches 100%. To cancel the creation of an image file, click **Cancel.**
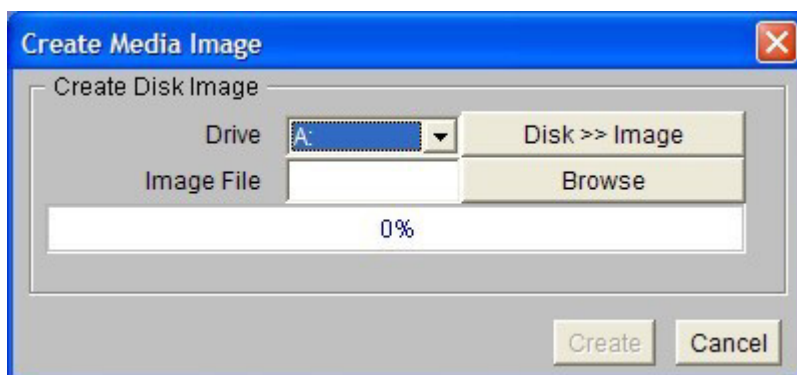
The Disk>>Image option is used to create image files from physical diskettes or CD-ROMs. The Image>>Disk option is not valid for a Virtual CD-ROM image. The Disk>>Image button changes to Image>>Disk when clicked. Use this button to switch from creating image files from physical diskettes to creating physical floppy diskettes from image files.

RILOE II Virtual Media privilege

The ability to use the RILOE II Virtual Media is restricted by an RILOE II User Privilege. Authorized users must have the Virtual Media privilege to select a Virtual Media Device and connect it to the host server.

Virtual Media applet timeout

The Virtual Media applet does not timeout when Virtual Media is connected to the host server. The Virtual Media applet closes if the user logs out.

Operating system USB support

To use virtual media devices your operating system must have support for USB devices. Your operating system must also support USB mass storage devices. Currently, Windows® 2000 SP4 and later, Windows® 2003, RedHat Enterprise Linux 3 and 4 and SUSE SLES 9 have the required support. Other operating systems may also support USB mass storage devices.

During system boot, the ROM BIOS will provide the USB support until the operating system loads. Since MS-DOS uses the BIOS to communicate with storage devices, utility diskettes that boot DOS will also function with virtual media.

NOTE: RedHat Enterprise Linux 3 will not allow you to provide a driver diskette using virtual media.

Resetting the RILOE II to the factory default settings

The RILOE II can be reset to the factory default settings by using the RBSU F8. To reset the board to the factory settings:

1. Restart or power up the server.
2. Press the **F8** key to enter RBSU F8 when the cursor flashes and the RILOE II prompt displays on the screen.
3. Select **File,** then select **Set Defaults.**
4. Select **Enter** when the screen displays **Set to Factory Defaults.**
5. Select **File,** then select **Exit.**

Getting help

Assistance for all RILOE II options is available by means of the Remote Insight Help hyperlink. This link provides summary information about the features of the board and helpful information for optimizing the operation of the RILOE II.

Pocket PC access with RILOE II

RILOE II provides support for network access from HP handheld devices supporting Pocket Internet Explorer. RILOE II provides a special user interface for connecting to RILOE II from the HP iPAQ Pocket PC.

Features on the handheld interface include:

- Remote Insight Summary
- Status
- Virtual Power Button
- Reboot Server
- Virtual Floppy Status
- Integrated Management Log
- Remote Insight Event Log
- SSL Encryption—40-bit and 128-bit options

You can enable or disable the HP iPAQ browser interface only from a desktop browser on the **Global Settings** page. If access is disabled, you are notified. Handheld access is disabled by default.

To enable the Pocket PC access feature:

1. Log in to RILOE II using an account with administrator privileges.
2. Click **Global Settings** on the **Administration** tab.
3. Click **Remote Access with Pocket PC.**
4. Click **Apply Settings** to save the changes.

When using a web browser to access RILOE II, the client is detected. If the client is an HP iPAQ running Pocket Internet Explorer, specific small form factor optimized content appears. The initial web page is not encrypted.

The following procedure is an example of accessing the RILOE II with the HP iPAQ H3600 Pocket PC:

1. Tap **Tap here to login to** *RILOE name.* An SSL session is negotiated and a certificate warning appears.
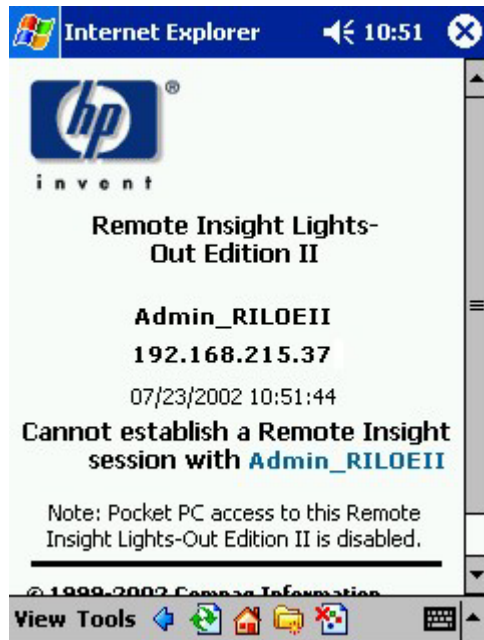
2. Tap **Yes** to proceed to the login page.

3. Enter a valid user ID and password in the login page, and tap **Go.** Do not enable the Save Password option.

If the user ID and password are valid, you are logged in to RILOE II and a web page similar to the following appears.
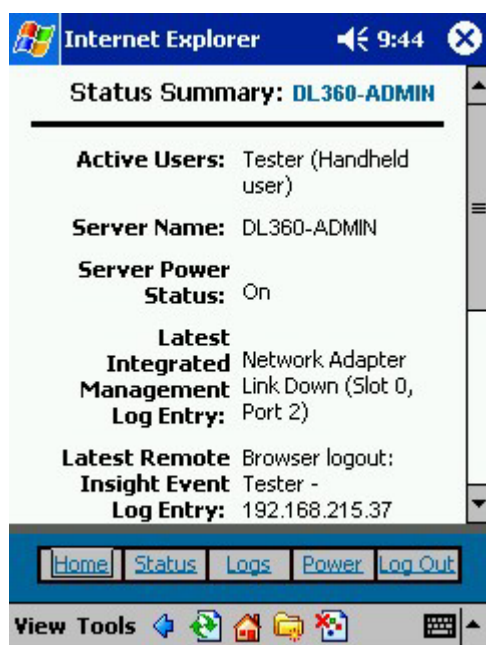
At a minimum, the HP iPAQ browser interface supports the Virtual Power button, rebooting the server, changing the Virtual Floppy status, viewing the logs, and display status information. If you attempt to browse to any unsupported web page, you are redirected to the initial HP iPAQ web page.

Browsing to an unsupported web page is considered an attempt to use the HP iPAQ browser interface for functions beyond the scope of the ones listed. For example, attempting to access Global Settings from the HP iPAQ redirects you to the initial display page.

In this case, because you are already logged in, tapping the **Tap here to login to** *RILOE name* at the initial display page bypasses the login page and takes you to the home page.

If Pocket PC access is disabled, a page similar to the following appears.
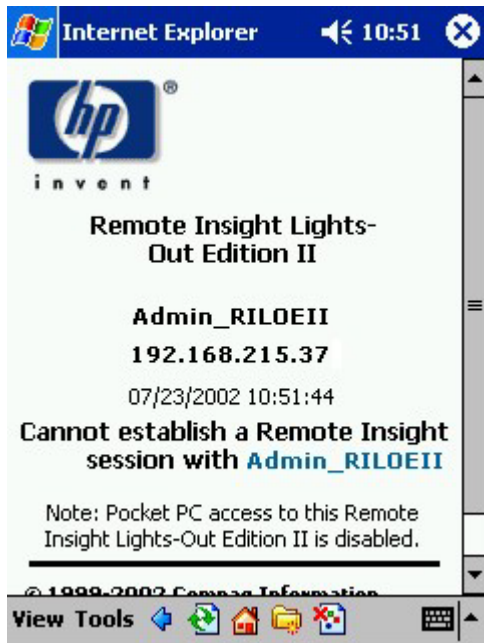
User authentication is required for access to RILOE II. After authentication, the Pocket PC user remains logged in until the session is ended by closing the Pocket PC browser. To close the browser, tap the **Q** key, tap **Close active task,** and close the browser.

RILOE II security

In this section

General security guidelines

The following are general guidelines concerning security for RILOE II:

- For maximum security, RILOE II should be set up on a separate management network.
- RILOE II should not be connected directly to the Internet.
- A 128-bit cipher strength browser must be used.

Password guidelines

The following is a list of recommended password guidelines:

- Never write down or recorded passwords.
- Never share passwords with others.
- Passwords generally should not be words that are in a dictionary or are easy to guess, such as company names, product names, user names, or a user's user ID.
- Passwords should include at least three of the following characteristics:
  - At least one numeric character
  - At least one special character
  - At least one lowercase character
  - At least one uppercase character

Passwords issued for a temporary user ID, a password reset, or a locked-out user ID should also conform to these standards. Each password must be a minimum length of zero characters and a maximum length of 40 characters. The default minimum length is set to eight characters. HP recommends that you do not set the minimum password length to fewer than eight characters is not recommended unless you have a physically secure management network that does not extend outside the secure data center.

Encryption

RILOE II provides strong security for remote management in distributed IT environments by using 128-bit SSL encryption of HTTP data transmitted across the network. SSL encryption ensures that the HTTP information is secure as it travels across the network.

Remote Console data is protected using 128-bit RC4 bidirectional encryption.

Two-factor authentication

RILOE II is a powerful tool for managing HP ProLiant servers. To prevent misuse of this tool, access to RILOE II requires reliable user authentication. This firmware release provides a stronger authentication scheme for RILOE II using two factors of authentication: a password or PIN and a private key for a digital certificate. Users are asked to verify their identities by providing both factors. Users can store their digital certificates and private keys wherever they choose, for example, smart card, USB token, or hard disk.

Setting up two-factor authentication for the first time

When setting up two-factor authentication for the first time you can use either local user accounts or directory user accounts. For more information on two-factor authentication settings, See the "Two-Factor Authentication Settings (on page 33)" section.

Setting up local user accounts:

1. Obtain the public certificate from the CA that issues user certificates or smart cards in your organization.
2. Export the certificate in Base64 encoded format to a file on your desktop, for example, CAcert.txt.
3. Obtain the public certificate of the user who needs access to RILOE II.
4. Export the certificate in Base64 encoded format to a file on your desktop, for example, Usercert.txt.
5. Open the file CAcert.txt in Notepad, select all of the text, and copy by pressing the **Ctrl+C** keys.
6. Log in to RILOE II and browse to the Two-Factor Authentication Settings page.
7. Click **Import Trusted CA Certificate**. Another page appears.
8. Click the white text area so that your cursor is in the text area, and paste the contents of the clipboard by pressing the **Ctrl+V** keys.
9. Click **Import Root CA Certificate**. The Two-Factor Authentication Settings page appears again with information displayed under Trusted CA Certificate Information.
10. From your desktop, open the file for the user certificate in Notepad, select all the text, and copy the text to the clipboard by pressing the **Ctrl+C** keys.
11. Browse to the User Administration page on RILOE II, and select the user for which you have obtained a public certificate or create a new user.
12. Click **View/Modify**.
13. Click **Add a certificate**.
14. Click the white text area so that your cursor is in the text area, and paste the contents of the clipboard by pressing the **CTRL+V** keys.
15. Click **Add user Certificate**. The Modify User page appears again with a 40 digit number in the Thumbprint field. You can compare the number to the thumbprint displayed for the certificate by using Microsoft® Certificate Viewer.
16. Browse to the Two-Factor Authentication Settings page.
17. Change Enforce Two-Factor Authentication to **Yes**.
18. Change Check for Certificate Revocation to **No (default)**.
19. Click **Apply**. RILOE II is reset. When RILOE II attempts to go to the login page again, the browser displays the Client Authentication page with a list of certificates that are available to the system.

   If the user certificate is not registered on the client machine, you will not see it in the list. The user certificate must be registered on the client system before you can use it. If there are no client certificates on the client system you may not see the Client Authentication page and instead see a Page cannot be displayed error. To resolve the error, the client certificate must be registered on the client machine. For more information on exporting and registering client certificates, See the documentation for your smart card, or certificate authority.

20. Choose the certificate that was added to the user in RILOE II. Click **OK**.

21. If prompted to do so, insert your smart card, or enter your PIN or password.

After completing the authentication process, you have access to RILOE II.

Setting up directory user accounts:

1. Obtain the public certificate from the CA that issues user certificates or smart cards in your organization.

2. Export the certificate in bas64 encoded format to a file on your desktop, for example, CAcert.txt.

3. Open the file in Notepad, select all the text, and copy the contents to the clipboard by pressing the **Ctrl+C** keys.

4. Log in to RILOE II and browse to the **Two-Factor Authentication Settings** page.

5. Click **Import Trusted CA Certificate**. Another page appears.

6. Click the white text area so that your cursor is in the text area, and paste the contents of the clipboard by pressing the **Ctrl+V** keys.

7. Click **Import Root CA Certificate**. The Two-Factor Authentication Settings page appears again with information displayed under Trusted CA Certificate Information.

8. Change Enforce Two-Factor authentication to **Yes**.

9. Change Check for Certificate Revocation to **No (default)**.

10. Change Certificate Owner Field to **SAN**. For more information, See the "Two-Factor Authentication Settings (on page 33)" section.

11. Click **Apply**. RILOE II is reset. When RILOE II attempts to go to the login page again, the browser displays the Client Authentication page with a list of certificates that are available to the system.

12. Select the certificate added to the user in RILOE II. Click **Ok**.

13. If prompted to do so, insert your smart card, or enter your PIN or password. The login page should be displayed with the e-mail address for the user in the Directory User field. You cannot change the Directory User field.

14. Enter the password for the directory user. Click **Login**.

After completing the authentication process, you have access to RILOE II. See the "Directory settings (on page 99)" section for more information on configuring directory users and privileges.

Two-factor authentication user certificates

To authenticated a user through locally on RILOE II, a certificate must be associated with the user's local user name. On the Administration>Modify User page, if a certificate has been mapped to the user a thumbprint (an SHA1 hash of the certificate) appears with a button that removes the certificate. If a certificate has not been mapped to the user, `Thumbprint: A certificate has NOT been mapped to this user` appears with a button that starts the certificate import process.

To set up a user for two-factor authentication and add a user certificate:

1. Log in to RILOE II using an account that has the Configure RILOE II Settings privilege. Click **Administration.**

2. Select a user.

3. Click **View/Modify.**

4. Under the User Certificate Information section, click **Add a certificate.**

5. On the Map User Certificate page, paste the user certificate into the text-box and click **Import Certificate**. For more information on creating, copying, and pasting certificate information, See the "Setting up two-factor authentication for the first time (on page 63)" section.

Two-factor authentication login

When you connect to RILOE II and two-factor authentication is required, the Client Authentication page prompts you to select the certificate you want to use. The Client Authentication page displays all of the certificates available to authenticate a client. Select your certificate. The certificate can be a certificate mapped to a local user in RILOE II, or a user specific certificate issued for authenticating to the domain.
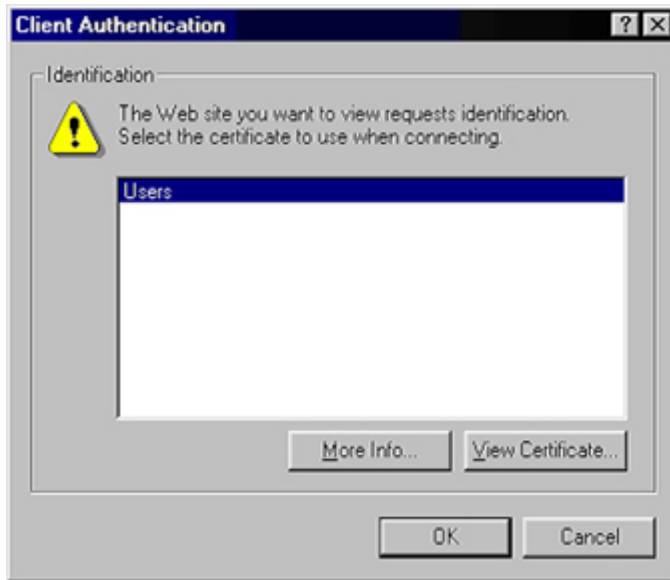
After you have selected a certificate, if the certificate is protected with a password or if the certificate is stored on a smart card, a second page appears prompting you to enter the PIN or password associated with the chosen certificate.

The certificate is examined by RILOE II to ensure it was issued by a trusted CA by checking the signature against the CA certificate configured in RILOE II. RILOE II determines if the certificate has been revoked and if it maps to a user in the RILOE II local user database. If all of these tests pass, then the normal RILOE II user interface appears.

If your credential authentication fails, the Login Failed page appears. If login fails, you are instructed to close the browser, open a new browser page, and try connecting again. If directory authentication is enabled, and local user authentication fails, RILOE II displays a login page with the directory user name field populated with either the User Principal Name from the certificate or the Distinguished Name (derived from the subject of the certificate). RILOE II requests the password for the account. After providing the password, you are authenticated.

Using two-factor authentication with directory authentication

In some cases, configuring two-factor authentication with directory authentication is complicated. RILOE II can use HP Extended schema or Default Directory schema to integrate with directory services. To ensure security when two-factor authentication is enforced, RILOE II uses an attribute from the client certificate as the directory user's login name. Which client certificate attribute RILOE II uses is determined by the Certificate Owner configuration setting on the Two-Factor Authentication Settings page. If Certificate

Owner is set to SAN, RILOE II obtains the directory user's login name from the UPN attribute of the SAN. If the Certificate Owner setting is set to Subject, RILOE II obtains the directory user's distinguished name from the subject of the certificate.

Which one of these settings to choose depends on which directory integration method is used, how the directory architecture is designed, and what information is contained in user certificates that are issued. The following examples assume you have the appropriate permissions.

Authentication using Default Directory Schema, part 1: The distinguished name for a user in the directory is CN=John Doe,OU=IT,DC=MyCompany,DC=com, and the following are the attributes of John Doe's certificate:

- Subject: DC=com/DC=MyCompany/OU=IT/CN=John Doe
- SAN/UPN: john.doe@MyCompany.com

Authenticating to RILOE II with username:john.doe@MyCompany.com and password, will work if two-factor authentication is **not** enforced. After two-factor authentication is enforced, if SAN is selected on the Two-Factor Authentication Settings page, the login page automatically populates the Directory User field with john.doe@MyCompany.com. The password can be entered, but the user will **not** be authenticated. The user is not authenticated because john.doe@MyCompany.com, which was obtained from the certificate, is not the distinguished name for the user in the directory. In this case, you must select **Subject** on the Two-Factor Authentication Settings page. Then the Directory User field on the login page will be populated with CN=John Doe,OU=IT,DC=MyCompany,DC=com, which is the user's actual distinguished name. If the correct password is entered, the user is authenticated.

Authentication using Default Directory Schema, part 2: The distinguished name for a user in the directory is CN=john.doe@MyCompany.com,OU=IT,DC=MyCompany,DC=com, and the following are the attributes of John Doe's certificate:

- Subject: DC=com/DC=MyCompany/OU=Employees/CN=John Doe/E=john.doe@MyCompany.com
- SAN/UPN: john.doe@MyCompany.com
- Search context on the Directory Settings page is set to: OU=IT,DC=MyCompany,DC=com

In this example, if SAN is selected on the Two-Factor Authentication Settings page, the Directory User field on the login page is populated with john.doe@MyCompany.com. After the correct password is entered, the user is authenticated. The user is authenticated even though john.doe@MyCompany.com is not the distinguished name for the user. The user is authenticated because RILOE II attempts to authenticate using the search context fields (CN=john.doe@MyCompany.com, OU=IT, DC=MyCompany, DC=com) configured on the Directory Settings page. Becasue this is the correct distinguished name for the user, RILOE II successfully finds the user in the directory.

NOTE: Selecting Subject on the Two-Factor Authentication Settings page causes authentication to fail, because the subject of the certificate is not the distinguished name for the user in the directory.

When using the HP Extended schema method, HP recommends selecting the SAN option on the Two-factor Authentication Settings page.

Introduction to certificate services

Certificate Services are 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 allows Active Directory to receive a certificate that allows Lights-Out processors to connect to the directory service. Without a certificate, RILOE II cannot connect to the directory server.

Each directory server that you want RILOE II 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 of the Active Directory controllers on the network.

Certificates

By default, RILOE II creates a self-signed certificate for use in SSL connections. The self-signed certificate enables RILOE II to work without any additional configuration steps. The security features of RILOE II can be enhanced by importing a trusted certificate.

- **Generate Certificate Request**—RILOE II can create a CR (in PKCS #10 format), which can be sent to a CA. The certificate request is Base64 encoded. A CA processes the request and returns a response (X.509 certificate) that can be imported into RILOE II.

  The CR contains a public/private key pair that is used for validation of communications between the client browser and RILOE II. The generated CR is held in memory until either a new CR is generated, a certificate is imported by this process, or RILOE II is reset, which means you can generate the CR and copy it to the client clipboard, leave RILOE II website to retrieve the certificate, then return to import the certificate.

  When submitting the request to the CA, be sure to:

  - Use the RILOE II name as listed on the System Status page as the URL for the server.
  - Request the certificate be generated in the RAW format.
  - Include the `Begin` and `End` certificate lines.

Every time you click **Generate Certificate Request**, a new certificate request is generated, even though the RILOE II name is the same.

- **Import Certificate**—If you are returning to the Create Certificate Request page with a certificate to import, click **Import Certificate** to go directly to the Certificate Import page without generating a new CR. A given certificate only works with the keys contained in the CR from which the certificate was generated. If RILOE II is reset or another CR is generated since the CR that was used to request the certificate generated, then another CR must be generated and a new certificate procured from the CA.

You can create a certificate request or import an existing certificate using RIBCL XML commands. These commands enable you to script and automate certificate deployment on RILOE II servers instead of manually deploying certificates through the web interface. For more information, See "CERTIFICATE_SIGNING_REQUEST" and "IMPORT_CERTIFICATE" in the "Remote Insight Command Language (on page)" section.

CERTIFICATE_SIGNING_REQUEST and IMPORT_CERTIFICATE cannot be used with the standard CPQLOCFG utility. However, you can use the PERL version of CPQLOCFG in combination with these commands.

Installing certificate services

1. Select **Start>Settings>Control Panel.**
2. Double-click **Add/Remove Programs.**
3. Click **Add/Remove Windows Components** to start the Windows Components wizard.
4. Select the **Certificate Services** check box. Click **Next.**
5. Click **OK** at the warning that the server cannot be renamed. The Enterprise root CA option is selected because there is no CA registered in the active directory.
6. Enter the information appropriate for your site and organization. Accept the default time period of two years for the `Valid for` field. Click **Next.**
7. Accept the default locations of the certificate database and the database log. Click **Next.**
8. Browse to the c:\I386 folder when prompted for the Windows® 2000 Advanced Server CD.
9. Click **Finish** to close the wizard.

Verifying directory services

Because management processors communicate with Active Directory using SSL, it is necessary to create a certificate or install Certificate Services. You must install an enterprise CA because you will be issuing certificates to objects within your organizational domain.

To verify that certificate services is installed:

1. Select **Start>Programs>Administrative Tools>Certification Authority.**
2. If Certificate Services is not installed an error message appears.

Configuring Automatic Certificate Request

To specify that a certificate be issued to the server:

1. Select **Start>Run,** and enter `mmc.`
2. Click **Add.**
3. Select **Group Policy,** and click **Add** to add the snap-in to the MMC.
4. Click **Browse,** and select the Default Domain Policy object. Click **OK.**
5. Select **Finish>Close>OK.**

6. Expand **Computer Configuration>Windows Settings>Security Settings>Public Key Policies.**

7. Right-click **Automatic Certificate Requests Settings,** and select **New>Automatic Certificate Request.**

8. Click **Next** when the Automatic Certificate Request Setup wizard starts.

9. Select the **Domain Controller** template, and click **Next.**

10. Select the certificate authority listed. (It is the same CA defined during the Certificate Services installation.) Click **Next.**

11. Click **Finish** to close the wizard.

Securing RBSU

The RILOE II RBSU allows user access for viewing and modifying the RILOE II configuration. RBSU access settings can be configured using RBSU, browser, RIBCL scripts, and the RILOE II Security Override Switch. RBSU has three levels of security:

- RBSU Disabled (most secure)

  If RILOE II RBSU is disabled, user access is prohibited. This prevents modification using the RBSU interface.

- RBSU Login Required (more secure)

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

- RBSU Login Not Required (default)

  Anyone with access to the host during POST may enter the RILOE II RBSU to view and modify configuration settings. This is an acceptable setting if host access is controlled.

Systems Insight Manager integration

In this section

Integrating RILOE II with Systems Insight Manager

RILOE II fully integrates with Systems Insight Manager in key operating environments. Full integration with Systems Insight Manager also provides a single management console for launching a standard Web browser to access. While the operating system is running, you can establish a connection to RILOE II using Systems Insight Manager.

Integration with Systems Insight Manager provides:

- Support for SNMP trap delivery to a Systems Insight Manager console

    Delivery to a Systems Insight Manager console can be configured to forward SNMP traps to a pager or e-mail.

- Support for SNMP management

    Systems Insight Manager is allowed to access the Insight Management Agents information through RILOE II.

- Support for a management processor

    Systems Insight Manager adds support for a new device type, the management processor. All RILOE II devices installed in servers on the network are discovered in Systems Insight Manager as management processors. The management processors are associated with the servers in which they are installed.

- Grouping of RILOE II management processors

    All RILOE II devices can be grouped together logically and displayed on one page. This capability provides access to RILOE II from one point in Systems Insight Manager.

- RILOE II hyperlinks

    Systems Insight Manager provides a hyperlink on the server device page to launch and connect to RILOE II.

- HP Management Agents

    RILOE II, combined with HP Management Agents, provides remote access to system management information through the RILOE II browser-based interface.

Systems Insight Manager functional overview

Systems Insight Manager enables you to:

- Identify RILOE II processors.
- Create an association between RILOE II and its server.
- Create links between RILOE II and its server.
- View RILOE II and server information and status.
- Control the amount of detailed information displayed for RILOE II.
- Draw a visualization of the ProLiant BL p-Class rack infrastructure.

The following sections give a summary of each function. For detailed information on these benefits and how to use Systems Insight Manager, refer to the *HP Systems Insight Manager Installation and User Guide,* provided with Systems Insight Manager.

Systems Insight Manager identification and association

Systems Insight Manager can identify RILOE II and create an association between RILOE II and the server. The administrator of the RILOE II device may configure RILOE II to respond to Systems Insight Manager identification requests.

Systems Insight Manager status

In Systems Insight Manager, RILOE II is identified as a management processor. Systems Insight Manager displays the management processor status within the Systems List.

The RILOE II management processor is displayed as an icon in the device list on the same row as its host server. The color of the icon represents the status of the management processor.

For a complete list of device statuses, refer to the *HP Systems Insight Manager Installation and User Guide.*

Systems Insight Manager links

For ease of management, Systems Insight Manager creates links to the following locations:
- RILOE II and the host server from any System List
- The server from the System Page of RILOE II

- RILOE II from the System Page of the server

The Systems List pages display RILOE II, the server, and the relationship between RILOE II and server. For example, the page can display the server, the RILOE II name next to the server, and *RILOE II name* **IN** *server* in the System Name field for RILOE II.

Clicking on a status icon for RILOE II takes you to the RILOE II Web interface. Clicking on the hardware status icon takes you to the Insight Management Agents for the device. Clicking on the RILOE II or server name takes you to the System Page of the device. Within the System Page are the Identity, Links, and Event tabs. These tabs provide identity and status information, event information, and links for the associated device.

Systems Insight Manager systems lists

RILOE II management processors can be viewed within Systems Insight Manager. The administrator can create and use customized system lists to group management processors. Refer to the *HP Systems Insight Manager Installation and User Guide* for further details.

Configuring Systems Insight Manager identification of RILOE II

RILOE II enables you to set how much data is returned on an Systems Insight Manager request for more information.

The level of data returned is controlled on the SNMP/Insight Manager Settings page. The identification data level options are:

- **High**—Associations are present, and all data is present on the summary page.
- **Medium**—Associations are present, but the summary page contains less detail than at high security.
- **Low**—Associations are present, if SNMP pass-through is supported. If not, the server and management processor are separate entities in the device list.
- **None**—No data is returned to Systems Insight Manager.

Display information	Low	Medium	High	None
Product Name	Y	Y	Y	—
Server Serial Number	—	Y	Y	—
Server State	—		Y	—
Management Processor Status	Y	Y	Y	—
Management Processor Serial Number	—	Y	Y	—
RILOE II Advanced License Status and Data	—	Y	Y	—
Hardware Revision Information	—	—	Y	—
Firmware Revision Information	—	—	Y	—
Rack Topology	—	Y	Y	—
Single Sign On*	—	—	Y	—
Secure Task Execution*	—	—	Y	—
CIMOM*	—	—	Y	—
Device Home Page URL	—	—	Y	—

* Reserved for future integration.

Receiving SNMP alerts in Systems Insight Manager

You can configure RILOE II to forward alerts from the host operating system management agents, and to send RILOE II-generated alerts to Systems Insight Manager.

Systems Insight Manager provides support for full SNMP management, and RILOE II supports SNMP trap delivery to Systems Insight Manager. You can view the event log, select the event, and view the additional information about the alert.

Configuring receipt of SNMP alerts in Systems Insight Manager is a two-step process. The process requires Systems Insight Manager to discover RILOE II and configuring RILOE II to enable SNMP alerts.

1. To enable RILOE II to send SNMP traps click **SNMP/Insight Manager Settings** on the Administration tab of RILOE II navigation frame to enable SNMP alerting and to provide an SNMP trap IP address to RILOE II. SNMP trap IP address should be the address of the computer running Systems Insight Manager. See the "SNMP alerts and settings (on page 31)" section for details.

2. To discover RILOE II in Systems Insight Manager configure RILOE II as a managed device for Systems Insight Manager. Adding RILOE II to Systems Insight Manager allows the NIC interface on RILOE II to function as a dedicated management port, isolating management traffic from the remote host server NIC interface.

   a. Start Systems Insight Manager. Click **Options>Discovery>Automatic Discovery** to discover any RILOE II devices to be managed by Systems Insight Manager.

   b. Select **IP range pinging** and, if the IP address does not already appear in the Ping Inclusion Ranges section, enter the IP address.

   c. Click **Save and Run** to add RILOE II to Systems Insight Manager. After the discovery is complete, subsequent queries displays the device as a management processor.

   d. You may need to edit the SNMP monitor community string (for example, by changing it to "public") so that RILOE II appears in the list of monitored devices. You can change the SNMP monitor community string by accessing the Systems Protocol Settings page. Click **Options>Protocol Settings>System Protocol Settings.**

      Another option is to click **Options>Protocol Settings>Global Protocol Settings** and set community strings to use during discovery under Default SNMP Settings. When set, you can use steps a through c to run discovery again.

   For major, uncleared events, RILOE II traps are displayed in All Events. You can use the orange button at the top of the page to obtain information about the major uncleared events. Click the **Event Type** to obtain further information about the event.

   HP Insight Agents for RILOE II must be installed on the remote host server to enable management of RILOE II. See "Installing RILOE II device drivers" for additional details about installing and configuring agents.

Systems Insight Manager port matching

Systems Insight Manager is configured to start an HTTP session to check for RILOE II at port 80. The port can be changed. If you want to change the port number, you must also change it in Network Settings and Systems Insight Manager.

To change the port number in Systems Insight Manager, add the port to the config\identification\additionalWsDisc.props file in the directory where Systems Insight Manager is installed. The entry must start with the HTTP port for RILOE II. No entry needs to be in this file for RILOE II if it remains at the standard Port 80. It is very important that the entry is on a single line and the port number is first, with all other items identical to the following example (including capitalization).

The following example shows what the entry is if RILOE II is to be discovered at port 55000 (this should all be on one line in the file):

```
55000=RILOE
II, ,true,false,com.hp.mx.core.tools.identification.mgmtproc.MgmtProcess
orParser
```

Directory services

In this section

Overview of directory integration

RILOE II can be configured to use a directory to authenticate and authorize its users. There are two configuration options available: using a directory that has been extended with HP Schema or using the directory's default schema (schema-free.)

There are white papers available for more information on directory integration on the HP website (http://www.hp.com/servers/lights-out).

Benefits of directory integration

Directory integration benefits include:

- Scalability—The directory can be leveraged to support thousands of users on thousands of RILOE IIs.
- Security—Robust user password policies are inherited from the directory. User password complexity, rotation frequency, and expiration are policy examples.
- Anonymity (lack thereof)—In some environments, users share Lights-Out accounts, which results in not knowing who performed an operation, instead of knowing what account (or role) was used.
- Role-based administration (when using HP Extended schema)—You can create roles (for instance, clerical, remote control of the host, complete control) and associate users or user groups with those roles. A change to a role applies to all users and Lights-Out devices associated with that role.
- Single point of administration—You can use native administrative tools, such as MMC and ConsoleOne to administrate Lights-Out users.
- Immediacy—A single change in the directory rolls-out immediately to associated Lights-Out processors, which eliminates the need to script the change process.
- Elimination of another username and password—You can use existing user accounts and passwords in the directory without having to record or remember a new set of credentials for Lights-Out.
- Flexibility—When configured for HP Extended schema, you can create a single role for a single user on a single RILOE II, you can create a single role for multiple users on multiple RILOEs, or you can use a combinations of roles as is suitable for your enterprise.
- Compatibility—Lights-Out directory integration applies to iLO, RILOE, and RILOE II products. The integration supports the popular Active Directory and eDirectory.

- Standards—Lights-Out directory support builds on top of the LDAP 2.0 standard for secure directory access.

How directory integration works

Schema-free

At the login page, enter a login name and a password. If ActiveX is enabled in the browser, the login name is converted to the directories DN format and stored in a security cookie in the browser. The browser then loads the home page for RILOE II.

RILOE II reads the security cookie and extracts the DN for each page displayed. RILOE II reads the directory object pointed to by the DN. RILOE II then determines what groups the object is a member of and compares this information with a list kept in RILOE II. If there is a match, then the privileges associated with this group in RILOE II determine whether you have access to the page requested.

When using a schema-free directory configuration, after you attempt to log in to RILOE II, RILOE II attempts to read your object in the directory to determine what groups you are a member of. RILOE II compares the list of groups to group names RILOE II is configured to recognize. If RILOE II finds a match, RILOE II determines what privileges you have based on the privileges configured for that group in RILOE II.

If you are a member of any group that RILOE II recognizes, you have login rights to RILOE II, regardless of what rights are associated with the group. User rights are a combination of all rights for the groups you are a member of that RILOE II recognizes.

If at login the ActiveX control does not run, then the complete login name or the login name prepended with a user context is used for the directory lookup process. For this to work, the login name must either be in full DN format or in a format that the combination of the login name with a user context is made into a full DN.

HP Extended schema

Refer to the "Directory-enabled remote management (on page 103)" section.

Advantages and disadvantages of schema-free and HP Extended schema

Before configuring RILOE II for directories, you must decide whether to use the directory's schema-free option (the default schema) or the HP Extended schema option.

The advantages of using the schema-free option are:

- There is no need to extend the directory's schema.
- When ActiveX controls are enabled on the browser, logging in using NetBIOS and e-mail formats is supported.

The advantages of using the HP Extended schema option are:

- There is much more flexibility in controlling access. For example, access can be limited to a time of day or from a certain range of IP addresses.
- Groups are maintained in the directory, not on each RILOE II.
- eDirectory works only with RILOE II using the HP Extended schema.

Setup for Schema-free directory integration

Before setting up the Schema-free option, your system must meet all the prerequisites outlined in the "Active Directory preparation (on page 77)" section.

You can set up RILOE II for directories in three ways:

- Manually using a browser ("Schema-free browser-based setup" on page 77).
- Using a script ("Schema-free scripted setup" on page 77).
- Using HPLOMIG ("Schema-free HPLOMIG-based setup" on page 78).

Active Directory preparation

The schema-free option is supported on the following operating systems:

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory

SSL must be enabled at the directory. To enable SSL, install a certificate for the domain in Active Directory. RILOE II only communicates with the directory over a secure SSL connection. For more information, refer to the Microsoft® Knowledge Base, article number 247078: *Enabling SSL Communication over LDAP for Windows® 2000 Domain Controllers* on the Microsoft® website (http://support.microsoft.com/).

To validate the setup, you should have the directory distinguished name for at least one user and the distinguished name of a security group the user is a member of.

Schema-free browser-based setup

Schema-free can be setup using the RILOE II browser-based interface.

1. Log on to RILOE II using an account that has the Configure RILOE II Settings privilege. Click **Administration.**

   IMPORTANT: Only users with the Configure RILOE II Settings privilege can change these settings. Users that do not have the Configure RILOE II Settings privilege can only view the assigned settings.

2. Click **Directory Settings.**
3. Select **Use Directory Default Schema** in the Authentication Settings section. For more information, refer to the "Schema-free setup options (on page 78)" section.
4. Click **Apply Settings**.
5. Click **Test Settings**.

Schema-free scripted setup

To setup the schema-free directories option using RIBCL XML scripting:

1. Download and review the scripting and command line resource guide.
2. Write a script that configures RILOE II for schema-free directories support and run it. The following script can be used as a template.

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="admin" PASSWORD="password">

   <DIR_INFO MODE = "write">

      <MOD_DIR_CONFIG>

      <DIR_ENABLE_GRP_ACCT value = "yes"/>
```

```
        <DIR_GRPACCT1_NAME value
        ="CN=Administrators,CN=Builtin,DC=HP,DC=com "/>

        <DIR_GRPACCT1_PRIV value = "1"/>

        </MOD_DIR_CONFIG>
    </DIR_INFO>
</LOGIN>
</RIBCL>
```

Schema-free HPLOMIG-based setup

HPLOMIG is the easiest way to set up a large number of LOM processors for directories. To use HPLOMIG, download the HPQLOMIG utility and additional documentation from the HP website (http://www.hp.com/servers/lights-out). HP recommends using HPLOMIG when configuring many LOM processors for directories. For more information on using HPLOMIG, refer to the "HPLOMIG Operation" section.

Schema-free setup options

Setup options are the same regardless of which method (browser, HPQLOMIG, or script) you use to configure the directory.

After enabling directories and selecting the Schema-free option, you have the following options.

Minimum Login Flexibility

- Enter the directory server's DNS name or IP address and LDAP port. Typically, the LDAP port for an SSL connection is 636.
- Enter the distinguished name for at least one group. The chosen 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 RILOE II users are members of the group.

  With a minimum configuration, you can log into RILOE II using your full distinguished name and password. You must be a member of a group that RILOE II 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's distinguished name. For instance, if the user logs in as JOHN.SMITH and a user context is set up as CN=USERS,DC=HP,DC=COM, then the distinguished name that RILOE II tries will be CN=JOHN.SMITH,CN=USERS,DC=HP,DC=COM.

Maximum Login Flexibility

- Configure RILOE II as described in the minimum and better login flexibility options.
- Configure RILOE II with a DNS name, not an IP address for the directory server's network address. The DNS name must be resolvable to an IP address from both RILOE II and the client system.
- Enable ActiveX controls in your browser. The RILOE II login script will attempt to call a Windows® control to convert the login name to a distinguished name.

  Configuring RILOE II with maximum login flexibility enables you to log in using your full distinguished name and password, your name as it appears in the directory, NetBIOS format (domain\login_name), or the e-mail format (login_name@domain).

NOTE: Your system security settings or installed software might prevent the login script from calling the Windows® ActiveX control. If this happens, your browser displays a warning message in the status bar, message box, or might stop responding. To help identify what software or setting is causing the problem, create another profile and log in to the system.

In some cases, you might not be able to get the maximum login flexibility option to work. For instance, if the client and RILOE II are in different DNS domains, one of the two might not be able to resolve the directory server name to an IP address.

Setting up HP schema directory integration

When using the HP schema directory integration, RILOE II supports both Active Directory and eDirectory. However, these directory services require the schema being extended.

Features supported by HP schema directory integration

RILOE II Directory Services functionality enables you to:

- Authenticate users from a shared, consolidated, scalable user database.
- Control user privileges (authorization) using the directory service.
- Use roles in the directory service for group-level administration of RILOE II management processors and RILOE II users.

Extending the schema must be completed by a Schema Administrator. 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 connected through the Diagnostics Port, the directory server is not available. You can log in using a local account only.

Setting up directory services

To successfully enable directory-enabled management on any Lights-Out management processor:

1. Review the following sections:
   - "Directory services (on page 75)"
   - "Directory services schema (on page 187)"
   - "Directory-enabled remote management (on page 103)"
2. Install:
   a. Download the HP Lights-Out Directory Package containing the schema installer, the management snap-in installer, and the migrations utilities from the HP website (http://www.hp.com/servers/lights-out).
   b. Run the schema installer (on page 81) once to extend the schema.
   c. Run the management snap-in installer (on page 83), and install the appropriate snap-in for your directory service on one or more management workstations.
3. Update:
   a. Flash the ROM on the Lights-Out management processor with the directory-enabled firmware.
   b. Set directory server settings and the distinguished name of the management processor objects on the Directory Settings (on page 99) page in the RILOE II GUI.
4. Manage:
   a. Create a management device object and a role object ("Directory services objects" on page 88) 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.

Directory services   79

For more information on managing the directory service, See "Directory-enabled remote management (on page 103)." Examples are available in the "Directory services for Active Directory (on page 83)" and "Directory services for eDirectory (on page 92)" sections.

5. Handle exceptions:

    - Lights-Out migration utilities are easier to use with a single Lights-Out role. If you plan to create multiple roles in the directory, you might need to use directory scripting utilities, such as LDIFDE or VB script, to create complex role associations. See the "Using bulk import tools (on page 108)" for more information.

    - If you have RILOE II or RILOE processors with old firmware, you might need to manually update the firmware using a browser. Minimum firmware requirements for remote firmware update using RIBCL and directory migration utility as follows:

LOM product	Minimum supported firmware
RILOE	2.41
RILOE II	All versions
iLO	1.10
iLO 2	1.00

After the schema has been extended, you can complete the directory services setup by using HP Lights-Out Directories Migration Utilities (on page 113). The migration utilities are included in the HP Lights-Out Directory Package. Version 1.13 of the Directories Migration Utility allows Lights-Out import and export and supports different user credentials for each Lights-Out processor.

Directory services support

Using HP schema directory integration, RILOE II supports the following directory services:

- Microsoft® Active Directory
- Microsoft® Windows® Server 2003 Active Directory
- Novell eDirectory 8.7.3
- Novell eDirectory 8.7.1

RILOE II software is designed to run within the Microsoft® Active Directory Users and Computers and Novell ConsoleOne management tools, enabling you to manage user accounts on Microsoft® Active Directory or Novell eDirectory. This solution makes no distinction between eDirectory running on NetWare, Linux, or Windows®. Spawning an eDirectory schema extension requires Java™ 1.4.0 or later for SSL authentication.

RILOE II supports Microsoft® Active Directory running on one of the following operating systems:

- Windows® 2000 family
- Windows® Server 2003 family

RILOE II supports eDirectory running on one of the following operating systems:

- NetWare 5.X
- NetWare 6.X
- Red Hat Enterprise Linux AS 2.1

Schema required software

RILOE II requires specific software, which will extend the schema and provide snap-ins to manage the RILOE II network. An HP Smart Component is available for download that contains the schema installer and the management snap-in installer. The HP Smart Component can be downloaded from the HP website (http://www.hp.com/servers/lights-out).

Schema installer

Bundled with the schema installer are one or more .xml files. These files contain the schema that will be added to the directory. Typically, one of these files will contain core schema that is common to all the supported directory services. Additional files contain only product-specific schemas. The schema installer requires the use of the .NET framework.

The installer includes three important screens:

- Schema Preview
- Setup
- Results

Schema Preview

The Schema Preview screen enables the user to view the proposed extensions to the schema. This screen reads the selected schema files, parses the XML, and displays it as a tree view. It lists all of the details of the attributes and classes that will be installed.
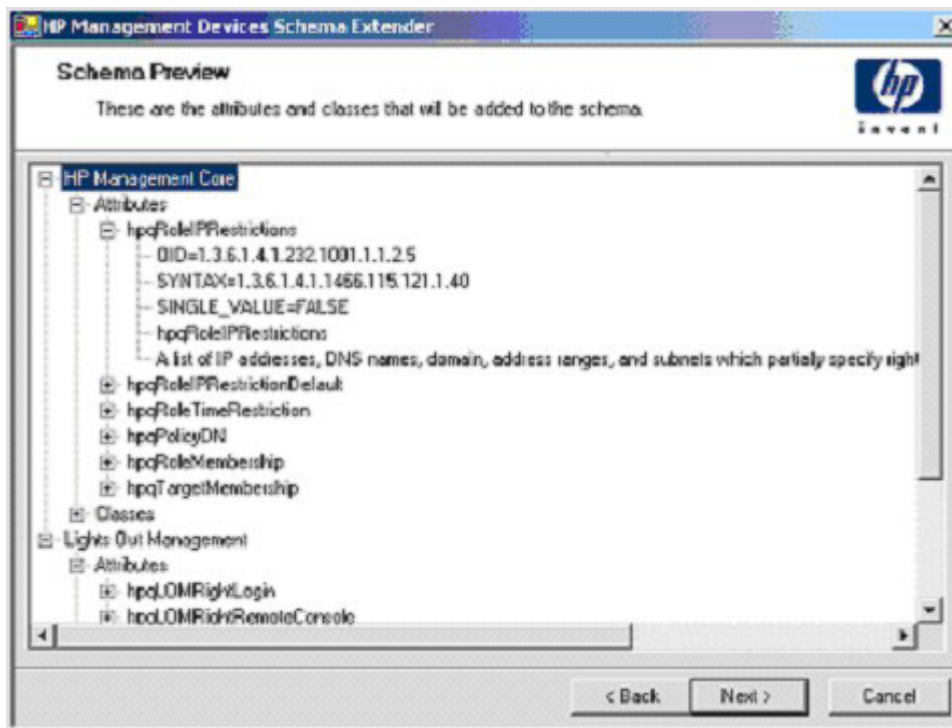
Setup

The Setup screen is used to enter the appropriate information before extending the schema.

The Directory Server section of the Setup screen enables you to select whether you will be using Active Directory or eDirectory, and to set the computer name and the port to be used for LDAP communications.

IMPORTANT: Extending the schema on Active Directory requires that the user be an authenticated Schema Administrator, that the schema is not write protected, and the directory is the FSMO role owner in the tree. The installer will attempt to make the target directory server the FSMO Schema Master of the forest.

To get write access to the schema on Windows® 2000 requires a change to the registry safety interlock. If the user selects the **Active Directory** option, the schema extender will attempt to make the registry change. It

will only succeed if the user has rights to do this. Write access to the schema is automatically enabled on Windows® Server 2003.

The Directory Login section of the Setup screen enables you to enter your login name and password. These might be required to complete the schema extension. The Use SSL during authentication option sets the form of secure authentication to be used. If selected, directory authentication using SSL is used. If not selected and Active Directory is selected, Windows NT® authentication is used. If not selected and eDirectory is selected, the administrator authentication and the schema extension will proceed using an unencrypted (clear text) connection.

Results

The Results screen displays the results of the installation, including whether the schema could be extended and what attributes were changed.
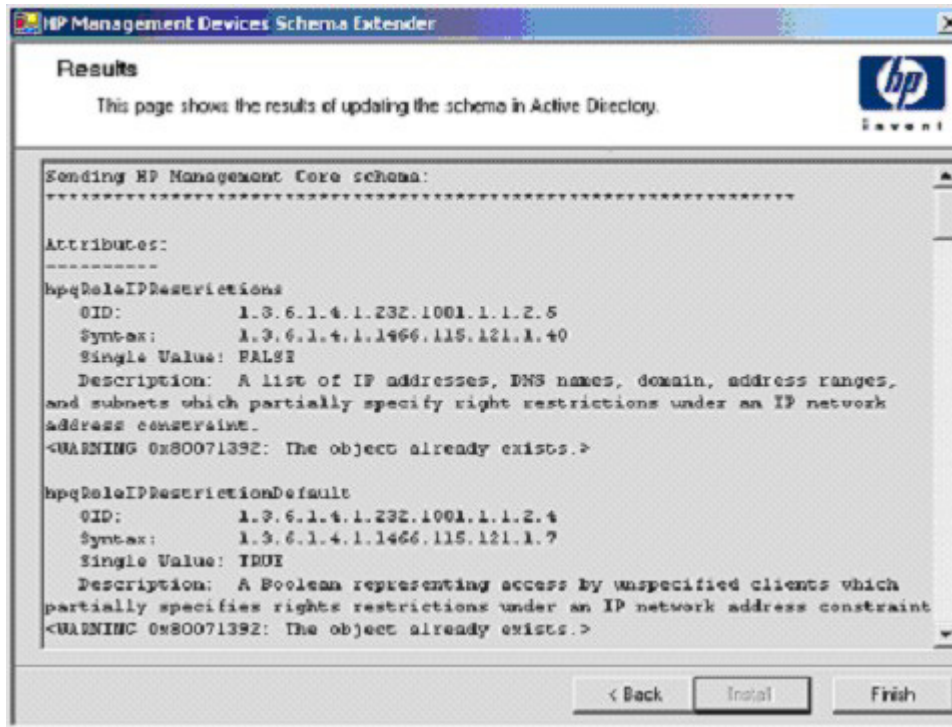
Management snap-in installer

The management snap-in installer installs the snap-ins required to manage RILOE II objects in a Microsoft® Active Directory Users and Computers directory or Novell ConsoleOne directory.

RILOE II snap-ins are used to perform the following tasks in creating an RILOE II directory:

- Creating and managing the RILOE II and role objects (policy objects will be supported at a later date)
- Making the associations between RILOE II objects and the role (or policy) objects

Directory services for Active Directory

The following sections provide installation prerequisites, preparation, 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 the HP Directories Support for Management Processors on the HP website (http://h18004.www1.hp.com/support/files/lights-out/us/index.html).

Active Directory installation prerequisites

Directory Services for RILOE II uses LDAP over SSL to communicate with the directory servers. Before installing snap-ins and schema for Active Directory, you should read and have available the following documentation:

📝 **IMPORTANT:** Installing Directory Services for RILOE II requires extending the Active Directory schema. Extending the schema must be completed by an Active Directory Schema Administrator.

- *Extending the Schema* in the Microsoft® Windows® 2000 Server Resource Kit, available at http://msdn.microsoft.com
- *Installing Active Directory* in the Microsoft® Windows® 2000 Server Resource Kit
- Microsoft® Knowledge Base Articles
  - 216999 *Installing the remote server administration tools in Windows® 2000*
  - 314978 *Using the Adminpak.msi to install a server administration tool in Windows® 2000*
  - 247078 *Enabling SSL communication over LDAP for Windows® 2000 domain controllers*
  - 321051 *Enabling LDAP over SSL with a third-party certificate authority*

Directory services preparation for Active Directory

To set up directory services for use with RILOE II management processors:

1. Install Active Directory. For more information, refer to *Installing Active Directory* in the Microsoft® Windows® 2000 Server Resource Kit.

2. Install the Microsoft® Admin Pack (the ADMINPAK.MSI file, which is located in the i386 subdirectory of the Windows® 2000 Server or Advance Server CD). For more information, refer to the Microsoft® Knowledge Base Article 216999.

3. In Windows® 2000, the safety interlock that prevents accidental writes to the schema must be temporarily disabled. The schema extender utility can do this if the remote registry service is running and the user has sufficient rights. This can also be done by setting
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ServicesParameters\Schema Update Allowed` in the registry to a non-zero value (refer to the "Order of Processing When Extending the Schema" section of *Installation of Schema Extensions* in the Windows® 2000 Server Resource Kit) or by the following steps. This step is not necessary if you are using Windows® Server 2003.

IMPORTANT: Incorrectly editing the registry can severely damage your system. HP recommends creating a back up of any valued data on the computer before making changes to the registry.

   a. Start MMC.
   b. Install the Active Directory Schema snap-in in MMC.
   c. Right-click **Active Directory Schema** and select **Operations Master.**
   d. Select **The Schema may be modified on this Domain Controller.**
   e. Click **OK.**

   The Active Directory Schema folder might need to be expanded for the checkbox to be available.

4. Create a certificate or install Certificate Services. This step is necessary to create a certificate or install Certificate Services because RILOE II communicates with Active Directory using SSL. Active Directory must be installed before installing Certificate Services.

5. To specify that a certificate be issued to the server running active directory:

   a. Launch Microsoft® Management Console on the server and add the default domain policy snap-in (Group Policy, then browse to Default domain policy object).
   b. Click **Computer Configuration>Windows Settings>Security Settings>Public Key Policies.**
   c. Right-click **Automatic Certificate Requests Settings,** and select **new>automatic certificate request.**
   d. Using the wizard, select the domain controller template, and the certificate authority you want to use.

6. Download the Smart Component, which contains the installers for the schema extender and the snap-ins. The Smart Component can be downloaded from the HP website (http://www.hp.com/servers/lights-out).

7. Run the schema installer application to extend the schema, which extends the directory schema with the proper HP objects.

   The schema installer associates the Active Directory snap-ins with the new schema. The snap-in installation setup utility is a Windows® MSI setup script and will run anywhere MSI is supported (Windows® XP, Windows® 2000, Windows® 98). However, some parts of the schema extension application require the .NET Framework, which can be downloaded from the Microsoft® website (http://www.microsoft.com).

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 RILOE II management.

   a. Use the management snap-ins from HP to create RILOE II, Policy, Admin, and User Role objects.

   b. Use the management snap-ins from HP to build associations between the RILOE II object, the policy object, and the role object.

   c. Point the RILOE II object to the Admin and User role objects (Admin and User roles will automatically point back to the RILOE II object).

   For more information on RILOE II objects, refer to "Directory services objects (on page 88)."

At a minimum, you must create:

- One Role object that will contain one or more users and one or more RILOE II objects.

- One RILOE II object corresponding to each RILOE II management processor that will be using the directory.

Example: Creating and configuring directory objects for use with RILOE II in Active Directory

The following example shows how to set up roles and HP devices in an enterprise directory with the domain *testdomain.local*, which consists of two organizational units, *Roles* and *RILOES*.

Assume that a company has an enterprise directory including the domain *testdomain.local,* arranged as shown in the following screen.
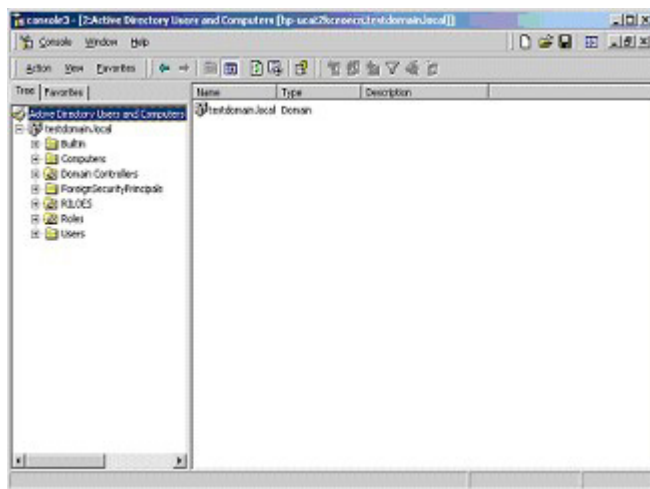
Create an organizational unit, which will contain the Lights-Out Devices managed by the domain. In this example, two organizational units are created called *Roles* and *RILOES.*

1. Use the HP provided Active Directory Users and Computers snap-ins to create Lights-Out Management objects in the *RILOES* organizational unit for several RILOE II devices.
   a. Right-click the RILOES organizational unit found in the *testdomain.local* domain, and select **NewHPObject.**
   b. Select **Device** in the Create New HP Management Object dialog box.
   c. Enter an appropriate name in the Name field of the dialog box. In this example, the DNS host name of the RILOE II device, *rib-email-server,* will be used as the name of the Lights-Out Management object, and the surname will be *RILOEII.*

Enter and confirm a password in the Device LDAP Password and Confirm fields. The device will use this password to authenticate to the directory, and should be unique to the device. This password is the password that is used in the Directory Settings screen of the RILOE II.

   d. Click **OK.**
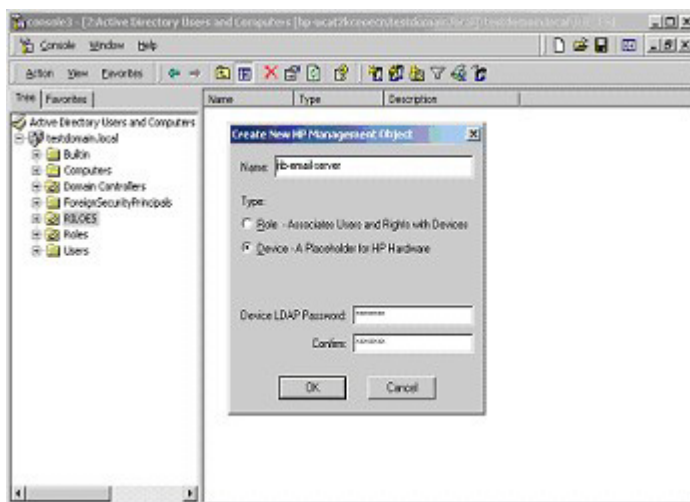
2. Use the HP provided Active Directory Users and Computers snap-ins to create HP Role objects in the *Roles* organizational unit.
   a. Right-click the Roles organizational unit, select **New** then **Object.**
   b. Select **Role** for the field type in the Create New HP Management Object dialog box.
   c. Enter an appropriate name in the Name field of the New HP Management Object dialog box. In this example, the role will contain users trusted for remote server administration and will be called *remoteAdmins.* Click **OK.**
   d. 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 the roles rights, 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 select **Properties.**
   b. Select the **HP Devices** tab, then click **Add.**

c. Using the Select Users dialog box, select the Lights-Out Management object created in step 2, *rib-email-server* in folder testdomain.local/RILOES. Click **OK** to close the dialog, then click **Apply** to save the list.
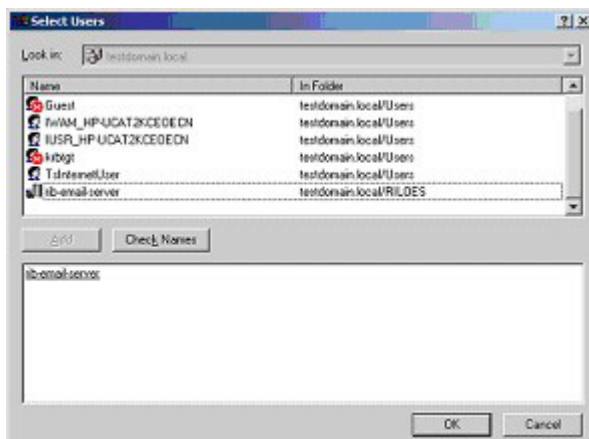
d. Add users to the role. Click the **Members** tab, and add users using the Add button and the Select Users dialog box. The devices and users are now associated.
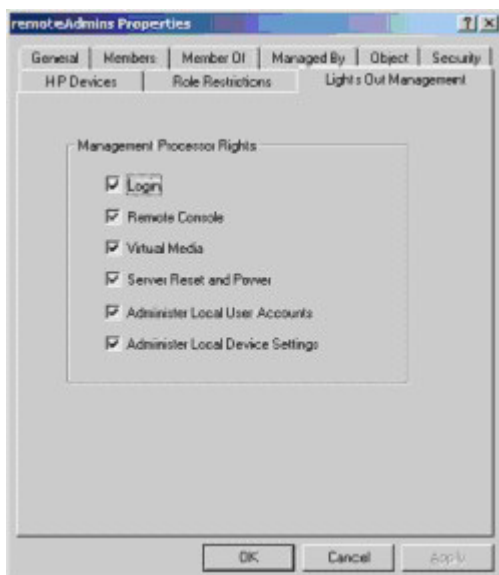
4. Use the Lights Out Management tab to set the rights for the role. All users and groups within a role will have the rights assigned to the role on all of the RILOE II devices managed by the role. In this example, the users in the *remoteAdmins* role will be given full access to the RILOE II functionality. Select the boxes next to each right, and then click **Apply.** Click **OK** to close the property sheet.

5. Using the same procedure as in step 4, edit the properties of the *remoteMonitors* role, add the *rib-email-server* device to the Managed Devices list on the HP Devices tab, and add users to the *remoteMonitors* role using the Members tab. Then, on the Lights Out Management tab, select the box next to the Login. Click **Apply** and **OK.** Members of the *remoteMonitors* role will be able to authenticate and view the server status.

User rights to any RILOE II are calculated as the sum of all the rights assigned by all the roles in which the user is a member, and in which the RILOE II is a Managed Device. Following the preceding examples, if a user is in both the *remoteAdmins* and *remoteMonitors* roles, they will have all the rights, because the *remoteAdmins* role has those rights.

To configure RILOE II and associate it with a Lights-Out Management object used in this example, use settings similar to the following on the Directory Settings screen.

```
RIB Object DN = cn=rib-email-server,ou=RILOES,dc=testdomain,dc=local
```

```
Directory User Context 1 = cn=Users,dc=testdomain,dc=local
```

For example, to gain access, user *Mel Moore*, with the unique ID *MooreM*, located in the users organizational unit within the *testdomain.local* domain, who is also a member of one of the *remoteAdmins* or *remoteMonitors* roles, would be allowed to log in to the RILOE II. Mel would enter `testdomain\moorem`, or `moorem@testdomain.local`, or `Mel Moore`, in the Login Name field of the RILOE II login screen, and use their Active Directory password in the Password field of that screen.

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 user or groups already contained within the directory service. User management of RILOE II requires three 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.

NOTE: After the snap-ins are installed, ConsoleOne and MMC must be restarted to show the new entries.

After the snap-in is installed, RILOE II objects and RILOE II roles can be created in the directory. Using the Users and Computers tool, the user will:

- Create RILOE II and role objects.
- Add users to the role objects.
- Set the rights and restrictions of the role objects.

Active Directory snap-ins

The following sections discuss the additional management options available within Active Directory Users and Computers after the HP snap-ins have been installed.

HP Devices

The HP Devices tab is used to add the HP devices to be managed within a role. Clicking **Add** enables you to browse to a specific HP device and add it to the list of member devices. Clicking **Remove** enables you to browse to a specific HP device and remove it from the list of member devices.

Members

After user objects are created, the Members tab enables you to manage the users within the role. Clicking **Add** enables you to browse to the specific user you want to add. Highlighting an existing user and clicking **Remove** removes the user from the list of valid members.
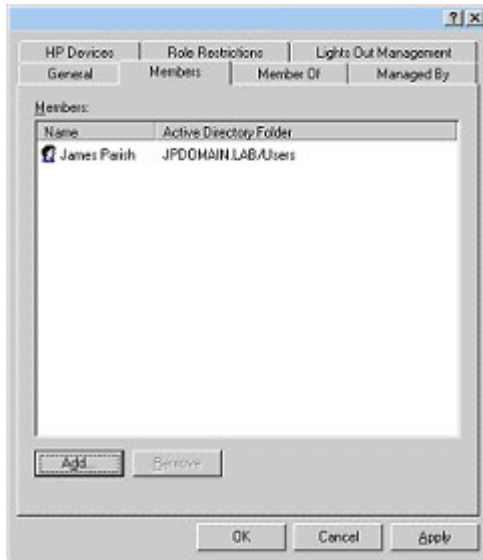
Active Directory role restrictions

The Role Restrictions subtab allows you to set login restrictions for the role. These restrictions include:

- Time restrictions
- IP network address restrictions
  - IP/mask
  - IP range

- DNS name
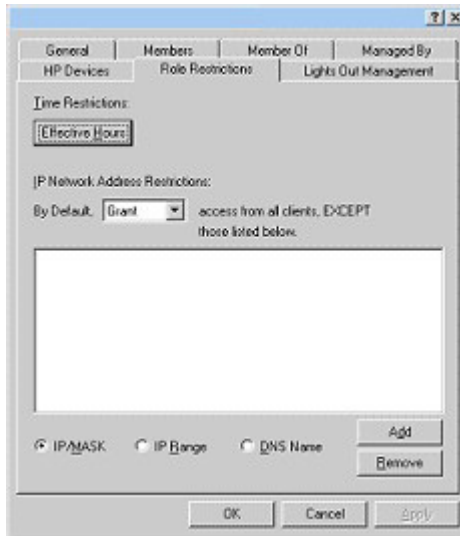
Time restrictions

You can manage the hours available for logon by members of the role by clicking **Effective Hours** in the Role Restrictions tab. In the Logon Hours pop-up window, 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.
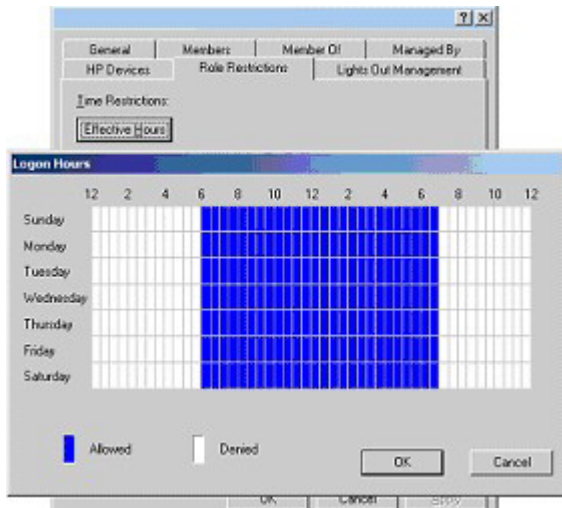
Enforced client IP address or DNS name access

Access can be granted or denied to an IP address, IP address range, or DNS names.

1. In the By Default dropdown menu, select whether to **Grant** or **Deny** access from all addresses except the specified IP addresses, IP address ranges, and DNS names.

2. Select the addresses to be added, select the type of restriction, and click **Add.**

3. In the new restriction pop-up window, enter the information and click **OK.** The new restriction pop-up window displays.

   The DNS Name option allows you to restrict access based on a single DNS name or a subdomain, entered in the form of host.company.com or *.domain.company.com.

4. Click **OK** to save the changes.

To remove any of the entries, highlight the entry in the display list and click **Remove.**
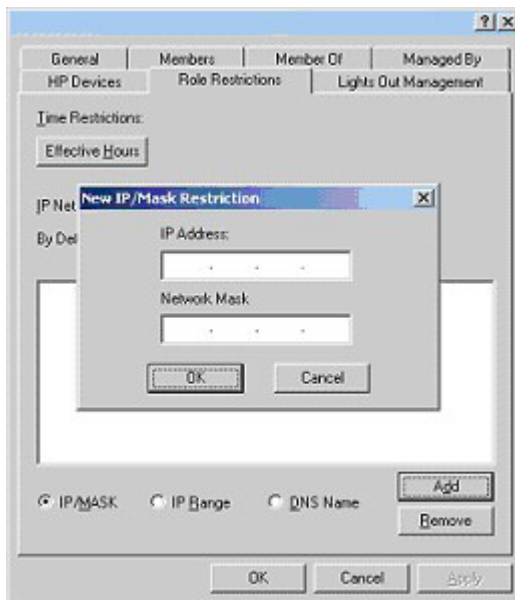
Active Directory Lights-Out management

After a role is created, rights for the role can be selected. Users and group objects can now be made 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.

The available rights are:

- **Login**—This option controls whether users can log in to the associated devices.
- **Remote Console**—This option enables the user access to the Remote Console.
- **Virtual Media**—This option enables the user access to the RILOE II virtual media functionality.
- **Server Reset and Power**—This option enables the user access to the RILOE II Virtual Power button to remotely reset the server or power it down.
- **Administer Local User Accounts**—This option enables the user to administer accounts. The user can modify their account settings, modify other user account settings, add users, and delete users.

- **Administer Local Device Settings**—This option enables the user to configure the RILOE II management processor settings. These settings include the options available on the Global Settings, Network Settings, SNMP Settings, and Directory Settings screens of the RILOE II Web browser.

Directory services for eDirectory

The following sections provide installation prerequisites, preparation, and a working example of Directory Services for eDirectory.

eDirectory installation prerequisites

Directory Services for RILOE II uses LDAP over SSL to communicate with the directory servers. RILOE II software is designed to install in an eDirectory version 8.6.1 (and above) tree. HP does not recommend installing this product if you have eDirectory servers with a version less than eDirectory 8.6.1. Before installing snap-ins and schema extensions for eDirectory, you should read and have available the following technical information documents, available at Novell Support (http://support.novell.com).

Installing Directory Services for RILOE II requires extending the eDirectory schema. Extending the schema must be completed by an Administrator.

- TID10066591 *Novell eDirectory 8.6 NDS compatibility*
- TID10057565 *Unknown objects in a mixed environment*
- TID10059954 *How to test whether LDAP is working correctly*
- TID10023209 *How to configure LDAP for SSL (secure) connections*
- TID10075010 *How to test LDAP authentication*

Snap-in installation and initialization for eDirectory

Refer to "Snap-in installation and initialization ("Snap-in installation and initialization for Active Directory" on page)" for step-by-step instructions on using the snap-in installation application.

📝 **NOTE:** After the snap-ins are installed, ConsoleOne and MMC must be restarted to show the new entries.

Example: Creating and configuring directory objects for use with LOM devices in eDirectory

The following example shows how to set up roles and HP devices in a company called *samplecorp*, which consist of two regions, *region1* and *region2*.

Assume *samplecorp* has an enterprise directory arranged according to the following screen.
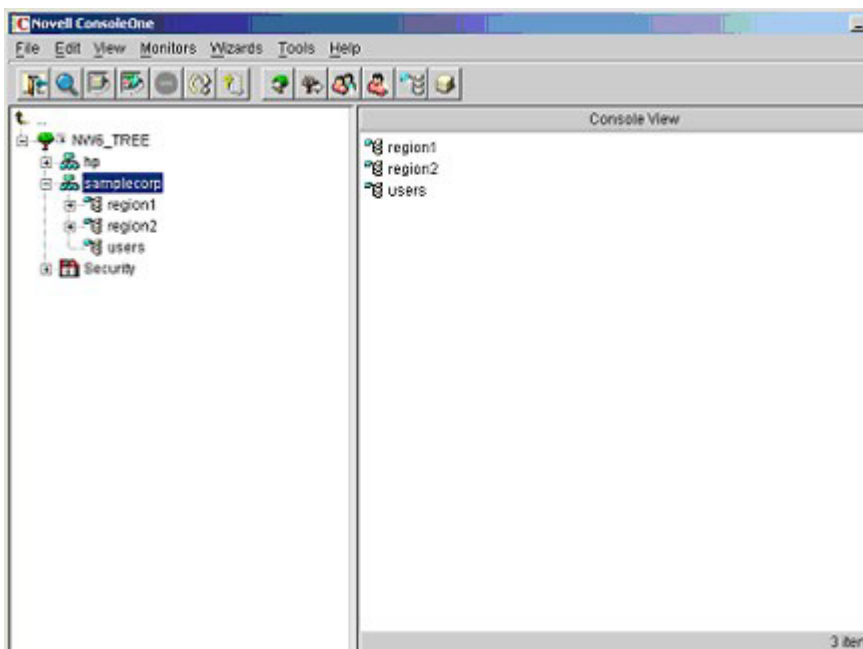
1. Begin by creating organizational units in each region, which will contain the Lights-Out Management devices and roles specific to that region. In this example, two organizational units are created, called *roles* and *hp devices*, in each organizational unit, *region1* and *region2*.

2. Use the HP provided ConsoleOne snap-ins to create Lights-Out Management objects in the *hp devices* organizational unit for several RILOE II devices.

   a. Right-click the *hp devices* organizational unit found in the *region1* organizational unit, and select **New** then **Object.**

   b. Select **hpqTarget** from the list of classes and click **OK.**

   c. Enter an appropriate name and surname in the **New hpqTarget** dialog box. In this example, the DNS host name of the RILOE II device, *rib-email-server* will be used as the name of the Lights-Out Management object, and the surname will be *RILOEII*. Click **OK.**

   d. The **Select Object Subtype** dialog box is displayed. Select **Lights Out Management Device** from the list, and click **OK.**

Directory services   93

Repeat the process for several more RILOE II devices with DNS names *rib-nntp-server* and *rib-file-server-users1* in *hp devices* under *region1*, and *rib-file-server-users2* and *rib-app-server* in *hp devices* under *region2*.
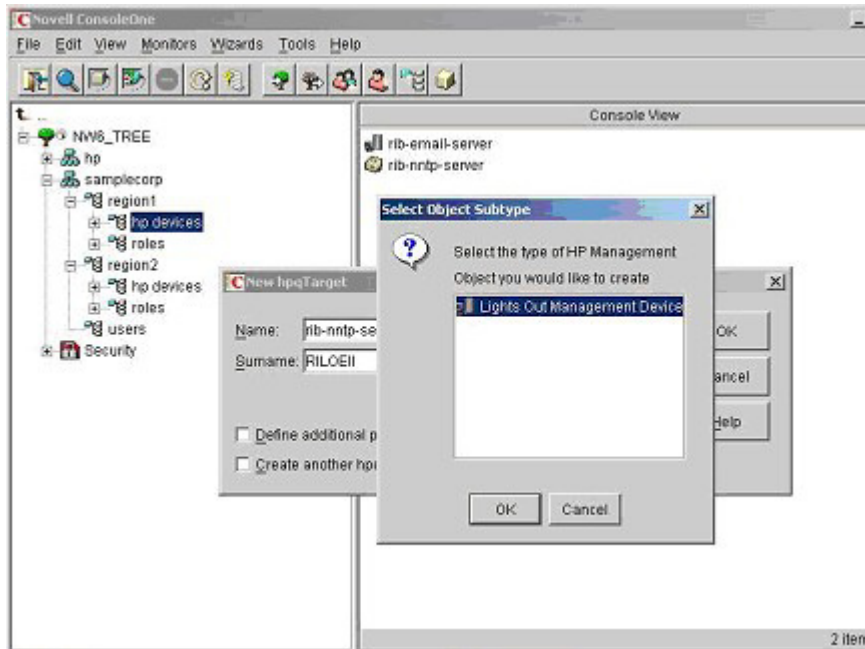
1. Use the HP provided ConsoleOne snap-ins to create HP Role objects in the *roles* organizational units.

   a. Right-click the *roles* organizational unit found in the *region2* organizational unit, and select **New** then **Object.**

   b. Select **hpqRole** from the list of classes and click **OK.**

   c. Enter an appropriate name in the **New hpqRole** dialog box. In this example, the role will contain users trusted for remote server administration and will be named *remoteAdmins.* Click **OK.**

   d. The **Select Object Subtype** dialog box is displayed. Because this role will be managing the rights to Lights-Out Management devices, select **Lights Out Management Devices** from the list, and click **OK.**

   e. Repeat the process, creating a role for remote server monitors, named *remoteMonitors,* in *roles* in *region1*, and a *remoteAdmins* and a *remoteMonitors* role in *roles* in *region2*.

2. Use the HP provided ConsoleOne snap-ins to assign rights to the role and associate the roles with users and devices.

   a. Right-click on the *remoteAdmins* role in the *roles* organizational unit in the *region1* organizational unit, and select **Properties.**

   b. Select the **Role Managed Devices** subtab of the **HP Management** tab, and click **Add.**

   c. Using the **Select Objects** dialog box, browse to the *hp devices* organizational unit in the *region1* organizational unit. Select the three Lights-Out Management objects created in step 2. Click **OK,** then click **Apply.**

   d. Next, add users to the role. Click the **Members** tab, and add users using the **Add** button and the **Select Object** dialog box.

e. The devices and users are now associated. Use the **Lights Out Management Device Rights** subtab of the **HP Management** tab to set the rights for the role. All users within a role will have the rights assigned to the role on all of the RILOE II devices managed by the role. In this example, the users in the *remoteAdmins* role will be given full access to the RILOE II functionality. Select the boxes next to each right, and click **Apply.** Click **Close** to close the property sheet.
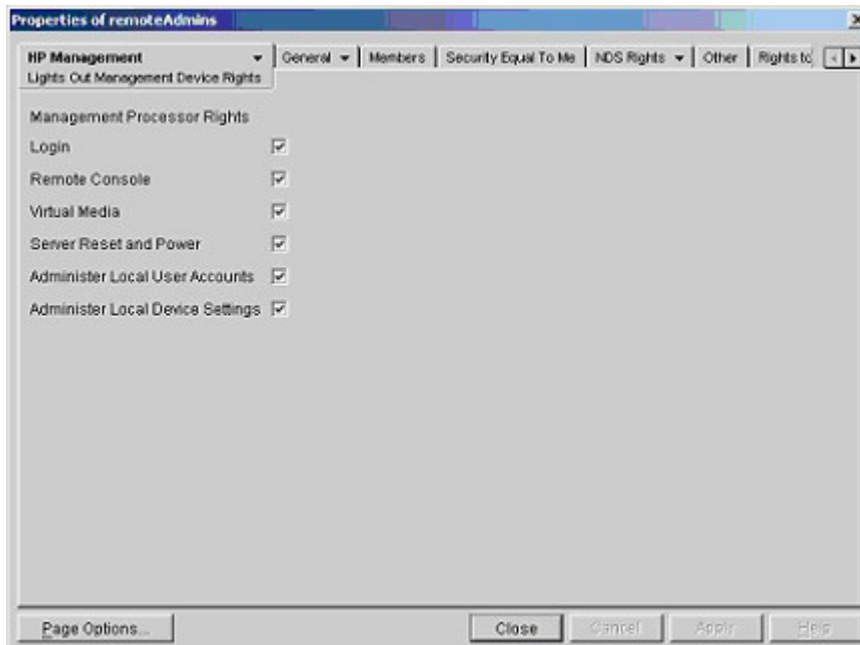
3. Using the same procedure as in step 1, edit the properties of the *remoteMonitors* role:

    a. Add the three RILOE II devices within *hp devices* under *region1* to the **Managed Devices** list on the **Role Managed Devices** subtab of the **HP Management** tab.

    b. Add users to the *remoteMonitors* role using the **Members** tab.

    c. Then, using the **Lights Out Management Device Rights** subtab of the **HP Management** tab, select the check box next to **Login,** and click **Apply** and **Close.** Members of the *remoteMonitors* role will be able to authenticate and view the server status.

User rights to any LOM device are calculated as the sum of all the rights assigned by all the roles in which the user is a member, and in which the LOM device is a Managed Device. Following the preceding examples, if a user is in both the *remoteAdmins* and *remoteMonitors* roles, they will have all the rights, because the *remoteAdmins* role has those rights.

To configure a LOM device and associate it with a Lights-Out Management object used in this example, use settings similar to the following on the **Directory Settings** screen.

📝 **NOTE:** Commas, not periods, are used in LDAP distinguished names to separate each component.

```
RIB Object DN = cn=rib-email-server,ou=hp
devices,ou=region1,o=samplecorp
Directory User Context 1 = ou=users,o=samplecorp
```

For example, user *CSmith*, located in the *users* organizational unit within the *samplecorp* organization, who is also a member of one of the *remoteAdmins* or *remoteMonitors* roles, would be allowed to log in to the RILOE II. They would type csmith (case insensitive) in the **Login Name** field of the RILOE II login screen and use their eDirectory password in the **Password** field of that screen to gain access.

Directory Services objects for eDirectory

Directory Services objects enable virtualization of the managed devices and the relationships between the managed device and user or groups already contained within the directory service.

Role managed devices

The Role Managed Devices subtab under the HP Management tab is used to add the HP devices to be managed within a role. Clicking **Add** allows you to browse to the specific HP device and add it as a managed device.
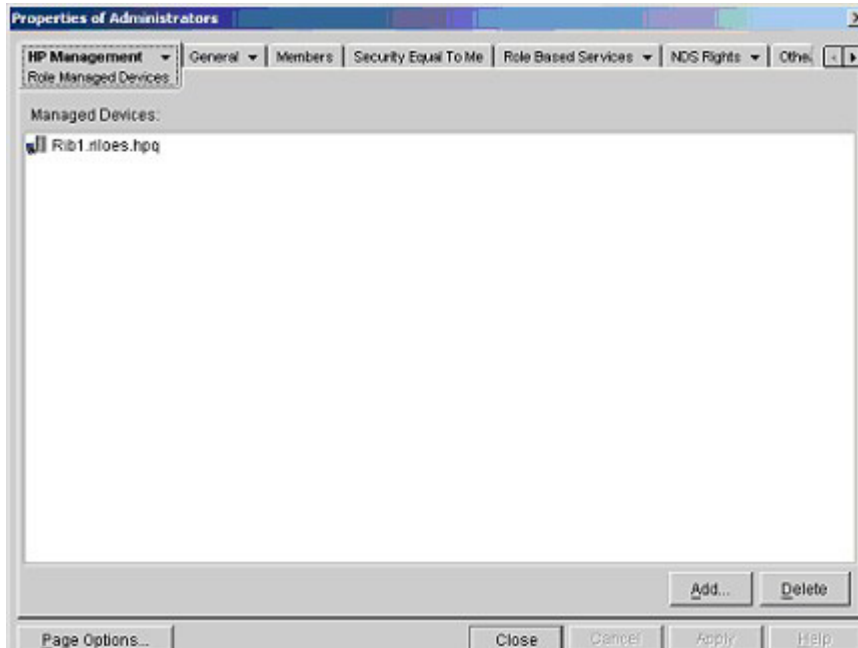
Members

After user objects are created, the Members tab allows you to manage the users within the role. Clicking **Add** allows you to browse to the specific user you want to add. Highlighting an existing user and clicking **Delete** removes the user from the list of valid members.
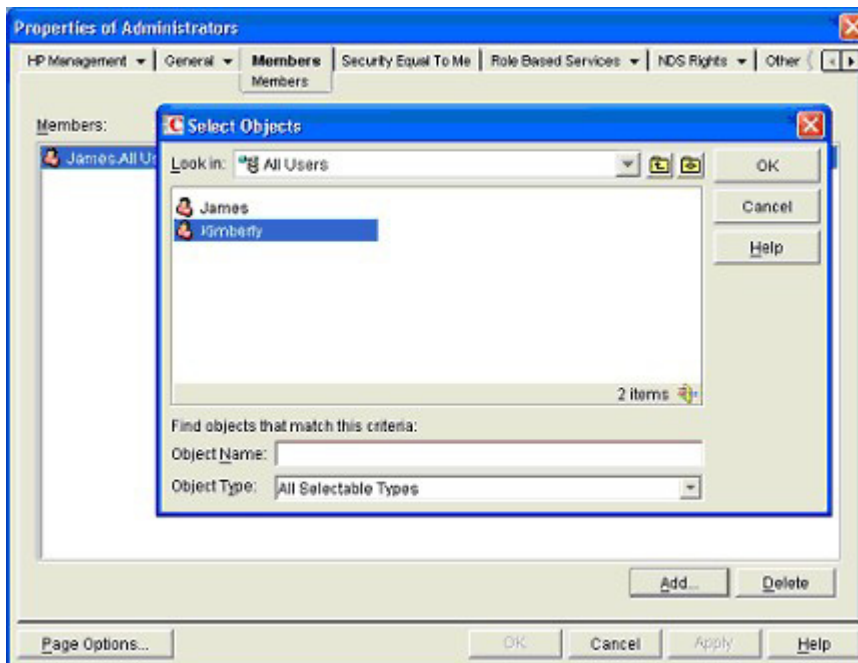
eDirectory Role Restrictions

The Role Restrictions subtab allows you to set login restrictions for the role. These restrictions include:

- Time restrictions
- IP network address restrictions
  - IP/mask
  - IP range
- DNS name
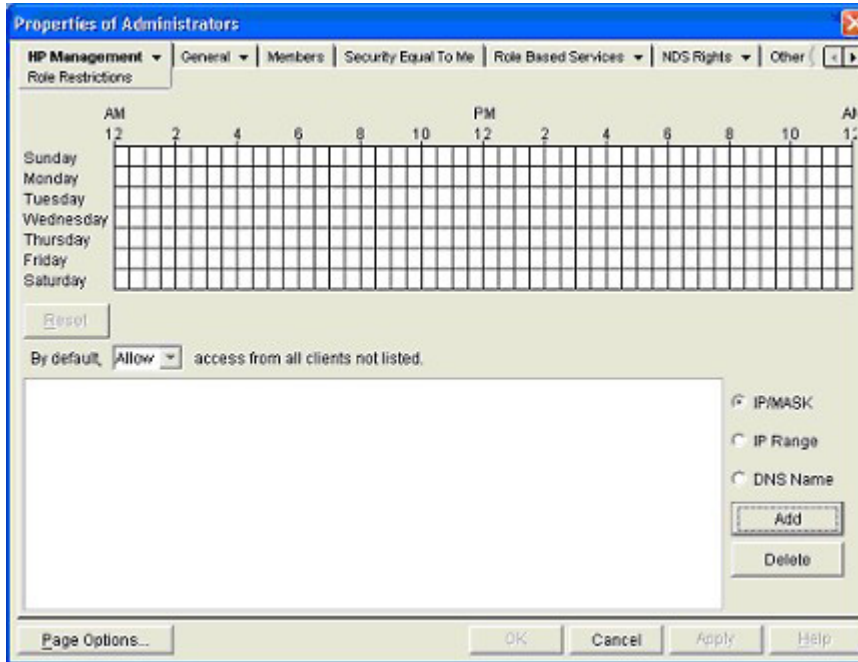
Time restrictions

You can manage the hours available for logon by members of the role by using the time grid displayed in the Role Restrictions subtab. You can select the times available for logon for each day of the week in half-hour increments. You can change a single square by clicking it, or a section of squares by clicking and holding the mouse button, dragging the cursor across the squares to be changed, and releasing the mouse button. The default setting is to allow access at all times.

Enforced client IP address or DNS name access

Access can be granted or denied to an IP address, IP address range, or DNS names.

1. In the By Default dropdown menu, select whether to **Allow** or **Deny** access from all addresses, except the specified IP addresses, IP address ranges, and DNS names.
2. Select the addresses to be added, select the type of restriction, and click **Add.**
3. In the Add New Restriction pop-up window, enter the information and click **OK.** The Add New Restriction pop-up for the IP/Mask option is shown.

   The DNS Name option allows you to restrict access based on a single DNS name or a subdomain, entered in the form of host.company.com or *.domain.company.com.
4. Click **Apply** to save the changes.

To remove any of the entries, highlight the entry in the display field and click **Delete.**
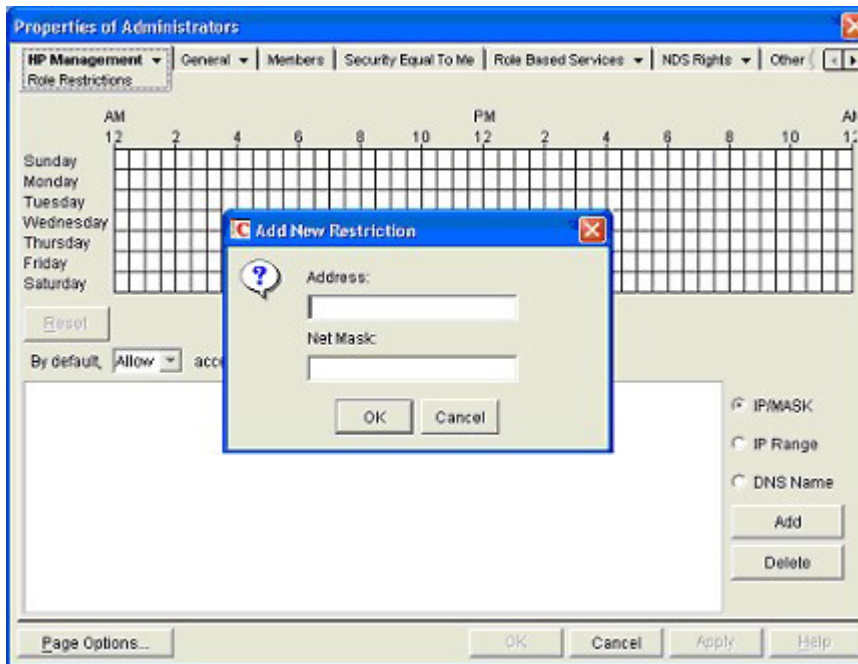
Lights-Out Management

After a role is created, rights for the role can be selected. Users and group objects can now be made 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 Device Rights subtab of the HP Management tab.
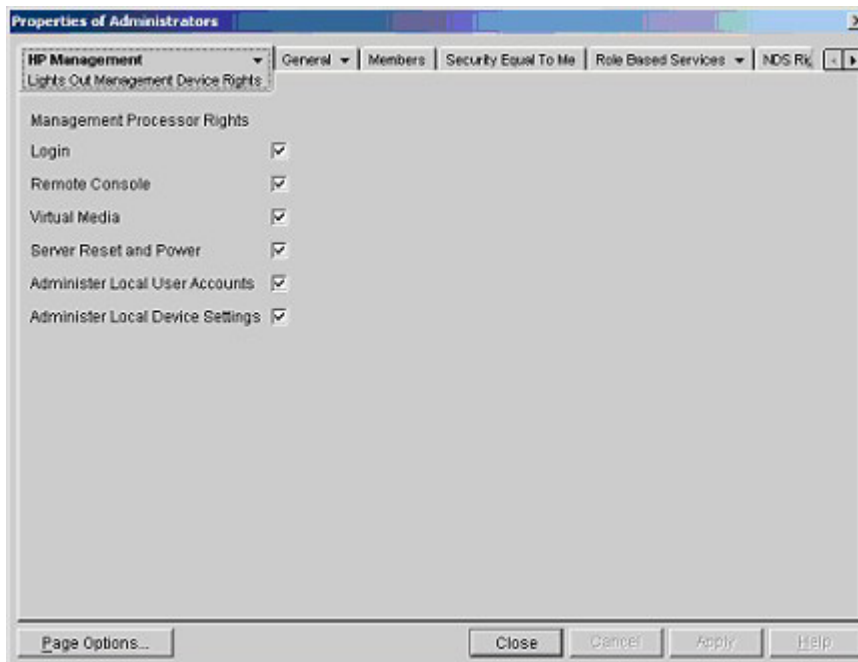
The available rights are:

- **Login**—This option controls whether users can to log in to the associated devices.

    Login access can be used to create a user who is a service provider and who receives alerts from the board but does not have login access to the RILOE II.

- **Remote Console**—This option allows the user access to the Remote Console.
- **Virtual Media**—This option allows the user access to the RILOE II Virtual Floppy and Virtual Media functionality.
- **Server Reset and Power**—This option allows the user to remotely reset the server or power it down.
- **Administer Local User Accounts**—This option allows the user to administer accounts. The user can modify their account settings, modify other user account settings, add users, and delete users.
- **Administer Local Device Settings**—This option allows the user to configure the RILOE II board settings. These settings include the options available on the **Global Settings, Network Settings, SNMP Settings,** and **Directory Settings** screens of the RILOE II Web browser.

User login using directory services

The RILOE II login page Login Name field accepts all of the following:

- Directory users
- LDAP Fully Distinguished Names

  Example: CN=John Smith,CN=Users,DC=HP,DC=COM, or @HP.com

NOTE: The short form of the login name by itself does not tell the directory which domain you are trying to access. You must provide the domain name or use the LDAP distinguished name of your account.

- DOMAIN\user name form (Active Directory Only)

  Example: HP\jsmith
- username@domain form (Active Directory Only)

  Example: jsmith@hp.com

NOTE: Directory users specified using the @ searchable form may be located in one of three searchable contexts, which are configured within Directory Settings.

- User name form

  Example: John Smith

NOTE: Directory users specified using the user name form may be located in one of three searchable contexts, which are configured within Directory Settings.

- Local users—Login-ID

NOTE: On the RILOE II login page, the maximum length of the login name is 39 characters for local users. For Directory Services users, the maximum length of the login name is 256 characters.

Directory settings

The Directory Settings page enables you to configure and test your directory services. Click **Apply Settings** to save any changes.

Administer Groups allows you to associate one of the six groups available in Group Administration page, with the groups in Active Directory server.

Test Settings allows you to test the communication between the directory server and RILOE II.
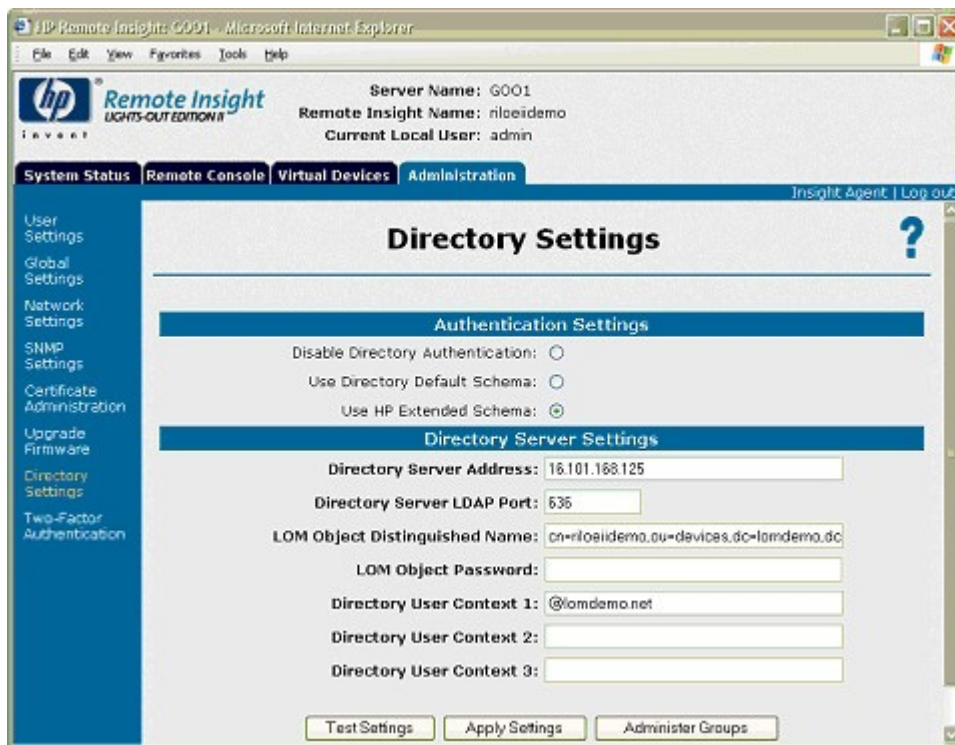
Parameter	Default value	Definition
Disable Directory Authentication	No	This parameter enables or disables directory authentication. If this parameter is set to Yes and directory support is properly configured, this parameter enables user login to RILOE II using directory credentials.
Use Directory Default Schema	Yes	This parameter enables or disables the use of schema-free directories.
Use HP Extended Schema	No	This parameter enables or disables the use of extended schema directories.
Directory Server Address	0.0.0.0	This parameter specifies the Directory Server DNS name or IP address. HP recommends using a DNS name or multi-host DNS name. If an IP address is used, the directory will not be available if that server is down.
Directory Server LDAP Port	636	This option sets the port number used to connect to the directory server. The SSL-secured LDAP port number is 636.
LOM Object Distinguished Name	N/A	This option specifies the unique name for RILOE II in the directory. LOM Object Distinguished Names are limited to 256 characters.
LOM Object Password	N/A	This parameter specifies the password for the RILOE II object to access the directory. LOM Object Passwords are limited to 40 characters.

Parameter	Default value	Definition
Directory User Context 1, Directory User Context 2, Directory User Context 3	N/A	This parameter enables you to specify up to three searchable contexts used to locate the user when the user is trying to authenticate using the directory. Directory User Contexts are limited to 128 characters each. Directory User Contexts enable you to specify directory user containers that are automatically searched when an RILOE II login is attempted. This eliminates the requirement of entering a fully distinguished user name at the login page. For example, the search context, "ou=lights out devices,o=corp" would allow the user "cn=manager,ou=lights out devices,o=corp" to log in to RILOE II using just "manager." Active Directory allows an additional search context format, "@hostname" for example, "@directory.corp."

Group administration

The Group Administration option on the Directory Settings page allows users with the Administer Directory Groups privilege to view RILOE II groups and modify the settings of those groups.

To modify a group:

1. Select the group and click **View/Modify**. The Modify Group page appears allowing you to assign the rights available to each users in the selected group in the Active Directory server.
2. Enter the full context of the group in the Security Group Distinguished Name field.
3. Click **Save Group Information** to accept any changes or click **Restore Group Information** to restore the previously saved settings.
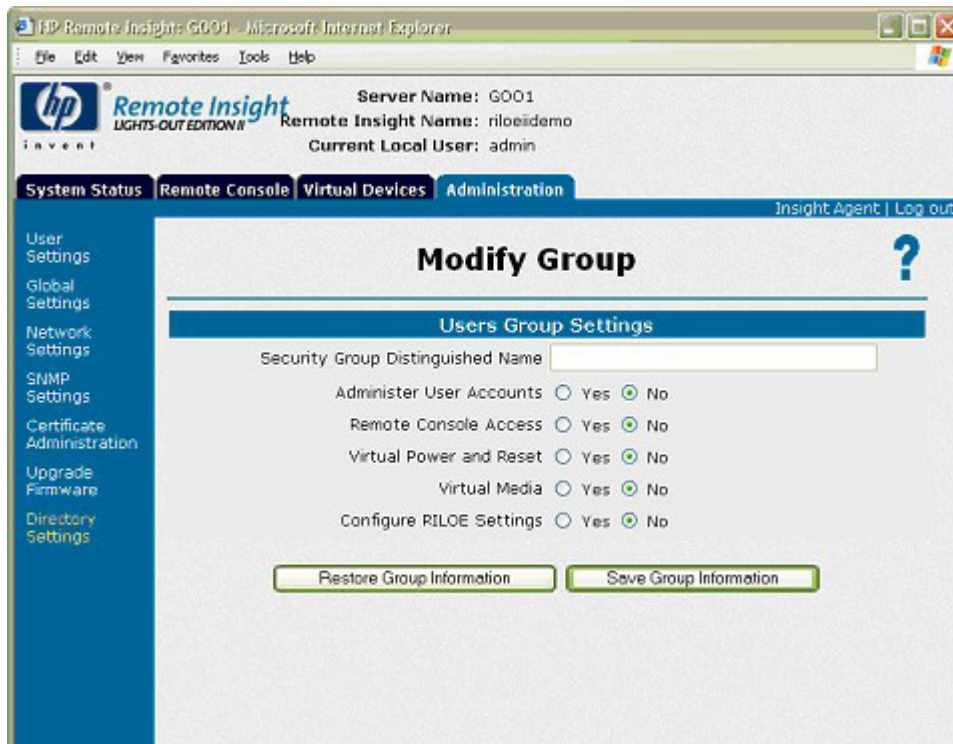
Directory tests

To validate current directory settings for RILOE II:

1. Click **Test Settings** on the Directory Settings page. The Directory Tests page appears.

2. Enter the distinguished name and password of a directory administrator. A good choice would be the same credentials used when creating RILOE II objects in the directory. These credentials are not stored by RILOE II. They are used to verify the RILOE II object and user search contexts.

3. Click **Test Directory Settings**.

4. Enter a test user name and password. Typically, the test account is intended to access the RILOE II being tested. It can be the same account as the directory administrator. However, the tests cannot verify user authentication with a superuser account. These credentials are not stored by RILOE II.

5. Click **Start Test**. Several tests begin in the background, starting with a network ping of the directory user through establishing an SSL connection to the server and evaluating user privileges as they would be evaluated during a normal login.

   While the tests are running, the page periodically refreshes. At any time during test execution you can stop the tests or manually refresh the page.

The test results page displays a series of simple tests designed to validate the current directory settings. A test log is included documenting test results and any errors detected. After directory settings are configured correctly, you do not need to rerun these tests. Consult the help link on the page for test details and actions in the event of trouble.

Directory-enabled remote management

In this section

Introduction to directory-enabled remote management

This section is for administrators who are familiar with directory services and the RILOE II product and want to use the HP schema directory integration option for RILOE II. You must be familiar with the "Directory services (on page 75)" section and comfortable with setting up and understanding the examples.

Directory-enabled remote management enables you to:

- 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. Refer to the "Directory services (on page 75)" section for additional information on creating LOM device objects for Active Directory ("Directory services for Active Directory" on page 83) and eDirectory ("Directory services for eDirectory" on page 92). In general, you can use the HP provided snap-ins 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 the 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. Refer to "Configuring directory settings" for details on the specific directory settings. In general, you can configure each device with the appropriate directory server address, LOM object distinguished name, and any user contexts. The server address is either the IP address or DNS name of a local directory server or, for more redundancy, a multi-host DNS name.

Creating roles to follow organizational structure

Often, the administrators within an organization are placed into 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 the subordinate administrators to create and manage their own roles.

Using existing groups

Many organizations will have their users and administrators arranged into groups. In many cases, it is convenient to use the existing groups and associate the groups 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, it is possible to place one group within another or 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. New users can be added to either the existing group or the role.

Novell eDirectory does not allow nested groups. In eDirectory, any user that can read a role is considered a member of that role. When adding an existing group, organizational unit or organization to a role, add the object as a read trustee of the role. All the members of the object are considered members of the role. New users can be added to either the existing object or the role.

When using trustee or directory rights assignments to extend role membership, users must be able to read the LOM object representing the LOM device. Some environments require the same trustees of a role to also be read trustees of the LOM object to successfully authenticate users.

Using multiple roles

Most deployments do not require the same user to be in multiple roles managing the same device. However, these configurations are useful for building complex rights relationships. When building multiple-role relationships, users receive all the 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 additional 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 group. More advanced rights are assigned through the Admin role, which assigns additional rights—Server Reset and Remote Console.
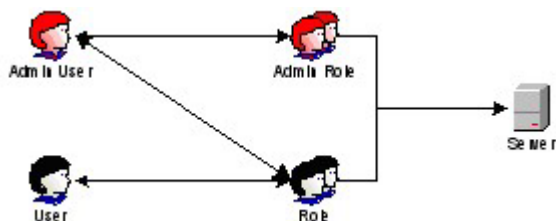
The Admin role assigns all admin rights—Server Reset, Remote Console, and Login.
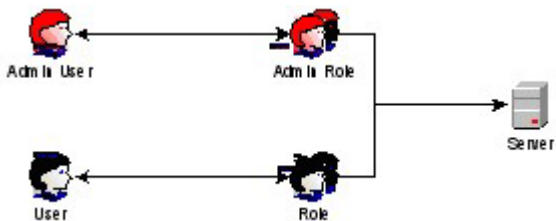
How directory login restrictions are enforced

Two sets of restrictions potentially limit a directory user's access to LOM devices. 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.
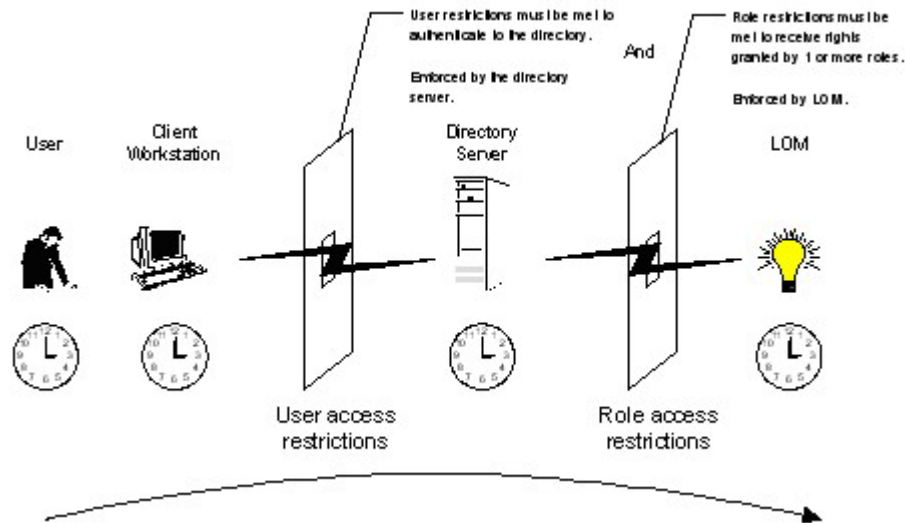
Restricting roles

Restrictions allow administrators to limit the scope of a role. A role only grants rights to those users that satisfy the role's restrictions. Using restricted roles results in users with dynamic rights that change based on the time of day or network address of the client.

For step-by-step instructions on how to create network and time restrictions on a role, refer to "Active Directory Role Restrictions (on page 89)" or "eDirectory Role Restrictions (on page 97)" sections.

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 that 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 on the role.

Role-based time restrictions can only be satisfied if the time is set on the LOM device. The time is normally set when the host is booted, and it is maintained by running the agents in the host operating system, which allows the LOM device to compensate for leap year 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's 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, and these restrictions are enforced by the directory server. Refer to the directory service documentation for details on the enforcement of address restrictions on LDAP clients, such as a user logging in to a LOM device.

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 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 by the restriction. 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 by the restriction. 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 using a subnet address and address bit mask that identifies addresses that are on the same logical network.

In binary math, if the bits of a client machine address, added with the bits of the subnet mask, match the restriction subnet address, then the client machine meets the restriction.

DNS-based restrictions

DNS-based restrictions use the network naming 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 will fail.

DNS-based restrictions can limit access to a single, specific machine name or to machines sharing a common domain suffix. For example, the DNS restriction, www.hp.com, matches hosts that are assigned the domain name www.hp.com. However, the DNS restriction, *.hp.com, matches any machine originating from HP.

DNS restrictions can cause some 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 some security complications. Name service protocols are insecure. Any individual with malicious intent and access to the network can place a rogue DNS service on the network creating fake address restriction criteria. Organizational security policies should be taken into consideration when implementing DNS-based address restrictions.

How user time restrictions are enforced

Administrators can place a time restriction on directory user accounts. 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, but if the directory server is located in a different time zone or a replica in a different time zone is accessed, then 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 authentication mechanism.
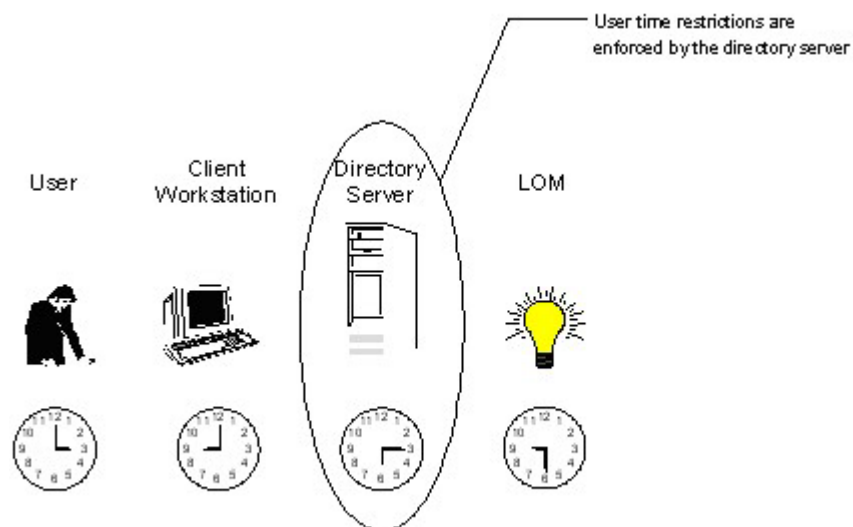
Creating multiple restrictions and roles

The most useful application of multiple roles includes 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 are only able to reset the server outside of 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 an after-hours application might allow administrators outside the corporate network to reset the server, which is contrary to most security policies.

In the example, security policy dictates general use is restricted to clients within the corporate subnet, and server reset capability is additionally restricted to after hours.
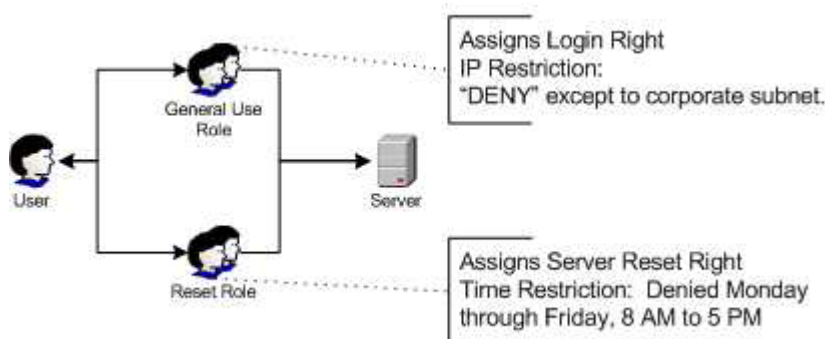
Alternatively, the directory administrator could create a role that grants the login right and restrict it to the corporate network, then create another role that grants only the server reset right and restrict it to after-hours operation. This configuration is easier to manage but more dangerous because on-going administration might create another role that grants users from addresses outside the corporate network the login right, which could unintentionally grant the LOM administrators in the server Reset role the ability to reset the server from anywhere, provided they satisfy the time constraints of that role.

The previous configuration meets corporate security policy. 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, as well as the General Use role.
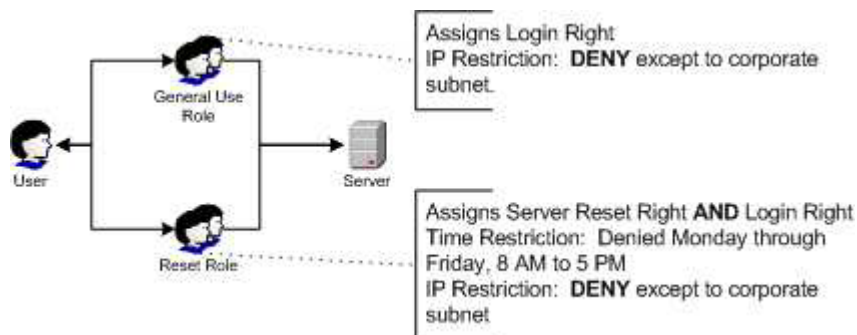
Using bulk import tools

Adding and configuring large numbers of LOM objects is time consuming. HP provides several utilities to assist in these tasks. Below is a brief description of the utilities available.

- HP Lights-Out Migration Utility

  The HP Lights-Out Migration utility, HPQLOMIG.EXE, imports and configures multiple LOM devices. HPQLOMIG.EXE 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 numerous management processors. For more information, refer to the "Lights-Out directories migration utilities (on page 113)" section.

- HP Lights-Out Migration Command Utility

  The HP Lights-Out Migration Command utility, HPQLOMGC.EXE, offers a command-line approach to migration, rather than a GUI-based approach. This utility works in conjunction with the Application Launch and query features of Systems Insight Manager to configure many devices at a time. Customers that must configure only a few LOM devices to use directory services might also prefer the command-line approach. For more information, refer to the "Lights-Out directories migration utilities (on page 113)" section.

- Systems Insight Manager can:

  - Manage multiple LOM devices.

  - Discover the LOM devices as management processors using CPQLOCFG to send a RIBCL XML script file to a group of LOM devices to manage those LOM devices. The LOM devices perform the actions designated by the RIBCL file and send a response to the CPQLOCFG log file. For more information, refer to the "Group administration and RILOE II scripting ("Group administration using the Lights-Out Configuration Utility" on page 125)" and the "Remote Insight command language (on page 138)" sections in the *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource 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. However, administrators must still configure the devices manually, as described previously, 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. The "Directory services schema (on page)" section provides details on attributes and attribute data formats when creating LOM objects.

Scripting, command line, and utility options

In this section

Overview of the Lights-Out DOS utility

CPQLODOS is a command line utility that is a part of the SmartStart Scripting Toolkit. It is intended to be an initial configuration program to set up only those essential RILOE II settings necessary to allow one of the other full-featured configuration methods. Because of this limited usage model, it processes only a small subset of the RILOE II scripting language.

NOTE: CPQLODOS is a DOS-only tool that requires MS-DOS® 6.0 or higher. Lights-Out scripting is not supported on Linux operating systems or when using the Novell NetWare Client.

CPQLODOS enables you to configure features exposed through F8 startup or the graphical user interface. This utility is not intended for continued administration. The RIBCL should be used to administer user rights and network functionality on the server.

CPQLODOS general guidelines

An opening command opens a database. The database remains open until the matching closing command is sent. All changes made within a single command block are applied simultaneously when the database is closed. Any errors within the block cause the enclosed changes to be discarded.

An example of an opening command and its matching closing command are:

```
<USER_INFO>
</USER_INFO>
```

In all examples, the opening and closing commands are displayed.

Command line arguments

All of the commands are grouped by functionality. All commands that manipulate user information are grouped together. Grouping commands allow the firmware to view the data to be manipulated as a block of information, similar to a text document, allowing for multithreaded access to the different kinds of information.

The following table lists the arguments recognized by CPQLODOS.

Command line argument	Description
/HELP or /?	Displays simple help messages.

Command line argument	Description
/RESET_RILOE	Resets the RILOE II management processor to default factory settings.
/DETECT	Detects the RILOE II management processor on the target server.
/RESET_RILOE	Resets the RILOE II management processor.
/VIRT_FLOPPY	Ignores the virtual floppy inserted error.
/MIN_FW-xxx	Enables you to set the minimum firmware version on which the RILOE II management processor runs.
/GET_STATUS	Returns the status of the RILOE II management processor.
/GET_HOSTINFO	Retrieves and displays the current host server information on the RILOE II management processor and displays the server name and number.
/GET_USERINFO	Obtains the current users stored in the RILOE II management processor board and displays the names, login names, and security mask information.
/GET_NICCONFIG	Retrieves and displays the NIC settings stored in the RILOE II management processor.
/GET_DHCPCONFIG	Retrieves and displays the DHCP settings stored in the RILOE II management processor.
/GET_DIRCONFIG	Retrieves and displays the DIRECTORY settings in the RILOE II management processor.
/WRITE_XML=path\file name.ext	Reads the settings on the RILOE II management processor and writes the NIC, DHCP, DIRECTORY, and user settings into an XML hardware configuration script file.
/LOAD_XML=path\file name.ext	Loads the script file and applies its changes to the current configuration on the RILOE II management processor.
/VERIFY_XML	Verifies the accuracy of the script file and generates an error message for any incorrect data.

RIBCL XML Commands for CPQLODOS

CPQLODOS uses the same RIBCL XML commands as CPQLOCFG for the `<MOD_NETWORK_SETTINGS>`, and the `<MOD_DIR_CONFIG>` XML scripting language blocks. Only those parameters unique to CPQLODOS are discussed. For more information on `<MOD_NETWORK_SETTINGS>`, and `<MOD_DIR_CONFIG>` refer to:

- MOD_NETWORK_SETTINGS
- MOD_DIR_CONFIG

The following XML blocks are unique to CPQLODOS:

- CPQLODOS (on page)
- ADD_USER (on page)

CPQLODOS

This command is used to start and end a CPQLODOS session. It can be used only once in a script, and it must be the first and last statement in an XML script.

Example:
```
<CPQLODOS VERSION="2.0">
</CPQLODOS>
```

CPQLODOS parameter

VERSION is a numeric string that indicates the version of CPQLODOS necessary to process this script. The VERSION string is compared to the version that CPQLODOS can process. An error is returned if the version of CPQLODOS and the version of the script do not match. The VERSION parameter can never be blank.

CPQLODOS runtime error

The possible CPQLODOS error messages include `Version must not be blank.`

ADD_USER

This command is used to add a user to the RILOE II. If there are multiple ADD_USER commands in the XML script, CPQLODOS will use only the settings from the last command.

Example:
```
<ADD_USER
   USER_NAME = "James Madison"
   USER_LOGIN = "jmadison"
   PASSWORD = "president">
</ADD_USER>
```

ADD_USER parameters

USER_NAME is the actual name of the user. The USER_NAME parameter has a maximum length of 40 characters and can be any ASCII string containing printable characters, including white spaces. This string is used for display only and must never be blank.

USER_LOGIN is the name that the user types to log in to the RILOE II. The USER_LOGIN parameter has a maximum length of 40 characters, can be an ASCII string containing any combination of printable characters, and is case sensitive. The USER_LOGIN parameter must never be blank.

PASSWORD is the password that will be associated with the user. This parameter has a minimum length of 8 characters, a maximum length of 40 characters, and is an ASCII string that may contain any combination of printable characters. The PASSWORD parameter cannot contain both single and double quote characters. This parameter is case sensitive and must never be blank.

ADD_USER runtime errors

The possible ADD_USER error messages include:

- Login name is too long. Maximum length is 40 characters.
- Password is too short. Minimum length is 8 characters.
- Password is too long. Maximum length is 40 characters.
- User table is full. No room for new user.
- Cannot add user. The user name already exists.
- User information is open for read-only access. Write access is required for this operation.
- User name cannot be blank.
- User login ID cannot be blank.
- Password must not be blank.
- Boolean value not specified.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.

Lights-Out directories migration utilities

For customers with previously installed management processors, HP created two utilities to simplify the migration of these processors to management by directories. The two utilities are the HPQLOMIG utility and the HPQLOMGC utility. These utilities automate some of the migration steps necessary for the management processors to support directory services.

The HPQLOMIG utility automates the process of migrating management processors by creating objects in the directory corresponding to each management processor and associating them to a role. HPQLOMIG has a GUI and provides a wizard for implementing or upgrading large numbers of management processors.

HPQLOMGC is a command line utility that enables you to migrate individual management processors. Used with Systems Insight Manager, HPQLOMGC upgrades the firmware of the management processor, (if necessary), HPQLOMGC configures the management processor, and configures the directory settings. HPQLOMGC creates a device object in the directory using the name in the XML file or the network name (depending on whether or not you selected to create device objects on the command line) and associates the device object to a role. You can launch by itself or from within a script (for example, a batch file or Perl script).

Compatibility

HPQLOMIG and HPQLOMGC run on Microsoft® Windows® versions that support the Microsoft® .NET Framework. The Microsoft® .NET Framework is required. Additional information and download of the .NET framework can be found at http://www.microsoft.com/net/. Both utilities support the following operating systems:

- Active Directory
  - Windows® 2000
  - Windows® Server 2003
- Novell eDirectory 8.6.2
  - Red Hat Linux 7.2
  - Red Hat Linux 7.3
  - Windows® 2000
  - NetWare 6.0

Pre-migration checklist

1. Verify your current firmware version supports the HPQLOMIG and HPQLOMGC utilities.

Management processor	Minimum firmware version
RILOE	2.41
RILOE II	any version
iLO	1.10

2. Install Microsoft® .NET Framework.
3. Download the management processor firmware supporting Directory Services from the HP website (http://www.hp.com/servers/lights-out).
4. Download the HP Lights-Out Directory Services Smart Component from the HP website (http://www.hp.com/servers/lights-out).
5. Apply the HP Lights-Out schema extensions to the directory.

6. Create a role for the users of the management processor using the HP Lights-Out management snap-in.

HP Lights-Out directory package

All of the migration software, as well as the schema extender and management snap-ins, are packaged together in an HP Smart Component. To complete the migration of your management processors, the schema must be extended and the management snap-ins must be installed before the migration tool is run. The Smart Component can be found on the HP Lights-Out management website (http://www.hp.com/servers/lights-out).

To install the migration utilities, click **LDAP Migration Utility** in the Smart Component. A Microsoft® MSI installer is launched, which installs HPQLOMIG, HPQLOMGC, required DLLs, the license agreement, and other files into the C:\Program Files\Hewlett-Packard\HP Lights-Out Migration Tool directory. You can select a different directory. A sample XML file is also installed, and a shortcut to HPQLOMIG is created on the Start menu.

📝 **NOTE:** The installation utility will present an error message and exit if it detects that the .NET Framework is not installed.

HPQLOMIG operation

The command line utility is intended to be used in conjunction with Systems Insight Manager. If you are not using Systems Insight Manager, consider using the HPQLOMIG utility.

📝 **IMPORTANT:** Installing directory support for any management processor requires downloading the HP Smart Component. Refer to the "Pre-migration checklist (on page 113)" and the "HP Lights-Out directory package" sections for additional information. Extending the schema must be completed by a Schema Administrator.

HPQLOMIG requires logon and upgrade firmware privileges for each management processor. Change directory setting privileges are required for directory services.

Finding management processors

The first step to migrating is discovering all the management processors you want directory services enabled. You can search for management processors using DNS names, IP addresses, or IP address wildcards. Address field variables must follow these rules:

- DNS names, IP addresses, and IP address wildcards must be delimited with a semicolon.
- The IP address wildcard uses the "*" character in the third and fourth octet fields. For example, IP address 16.100.*.* is valid, whereas IP address 16.*.*.* is not.
- Ranges can 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**, HPQLOMIG begins pinging and connecting to port 443 (the default SSL port). The purpose of these actions is to quickly determine if the target network address is a management processor. If the device does not respond to the ping or connect appropriately on port 443, then it is determined not to be a management processor.

If you click **Next**, or **Back**, or exit the application during discovery, operations on the current network address are completed, but those on subsequent network addresses are canceled.

To start the process of discovering your management processors:

1.   Click **Start** and select **Programs>Hewlett-Packard, Lights-Out Migration Utility**.
2.   Click **Next** to move past the Welcome page.
3.   Enter the address or address range you want to search for management processors in the Addresses field.
4.   Enter your login name and password. Click **Find** or click **Import** to use a file. When the search is complete, the Find button changes to Verify.

     When using a file to enter a list of management processors, the file must be a simple text file with one management processor listed per line using semicolon delimited fields. The fields are delimited in the following order:

     - Network Address
     - Management Processor Type
     - Firmware Version
     - DNS Name
     - User Name
     - Password
     - Directory Configuration

     For example, one line could have:

     `16.100.225.20;RILOEII;1.20;RILOE2DB;user;password;Default Schema`

     If for security reasons, you cannot store the user name and password in the file, leave these fields empty and delimitated with semicolons.

After the discovery process is complete, you can click **Verify** to verify the displayed list of management processors or click **Next** to continue.

Upgrading firmware on management processors

The Upgrade Firmware page displays after you have completed the discovery p enables you to update the management processors to the firmware version that supports directories or designate the location of the firmware image for each management processor by either entering the path or clicking **Browse.**

IMPORTANT: Binary images of the firmware for the management processors are required to be accessible from the system that is running the migration utility. These binary images can be downloaded from the HP website (http://www.hp.com/servers/lights-out).

Management processor	Minimum firmware version
RILOE	2.50
RILOE II	1.10
iLO	1.40
iLO 2	1.00

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 five minutes to complete. If an upgrade fails, a message appears in the Results column and HPQLOMIG continues to upgrade the other discovered management processors.

IMPORTANT: HP recommends testing the upgrade process and verifying 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 could result in having to locally reprogram the management processor using a floppy diskette.

To upgrade the firmware on your management processors:

1. Select the management processors to be upgraded.

2. For each discovered management processor type, enter the correct pathname to the firmware image or browse to the image.

3. Click **Upgrade Firmware.** The selected management processors are upgraded. Although the migration utility enables you to upgrade hundreds of management processors, only 25 management processors are upgraded simultaneously. Network activity is considerable during the upgrade process.

   During the firmware upgrade process, all buttons are deactivated to prevent navigation. You can still close the application using the X option located at the top right of the page. If the GUI is closed while programming firmware, the application continues to run in the background and completes the firmware upgrade on all selected devices.

4. After the upgrade is completed, click **Next.**
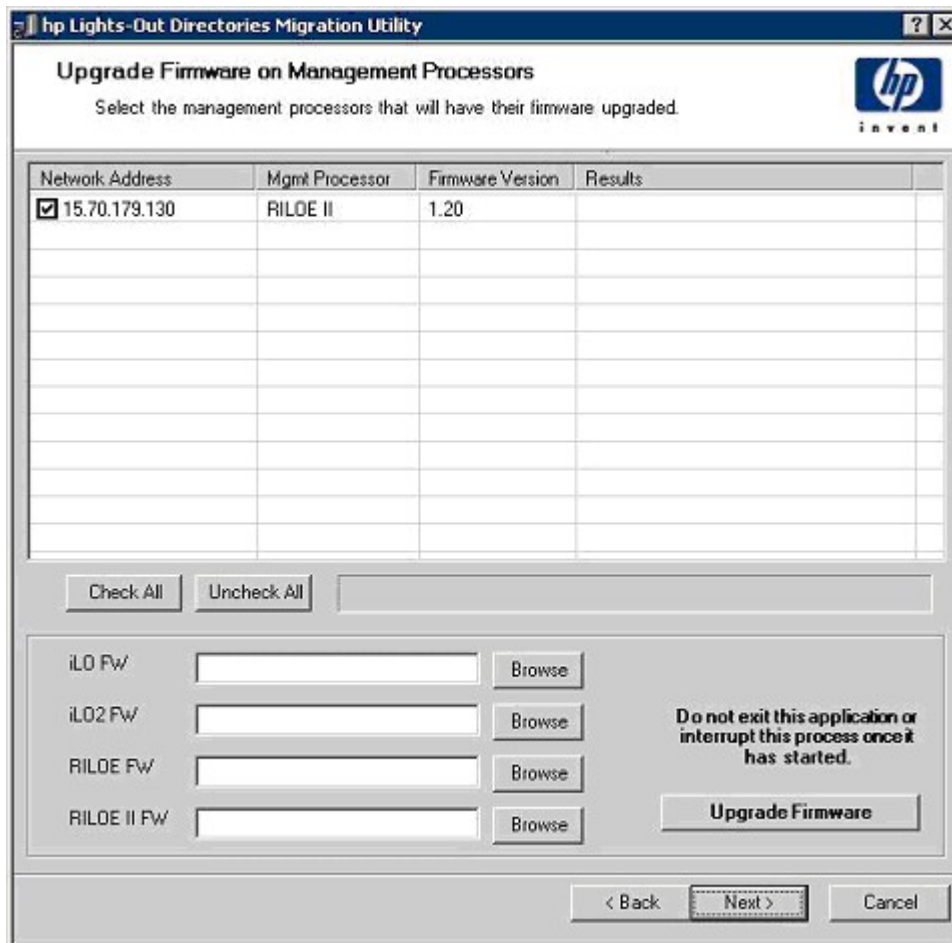
Selecting a directory access method

After completing the firmware upgrade process, the Select Directory Access Method page appears. You can select which management processors to configure (with respect to schema usage) and how they will be configured. The Select Directory Access Method page helps to prevent an accidental overwrite of RILOE IIs already configured for HP schema or those that have directories turned off.

The Select Directory Access Method page determines if the HP Extended schema, schema-free (default schema), or no directories support configuration pages follow.

To configure the management processor for:

- Directory services, See the "Configuring directories when HP Extended schema is selected (on page 119)" section.
- Schema-free (default schema) directories support, See the "Setup for Schema-free directory integration (on page 77)" section.

Naming management processors

The Name the management processors page enables you to name Lights-Out management device objects in the directory and create corresponding device objects for all management processors to be managed. You can create names using one or more of the following:

- The network address
- The DNS name
- An index
- A name (entered manually)
- A prepend prefix to all
- An append suffix to all

To name the management processors, select the **Name** option and enter the name, or use the following procedure:

1. Select **Use Network Address**, **Use DNS Names**, or **Create Name Using Index.** You can also name each management processor directory object manually by clicking twice in the Name check box with a short delay between clicks.

2. If you want to prepend or append the same identifying text to the name of the management processors, enter text in the Prefix or Suffix fields as required. The Prefix and Suffix options are useful in naming groups of related management processors.

3. Click **Generate Names.** The names display in the Name column as they are generated. Names are stored and not written to the directory or the management processors until the next step of the migration process.

4. To change the names, click **Clear All Names** and rename the management processors.

5. After the names are correct, click **Next.**

Configuring directories when HP Extended schema is selected

The Configure Directory page appears after clicking **Next** on the Name the management processors page. The Configure Directory page enables you to create a device object for each discovered management processor and to associate the new device object to 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 (such as a RILOE II).

The fields in the Configure Directory page are:

- Network Address is the network address of the directory server and can either be a valid DNS name or IP address.

- Port is the SSL port to the directory. The default entry is 636. Management processors can only communicate with the directory only by using SSL.
- Login Name and Password fields are used to log in with an account that has domain administrator access to the directory.
- Container DN is location of all the management processor objects in the directory created by the migration utility. After you have the network address, port, and login information, you can click **Browse** to navigate for the container and role distinguished name.
- Role DN is the location of the role you want associated with the device objects. The role must be created before running the configuration utility.

To configure device objects and associate the object 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 field, or click **Browse.**
3. Associate device objects with a member of a role by entering the role distinguished name in the Role DN field, or click **Browse.**
4. Click **Update Directory**. The configuration utility connects to the directory, creates the management processor objects, and adds them to the selected roles.
5. After the device objects are associated with a role, click **Next.**

Configuring directories when schema-free integration is selected

The Configure Management Processors page appears after selecting to use the directory's default schema and clicking **Next** on the Select Directory Access Method page. The Configure Management Processors page allows you to configure:

- **Network Address** is the network address of the directory server. The address is either a valid DNS name or IP address.

- **Login Name** and **Password** fields are used to log in with an account that has domain administrator access to the directory.

- **Security Group Distinguished Name** is the distinguished name of the group in the directory containing a set of RILOE II 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** are RILOE II 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 and not saved or written to the directory until the next page appears.

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 page enables you to create user contexts.

User contexts enable the user to use short or user object names, rather than the full distinguished name, to log in. For example, having a user context such as CN=Users,DC=RILOETEST2,DC=HP enables user John

Smith to log in using John Smith, rather than CN=John Smith,CN=Users, DC=RILOETEST2,DC=HP. The @ format is also supported. For example, @RILOETEST2.HP in a context field enables the user to log in using jsmith (assuming that jsmith is the user's short name).

To configure the management processors to communicate with the directory:

1. Enter the user contexts, or click **Browse.**

2. For Directories Support and Local Accounts option, select **Enabled** or **Disabled.**

   Remote access is disabled if both Directory Support and Local Accounts are disabled. To reestablish access, reboot the server and use RBSU F8 to restore access.

3. Click **Configure**. The migration utility connects to all of the selected management processors and updates their configuration as you have specified.

4. When the process is complete, click **Done.**

📝 **NOTE:** The feature associated with the Management Processor Password field is not available at this time. This field is provided for forward compatibility with future releases.
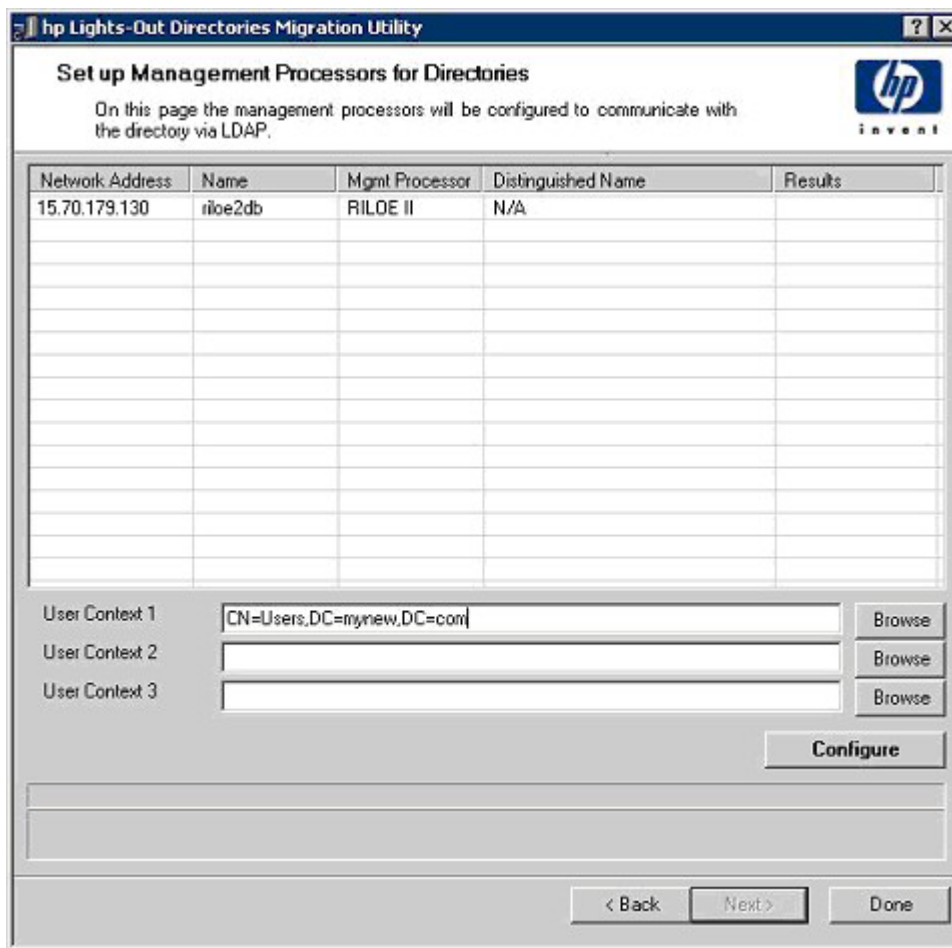
HPQLOMGC operation

The command line utility is intended to be used in conjunction with Systems Insight Manager. If you are not using Systems Insight Manager, consider using the HPQLOMIG utility. The command line mode does not present a GUI and runs unattended. This mode is intended to work in conjunction with the Application launch ("Application Launch using Systems Insight Manager" on page 127) functionality.

IMPORTANT: Installing directory support for any management processor requires downloading the HP Smart Component. Refer to the "Pre-migration checklist (on page 113)" and the "HP Lights-Out directory package" sections for additional information. Extending the schema must be completed by a Schema Administrator.

To implement directory support on a few management processors.

1. Use Systems Insight Manager to locate all of the management processors in the network.
2. Execute the HPQLOMGC utility.
3. Invoke the XML file to migrate the management processor.

HPQLOMGC goes through three phases to complete the migration of a management processor.

1. **The firmware version is validated and updated if necessary.**

   HPQLOMGC determines the type of management processor and the firmware level. If the firmware does not meet the minimum requirement ("Upgrading firmware on management processors" on page 116), HPQLOMGC upgrades the firmware and resets the management processor. After the management processor resets, HPQLOMGC begins the next phase.

2. **The management processor directory settings are updated.**

   HPQLOMGC uses the scripting interface to send the directory settings to the management processor.

3. **The directory is updated.**

   HPQLOMGC creates a device object in the directory at the location specified by the user. HPQLOMGC uses either the object name specified in the XML file or the network name of the management processor. After the device object is created, the specified role object is then amended to include the newly created device object.

Launching HPQLOMGC using application launch

Application Launch can be used to create tasks associated with administration of management processors. For example, the management processors can be discovered using Application Launch and could be used to automatically configure new management processors as they are added to the network.

To create an Application Launch task:

1. Click **Device** in the navigation bar on the top left side of the screen.
2. Click **Tasks** to open the Tasks screen.
3. Click **New Control Task.** A dropdown menu is displayed.
4. Click **Application Launch** from the dropdown menu to open the Create/Edit Task screen.
5. Enter the full path and name for the Lights-Out Migration Command Line Utility in the area provided. For example, if the HPQLOMGC.exe file is in the root directory of the C drive, then the path is: C:\HPQLOMGC.exe.
6. Enter the parameters in the area provided.

   Command line switches enable you to designate items such as the management processor to be upgraded, the XML file to be used, and where a log file is generated.

   -S <network address>—This switch contains the IP address or DNS name of the management processor. By default, the IP address of the management processor is automatically provided. The environment variable <DEVICEIPADDRESS0> can also be used to specify a network address.

   Use the -S switch to override the default behavior. If present, this switch has precedence over the IP address environment variable <DEVICEIPADDRESS0>.

   -F <filename>—This switch contains the path of the XML file that has the management processor directory settings and the location of the firmware images. This switch causes an error if an IP address is not designated.

   -A—This switch uses the network name for the name of the device object created in the directory.

-V—This switch is optional and sets the HPQLOMGC to Verbose mode.

-L <filename>—This switch defines where the log file is generated. This switch causes an error if an IP address is not designated.

-Q—This switch is optional and sets the HPQLOMGC to Quiet mode.

7. Click **Next.** A screen is displayed with options for naming the task, defining the query association, and setting a schedule for the task.

8. Enter a task name in the Enter a name for this task field.

9. Select the query that had been created earlier, for example "Mgmt Processors."

10. Click **Schedule** to define when the Application Launch task will run. A schedule configuration window is displayed.

11. Click **OK** to set the schedule.

NOTE: The default schedule for a control task is **Now.**

12. Click **Finish** to save the Application Launch task.

13. Click the **Execute a Task** icon (the green triangle) to execute the Group Administration.

HPQLOMGC command language

When using HPQLOMGC, the directory settings for the management processor are read from an XML file. The script used is a subset of the RIBCL and has been extended to support multiple management processor firmware images. For more information concerning RIBCL for your management processor, refer to the RILOE, RILOE II, or iLO user guide.

The following is an example of an XML file:

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="user" PASSWORD="password">
<DIR_INFO MODE="write">
<ILO_CONFIG>

   <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\fw\ilo140.brk" />
</ILO_CONFIG>
<RILOE_CONFIG>

   <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\fw\riloe.brk" />
</RILOE_CONFIG>
<RILOE2_CONFIG>

   <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\fw\riloeii.brk" />
</RILOE2_CONFIG>
<MOD_DIR_CONFIG>

   <DIR_AUTHENTICATION_ENABLED value="YES" />

   <DIR_LOCAL_USER_ACCT value="YES" />

   <DIR_SERVER_ADDRESS value="administration.wins.hp.com" />

   <DIR_SERVER_PORT value="636" />

   <DIR_OBJECT_DN value="CN=RILOP5,CN=Users,DC=RILOEGRP2,DC=HP" />

   <DIR_OBJECT_PASSWORD value="aurora" />

   <DIR_USER_CONTEXT_1 value="CN=Users,DC=RILOEGRP2,DC=HP" />

   <DIR_USER_CONTEXT_2 value="" />

   <DIR_USER_CONTEXT_3 value="" />

   <DIR_ROLE value="CN=RILOEROLE,CN=Users,DC=RILOEGRP2,DC=HP" />

   <DIR_LOGIN_NAME value="RILOEGRP2\Adminl" />
```

```
            <DIR_LOGIN_PASSWORD value="aurora" />
        </MOD_DIR_CONFIG>
        </DIR_INFO>
    </LOGIN>
    </RIBCL>
```

RILOE2_CONFIG

RIBCL allows for only one firmware image per XML file. The command language for HPQLOMGC has been modified to allow for each management processor to have a specified firmware image within a single XML file. These commands must be displayed within a DIR_INFO block, and DIR_INFO must be in write mode. The management processor is reset after the firmware upgrade is complete. To update the firmware, the user must be logged in with the appropriate privilege.

This command line uses the following parameters:

- UPDATE_RIB_FIRMWARE IMAGE_LOCATION ("UPDATE_RIB_FIRMWARE parameters" on page 157)

- MOD_DIR_CONFIG

Lights-Out Configuration Utility

The Lights-Out Configuration Utility (CPQLOCFG.EXE) is a Microsoft® Windows®-based utility that connects to RILOE II using a secure connection over the network. RIBCL scripts are passed to RILOE II over the secure connection to CPQLOCFG. The Lights-Out Configuration Utility requires a valid user ID and password with the appropriate privileges. The CPQLOCFG utility can be launched from Systems Insight Manager for Group Administration or used independently from a command prompt for batch processing. You can download CPQLOFG.EXE from the HP website (http://h18004.www1.hp.com/support/files/lights-out/us/index.html).

Systems Insight Manager discovers RILOE II devices as management processors. The Lights-Out Configuration Utility sends a RIBCL file to a group of RILOE IIs to manage user accounts for those RILOE IIs. RILOE IIs then perform the action designated by the RIBCL file and send a response to the log file.

The Lights-Out Configuration Utility is used to execute RIBCL scripts on RILOE II and must reside on the same server as Systems Insight Manager. The Lights-Out Configuration Utility generates two types of error messages: runtime and syntax.

- Runtime errors occur when an invalid action is requested. Runtime errors are logged to the C:\PROGRAM FILES\INSIGHT MANAGER\HP\SYSTEMS directory.

- Syntax errors occur when an invalid XML tag is encountered. When a syntax error occurs, the Lights-Out Configuration Utility stops running and logs the error in the runtime script and output log file.

    Syntax errors take the format of `Syntax error: expected` X `but found` Y. For example: `Syntax error: expected USER_LOGIN=userlogin` but found `USER_NAME=username`.

See to the RIBCL section ("Remote Insight command language" on page 138) for a complete listing of errors.

Group administration using the Lights-Out Configuration Utility

The IT administrator can manage multiple RILOE IIs through Systems Insight Manager. The components of Group Administration are:

- RIBCL ("Remote Insight command language" on page 138)

- Lights-Out Configuration Utility (on page 125)

- Creating a Customized List ("Create a customized list" on page 126)

- Creating a Custom Command ("Create a custom command" on page 126)
- Creating a Task ("Create a task" on page 126)

Create a customized list

A customized list allows you to create a list of a group of management processors and run a task on that list. To create a customized list:

1. In the Systems List pane in the left window, click **Customize.**
2. In the Customize Lists window, select System List using the Show dropdown menu and click **New List.**
3. Select the search parameters using the **Search for** and **where** dropdown menus. Click **Go.**
4. When the systems display, click **Save As.**
5. Enter a name for your list and where it is to be saved.
6. Click **OK.**

Create a custom command

To create a custom command:

1. Click **Tools>Custom Commands>New Custom Command.**
2. In the New Custom Command screen, enter the appropriate information in the **Name, Description,** and **Comments** fields.
3. In the Command field, be sure to enter the full path and the file name of the application. If the CPQLOCFG.EXE file is in the root directory of the C:\ drive, then the path is C:\cpqlocfg.exe.
4. Enter the Parameters.
5. Enter the Variable Name and Value. Click Add after entering each set of variables and values. To clear an added variable, select the variable, and click **Delete.**
6. After entering the Custom Command information, click **OK.** The new tool is added to the dropdown menu Tools>Custom Commands.

Create a task

Create a task to execute a custom command on specific systems or events.

1. Select the custom command from the Tools>Custom Commands dropdown menu. The Target Selection page is displayed.
2. Choose targets by selecting either:
   - **All systems in the list**—Selecting an option in the drop-down menu automatically targets all systems in that list.
   - **Individual systems in the list**—Selecting an option in the drop-down menu displays the available systems for the selected list. Select the target system.
3. Click **Apply Selections.** The items selected display in the Verify Target Systems page.

   If the systems selected are not compatible with the tool, the Tool Launch OK column provides a brief explanation of the problem. To change the selected target list click **Change Targets.** If you want to remove the system selected, click **Remove** and you will return to the Select Target Systems page.
4. Click **Next** to specify the tool parameters.

   The Next option displays only if the tool parameters need to be specified.
5. Click either **Schedule** or **Run Now.**
   - If you click **Schedule,** the schedule task screen appears. Schedule the task. For more information on the scheduling options, see the HP Systems Insight Manager documentation.

The Schedule option is available only if the tool can be scheduled.

- If you click **Run Now,** the Task Results screen appears with a summary of the task, the target details, and the status.

Query definition in Systems Insight Manager

To group all of the RILOE II devices, log in to Systems Insight Manager and create a query.

To create the query:

1. Log in to Systems Insight Manager.
2. Click **Device** in the navigation bar on the top left side of the screen.
3. Click **Queries**>**Device.**
4. Locate the Personal Queries section in the main window. If a query category exists, proceed to step 7, otherwise proceed to step 5.
5. Click **New** to create a new category. For this example, the name of the new category is RIB Cards. Click **Create Category.**
6. Click **Queries** to return to the Device Queries screen.
7. Click **New,** within the appropriate query category, to open the Create/Edit Query screen where the query definition is created.
8. Define the query name, for example "Mgmt Processors."
9. Select **Device(s) of type,** and then select **Devices by product name.** In the criteria windows, set the product name to **Remote Insight Lights-Out Edition II.**
10. Click **type** in the Query Description field. A window opens where you define the device type.
11. Select **Management Processor** and click **OK.**
12. Click **Save** to return to the Device Query screen.
13. Find the newly created query in the appropriate query category, and click the query name to run it for verification.
14. Click **Overview** on the left side of the screen after the verification has taken place. The initial page for devices opens.

Application Launch using Systems Insight Manager

The Application Launch combines the RIBCL, the Lights-Out Configuration Utility, and the query definition to manage the Group Administration of the RILOE IIs.

To create an Application Launch task:

1. Click **Device** in the navigation bar on the top left side of the screen.
2. Click **Tasks** to open the Tasks screen.
3. Click **New Control Task** and select **Application Launch** from the dropdown menu to open the Create/Edit Task screen.
4. Enter the full path and name for the Lights-Out Configuration Utility in the area provided. If the CPQLOCFG.EXE file is in the root directory of the C:\ drive, then the path is C:\cpqlocfg.exe.
5. Enter the parameters in the area provided. Systems Insight Manager requires the following parameters for the Lights-Out Configuration Utility:

   -F is the full path of the RIBCL file name.

   -V is the verbose message (optional).

   If the RIBCL file is in the root directory of on the C:\ drive, then the parameters are:
   ```
   -F C:\MANAGEUSERS.xml -V
   ```

NOTE: The -L parameter cannot designate an output log file. A default log file named with the DNS name or the IP address is created in the same directory where CPQLOCFG is launched.

6. Click **Next.** A screen displays the options for naming the task, defining the query association, and setting a schedule for the task.

7. Enter a task name in the Enter a name for this task field.

8. Select the query that had been created earlier, for example "Mgmt Processors."

9. Click **Schedule** to define when the Application Launch task will run. A schedule configuration window appears.

10. Click **OK** to set the schedule.

NOTE: The default schedule for a control task is **Now.**

11. Click **Finish** to save the Application Launch task.

12. Click the **Execute a Task** icon (the green triangle) to execute the Group Administration.

Batch processing using the Lights-Out Configuration Utility

Group Administration can also be delivered to RILOE II through batch processing. The components used by batch processing are the Lights-Out Configuration Utility, an RIBCL file, and a batch file.

The following example shows a sample batch file that can be used to perform the Group Administration for RILOE II:

```
REM Updating the Remote Insight Lights-Out Edition II board
REM Repeat line for each board to be updated
REM
CPQLOCFG -S RIB1 -F C:\...SCRIPT.XML -L RIB1LOG.TXT -V
CPQLOCFG -S RIB2 -F C:\...SCRIPT.XML -L RIB2LOG.TXT -V
CPQLOCFG -S RIB3 -F C:\...SCRIPT.XML -L RIB3LOG.TXT -V
.
.
.
RIBNLOG -S RIBN -F C:\...SCRIPT.XML -L LOGFILE.TXT -V
```

The Lights-Out Configuration Utility overwrites any existing log files.

Lights-Out Configuration Utility parameters

- -S is the switch that determines the RILOE II that is to be updated. This switch is either the DNS name or IP address of the target server.

  Do **not** use this switch if you are launching from Systems Insight Manager. Systems Insight Manager will provide the address of the RILOE II when CPQLOCFG.EXE is launched.

- -F is the switch that gives the full path location and name of the RIBCL file that contains the actions to be performed on the board.

- -U and -P specify the user login name and password. These options allow the login information within the script file to be overridden and allows the login information to be left out of the script.

Be sure that the Lights-Out Configuration Utility is in a directory referenced by the PATH environment variable. Any log files generated are placed in the same directory as the Lights-Out Configuration Utility executable

The switches -L and -V might or might not be set depending on the IT administrator's preferences.

- -L is the switch that defines where the log file will be generated and what the file name will be. If this switch is omitted, a default log file with the DNS name or the IP address is created in the same directory used to launch CPQLOCFG.

Scripting, command line, and utility options 128

Do **not** use this switch if launching from Systems Insight Manager.

📝 **NOTE:** The output values might need to be modified to match the RIBCL syntax.

📝 **NOTE:** The -L parameter cannot designate an output log file. A default log file named with the DNS name or the IP address is created in the same directory where CPQLOCFG is launched.

- -V is the optional switch that turns on the verbose message return. The resulting log file contains all commands sent to the Remote Insight board, all responses from the Remote Insight board, and any errors. By default, only errors and responses from GET commands are logged without this switch.

See the "Remote Insight Command Language (on page 138)" section for information on the syntax of the XML data files. Sample XML scripts are available on the HP website (http://www.hp.com/servers/lights-out) in the Best Practices section.

Using Perl with the XML scripting interface

The scripting interface provided enables administrators to manage virtually every aspect of the device in an automated fashion. Primarily, administrators use tools like the `cpqlocfg.exe` to assist deployment efforts. Administrators using a non-Windows® client can use Perl scripts to send XML scripts to the Lights-Out devices. Administrators can also use Perl to perform more complex tasks than `cpqlocfg.exe` can perform.

This section discusses how to use Perl scripting in conjunction with the Lights-Out XML scripting language. Perl scripts require a valid user ID and password with appropriate privileges. Sample XML scripts for Lights-Out devices and a sample Perl script are available on the HP website (http://www.hp.com/servers/lights-out) in the Best Practices section.

XML enhancements

Previous versions of RILOE II firmware do not return properly formatted XML syntax. If the RILOE II firmware determines the client utility being used does not support the return of properly formatted XML syntax, the following message appears:

```
<INFORM>Scripting utility should be updated to the latest
version.</INFORM>
```

This message informs the customer to update to a later version of the cpqlocfg scripting utility. The latest version of cpqlocfg.exe is currently 2.21.

For customers using a utility other than cpqlocfg.exe, such as Perl scripts, the following steps can help ensure the RILOE II firmware returns properly formatted XML. Assuming the version of firmware is 1.20, `<LOCFG version="2.21">` should be incorporated into the script sent to RILOE II. This tag can be placed in either the Perl script or the XML script. Placement of this tag is important. If placing this tag in the Perl script, the tag should be sent after `<?xml version="1.0"?>` and before the XML script is sent. If placing the tag in the XML script, the tag should be placed before `<RIBCL version="2.0">`. If you are using the Perl script provided by HP, then the bold line in the following example can be added to return properly formatted XML syntax.

- Perl script modification

```
…
# Open the SSL connection and the input file
my $client = new IO::Socket::SSL->new(PeerAddr => $host);
open(F, "<$file") || die "Can't open $file\n";

# Send the XML header and begin processing the file
print $client '<?xml version="1.0"?>' . "\r\n";
#Send tag to RILOE II firmware to insure properly formatted XML is
returned.
```

```
print $client '<LOCFG version="2.21">' . "\r\n";
…
```

- XML script modification

```
<!--
The bold line could be added for the return of properly formatted XML.
-->
<LOCFG version="2.21"/>
<RIBCL version="2.0">
    <LOGIN USER_LOGIN="Adminname" PASSWORD = "password">
        <!--
        Add XML script here.
        -->
    </LOGIN>
</RIBCL>
</LOCFG>
```

Opening an SSL connection

Perl scripts must open an SSL connection to the device's HTTPS port, by default port 443. For example:

```
use Socket;
use Net::SSLeay qw(die_now die_if_ssl_error);

Net::SSLeay::load_error_strings();
Net::SSLeay::SSLeay_add_ssl_algorithms();
Net::SSLeay::randomize();

#
# opens an ssl connection to port 443 of the passed host
#
sub openSSLconnection($)
{
    my $host = shift;
    my ($ctx, $ssl, $sin, $ip, $nip);

    if (not $ip = inet_aton($host))
    {
        print "$host is a DNS Name, performing lookup\n" if $debug;
        $ip = gethostbyname($host) or die "ERROR: Host $hostname not
        found.\n";
    }
    $nip = inet_ntoa($ip);
    print STDERR "Connecting to $nip:443\n";

    $sin = sockaddr_in(443, $ip);
    socket  (S, &AF_INET, &SOCK_STREAM, 0) or die "ERROR: socket: $!";
    connect (S, $sin) or die "connect: $!";
```

```
$ctx = Net::SSLeay::CTX_new() or die_now("ERROR: Failed to create
SSL_CTX $! ");

Net::SSLeay::CTX_set_options($ctx, &Net::SSLeay::OP_ALL);

die_if_ssl_error("ERROR: ssl ctx set options");

$ssl = Net::SSLeay::new($ctx) or die_now("ERROR: Failed to create SSL
$!");

Net::SSLeay::set_fd($ssl, fileno(S));

Net::SSLeay::connect($ssl) and die_if_ssl_error("ERROR: ssl connect");

print STDERR 'SSL Connected ';

print 'Using Cipher: ' . Net::SSLeay::get_cipher($ssl) if $debug;

print STDERR "\n\n";


return $ssl;
}
```

Sending the XML header and script body

After the connection is established, the first line of script sent must be an XML document header, which tells the device's HTTPS Web server that the following content is an XML script. The header must match the header used in the example exactly. After the header has been completely sent, the remainder of the script can be sent. In this example, the script is sent all at once. For example:

```
# usage: sendscript(host, script)
# sends the xmlscript script to host, returns reply
sub sendscript($$)
{
   my $host = shift;

   my $script = shift;

   my ($ssl, $reply, $lastreply, $res, $n);


   $ssl = openSSLconnection($host);


   # write header
   $n = Net::SSLeay::ssl_write_all($ssl, '<?xml version="1.0"?>'."\r\n");
    rint "Wrote $n\n" if $debug;


   # write script
   $n = Net::SSLeay::ssl_write_all($ssl, $script);

   print "Wrote $n\n$script\n" if $debug;


   $reply = "";

   $lastreply = "";


   READLOOP:

   while(1)

   {
```

```perl
        $n++;
        $reply .= $lastreply;
        $lastreply = Net::SSLeay::read($ssl);
        die_if_ssl_error("ERROR: ssl read");
        if($lastreply eq "")
        {
        sleep(2); # wait 2 sec for more text.
        $lastreply = Net::SSLeay::read($ssl);
last READLOOP if($lastreply eq "");
        }
        sleep(2); # wait 2 sec for more text.
        $lastreply = Net::SSLeay::read($ssl);
        last READLOOP if($lastreply eq "");
        }
        print "READ: $lastreply\n" if $debug;
        if($lastreply =~ m/STATUS="(0x[0-9A-F]+)"[\s]+MESSAGE=
        '(.*)'[\s]+\/>[\s]*(([\s]|.)*?)<\/RIBCL>/)
        {
        if($1 eq "0x0000")
        {
        print STDERR "$3\n" if $3;
        }
        else
        {
        print STDERR "ERROR: STATUS: $1, MESSAGE: $2\n";
        }
        }
    }
    $reply .= $lastreply;
    closeSSLconnection($ssl);
    return $reply;
}
```

PERL scripts can also send a portion of the XML script, wait for the reply, and send more XML later. Using this technique, it is possible to use the reply produced by an earlier command as input to a later command. However, the PERL script must send data within a few seconds or the device will time out and disconnect.

When using the XML scripting interface with PERL scripts, the following restrictions apply:

- PERL scripts must send the XML header before sending the body of the script.
- PERL scripts must provide script data fast enough to prevent the device from timing out.
- XML scripts cannot contain the update firmware command, which requires extra work on the part of the PERL script to open the file containing the firmware image and send it to the device.
- Only one XML document is allowed per connection, which means one pair of RIBCL tags.

- The device will not accept additional XML tags after a syntax error occurs. To send additional XML, a new connection must be established.

HPONCFG

The HPONCFG utility is an online configuration tool used to set up and configure the iLO management processor and RILOE II from within the Windows® and Linux operating systems without requiring a reboot of the server operating system. The utility runs in a command line mode and must be executed from an operating system command line using an account with administrator or root access.

HPONCFG supported operating systems

HPONCFG is supported on:
- Windows® 2000 Server
- Windows® 2003 Server
- Red Hat Linux Enterprise Linux 2.1
- Red Hat Linux Enterprise Linux 3.0
- United Linux 1.0/SUSE LINUX Enterprise Server 8

HPONCFG requirements

- iLO management processor-based server

  For an iLO management processor-based server, the server must have the RILOE II Management Interface Driver loaded. The SmartStart operating system install process normally installs this driver. During execution, HPONCFG will warn if it cannot find the driver. If the driver is not installed, it must be downloaded and installed on the server: You can download the driver from the HP website (http://h18023.www1.hp.com/support/files/lights-out/us/locate/20_5867.html#0).

  For iLO management processor-based servers, HPONCFG requires iLO management processor firmware version 1.41 or later.

- RILOE II-based server

  For RILOE II-based servers, the server must have the RILOE II Management Interface Driver loaded. During execution, HPONCFG will warn if it cannot find the driver. If the driver is not installed, it must be downloaded and installed on the server. You can download the driver from the HP website (http://h18023.www1.hp.com/support/files/lights-out/us/locate/20_5868.html).

  For RILOE II-based servers, HPONCFG requires RILOE II firmware version 1.13 or later. For a server Windows® 2000/Windows® 2003, it requires RILOE II Management Interface Driver version 3.2.1.0 or later.

- All servers

  For both iLO management processor-based servers and RILOE II-based servers, the server must have sm2user.dll loaded. This file is automatically loaded along with the HP Insight Management Agents. During execution, HPONCFG will warn if it cannot find the sm2user.dll file. This file can be installed separately from the component HP Insight Management Agents for Windows® 2000/Windows® Server 2003, that can be downloaded as a part of the ProLiant Support Pack on the HP website (http://h18004.www1.hp.com/support/files/server/us/download/18416.html).

  After downloading the ProLiant Support Pack, extract its contents to a temporary directory. In the temporary directory, locate CP004791.exe. Extract the contents of this component to a temporary directory. In the temporary directory, locate the subdirectory cqmgserv. The sm2user.dll file can be found in this subdirectory. Copy the sm2user.dll file to the following directory on the server: `Winnt\system32\`

Installing HPONCFG

The HPONCFG utility is delivered in separate packages for Windows® and Linux systems. For Windows® systems, it is delivered as a smart component. For Linux systems, it is delivered as an RPM package file. HPONCFG 1.1 is part of SmartStart 7.30.

Windows server installation

HPONCFG will be installed automatically when ProLiant support pack version 7.30 is installed. The individual HPONCFG 1.1 component cp005299.exe can be downloaded from the HP website (http://h18023.www1.hp.com/support/files/lights-out/us/download/22571.html).

To install HPONCFG, run the self-extracting executable delivered in this package from within a directory of your choice on the managed server. This will be the directory from which the HPONCFG utility is executed. This directory will also contain the XML formatted input scripts, and will store the output files from execution of the utility. Be sure that the appropriate Management Interface Driver is installed. The sm2user.dll file must also be installed. Refer to the "HPONCFG requirements (on page 133)" for details on where to obtain this driver and file.

Linux server installation

HPONCFG will be installed automatically when ProLiant support pack version 7.30 is installed. The rpm of HPONCFG 1.1 for the respective Linux distributions can be downloaded from the HP website (http://h18023.www1.hp.com/support/files/lights-out/us/).

The following is a list of HPONCFG RPMs and the Linux distributions they support:

RPM supported	Distributions
hponcfg-1.1.0-5.rhel21.i386.rpm	Red Hat Enterprise Linux 2.1
hponcfg-1.1.0-5.rhel3.i386.rpm	Red Hat Enterprise Linux 3.0
hponcfg-1.1.0-5.sles8.i386.rpm	SUSE Linux Enterprise Server 8 / United Linux 1.0

Install the appropriate package using the RPM installation utility. As an example for package installation, hponcfg RPM on Red Hat Enterprise Linux 3.0 can be installed by:

```
rpm -ivh hponcfg-1.1.0-5.rhel3.i386.rpm
```

If an older version of hponcfg RPM package is already installed on the system, run the following command to remove the older version before installing the new version of HPONCFG:

```
rpm –e hponcfg
```

The hprsm RPM package must be installed on the system before installing the hponcfg RPM package.

After installation, the HPONCFG executable can be found in the /sbin directory. Be sure that the appropriate Management Interface Driver is installed. Refer to the "HPONCFG requirements (on page 133)" for details on where to obtain this driver and file.

Using HPONCFG

The HPONCFG configuration utility reads an XML input file, formatted according to the rules of the RIBCL language, and produces a log file containing the requested output. A few sample scripts are included in the HPONCFG delivery package. A package containing various and comprehensive sample scripts is available for download on the HP website (http://h18004.www1.hp.com/support/files/lights-out/us/download/20110.html).

Typical usage is to select a script that is similar to the desired functionality and modify it for the exact desired functionality. Note that, although no authentication to the iLO management processor or the RILOE II is required, the XML syntax requires that the USER_LOGIN and PASSWORD tags be present in the LOGIN tag, and that these fields contain data. Any data will be accepted in these fields. To successfully execute HPONCFG, the utility must be invoked as `Administrator` on Windows® servers and as `root` on Linux servers. An error message will be returned by HPONCFG if the user does not possess sufficient privileges.

Using HPONCFG on Linux servers

Invoke the HPONCFG configuration utility from the command line. HPONCFG displays a usage page if it is entered with no command line parameters.

HPONCFG accepts as input an XML script formatted according to the rules of RIBCL (documented in the user guide in the section describing the use of CPQLOCFG).

The command line format is:

```
hponcfg  -?
hponcfg  -h
hponcfg  -m minFw
hponcfg  -r  [-m minFw ]
hponcfg  -w filename  [-m minFw]
hponcfg  -g  [-m minFw]
hponcfg  -f filename [-l filename] [-v]  [-m minFw]
```

See the "HPONCFG command line parameters (on page 135)" section for an explanation of the usage.

HPONCFG command line parameters

HPONCFG accepts the following command line parameters:

- /help or ?—Displays the help page.
- /reset—Resets the RILOE II or iLO management processor to factory default values.
- /f *<filename>*—Sets the RILOE II or iLO management processor configuration from the information given in the XML input file that has name "filename."
- /w <filename>—Writes the RILOE II or iLO management processor configuration obtained from the device to the XML output file that has name *filename*.
- /l *<filename>*—Log replies to the text log file that has name *filename*.
- /get_hostinfo—Gets the host information. Returns the server name and server serial number.
- /m—Indicates to HPONCFG the minimum firmware level that should be present in the management device to execute the RIBCL script. If at least this level of firmware is not present, HPONCFG returns an error without performing any additional action.
- /mouse—Tells HPONCFG to configure the server for optimized mouse handling, there by optimizing graphical remote console performance. By default it optimizes for remote console single cursor mode for the current user. The `dualcursor` command line option along with the `mouse` option will optimize mouse handling as suited for remote console dual cursor mode. The 'allusers' command line option will optimize the mouse handling for all the users on the system. This option is available only for Windows®.

The options must be preceded by a / (slash) for Windows® and - or - for Linux as specified in the usage string.

Example HPONCFG command line:

```
HPONCFG /f add_user.xml /l log.txt > output.txt
```

Scripting, command line, and utility options   135

Using HPONCFG on Windows servers

Start the HPONCFG configuration utility from the command line. When using Microsoft® Windows®, cmd.exe is available by selecting **Start>Run>cmd.** HPONCFG displays a usage page if HPONCFG is entered with no command line parameters. HPONCFG accepts a correctly formatted XML script. Refer to the "Remote Insight Command Language (on page 138)" section for more information on formatting XML scripts. HPONCFG sample scripts are included in the HPONCFG package.

The command line format is:

```
HPONCFG [ /help | /? | /m firmwarelevel | /reset [/m firmwarelevel]
    | /f filename [/l filename][/xmlverbose or /v][/m firmwarelevel]
    | /w filename [/m firmwarelevel]
    | /get_hostinfo [/m firmwarelevel]
    | /mouse [/dualcursor][/allusers]  ]
```

Refer to the "HPONCFG command line parameters (on page 135)" section for an explanation of the usage.

Obtaining an entire configuration

HPONCFG can be used to obtain an entire configuration from an iLO management processor or a RILOE II. In this case, the utility executes from the command line without specification of an input file. The name of the output file is given on the command line. For example:

```
HPONCFG /w config.xml
```

In this example, the utility indicated that it obtained the data successfully and wrote it to the output file as requested. The following is a typical example of the contents of the output file:

```
<HPONCFG VERSION = "1.1">
<!--- Generated 04/15/04 15:20:36 --->
<MOD_DIR_CONFIG>
<DIR_AUTHENTICATION_ENABLED VALUE = "N"/>
<DIR_LOCAL_USER_ACCT VALUE = "Y"/>
<DIR_SERVER_ADDRESS VALUE = ""/>
<DIR_SERVER_PORT VALUE = "25"/>
<DIR_OBJECT_DN VALUE = " "/>
<DIR_OBJECT_PASSWORD VALUE = ""/>
<DIR_USER_CONTEXT_1 VALUE = ""/>
<DIR_USER_CONTEXT_2 VALUE = "_"/>
<DIR_USER_CONTEXT_3 VALUE = ""/>
</MOD_DIR_CONFIG>
<MOD_NETWORK_SETTINGS>
<SPEED_AUTOSELECT VALUE = "Y"/>
<NIC_SPEED VALUE = "100"/>
<FULL_DUPLEX VALUE = "Y"/>
<IP_ADDRESS VALUE = "16.100.241.229"/>
<SUBNET_MASK VALUE = "255.255.252.0"/>
<GATEWAY_IP_ADDRESS VALUE = "16.100.240.1"/>
<DNS_NAME VALUE = "ILOD234KJ44D002"/>
<PRIM_DNS_SERVER value = "16.81.3.242"/>
<DHCP_ENABLE VALUE = "Y"/>
<DOMAIN_NAME VALUE = "americas.cpqcorp.net"/>
<DHCP_GATEWAY VALUE = "Y"/>
<DHCP_DNS_SERVER VALUE = "Y"/>
<DHCP_STATIC_ROUTE VALUE = "Y"/>
<DHCP_WINS_SERVER VALUE = "Y"/>
<REG_WINS_SERVER VALUE = "Y"/>
```

```
<PRIM_WINS_SERVER value = "16.81.3.247"/>
<STATIC_ROUTE_1 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
<STATIC_ROUTE_2 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
<STATIC_ROUTE_3 DEST = "0.0.0.0" GATEWAY = "0.0.0.0"/>
</MOD_NETWORK_SETTINGS>
<ADD_USER
USER_NAME = "Administrator"
USER_LOGIN = "Administrator"
PASSWORD = "">
</ADD_USER>
<ADD_USER
USER_NAME = "Landy9"
USER_LOGIN = "mandy9"
PASSWORD = "">
</ADD_USER>
<RESET_RIB VALUE = "Y"/>
</HPONCFG>
```

For security reasons, the user passwords are not returned.

Obtaining a specific configuration

A specific configuration can be obtained using the appropriate XML input file. For example, here are the contents of a typical XML input file, `get_global.xml`:

```
<!-- Sample file for Get Global command -->
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="x" PASSWORD="x">
<RIB_INFO MODE="read">
<GET_GLOBAL_SETTINGS />
</RIB_INFO>
</LOGIN>
</RIBCL>
```

The XML commands are read from the input file `get_global.xml` and are processed by the device:

```
HPONCFG /f get_global.xml /l log.txt > output.txt
```

The requested information is returned in the log file, which, in this example, is named `log.txt`. The contents of the log file are shown below.

```
<GET_GLOBAL_SETTINGS>

    <SESSION_TIMEOUT VALUE ="15"/>

    <F8_PROMPT_ENABLED VALUE ="YES"/>

    <HOST_KEYBOARD_ENABLED VALUE ="YES"/>

    <REMOTE_KEYBOARD_MODEL VALUE ="US"/>

    <REMOTE_CONSOLE_PORT_STATUS VALUE ="ENABLED"/>

    <PASSTHROUGH_CONFIG VALUE ="3"/>

    <SNMP_PASSTHROUGH_STATUS VALUE ="YES"/>

    <POCKETPC_ACCESS VALUE ="NO"/>

    <EMS_STATUS VALUE ="NO"/>

    <BYPASS_POWER_CABLE_REPORTING VALUE ="NO"/>

    <CIPHER_STRENGTH VALUE ="40"/>

    <HTTPS_PORT VALUE ="443"/>

    <HTTP_PORT VALUE ="80"/>
```

```
            <REMOTE_CONSOLE_PORT VALUE ="23"/>

            <TERMINAL_SERVICES_PORT VALUE ="3389"/>

            <SNMP_ADDRESS_1 VALUE ="1.1.5.5"/>

            <SNMP_ADDRESS_2 VALUE ="1.1.5.8"/>

            <SNMP_ADDRESS_3 VALUE ="1.1.5.7"/>

            <OS_TRAPS VALUE ="YES"/>

            <RIB_TRAPS VALUE ="YES"/>

            <CIM_SECURITY_MASK  VALUE ="NONE"/>
      </GET_GLOBAL_SETTINGS>
```

Setting a configuration

A specific configuration can be sent to RILOE II by using the command format:
```
HPONCFG /f add_user.xml /l log.txt
```

In this example, the input file has contents:
```
<!-- Add user with minimal privileges to test default setting of
assigned privileges to 'N' -->
<RIBCL version="1.2">
<LOGIN USER_LOGIN="x" PASSWORD="x">
<USER_INFO MODE="write">
<ADD_USER USER_NAME="Landy9" USER_LOGIN="mandy9"
PASSWORD="floppyshoes">
<RESET_SERVER_PRIV value="Y" />
<ADMIN_PRIV value="Y" />
</ADD_USER>
</USER_INFO>
</LOGIN>
</RIBCL>
```

The specified user will be added to the device.

Remote Insight command language

The Remote Insight Board Command Language enables you to write scripts to manage user accounts and to configure settings.

IMPORTANT: Comments should not interrupt a command. If they do, an error message will be generated.

RIBCL sample scripts

Sample scripts for all RILOE II commands described in this section are available for download from the HP website (http://www.hp.com/servers/lights-out).

RIBCL general guidelines

In this section, all of the commands are grouped by functionality. All commands that manipulate user information are grouped together. Grouping commands allows the firmware to view the data to be manipulated as a block of information, similar to a text document, allowing for multithreaded access to the different kinds of information.

An opening command opens a database. The database remains open until the matching closing command is sent. All changes made within a single command block are applied simultaneously when the database is closed. Any errors within the block cause the enclosed changes to be discarded.

An example of an opening command and its matching closing command are as follows:

```
<USER_INFO>
</USER_INFO>
```

In all examples, the opening and closing commands are displayed.

XML header

The XML header ensures the connection is an XML connection, not an HTTP connection. The XML header is built into the cpqlocfg utility and has the following format:

```
<?xml version="1.0"?>
```

Data types

The three data types that are allowed in the parameter are:

- String
- Specific string
- Boolean string

String

A string is any text enclosed in quotes. It can include spaces, numbers, or any printable character. A string may start with either a double or single quote and it must end with the same type of quote. The string may contain a quote if it is different from the string delimiter quotes.

For example, if a string is started with a double quote, a single quote can be used within the string and the string must be closed with a double quote.

Specific string

A specific string is one that is required to contain certain characters. In general, you have a choice of words that are accepted as correct syntax and all other words produce an error.

Boolean string

A Boolean string is a specific string that specifies a "yes" or "no" condition. Acceptable Boolean strings are "yes," "y," "no," "n," "true," "t," "false," and "f." These strings are not case sensitive.

Response definitions

Every command that is sent to the RILOE II generates a response. The response indicates whether the command succeeded or failed. Some commands generate additional information. The additional information is displayed in execution sequence, provided no errors occurred.

Example:

```
<RESPONSE
    STATUS="0x0001"
    MSG="There has been a severe error."
/>
```

- RESPONSE

This tag name indicates that the RILOE II is sending a response to the previous commands back to the client application to indicate the success or failure of the commands that have been sent to the RILOE II.

- STATUS

  This parameter contains an error number. The number 0x0000 indicates that there is no error.

- MSG

  This element contains a message describing the error that happened. If no error occurred, the message `No error` appears.

RIBCL

This command is used to start and end an RIBCL session. You can use it only once to start an RIBCL session, and it must be the first command to display in the script. The RIBCL tags are required to mark the beginning and the end of the RIBCL document.

Example:
```
<RIBCL VERSION="2.0">
</RIBCL>
```

RIBCL parameters

VERSION is a string that indicates the version of the RIBCL that the client application is expecting to use. The VERSION string is compared to the version of the RIBCL that is expected, and an error is returned if the string and the version do not match. The preferred value for the VERSION parameter is "2.0." The VERSION parameter is no longer checked for an exact match; however, this parameter can never be blank.

RIBCL runtime errors

The possible RIBCL error messages include:

Version must not be blank.

LOGIN

The LOGIN command provides the information that is used to authenticate the user whose permission level will be used when performing RIBCL actions. The specified user must have a valid account on the respective RILOE II to execute RIBCL commands. The user's privileges are checked against the required privilege for a particular command, and an error is returned if the privilege level does not match.

Example:
```
<LOGIN USER_LOGIN="username" PASSWORD="password">
</LOGIN>
```

Alternatively, the CPQLOCFG utility can specify the login information as parameters on its command line:
```
cpqlocfg  -u <username> -p <password>
```

When using this format, the utility returns an `Overriding credentials` warning message but still shows the error log message entry as `Login name must not be blank.`

LOGIN parameters

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must never be blank.

PASSWORD is the password associated with the user. This parameter is case sensitive and can be a combination of any printable characters.

LOGIN runtime errors

The possible runtime error messages include:

- User login name was not found.
- Password must not be blank.
- Logged-in user does not have required privilege for this command.

USER_INFO

The USER_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the local user information database into memory and prepares to edit it. Only commands that are USER_INFO type commands are valid inside the USER_INFO command block. The USER_INFO command generates a response that indicates to the host application whether the database was successfully read or not. If database is open for writing by another application, then this call will fail.

Example:
```
<USER_INFO MODE="write">

    ......... USER_INFO commands ......
</USER_INFO>
```

USER_INFO parameter

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information. Valid arguments are "read" and "write."

Write mode enables both reading and writing of RILOE II information. Read mode prevents modification of the RILOE II information.

USER_INFO runtime error

None

ADD_USER

The ADD_USER command is used to add a local user account. The USER_NAME and USER_LOGIN parameters must not exist in the current user database. Use the MOD_USER command to change an existing user's information. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE must be set to write. The user must have the administrative privilege.

All of the attributes that pertain to the user are set using the following parameters.
```
<RIBCL VERSION="2.0">

    <LOGIN USER_LOGIN="loginname" PASSWORD="password">

    <USER_INFO MODE="write">

    <ADD_USER

        USER_NAME="User"

        USER_LOGIN="username" PASSWORD="password">

        <ADMIN_PRIV value ="No"/>

        <REMOTE_CONS_PRIV value ="Yes"/>

        <RESET_SERVER_PRIV value ="No"/>

        <VIRTUAL_MEDIA_PRIV value ="No"/>
```

Scripting, command line, and utility options   141

```
        <CONFIG_ILO_PRIV value ="No"/>
      </ADD_USER>
      </USER_INFO>
      </LOGIN>
    </RIBCL>
```

ADD_USER parameters

USER_NAME is the actual name of the user. This parameter can be a combination of any printable characters up to a maximum length of 39 characters. This parameter is case sensitive and must never be blank.

USER_LOGIN is the name used to gain access to the respective RILOE II. This parameter can be a combination of any printable characters up to a maximum length of 39 characters. This parameter is case sensitive and must never be blank.

PASSWORD is the password associated with the user. This parameter is case sensitive and can be a combination of any printable characters. The length is user defined and can be a minimum of zero characters and a maximum of 40 characters. The minimum length is defined in the RILOE II Global Settings and has a default value of eight characters.

ADMIN_PRIV is a Boolean parameter that allows the user to administer user accounts. The user can modify their account settings, modify other user account settings, add users, and delete users. Omitting this parameter prevents the user from adding, deleting, or configuring user accounts.

REMOTE_CONS_PRIV is a Boolean parameter that gives permission for the user to access the Remote Console functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter denies the user access to Remote Console functionality.

RESET_SERVER_PRIV is a Boolean parameter that gives the user permission to remotely manipulate the server power setting. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter prevents the user from manipulating the server power settings.

VIRTUAL_MEDIA_PRIV is a Boolean parameter that gives the user permission to access the virtual media functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be left blank. Omitting this parameter denies the user virtual media privileges.

CONFIG_RILO_PRIV is a Boolean parameter that allows the user to configure RILOE II settings. This privilege includes network settings, global settings, Insight Manager settings, and SNMP settings. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have this privilege. If this parameter is used, the Boolean string value must never be blank. Omitting this parameter prevents the user from manipulating the current configuration.

LOGIN_PRIV is a Boolean parameter that allows the user to log in to the RILOE II and use resources such as web pages. Marking this parameter with a "No" value or leaving out this parameter effectively disables the account without deleting it.

The following parameters are not applicable to a user's privileges in the RILOE II firmware versions 1.10 and later. The parameters parse correctly, but user privileges are not affected.

VIEW_LOGS_PRIV is a Boolean parameter that gives the user permission to view the RILOE II system logs. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to view logs. If this parameter is used, the Boolean string value must never be blank.

CLEAR_LOGS_PRIV is a Boolean parameter that gives the user permission to clear the event log. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to clear the RILOE II event log. If this parameter is used, the Boolean string value must never be blank.

Scripting, command line, and utility options   142

EMS_PRIV is a Boolean parameter that gives the user permission to use the Windows® Server 2003 EMS service. This parameter is optional, and the Boolean string must be set to "Yes" if the user should be allowed to use EMS services. If this parameter is used, the Boolean string value must never be blank.

ADD_USER runtime errors

The possible ADD_USER error messages include:

- Login name is too long.
- Password is too short.
- Password is too long.
- User table is full. No room for new user.
- Cannot add user. The user name already exists.
- User information is open for read-only access. Write access is required for this operation.
- User name cannot be blank.
- User login ID cannot be blank.
- Boolean value not specified.
- User does not have correct privilege for action. ADMIN_PRIV required.

DELETE_USER

The DELETE_USER command is used to remove an existing local user's account. The USER_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE must be set to write. The user must have the administrative privilege.

Example:

```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname"
    PASSWORD="password">
    <USER_INFO MODE="write">
    <DELETE_USER USER_LOGIN="username"/>
    </USER_INFO>
    </LOGIN>
</RIBCL>
```

DELETE_USER parameter

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must never be blank.

DELETE_USER runtime errors

The possible DELETE_USER errors include:

- User information is open for read-only access. Write access is required for this operation.
- Cannot delete user information for currently logged in user.
- User login name was not found.
- User login name must not be blank.
- User does not have correct privilege for action. ADMIN_PRIV required.

GET_USER

The GET_USER command will return a local user's information, excluding the password. The USER_LOGIN parameter must exist in the current user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE can be in read or write. The user must have the administrative privilege to retrieve other user accounts; else the user can only view their individual account information.

Example:

```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <USER_INFO MODE="read">
    <GET_USER USER_LOGIN="username"/>
    </USER_INFO>
    </LOGIN>
</RIBCL>
```

GET_USER parameter

USER_LOGIN is the login name of the user account. This parameter is case sensitive and must never be blank.

GET_USER runtime errors

The possible GET_USER error messages include:

- User login name must not be blank.
- User login name was not found.
- User does not have correct privilege for action. ADMIN_PRIV required.

GET_USER return messages

A possible GET_USER return message includes the following:

```
<RESPONSE
    STATUS="0x0000"
    MSG="No Errors"
/>
    <GET_USER
    USER_NAME="Admin User"
    USER_LOGIN= "username"
    ADMIN_PRIV="N"
    CONFIG_RILO_PRIV="Y"
    LOGIN_PRIV="Y"
    REMOTE_CONS_PRIV="Y"
    RESET_SERVER_PRIV="N"
    VIRTUAL_MEDIA_PRIV="N"
    CLIENT_IP=""
/>
```

MOD_USER

The MOD_USER command is used to modify an existing local user's information. You are not required to enter any of the fields except for the first one, which specifies which user to modify. If any parameter does not need to be modified, you should omit it. MOD_USER must be displayed within a USER_INFO parameter, and USER_INFO must be in write mode. The user login name used to gain access cannot be modified.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <USER_INFO MODE="write">
   <MOD_USER USER_LOGIN="loginname">
      <USER_NAME value="username"/>
      <PASSWORD value="password"/>
      <ADMIN_PRIV value="No"/>
      <LOGIN_PRIV value="Yes"/>
      <REMOTE_CONS_PRIV value="Yes"/>
      <RESET_SERVER_PRIV value="No"/>
      <CONFIG_RILO_PRIV value="Yes"/>
      <VIRTUAL_MEDIA_PRIV value="No"/>
      <CLIENT_IP value="255.255.255.255"/>
   </MOD_USER>
   </USER_INFO>
   </LOGIN>
</RIBCL>
```

MOD_USER Parameters

USER_LOGIN is the name that the user types to log in to the RILOE II. The USER_LOGIN parameter has a maximum length of 40 characters, can be an ASCII string containing any combination of printable characters, and is case sensitive. The USER_LOGIN parameter must never be blank.

NOTE: If the following parameters are not specified, then the parameter value for the specified user is not changed.

USER_NAME is the actual name of the user. The USER_NAME parameter has a maximum length of 40 characters and can be any ASCII string containing printable characters, including white spaces. This string is used for display only and must never be blank.

PASSWORD is the password that will be associated with the user. This parameter has a minimum length of 8 characters, a maximum length of 40 characters, and is an ASCII string that may contain any combination of printable characters. The PASSWORD parameter cannot contain both single and double quote characters. This parameter is case sensitive and must never be blank.

ADMIN_PRIV is a Boolean parameter that allows the user to administer user accounts. The user can modify their account settings, modify other user account settings, add users, and delete users. Leaving out this parameter prevents the user from adding, deleting, or configuring accounts.

LOGIN_PRIV is a Boolean parameter that allows the user to log in to the RILOE II and use resources such as Web pages. Marking this parameter with a "No" value or leaving out this parameter effectively disables the account without deleting it.

REMOTE_CONS_PRIV is a Boolean parameter that gives permission for the user to access the Remote Console functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have Remote Console privileges. If this parameter is used, the Boolean string value must never be left blank. Leaving out this privilege will deny the user access to any Remote Console functionality.

RESET_SERVER_PRIV is a Boolean parameter that gives the user permission to remotely reset the server or power it down. This parameter is optional, and the Boolean string must be set to "Yes" if the user is allowed to modify the server power. If this parameter is used, the Boolean string value must never be left blank. Leaving out this parameter denies the user server reset privileges.

CONFIG_RILO_PRIV is a Boolean parameter that gives the user permission to configure the board settings. The settings include network, global, Insight Manager, and SNMP settings. Leaving out the parameter denies the user the ability to configure board settings.

VIRTUAL_MEDIA_PRIV is a Boolean parameter that gives the user permission to access the virtual floppy functionality. This parameter is optional, and the Boolean string must be set to "Yes" if the user should have virtual floppy privileges. If this parameter is used, the Boolean string value must never be left blank. Leaving out this parameter denies the user virtual floppy privileges.

IMPORTANT: The following parameters limit the address from which the user may log in. If the user attempts to log in from other addresses, the request will be refused as though the user has typed an incorrect password. Exactly one of the following parameters must be present for a restriction to apply. To indicate that there is no limit to the locations from which the user can log in, do not enter one of these parameters. If the parameter is not blank, then the client addresses are limited as indicated.

CLIENT_IP specifies a single IP address that the user may use to connect to the RILOE II. This parameter must be a complete numerical IP address in the 0.0.0.0 format.

CLIENT RANGE specifies a range of addresses that the user is allowed to use to access the RILOE II in the 0.0.0.0 format. Two addresses are specified with a dash (—) between them. Both addresses must be valid and complete TCP/IP numerical addresses. Any address that falls inside the range numerically will be accepted. This data parameter is mutually exclusive to the CLIENT_IP and the DNS_NAME parameters.

DNS_NAME specifies a DNS name with which the user logs in to the RILOE II and has a maximum length of 50 characters. This parameter is mutually exclusive to the CLIENT_IP and the CLIENT_RANGE parameters.

MOD_USER runtime errors

The possible MOD_USER error messages include:
- Login name is too long.
- Password is too short.
- Password is too long.
- User information is open for read-only access. Write access is required for this operation.
- User login name must not be blank.
- Cannot modify user information for currently logged user.
- User does not have correct privilege for action. ADMIN_PRIV required.

GET_ALL_USERS

The GET_ALL_USERS command will return all USER_LOGIN parameters in the user database. For this command to parse correctly, the command must appear within a USER_INFO command block, and USER_INFO MODE can be in read or write. The user must have the administrative privilege to retrieve all user accounts.

Example:

```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <USER_INFO MODE="read">
    <GET_ALL_USERS />
    </USER_INFO>
    </LOGIN>
</RIBCL>
```

GET_ALL_USERS parameters

None

GET_ALL_USERS runtime errors

The possible GET_ALL_USERS error messages include:

User does not have correct privilege for action. ADMIN_PRIV required.

GET_ALL_USERS return messages

A possible GET_ALL_USERS return message is:
```
<RESPONSE
    STATUS="0x0000"
    MESSAGE='No Error'
/>
<GET_ALL_USERS>
    <USER_LOGIN VALUE="username"/>
    <USER_LOGIN VALUE="user2"/>
    <USER_LOGIN VALUE="user3"/>
    <USER_LOGIN VALUE="user4"/>
    <USER_LOGIN VALUE="user5"/>
    <USER_LOGIN VALUE="user6"/>
    <USER_LOGIN VALUE="user7"/>
    <USER_LOGIN VALUE="user8"/>
    <USER_LOGIN VALUE="user9"/>
    <USER_LOGIN VALUE="user10"/>
    <USER_LOGIN VALUE=""/>
    <USER_LOGIN VALUE=""/>
</GET_ALL_USERS>
```
A possible unsuccessful request is:
```
<RESPONSE
    STATUS = "0x0001"
    MSG = "Error Message"/>
```

GET_ALL_USER_INFO

The GET_ALL_USER_INFO command will return all local users information in the user database, excluding passwords. For this command to parse correctly, the command must appear within a USER_INFO

command block, and USER_INFO MODE can be in read or write. The user must have administrative privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">

   <LOGIN USER_LOGIN="adminname" PASSWORD="password">

   <USER_INFO MODE="read">

   <GET_ALL_USER_INFO />

   </USER_INFO>

   </LOGIN>
</RIBCL>
```

GET_ALL_USER_INFO parameters

None

GET_ALL_USER_INFO runtime errors

The possible GET_ALL_USER_INFO error message include:

User does not have correct privilege for action. ADMIN_PRIV required.

GET_ALL_USER_INFO return messages

A possible GET_ALL_USER_INFO return message is:

```
<GET_ALL_USER_INFO/>

   <GET_USER

   USER_NAME="Admin"

   USER_LOGIN="Admin"

   ADMIN_PRIV="Y"

   CONFIG_RILO_PRIV="Y"

   LOGIN_PRIV="Y"

   REMOTE_CONS_PRIV="Y"

   RESET_SERVER_PRIV="Y"

   VIRTUAL_MEDIA_PRIV="Y"

/> ......
The same information will be repeated for all the users.
</GET_ALL_USER_INFO>
```

A possible unsuccessful request is:

```
<RESPONSE

   STATUS = "0x0001"
MSG = "Error Message"/>
```

RIB_INFO

The RIB_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the RILOE II configuration information database into memory and prepares to edit it. Only commands that are RIB_INFO type commands are valid inside the RIB_INFO command block. The RIB_INFO command generates a response that indicates to the host application whether the database was successfully read or not. If the database is open for writing by another application, then this call will fail.

Example:
```
<RIB_INFO MODE="write">
......... RIB_INFO commands ......
</RIB_INFO>
```

RIB_INFO parameters

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information. Valid arguments are "read" and "write."

Write mode enables both reading and writing of RILOE II information. Read mode prevents modification of RILOE II information.

RIB_INFO runtime errors

None

RESET_RIB

The RESET_RIB command is used to reset RILOE II. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write. The user must have the configure RILOE II privilege to execute this command.

Example:
```
<RIBCL VERSION="2.0">

    <LOGIN USER_LOGIN="Admin" PASSWORD="Password">

    <RIB_INFO MODE = "write">

    <RESET_RIB/>

    </RIB_INFO>

    </LOGIN>
</RIBCL>
```

RESET_RIB parameters

None

RESET_RIB runtime errors

The possible RESET_RIB error message include:

User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_NETWORK_SETTINGS

The GET_NETWORK_SETTINGS command allows the user to retrieve the network settings. GET_NETWORK_SETTINGS must display inside a RIB_INFO block. The user must have login privilege to execute this command.

Example:
```
<RIBCL VERSION="2.0">

    <LOGIN USER_LOGIN="adminname" PASSWORD="password">

    <RIB_INFO MODE="read">

    <GET_NETWORK_SETTINGS/>

    </RIB_INFO>
```

```
        </LOGIN>
    </RIBCL>
```

GET_NETWORK_SETTINGS Parameters

There are no parameters for this command.

GET_NETWORK_SETTINGS Runtime Errors

There are no errors for this command.

GET_NETWORK_SETTINGS Return Messages

A possible GET_NETWORK_SETTINGS return message is:

```
<GET_NETWORK_SETTINGS
    SPEED_AUTOSELECT="YES"
    NIC_SPEED="100"
    FULL_DUPLEX="NO"
    DHCP_ENABLE="YES"
    DHCP_GATEWAY="YES"
    DHCP_DNS_SERVER="YES"
    DHCP_STATIC_ROUTE="YES"
    DHCP_WINS_SERVER="YES"
    REG_WINS_SERVER="YES"
    IP_ADDRESS="111.111.111.111"
    SUBNET_MASK="255.255.255.0"
    GATEWAY_IP_ADDRESS="111.111.111.1"
    DNS_NAME="test"
    DOMAIN_NAME="test.com"
    PRIM_DNS_SERVER="111.111.111.242"
    SEC_DNS_SERVER="111.111.111.242"
    TER_DNS_SERVER="111.111.111.242"
    PRIM_WINS_SERVER="111.111.111.246"
    SEC_WINS_SERVER="111.111.111.247"
    STATIC_ROUTE_1 DEST="0.0.0.0" GATEWAY="0.0.0.0"
    STATIC_ROUTE_2 DEST="0.0.0.0" GATEWAY="0.0.0.0"
    STATIC_ROUTE_3 DEST="0.0.0.0" GATEWAY="0.0.0.0"
    WEB_AGENT_IP_ADDRESS=""
/>
```

A possible unsuccessful request is:

```
<RESPONSE
    STATUS = "0x0001"
    MSG = "Error Message"/>
```

MOD_NETWORK_SETTINGS

The MOD_NETWORK_SETTINGS command modifies certain network settings. This command is only valid inside a RIB_INFO block. The logged-in user must have the configure RILOE privilege, and the mode of the containing RIB_INFO block must be "write." All of these elements are optional and may be left out. If an element is left out, then the current setting is preserved.

Example:

```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
    <MOD_NETWORK_SETTINGS>
        <SPEED_AUTOSELECT value="No"/>
        <FULL_DUPLEX value="Yes"/>
        <NIC_SPEED value="100"/>
        <DHCP_ENABLE value="Yes"/>
        <IP_ADDRESS value="255.255.255.255"/>
        <SUBNET_MASK value="255.255.0.0"/>
        <GATEWAY_IP_ADDRESS value="255.255.255.255"/>
        <DNS_NAME value="demorib.internal.net"/>
        <DOMAIN_NAME value="internal.net"/>
        <DHCP_GATEWAY value="No"/>
        <DHCP_DNS_SERVER value="No"/>
        <DHCP_STATIC_ROUTE value="No"/>
        <REG_WINS_SERVER value="No"/>
        <PRIM_DNS_SERVER value="255.255.255.255"/>
        <SEC_DNS_SERVER value="255.255.255.255"/>
        <STATIC_ROUTE_1 DEST="255.255.0.0" GATEWAY="255.0.0.0"/>
        <STATIC_ROUTE_2 DEST="255.255.0.0" GATEWAY="255.0.0.0"/>
        <WEB_AGENT_IP_ADDRESS value="255.255.255.255"/>
    </MOD_NETWORK_SETTINGS>
    </RIB_INFO>
    </LOGIN>
</RIBCL>
```

MOD_NETWORK_SETTINGS Parameters

SPEED_AUTOSELECT is used to automatically select the transceiver speed. The possible values are "Yes" or "No." It is case insensitive.

FULL_DUPLEX is used to decide if the RILOE II is to support full-duplex or half-duplex mode. It is only applicable if SPEED_AUTOSELECT was set to "No." The possible values are "Yes" or "No." It is case insensitive.

NIC_SPEED is used to set the transceiver speed if SPEED_AUTOSELECT was set to "No." The possible values are "10" or "100." Any other values will result in a syntax error.

DHCP_ENABLE is used to enable DHCP. The possible values are "Yes" or "No." It is case insensitive.

IP_ADDRESS is used to select the IP address for the RILOE II if DHCP is not enabled. If an empty string is entered, the current value is deleted.

SUBNET_MASK is used to select the subnet mask for the RILOE II if DHCP is not enabled. If an empty string is entered, the current value is deleted.

GATEWAY_IP_ADDRESS is used to select the default gateway IP address for the RILOE II if DHCP is not enabled. If an empty string is entered, the current value is deleted.

DNS_NAME is used to specify the DNS name for the RILOE II. If an empty string is entered, the current value is deleted.

DOMAIN_NAME is used to specify the domain name for the network where the RILOE II resides. If an empty string is entered, the current value is deleted.

DHCP_GATEWAY specifies if the DHCP-assigned gateway address is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP_DNS_SERVER specifies if the DHCP-assigned DNS server is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP_WINS_SERVER specifies if the DHCP-assigned WINS server is to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

DHCP_STATIC_ROUTE specifies if the DHCP-assigned static routes are to be used. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

REG_WINS_SERVER specifies if the RILOE II needs to register with the WINS server. The possible values are "Yes" or "No." It is case sensitive. This selection is only valid if DHCP is enabled.

PRIM_DNS_SERVER specifies the IP address of the primary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

SEC_DNS_SERVER specifies the IP address of the secondary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

TER_DNS_SERVER specifies the IP address of the tertiary DNS server. This parameter is only relevant if the DHCP-assigned DNS server address feature is disabled. If an empty string is entered, the current value is deleted.

PRIM_WINS_SERVER specifies the IP address of the primary WINS server. This parameter is only relevant if the DHCP-assigned WINS server address feature is disabled. If an empty string is entered, the current value is deleted.

SEC_WINS_SERVER specifies the IP address of the secondary WINS server. This parameter is only relevant if the DHCP-assigned WINS server address feature is disabled. If an empty string is entered, the current value is deleted.

STATIC_ROUTE_1, STATIC_ROUTE_2, and STATIC_ROUTE_3 are used to specify the destination and gateway IP addresses of the static routes. The following two parameters are used within the static route commands. If an empty string is entered, the current value is deleted.

- DEST specifies the destination IP addresses of the static route. This parameter is only relevant if the DHCP-assigned static route feature is disabled. If an empty string is entered, the current value is deleted.

- GATEWAY specifies the gateway IP addresses of the static route. This parameter is only relevant if the DHCP-assigned static route feature is disabled. If an empty string is entered, the current value is deleted.

WEB_AGENT_IP_ADDRESS specifies the address for the Web-enabled agents. If an empty string is entered, the current value is deleted.

MOD_NETWORK_SETTINGS Runtime Errors

The possible MOD_NETWORK_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.

GET_GLOBAL_SETTINGS

The GET_GLOBAL_SETTINGS command requests the respective RILOE II global settings. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write.

GET_GLOBAL_SETTINGS parameters

None

GET_GLOBAL_SETTINGS runtime errors

None

GET_GLOBAL_SETTINGS return messages

A possible GET_GLOBAL_SETTINGS return message is:

```
<GET_GLOBAL_SETTINGS
    SESSION_TIMEOUT="120"
    F8_PROMPT_ENABLED="YES"
    HOST_KEYBOARD_ENABLED="YES"
    REMOTE_CONSOLE_PORT_STATUS ="ENABLED"
    POCKETPC_ACCESS ="NO"
    EMS_STATUS ="NO"
    BYPASS_POWER_CABLE_REPORTING ="NO"
    CIPHER_STRENGTH ="40"
    HTTPS_PORT ="443"
    HTTP_PORT ="80"
    REMOTE_CONSOLE_PORT ="23"
    SNMP_ADDRESS_1 =""
    SNMP_ADDRESS_2 =""
    SNMP_ADDRESS_3 =""
    OS_TRAPS ="NO"
    RIB_TRAPS ="NO"
    CIM_SECURITY_MASK ="MEDIUM"
/>
```

The following is an example of an unsuccessful request:

```
<RESPONSE
    STATUS = "0x0001"
```

```
            MSG = "Error Message"/>
```

MOD_GLOBAL_SETTINGS

This command modifies certain global settings. This command is only valid inside a RIB_INFO block. The logged-in user must have the configure RILOE privilege, and RIB_INFO must be in write mode. All of these elements are optional and may be left out. If an element is left out, then the current setting is preserved.

Example:

```
<RIBCL VERSION="2.0">

   <LOGIN USER_LOGIN="adminname" PASSWORD="password">

   <RIB_INFO MODE="write">

   <MOD_GLOBAL_SETTINGS>

      <SESSION_TIMEOUT value="60"/>

      <F8_PROMPT_ENABLED value="Yes"/>

      <HOST_KEYBOARD_ENABLED value="Yes"/>

      <REMOTE_CONSOLE_PORT_STATUS value="3"/>

      <POCKETPC_ACCESS value="Yes"/>

      <REMOTE_CONSOLE_ENCRYPTION value="Yes"/>

      <CIPHER_STRENGTH value="128"/>

      <HTTPS_PORT value="443"/>

      <HTTP_PORT value="80"/>

      <REMOTE_CONSOLE_PORT value="23"/>

      <SNMP_ADDRESS_1 value="123.124.125.126"/>

      <SNMP_ADDRESS_2 value="Test"/>

      <SNMP_ADDRESS_3 value="Test"/>

      <OS_TRAPS value="Yes"/>

      <RIB_TRAPS value="No"/>

      <EMS_SETTINGS value="No"/>

      <BYPASS_POWER_CABLE_REPORTING value="No"/>

      <CIM_SECURITY_MASK="3"/>

   </MOD_GLOBAL_SETTINGS>

   </RIB_INFO>

   </LOGIN>
</RIBCL>
```

MOD_GLOBAL_SETTINGS parameters

SESSION_TIMEOUT determines the maximum session timeout value in minutes. The accepted values are from 0 to 120. If a value greater than 120 is specified, the SESSION_TIMEOUT returns an error.

F8_PROMPT_ENABLED determines if the F8 prompt for ROM-based configuration is displayed during POST. The possible values are "Yes" or "No."

HOST_KEYBOARD_ENABLED determines if the host keyboard is enabled or disabled. The possible values are "Yes" or "No."

REMOTE_CONSOLE_PORT_STATUS determines the configuration for the Remote Console port. The valid values for this setting are:

Scripting, command line, and utility options   154

- 0 = No Change
- 1 = Disabled
- 2 = Automatic
- 3 = Enabled

In the Automatic setting, the Remote Console port is enabled only when a Remote Console session through a browser is in progress, and is disabled otherwise.

POCKETPC_ACCESS determines if the PocketPC access is allowed. The possible values are "Yes" or "No."

REMOTE_CONSOLE_ENCRYPTION determines if Remote Console Data Encryption is enabled or disabled. The possible values are "Yes" and "No."

CIPHER_STRENGTH determines the SSL encryption strength. The possible values are "40" and "128," which enable 40-bit and 128-bit encryption respectively.

HTTPS_PORT—Specifies the HTTPS (SSL) port number for the RILOE II. If this value is changed, the RILOE II must be reset.

HTTP_PORT—Specifies the HTTP port number for the RILOE II. If this value is changed, the RILOE II must be reset.

REMOTE_CONSOLE_PORT—This parameter specifies the Remote Console port for the RILOE II. The RILOE II needs to be reset if this value is changed.

SNMP_ADDRESS_1, SNMP_ADDRESS_2, and SNMP_ADDRESS_3 are the addresses that receive traps sent to the user. Each of these parameters can be any valid IP address or DNS name and has a maximum value of 50 characters.

SNMP Traps send trap information according to the value, if the tag is set with a value attribute. If the tag is not set, "No" is assumed, and traps are not sent.

OS_TRAPS indicates that the user should receive SNMP traps that are generated by the operating system. The possible values are "Yes" and "No." If the value is not set, then the default "No" is assumed, and traps are not sent.

RIB_TRAPS indicates that the user should receive SNMP traps that are generated by the RIB. The possible values are "Yes" and "No." If the value is not set, then the default "No" is assumed, and traps are not sent.

BYPASS_POWER_CABLE_REPORTING determines how the external power cable status is reported. The possible values are "Yes" and "No."

- The value of "Yes" causes the RILOE II board to report to the operating system that the external power cable is connected irrespective of the actual status. This will cause Insight Manager 7 to report a green status for the board if the external cable is not connected, barring other status problems.

The value of "No" will cause the board to report the true status of the external power connector. This will cause RILOE II to report the status of the board as degraded if the external connector is not connected.

CIM_SECURITY_MASK accepts an integer between 0 and 4. The possible values are:

- **0**—No change
- **1**—None (No data is returned to Systems Insight Manager.)
- **2**—Low (Name and status data are returned. Associations are present if SNMP pass-through is supported. If not, the server and management processor are separate entities in the device list.)
- **3**—Medium (RILOE II and server associations are present but the summary page contains less detail than at high security.)
- **4**—High (Associations are present and all data is present on the summary page.)

Each value indicates the level of data returned to an Systems Insight Manager request.

MOD_GLOBAL_SETTINGS runtime errors

The possible MOD_GLOBAL_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- The remote console port status value specified is invalid. It needs to be either 0, 1, 2, or 3.
- Invalid SSL Encryption Strength specified. The valid values are 40 and 128.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.

CLEAR_EVENTLOG

The CLEAR_EVENTLOG command clears the RILOE II Event Log. The CLEAR_EVENTLOG command must be displayed within a RIB_INFO block, and RIB_INFO must be in write mode. To clear the event log, the user must be logged in with the configure RILOE privilege.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="write">
   <CLEAR_EVENTLOG/>
   </RIB_INFO>
   </LOGIN>
</RIBCL>
```

CLEAR_EVENTLOG Parameters

There are no parameters for this command.

CLEAR_EVENTLOG Runtime Errors

The possible CLEAR_EVENTLOG error messages are:

- RIB information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.

UPDATE_RIB_FIRMWARE

The UPDATE_RIB_FIRMWARE command copies a specified file to RILOE II, starts the upgrade process and reboots the board after the image has been successfully flashed. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure RILOE II privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
   <LOGIN USER_LOGIN="adminname" PASSWORD="password">
   <RIB_INFO MODE="write">
   <UPDATE_RIB_FIRMWARE IMAGE_LOCATION="C:\ILO140.BIN"/>
```

```
        </RIB_INFO>
      </LOGIN>
    </RIBCL>
```

UPDATE_RIB_FIRMWARE parameters

IMAGE_LOCATION takes the full path file name of the firmware upgrade file.

UPDATE_RIB_FIRMWARE runtime errors

The possible UPDATE_RIB_FIRMWARE error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- Unable to open the firmware image update file.
- Unable to read the firmware image update file.
- The firmware upgrade file size is too big.
- The firmware image file is not valid.
- A valid firmware image has not been loaded.
- The flash process could not be started.
- IMAGE_LOCATION must not be blank.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

GET_FW_VERSION

The GET_FW_VERSION command requests the respective RILOE II firmware information. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure RILOE II privilege to execute this command.

Example:
```
    <RIBCL VERSION="2.0">
      <LOGIN USER_LOGIN="adminname" PASSWORD="password">
      <RIB_INFO MODE="read">
      <GET_FW_VERSION/>
      </RIB_INFO>
      </LOGIN>
    </RIBCL>
```

GET_FW_VERSION parameters

None

GET_FW_VERSION runtime errors

None

GET_FW_VERSION return messages

The following information is returned within the response:
```
    <GET_FW_VERSION
      FIRMWARE_VERSION = <firmware version>
```

```
        FIRMWARE_DATE = <firmware date>

        MANAGEMENT_PROCESSOR = <management processor type>

    />
```

HOTKEY_CONFIG

The HOTKEY_CONFIG command configures the remote console hot key settings in RILOE II. For this command to parse correctly, the command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. The user must have the configure RILOE II privilege to execute this command.

Uppercase letters are not supported, and they will be converted automatically to lowercase. If either a double quote or a single quote is used, it must be different from the delimiter. Specifying a blank string removes the current value.

Refer to the "Supported Hot Keys" section for a complete list of supported hotkeys.

Example:

```
<RIBCL VERSION="2.0">

    <LOGIN USER_LOGIN="adminname" PASSWORD="password">

    <RIB_INFO MODE="write">

    <HOTKEY_CONFIG>

        <CTRL_T value="CTRL,ALT,ESC"/>

        <CTRL_U value="L_SHIFT,F10,F12"/>

        <CTRL_V value=""/>

        <CTRL_Y value=""/>

        <CTRL_X value=""/>

        <CTRL_Y value=""/>

    </HOTKEY_CONFIG>

    </RIB_INFO>

    </LOGIN>

</RIBCL>
```

HOTKEY_CONFIG parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

CTRL_T specifies settings for the CTRL_T hot key. The settings must be separated by commas. For example, CTRL_T="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_U specifies settings for the CTRL_U hot key. The settings must be separated by commas. For example, CTRL_U="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_V specifies settings for the CTRL_V hot key. The settings must be separated by commas. For example, CTRL_V="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_W specifies settings for the CTRL_W hot key. The settings must be separated by commas. For example, CTRL_W="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_X specifies settings for the CTRL_X hot key. The settings must be separated by commas. For example, CTRL_X="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

CTRL_Y specifies settings for the CTRL_Y hot key. The settings must be separated by commas. For example, CTRL_Y="CTRL,ALT,ESC." Up to five keystrokes can be configured for each hot key.

HOTKEY_CONFIG runtime errors

The possible HOTKEY_CONFIG error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- The hot key parameter specified is not valid.
- Invalid number of hot keys. The maximum allowed is five.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

DIR_INFO

The DIR_INFO command can only appear within a LOGIN command block. When the command is parsed, it reads the local directory information database into memory and prepares to edit it. Only commands that are DIR_INFO type commands are valid inside the DIR_INFO command block. The DIR_INFO command generates a response that indicates to the host application whether the database was successfully read or not. If the database is open for writing by another application, then this call will fail.

Example:
```
<DIR_INFO MODE="read">

    ......... DIR_INFO commands ......
</DIR_INFO>
```

DIR_INFO parameters

MODE is a specific string parameter with a maximum length of 10 characters that specifies what you intend to do with the information. Valid arguments are "read" and "write."

Write mode enables both reading and writing of directory information. Read mode prevents modification of directory information.

DIR_INFO runtime errors

None

GET_DIR_CONFIG

The GET_DIR_CONFIG command requests the respective RILOE II directory settings. For this command to parse correctly, the GET_DIR_CONFIG command must appear within a DIR_INFO command block, and DIR_INFO MODE can be set to read or write.

Example:
```
<RIBCL VERSION="2.0">

    <LOGIN USER_LOGIN="adminname" PASSWORD="password">

    <DIR_INFO MODE="read">

    <GET_DIR_CONFIG/>

    </DIR_INFO>

    </LOGIN>
</RIBCL>
```

GET_DIR_CONFIG parameters

None

GET_DIR_CONFIG runtime errors

None

GET_DIR_CONFIG return messages

Starting with RILOE II 1.80, directory integration can work with HP Lights-Out schema with or without extensions (schema-free). Depending on your directory configuration, the response to GET_DIR_CONFIG contains different data.

Possible GET_DIR_CONFIG return messages are:

- Example of a directory services (with schema extension) return message:

```
<GET_DIR_CONFIG>
    <DIR_AUTHENTICATION_ENABLED VALUE="Y"/>
    <DIR_LOCAL_USER_ACCT VALUE="Y"/>
    <DIR_SERVER_ADDRESS VALUE="adserv.demo.com"/>
    <DIR_SERVER_PORT VALUE="636"/>
    <DIR_OBJECT_DN VALUE="CN=SERVER1_RIB,OU=RIB,DC=HPRIB, DC=LABS"/>
    <DIR_USER_CONTEXT1 VALUE="CN=Users0,DC=HPRIB0, DC=LABS"/>
    <DIR_USER_CONTEXT2 VALUE="CN=Users1,DC=HPRIB1, DC=LABS"/>
    <DIR_USER_CONTEXT3 VALUE=""/>
    <DIR_ENABLE_GRP_ACCT VALUE="N"/>
</GET_DIR_CONFIG>
```

- Example of a schema-free directory (without schema extension) return message:

```
<GET_DIR_CONFIG>
    <DIR_AUTHENTICATION_ENABLED VALUE="Y"/>
    <DIR_LOCAL_USER_ACCT VALUE="Y"/>
    <DIR_SERVER_ADDRESS VALUE="adserv.demo.com"/>
    <DIR_SERVER_PORT VALUE="636"/>
    <DIR_OBJECT_DN VALUE=""/>
    <DIR_USER_CONTEXT1 VALUE="CN=Users,DC=demo,DC=com"/>
    <DIR_USER_CONTEXT2 VALUE=""/>
    <DIR_USER_CONTEXT3 VALUE=""/>
    <DIR_ENABLE_GRP_ACCT VALUE="Y"/>
    <DIR_GRPACCT1_NAME VALUE="CN=iLOAdmins,CN=Users,DC=demo,DC=com"/>
    <DIR_GRPACCT1_PRIV VALUE="1,2,3,4,5"/>
    <DIR_GRPACCT2_NAME VALUE="" />
    <DIR_GRPACCT2_PRIV VALUE="" />
    <DIR_GRPACCT3_NAME VALUE="" />
    <DIR_GRPACCT3_PRIV VALUE="" />
    <DIR_GRPACCT4_NAME VALUE="" />
    <DIR_GRPACCT4_PRIV VALUE="" />
    <DIR_GRPACCT5_NAME VALUE="" />
    <DIR_GRPACCT5_PRIV VALUE="" />
    <DIR_GRPACCT6_NAME VALUE="" />
```

```
        <DIR_GRPACCT6_PRIV VALUE="" />
    </GET_DIR_CONFIG><GET_DIR_CONFIG>
```

MOD_DIR_CONFIG

MOD_DIR_CONFIG command is used modify the directory settings on RILOE II. For this command to parse correctly, the MOD_DIR_CONFIG command must appear within a DIR_INFO command block, and DIR_INFO MODE must be set to write. The user must have the configure RILOE II privilege to execute this command.

Examples:

- Extended schema (directory services) configuration example:

```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <DIR_INFO MODE="write">
    <MOD_DIR_CONFIG>
        <DIR_AUTHENTICATION_ENABLED value="Yes"/>
        <DIR_LOCAL_USER_ACCT value="Yes"/>
        <DIR_SERVER_ADDRESS value="16.141.100.44"/>
        <DIR_SERVER_PORT value="636"/>
        <DIR_OBJECT_DN value="CN=server1_rib, OU=RIB, DC=HPRIB, DC=LABS"/>
        <DIR_OBJECT_PASSWORD value="password"/>
        <DIR_USER_CONTEXT_1 value="CN=Users, DC=HPRIB, DC=LABS"/>
    </MOD_DIR_CONFIG>
    </DIR_INFO>
    </LOGIN>
</RIBCL>
```

📝 **NOTE:** When using directory integration with schema extension, the following tags must not be used:
- DIR_ENABLE_GRP_ACCT
- DIR_GRPACCT1_NAME
- DIR_GRPACCT1_PRIV

- Schema-free (without extension) configuration example:

```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="admin" PASSWORD="password">
    <DIR_INFO MODE = "write">
    <MOD_DIR_CONFIG>
        <DIR_ENABLE_GRP_ACCT value = "yes"/>
        <DIR_GRPACCT1_NAME value = "test1"/>
        <DIR_GRPACCT1_PRIV value = "1"/>
        <DIR_GRPACCT2_NAME value = "test2"/>
        <DIR_GRPACCT2_PRIV value = "2"/>
    </MOD_DIR_CONFIG>
    </DIR_INFO>
    </LOGIN>
</RIBCL>
```

📝 **NOTE:** When using schema-free directories, the following tags must not be used:
- DIR_OBJECT_DN
- DIR_OBJECT_PASSWORD

MOD_DIR_CONFIG parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

DIR_AUTHENTICATION_ENABLED enables or disables directory authentication. The possible values are "Yes" and "No."

DIR_ENABLE_GRP_ACCT causes RILOE II to use schama-less directory integration. The possible values are "Yes" and "No."

When using schema-free directory integration, RILOE II supports variable privileges associated with different directory groups. These groups are contained in the directory, and the corresponding member RILOE II privileges are stored in RILOE II.

- DIR_GRPACCT1_NAME identifies a group container in the directory, such as Administrators, Users, or Power Users.
- DIR_GRPACCT1_PRIV numerically identify RILOE II privileges for members of the group. You can mix and match privileges by including more than one value. These privileges are expressed as a comma separated list of numbers (1,2,3,4,5) which correlate to:

1. Administer Group Accounts
2. Remote Console Access
3. Virtual Power and Reset
4. Virtual Media
5. Configure RILOE II Settings

📝 **NOTE:** When using directory integration with schema extension, the following tags must not be used:
- DIR_ENABLE_GRP_ACCT
- DIR_GRPACCT1_NAME
- DIR_GRPACCT1_PRIV

📝 **NOTE:** When using schema-free directories, the following tags must not be used:
- DIR_OBJECT_DN
- DIR_OBJECT_PASSWORD

DIR_LOCAL_USER_ACCT enables or disables local user accounts. The possible values are "Yes" and "No."

DIR_SERVER_ADDRESS specifies the location of the directory server. The directory server location is specified as an IP address or DNS name.

DIR_SERVER_PORT specifies the port number used to connect to the directory server. This value is obtained from the directory administrator. The secure LDAP port is 636, but the directory server can be configured for a different port number.

DIR_OBJECT_DN specifies the unique name of RILOE II in the directory server. This value is obtained from the directory administrator. Distinguished names are limited to 256 characters.

DIR_OBJECT_PASSWORD specifies the password associated with the RILOE II object in the directory server. Passwords are limited to 39 characters.

DIR_USER_CONTEXT_1, DIR_USER_CONTEXT_2, and DIR_USER_CONTEXT_3 specify searchable contexts used to locate the user when the user is trying to authenticate using directories. If the user could not be located using the first path, then the parameters specified in the second and third paths are used.

The values for these parameters are obtained from the directory administrator. Directory User Contexts are limited to 128 characters each.

MOD_DIR_CONFIG runtime errors

The possible MOD_DIR_CONFIG error messages include:

- Directory information is open for read-only access. Write access is required for this operation.
- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

SERVER_INFO

The SERVER_INFO command tells the firmware that the configuration of the RILOE II is about to be changed.

Example:

```
<SERVER_INFO MODE="read">
......... SERVER_INFO commands .........
</SERVER_INFO>
```

SERVER_INFO Parameter

MODE is a specific string parameter that has a maximum length of 10 characters. It tells the RILOE II what you intend to do with the server information. Valid arguments are "read" and "write." If the parameter is open in write mode, then both reading and writing are enabled. If it is open in read mode, the user cannot perform any server actions. If this parameter is not specified, "read" is assumed.

SERVER_INFO Runtime Error

A possible SERVER_INFO error is: `Mode parameter must not be blank.`

RESET_SERVER

The RESET_SERVER command will force a warm boot of the server, if the server is currently on. For this command to parse correctly, the RESET_SERVER command must appear within a SERVER_INFO command block, and SERVER_INFO MODE must be set to write. The user must have the virtual power and reset privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
    <RESET_SERVER/>
    </SERVER_INFO>
    </LOGIN>
</RIBCL>
```

RESET_SERVER errors

The possible RESET_SERVER error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Server is currently powered off.
- User does NOT have correct privilege for action. RESET_SERVER_PRIV required.

RESET_SERVER parameters

None

INSERT_VIRTUAL_FLOPPY

The INSERT_VIRTUAL_FLOPPY command copies a floppy image to the RILOE II. The INSERT_VIRTUAL_FLOPPY command must be displayed within a RIB_INFO element, and RIB_INFO must be in write mode. The user must be logged in with virtual media privilege to execute this command.

Example:
```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
    <INSERT_VIRTUAL_FLOPPY IMAGE_LOCATION="C:\test.img"/>
    </RIB_INFO>
    </LOGIN>
</RIBCL>
```

INSERT_VIRTUAL_FLOPPY Parameter

IMAGE_LOCATION takes the full path file name for the floppy image file.

INSERT_VIRTUAL_FLOPPY Runtime Errors

The possible INSERT_VIRTUAL_FLOPPY error messages are:
- RIB information is open for read-only access. Write access is required for this operation.
- IMAGE_LOCATION must not be blank.
- The Virtual Floppy image is invalid.
- Unable to open the Virtual Floppy image file.
- Unable to read the Virtual Floppy image file.
- The Virtual Floppy image file size is too big.
- No image present in the Virtual Floppy drive.
- Failed to allocate Virtual Floppy image space.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.

EJECT_VIRTUAL_FLOPPY

The EJECT_VIRTUAL_FLOPPY command ejects the Virtual Floppy image if one is inserted. The EJECT_VIRTUAL_FLOPPY command must be displayed within a RIB_INFO element, and RIB_INFO must be in write mode. The user must be logged in with virtual media privilege to execute this command.

Example:
```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
    <EJECT_VIRTUAL_FLOPPY/>
    </RIB_INFO>
    </LOGIN>
```

```
      </RIBCL>
```

EJECT_VIRTUAL_FLOPPY Parameters

There are no parameters for this command.

EJECT_VIRTUAL_FLOPPY Runtime Errors

The possible EJECT_VIRTUAL_FLOPPY error messages are:

- RIB information is open for read-only access. Write access is required for this operation.
- No image present in the Virtual Floppy drive.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.

COPY_VIRTUAL_FLOPPY

The COPY_VIRTUAL_FLOPPY command copies a floppy image from the RILOE II to the local system. The COPY_VIRTUAL_FLOPPY command must be displayed within a RIB_INFO element, and RIB_INFO must be in write mode. The user must be logged in with virtual media privilege to execute this command.

Example:
```
<RIBCL VERSION="2.0">

   <LOGIN USER_LOGIN="adminname" PASSWORD="password">

   <RIB_INFO MODE="write">

   <COPY_VIRTUAL_FLOPPY IMAGE_LOCATION="C:\test.img"/>

   </RIB_INFO>

   </LOGIN>
</RIBCL>
```

COPY_VIRTUAL_FLOPPY Parameter

IMAGE_LOCATION takes the full path file name for the location where the floppy image file needs to be copied.

COPY_VIRTUAL_FLOPPY Runtime Errors

The possible COPY_VIRTUAL_FLOPPY error messages are:

- RIB information is open for read-only access. Write access is required for this operation.
- IMAGE_LOCATION must not be blank.
- Unable to open the Virtual Floppy image file.
- Unable to write the Virtual Floppy image file.
- No image present in the Virtual Floppy drive.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.

GET_VF_STATUS

The GET_VF_STATUS command gets the Virtual Floppy Drive status from the RILOE II. The GET_VF_STATUS command must be displayed within a RIB_INFO element, and RIB_INFO must be in write mode. The user must be logged in with login privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="read">
    <GET_VF_STATUS/>
    </RIB_INFO>
    </LOGIN>
</RIBCL>
```

GET_VF_STATUS Parameters

There are no parameters for this command.

GET_VF_STATUS Runtime Errors

There are no errors for this command.

GET_VF_STATUS Return Messages

The following information is returned within the response:

```
BOOT_OPTION = BOOT_ALWAYS | BOOT_ONCE | NO_BOOT
WRITE_PROTECT_FLAG = YES | NO
IMAGE_INSERTED = YES | NO
```

SET_VF_STATUS

The SET_VF_STATUS command sets the Virtual Floppy Drive status on the RILOE II. The SET_VF_STATUS command must be displayed within a RIB_INFO element, and RIB_INFO must be in write mode. All the parameters in the command are optional. The user must be logged in with virtual media privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
    <SET_VF_STATUS>
        <VF_BOOT_OPTION="BOOT_ONCE"/>
        <VF_WRITE_PROTECT value="Yes"/>
    </SET_VF_STATUS>
    </RIB_INFO>
    </LOGIN>
</RIBCL>
```

SET_VF_STATUS Parameters

VF_BOOT_OPTION specifies the boot option parameter for the Virtual Floppy. The possible values are "BOOT_ALWAYS", "BOOT_ONCE", or "NO_BOOT." The value is case sensitive.

VF_WRITE_PROTECT sets the write-protect flag value for the Virtual Floppy. The possible values are "Yes" or "No."

SET_VF_STATUS Runtime Errors

The possible SET_VF_STATUS error messages are:

- RIB information is open for read-only access. Write access is required for this operation.
- An invalid Virtual Floppy option has been given.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.

GET_HOST_POWER_STATUS

The GET_HOST_POWER_STATUS command displays the server power state from the Virtual Power Button cable. The GET_HOST_POWER_STATUS command must be displayed within a SERVER_INFO element, and SERVER_INFO must be in write mode. The user must be logged in with login privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
    <GET_HOST_POWER_STATUS/>
    </SERVER_INFO>
    </LOGIN>
</RIBCL>
```

GET_HOST_POWER_STATUS Parameters

There are no parameters for this command.

GET_HOST_POWER_STATUS Runtime Errors

The possible GET_HOST_POWER_STATUS error messages include:

- Host power is OFF.
- Host power is ON.

GET_HOST_POWER_STATUS Return Messages

The following information is returned within the response:

```
<GET_HOST_POWER
    HOST POWER="OFF"
/>
```

SET_HOST_POWER

The SET_HOST_POWER command sets the Virtual Power Button feature. This feature is used to turn the server on or off if the feature is supported. The SET_HOST_POWER command must be displayed within a SERVER_INFO element, and SERVER_INFO must be in write mode. The user must be logged in with reset server privilege to execute this command.

Example:

```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <SERVER_INFO MODE="write">
```

```
                    <SET_HOST_POWER HOST_POWER="Yes"/>

                </SERVER_INFO>

                </LOGIN>
          </RIBCL>
```

SET_HOST_POWER Parameters

HOST_POWER enables or disables the Virtual Power Button. The possible values are "Yes" or "No."

SET_HOST_POWER Runtime Errors

The possible SET_HOST_POWER error messages include:

- Server information is open for read-only access. Write access is required for this operation.
- Virtual Power Button feature is not supported on this server.
- Host power is already ON.
- Host power is already OFF.
- User does not have correct privilege for action.
- Logged-in user does not have required privilege for this command.

GET_VPB_CABLE_STATUS

The GET_VPB_CABLE_STATUS command displays the Virtual Power Button cable status on the RILOE II. The GET_VPB_CABLE_STATUS command must be contained within a SERVER_INFO block, and SERVER_INFO must be in write mode. The user must be logged in with login privilege to execute this command.

Example:
```
          <RIBCL VERSION="2.0">

              <LOGIN USER_LOGIN="adminname" PASSWORD="password">

              <SERVER_INFO MODE="write">

              <GET_VPB_CABLE_STATUS/>

              </SERVER_INFO>

              </LOGIN>
          </RIBCL>
```

GET_VPB_CABLE_STATUS Parameters

There are no parameters for this command.

GET_VPB_CABLE_STATUS Runtime Errors

The possible GET_VPB_CABLE_STATUS error messages include:

- Virtual Power Button cable is attached.
- Virtual Power Button cable is not attached.

GET_VPB_CABLE_STATUS Return Messages

The following information is returned within the response:
```
          <GET_VPB_CABLE

              VIRTUAL POWER BUTTON CABLE="ATTACHED"

          />
```

GET_ALL_CABLES_STATUS

The GET_ALL_CABLES_STATUS command displays the status of all the cables on the RILOE II. The GET_ALL_CABLES_STATUS command must be contained within a SERVER_INFO block.

Example:

```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password>
    <SERVER_INFO MODE="read">
    <GET_ALL_CABLES_STATUS/>
    </SERVER_INFO>
    </LOGIN>
</RIBCL>
```

GET_ALL_CABLES_STATUS Parameters

There are no parameters for this command.

GET_ALL_CABLES_STATUS Runtime Errors

There are no errors for this command.

GET_ALL_CABLE_STATUS Return Messages

The following information is returned within the response:

```
<GET_ALL_CABLES_STATUS
    EXTERNAL_POWER_ADAPTER="NOT CONNECTED"
    AUXILLARY_POWER_CABLE="CONNECTED"
    16-PIN_CABLE="NOT CONNECTED"
    30-PIN_CABLE="CONNECTED"
    VPB_CABLE="NOT CONNECTED"
    REMOTE_INSIGHT_KEYBOARD_CABLE="HOST_OFF"
    REMOTE_INSIGHT_MOUSE_CABLE="HOST_OFF"
/>
```

GET_TWOFACTOR_SETTINGS

The GET_TWOFACTOR_SETTINGS command requests the respective RILOE II Two-Factor Authentication settings. For this command to parse correctly, the GET_TWOFACTOR_SETTINGS command must appear within a RIB_INFO command block, and RIB_INFO MODE can be set to read or write.

Example:

```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="read">
    <GET_TWOFACTOR_SETTINGS/>
    </RIB_INFO>
    </LOGIN>
</RIBCL>
```

GET_TWOFACTOR_SETTINGS parameters

None

GET_TWOFACTOR_SETTINGS runtime errors

None

GET_TWOFACTOR_SETTINGS return messages

Starting with RILOE II 1.20, users can be authenticated with a digital certificate. Depending on the RILOE II Two-Factor Authentication settings, the response to GET_TWOFACTOR_SETTINGS will contain different data.

Examples of GET_TWOFACTOR_SETTINGS return messages are:

Example of a Two-Factor Authentication settings return message with default settings:

```
<GET_TWOFACTOR_SETTINGS>

    <AUTH_TWOFACTOR_ENABLE VALUE="N"/>

    <CERT_REVOCATION_CHECK VALUE="N"/>

    <CERT_OWNER_SUBJECT/>
</GET_TWOFACTOR_SETTINGS>
```

Example of a Two-Factor Authentication settings return message when SAN field in the certificate for directory authentication is enabled:

```
<GET_TWOFACTOR_SETTINGS>

    <AUTH_TWOFACTOR_ENABLE VALUE="Y"/>

    <CERT_REVOCATION_CHECK VALUE="N"/>

    <CERT_OWNER_SAN/>
</GET_TWOFACTOR_SETTINGS>
```

MOD_TWOFACTOR_SETTINGS

The MOD_TWOFACTOR_SETTINGS command is used modify the Two-Factor Authentication settings on the RILOE II. For this command to parse correctly, the MOD_TWOFACTOR_SETTINGS command must appear within a RIB_INFO command block, and RIB_INFO MODE must be set to write. You must have the configure RILOE II privilege to execute this command. Changing the value of AUTH_TWOFACTOR_ENABLE will cause the RILOE II to reset in order for the new setting to take effect.

📝 **NOTE:** The GET_TWOFACTOR_SETTINGS and MOD_TWOFACTOR_SETTINGS commands are supported with iLO firmware version 1.80 and above and with iLO 2 firmware version 1.10 and above. iLO 1.80 requires CPQLOCFG version 2.24, and iLO 1.10 requires CPQLOCFG version 2.25.

A Trusted CA Certificate is required for Two-Factor Authentication to function. The RILOE II will not allow the AUTH_TWOFACTOR_ENABLE setting to be set to Yes if a Trusted CA certificate has not been configured. Also, a client certificate must be mapped to a local user account if local user accounts are being used. If the RILOE II is using directory authentication, client certificate mapping to local user accounts is optional.

To provide the necessary security, the following configuration changes are made when Two-Factor Authentication is enabled:

- Remote Console Data Encryption: Yes (This will disable telnet access)
- Enable Secure Shell (SSH) Access: No
- Serial Command Line Interface Status: Disabled

If telnet, SSH or Serial CLI access is required, re-enable these settings after Two-Factor Authentication is enabled. However, because these access methods do not provide a means of Two-Factor Authentication, only a single factor is required to access the RILOE II with telnet, SSH or serial CLI.

When Two-Factor Authentication is enabled, access with the CPQLOCFG utility is disabled, because CPQLOCFG does not supply all authentication requirements. However, the HPONCFG utility is functional, since administrator privileges on the host system are required to execute this utility.

- **Example of enabling Two-Factor Authentication:**

```
<RIBCL VERSION="2.0">
    <LOGIN USER_LOGIN="adminname" PASSWORD="password">
    <RIB_INFO MODE="write">
    <MOD_TWOFACTOR_SETTINGS>
        <AUTH_TWOFACTOR_ENABLE value="Yes"/>
        <CERT_REVOCATION_CHECK value="No"/>
        <CERT_OWNER_SAN/>
    </MOD_TWOFACTOR_SETTINGS>
    </RIB_INFO>
    </LOGIN>
</RIBCL>
```

- **Importing a CA and a user certificate example:**

```
<RIBCL VERSION="2.0">
<LOGIN USER_LOGIN="test" PASSWORD="password">
    <RIB_INFO MODE="write">
    <MOD_TWOFACTOR_SETTINGS>
        <CERT_OWNER_SAN/>
        <IMPORT_CA_CERTIFICATE>
-----BEGIN CERTIFICATE-----
MIIEtzCCA5+gAwIBAgIQBGg9C0d7B5pF/l4bVA44hjANBgkqhkiG9w0BAQUFADBM
MRMwEQYKCZImiZPyLGQBGRYDTEFCMRUwEwYKCZImiZPyLGQBGRYFSkpSSUIxHjAc
...
9gVCPSOQUGMMZUeNYOBkTE0e+MrPGL+TqQEyIakF3rjA2PbL1uSY6d4dlCx7izkO
buEpHTPDqs9gZ3U5ht9bjES93UHnDENLopkZ2JgGwH8Y50eBnjq4xml9psbYZn5Y
yWpONE/IjIjJyww=
-----END CERTIFICATE-----
        </IMPORT_CA_CERTIFICATE>
        <IMPORT_USER_CERTIFICATE USER_LOGIN="apollo">
-----BEGIN CERTIFICATE-----
CZImiZPyLGQBGRYDTEFCMRUwEwYKCZImiZPyLGQBGRYFSkpSSUIxHjAcBgNVBAMT
ODU5NDRaMFYxEzARBgoJkiaJk
...
sjbbpNGpxGsK9GZi5j6UeOYklePyau0TJ3KIm2RPlR2C6XAGz2PTWgsxGlUP9lNH
bfz0+TD0Jsschjqk23/vr2GxQ9C/835zRxdu5Dn8JGm3/dFHR2VxgCetIxyR9TQC
ZKTfvIa8N9KvMLZdclSj94jUyMZjYYmCWULW8WySMV70nclvrsI2hi3nwMtt2Zvj
WnbeZujBX9LGz3HdmghgUw4GTwYl3ZG88snuTyXliLPFXVYXvNAhGeWqXtrh7A90
3NprjG7DM1uw
-----END CERTIFICATE-----
        </IMPORT_USER_CERTIFICATE>
    </MOD_TWOFACTOR_SETTINGS>
    </RIB_INFO>
```

```
        </LOGIN>
     </RIBCL>
```

MOD_TWOFACTOR_SETTINGS parameters

All of the following parameters are optional. If a parameter is not specified, then the parameter value for the specified setting is preserved.

AUTH_TWOFACTOR_ENABLE enables or disables Two-Factor authentication. The possible values are "Yes" and "No."

CERT_REVOCATION_CHECK causes RILOE II to use the CRL distribution point attribute of the client certificate, to download the CRL and check against revocation. The possible values are "Yes" and "No." If this setting is set to Yes, and the CRL cannot be downloaded for any reason, authentication will be denied.

CERT_OWNER_SAN causes RILOE II to extract the User Principle Name from the Subject Alternative Name, and use that for authentication with the directory, for example: username@domain.extension.

CERT_OWNER_SUBJECT causes RILOE II to derive the user's distinguished name from the subject name. For example if the subject name is "/DC=com/DC=domain/OU=organization/CN=user", RILOE II will derive: "CN=user,OU=organization,DC=domain,DC=com".

The CERT_OWNER_SAN and CERT_OWNER_SUBJECT settings are only used if directory authentication is enabled.

IMPORT_CA_CERTIFICATE imports the certificate into RILOE II as the trusted Certificate Authority. RILOE II will only allow client certificates that are issued by this CA. A Trusted CA certificate must be configured in RILOE II in order for Two-Factor authentication to function.

IMPORT_USER_CERTIFICATE imports the certificate into RILOE II and maps it to the specified local user. Any client that authenticates with this certificate will authenticate as the local user to which it is mapped. The SHA1 hash of this certificate will be displayed on the Modify User web page for the user to whom it is mapped. If RILOE II is using directory authentication, client certificate mapping to local user accounts is optional and only necessary if authentication with local accounts is desired.

The IMPORT_CA_CERTIFICATE and IMPORT_USER_CERTIFICATE settings require that base64 encoded certificate data be included between the begin and end tags.

MOD_TWOFACTOR_SETTINGS runtime errors

The possible MOD_TWOFACTOR_SETTINGS error messages include:

- RIB information is open for read-only access. Write access is required for this operation.
- This setting cannot be changed while Shared Network port is enabled.

  RILOE II has been configured to use shared network port, which will not function if Two-factor authentication is enabled

- This setting cannot be enabled unless a trusted CA certificate has been imported.

  A CA certificate must be imported before enabling Two-factor authentication.

- User does not have correct privilege for action. CONFIG_ILO_PRIV required.

Troubleshooting the RILOE II

In this section

This section discusses common issues that may arise when working with the RILOE II and offers possible causes and solutions.

Supported client operating systems and browsers

Operating system	Internet Explorer 6.0 SP1	Mozilla Firefox 1.7.5	Mozilla Firefox 1.0.2
Windows® 2000 Professional	Yes	No	No
Windows® XP	Yes	No	No
Microsoft® Windows Server™ 2003	Yes	No	NO
Red Hat Enterprise Desktop 4.00	No	No	No
Novell Linux Desktop 9	No	No	No

Supported hardware and software

You can use RILOE II in ProLiant servers and selected HP servers. For a detailed list of supported servers, See the "Server PCI slot and cable matrix (on page 174)" section.

You can use RILOE II with the following network operating systems:

- Microsoft®
  - Microsoft® Windows 2000 Server, Advanced Server (SP 3 & SP4)
  - Microsoft® Windows Server™ 2003, Standard Edition, Web Edition, Enterprise Edition, SBS Edition, x64 bit Edition (base edition and SP1)
- Novell
  - NetWare 5.1
  - NetWare 6.5
- Linux®

- Red Hat Enterprise Linux ES 2.1
- Red Hat AS 2.1 (including Update 6 & 7)
- Red Hat EL 3.0 - WS, ES, AS (including Update 4 & 5)
- SLES 8 (was UL 1.0)
- SLES 9 (base edition and SP1)

Server PCI Slot and Cable Matrix

For the most recent information, refer to the matrix at the HP website (http://www.hp.com/servers/lights-out).

📝 **IMPORTANT:** All servers support the keyboard/mouse external cable as well as the AC adapter. However, the default configuration always relies on having the internal cable connected so RILOE II can provide the virtual power buttons, Virtual Floppy, and Virtual Media USB applet. Whenever the 16- or 30-pin internal cables are used, the external cables should not be used. Frequently, customers try to use the external mouse/keyboard cables with the internal cables, causing conflicts with the mouse and keyboard functions.

Server	PCI Slot	Virtual Power Button Cable (see legend)	USB Virtual Floppy/ CD	AC Power Adapter	Keyboard Mouse Adapter Cable Required	Disable Onboard Video Using
ProLiant CL380	1	A		Yes	Yes	
ProLiant DL320	Any	B		Yes		
ProLiant DL320 G2	Any	G	Yes			
ProLiant DL360	1	C		Yes		
ProLiant DL360 G2	Any	G	Yes			
ProLiant DL360 G3	Any	G	Yes			
ProLiant DL380	1	A		Yes	Yes	
ProLiant DL380 G2	1	G	No (see note 1)			
ProLiant DL380 G3, 2.4-2.8 GHz	Any	G	No (see note 2)			
ProLiant DL380 G3, 3.06 GHz or higher	Any	G	Yes			
ProLiant DL560	Any	G (see note 3)	Yes			
ProLiant DL580	6	A		Yes	Yes	
ProLiant DL580 G2	1	G	Yes			
ProLiant DL740	Any	G	Yes			
ProLiant DL760	7, 8, 9	H		Yes		
ProLiant DL760 G2	9	G	Yes			
ProLiant ML310	Any	G	Yes			

Server	PCI Slot	Virtual Power Button Cable (see legend)	USB Virtual Floppy/ CD	AC Power Adapter	Keyboard Mouse Adapter Cable Required	Disable Onboard Video Using
ProLiant ML330	4, 5	B		Yes		Yes
ProLiant ML330 G2	5	G	Yes (see note 1)			Yes
ProLiant ML330 G3	Any	G	Yes			
ProLiant ML330e	4, 5	B		Yes		Yes
ProLiant ML350, 600-933 MHz	4, 5, 6	A		Yes	Yes	Yes
ProLiant ML350, 1 GHz	6, 7	B		Yes		Yes
ProLiant ML350 G2	6	G	Yes (see note 1)			Yes
ProLiant ML350 G3	Any	G	Yes			
ProLiant ML370	1, 2	A		Yes	Yes	
ProLiant ML370 G2	6	G	Yes (see note 1)			
ProLiant ML370 G3, 2.4-2.8 GHz	6	G	No (see note 2)			
ProLiant ML370, 3.06 GHz or higher	6	G	Yes			
ProLiant ML530	1	A		Yes	Yes	
ProLiant ML530 G2	7	G	Yes			
ProLiant ML570	6	A		Yes	Yes	
ProLiant ML570 G2	6	G	Yes			
ProLiant ML750	1, 2, 3, 4	E		Yes	Yes	
ProLiant 7000 Xeon 500 MHz	3, 4, 5, 6	None		Yes	Yes	
ProLiant 8000 Xeon	1, 2, 3, 4	E		Yes	Yes	
ProLiant 8500 Xeon (servers shipped with 550 MHz processors with configuration codes CL61, CL64, BX71, or BX72)	7, 8, 9	D		Yes	Yes	
ProLiant 8500 Xeon (server shipped with 700 MHz and higher processors)	7, 8, 9	A		Yes	Yes	

Legend: Virtual Power Button cable descriptions and part numbers

- A = P/N 160011-001 (4-pin cable) ships with the RILOE II kit.
- B = P/N 177634-001 (16-pin cable) ships with the RILOE II kit.
- C = P/N 177634-002 (16-pin cable) ships with ProLiant DL360 servers.

- D = P/N 195254-B21 (split 4-pin cable) available as a spare kit P/N 195724-001.
- E = P/N 162816-001 (split 4-pin cable) available as a spare kit P/N 166655-001.
- F = P/N 233736-001 (16-to 30-pin cable) Not used with RILOE II.
- G = P/N 241793-010 (30-pin cable) ships with the RILOE II kit.
- H = P/N 216373-001 (16-pin to 13-pin cable) ships with the ProLiant DL760 server.

Notes:

1. The USB Virtual Floppy/CD works under an operating system that natively supports USB. The USB Virtual Floppy/CD does not work until the operating system and appropriate device drivers are loaded. More information can be found at the ProLiant Support Page (http://h18013.www1.hp.com/products/servers/platforms/usb-support.html).

2. RILOE II USB Virtual Media is not supported on the ProLiant DL380 G3 and ProLiant ML370 G3 servers. For more information, refer to the HP website (http://h18000.www1.hp.com/products/servers/management/riloe2/virtualmedia.html).

3. RILOE II cards (Hardware Revisions F and earlier) do not maintain power when the ProLiant DL560 server is powered off. To resolve this issue, use a Revision G or later card or use the AC adapter in addition to the 30-pin cable to maintain power.

Network connection problems

The following sections provide troubleshooting information for common network connection problems.

Inability to connect to the board through the NIC

If you cannot connect to RILOE II through the NIC, try any or all of the following troubleshooting methods:

- Confirm that the green LED indicator (link status) on the board connector bracket 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 indicate normal network traffic.
- Run the RBSU F8 to confirm that the NIC is enabled and to verify the assigned IP address and subnet mask.
- From another workstation on the same network, ping the RILOE II IP address.
- Attempt to connect with browser software by typing the RILOE II IP address. You can see the Remote Insight home page from this address.
- Reset the RILOE II.

  To reset the RILOE II in a Windows NT® or Windows® 2000 server:

  a. In **Control Panel,** select **Services** and stop the Insight Agents.

  b. In **Control Panel,** select **Insight Agents.**

  c. Select **Remote Insight** and click **Reset.**

  d. Restart the Insight Agents.

Inability to obtain SNMP information from Insight Manager 7 when connected to the Remote Insight Network interface

The agents running on the managed server supply the SNMP information provided to Systems Insight Manager. For those agents to pass information through the RILOE II, the Remote Insight device drivers must be installed. Refer to "Installing RILOE II device drivers" for installation instructions.

If you have installed the drivers and agents for the RILOE II, verify that the RILOE II and the management PC are on the same subnet. You can verify this quickly by pinging the Remote Insight board from the management PC. See your network administrator for proper routes to access the network interface of the RILOE II.

Web browser not connecting to the RILOE II IP address

If the Web browser software is configured to use a proxy server, it will not connect to the RILOE II IP address. To resolve this issue, configure the browser not to use the proxy server for the IP address of the RILOE II. For example, in Internet Explorer, select **View, Options,** click **Connection Settings,** and then enter the IP address in the **Exceptions** field.

NOTE: If the RILOE II is using 128-bit encryption, be sure that the client browser supports 128-bit encryption.

Alert and trap problems

The following sections provide troubleshooting information for common alert and trap errors.

Inability to Receive Insight Manager 7 Alerts (SNMP Traps) from the RILOE II

1. Be sure that the correct Systems Insight Manager alert types are enabled.
2. Log on to the RILOE II with administrative access.
3. Click **SNMP Settings** on the Administration tab.
4. Enter the SNMP IP addresses in the SNMP Trap Destination fields.

Server power status reported incorrectly and send test trap not responding

The power status of the server may be reported as off when the server is actually on. This problem may occur if the server is powered off and then powered back on within four minutes. The following configuration will cause this error to occur:

- The supplied DNS server IP address on the Network Settings page is invalid or unavailable.
- An SNMP trap destination is set as a DNS name is invalid or unavailable.
- Remote Insight Board SNMP Traps are enabled with no destination address defined.

If the preceding configuration is set, Send Test Trap also will not respond for a period of approximately four minutes.

To correct this problem, be sure the DNS server specified in Network Settings is correct. If a DNS server is not on the network, the setting should be 0.0.0.0. Alternately, use IP addresses instead of DNS names when configuring SNMP trap destinations.

NetWare initialization errors

When a NetWare server is started, each driver loaded in the AUTOEXEC.NCF is executed. If a problem is found during execution, an initialization error is displayed. The NetWare error messages table ("NetWare error message table" on page 178) shows potential initialization error messages and suggested courses of action.

NetWare error message table

Error message	Action
Adapter IRQ or memory settings not set	Run the System Configuration Utility.
Unable to allocate resource tag	Apply any relevant NetWare patches. Contact your service provider.
Unable to register NetWare hardware options	Apply any relevant NetWare patches. Run Diagnostics on the RILOE II.
Remote Insight interface type unknown	Upgrade CPQRI.NLM to a newer version.
Unable to initialize the RILOE II	Run Diagnostics on the RILOE II.
Unable to allocate memory	Check available NetWare resources.
RILOE II not found	The RILOE II board is not installed in the server. The board must be installed before loading the device driver.

Miscellaneous problems

The following sections provide troubleshooting information for miscellaneous errors.

Accessing System Partition Utilities

When booting a ProLiant server configured with a RILOE II and **F10** is selected to access the System Partition Utilities, an error message may be displayed stating that the system is not configured. The error message is false. The server is properly configured.

After entering the date and time and pressing **Enter,** the server immediately reboots. The System Partition Utility options are never displayed. The problem recurs on subsequent reboots when **F10** is pressed.

📝 **NOTE:** The problem does not occur when pressing **F8** to access RBSU.

To access the System Partition Utilities:

1. Remove the RILOE II and reboot the server.
2. Press **F10** to access the System Partition Utilities.

Inability to reboot the server

If you added the RILOE II board to a previously configured server, run RBSU F8 to properly configure the RILOE II with the server information. See Configuring the RILOE II (on page 19) for more information on using RBSU F8.

Make sure the RILOE II is installed in a supported PCI slot. For more information, See the "Server PCI slot and cable matrix" ("Server PCI Slot and Cable Matrix" on page 174) to verify the PCI slot configuration for the server. If the server is not listed, See the HP website (http://www.hp.com/servers/lights-out) for an updated table.

When using the Virtual Power Button feature, verify that the Remote Insight internal cable or Virtual Power Button cable is installed correctly.

Inability to upgrade the RILOE II firmware

If you attempt to upgrade the firmware of the RILOE II, and the board does not respond or does not accept the firmware upgrade, you must force the ROM upgrade procedure by changing the default switch settings of SW3 ("Switch settings (SW3) to force ROM upgrade" on page 179). Upgrade the firmware of the RILOE II by downloading the RILOE II Smart Component available on the HP website (http://www.hp.com).

1. Download and extract the Smart Component.
2. Use the `makedisk.bat` file to create a bootable firmware diskette.
3. Insert the bootable diskette into the host server.
4. Power on the server.
5. Follow the onscreen instructions to upgrade the RILOE II firmware.

When the firmware upgrade is complete, return the switches to the factory default position.

Switch settings (SW3) to force ROM upgrade

Switch	Default	Force ROM upgrade
1	OFF	OFF
2	OFF	OFF
3	OFF	ON
4	OFF	OFF

Incorrect time or date of entries in the event log

The time and date are updated by Insight Management agents on supported network operating systems. The RILOE II time and date are updated at boot time and the agents automatically update the time and date periodically.

Interpreting LED indicators

The LED indicators are located on the front of the RILOE II board. The LED indicators have the following assignments.

FB	7	6	5	4	3	2	1	0

During initial boot of the RILOE II, the LED indicators flash randomly. After the board has booted, the 7 LED flashes every second and the other LED indicators (0 through 6) light up. The FB LED lights up after the system has booted to indicate a hardware failure.

If a hardware failure is detected, reset RILOE II. See "Resetting the RILOE II to factory default settings" for more information. If you continue to have problems, you can contact HP technical support or visit the HP website (http://www.hp.com).

Invalid Source IP address

An `Invalid Source IP address` error might display on the login screen if caching is enabled in the Java Plug-in Control Panel applet for Java™ Plug-in 1.4.1. Although this error message appears, authentication will work properly. To resolve this issue, deselect the enable caching checkbox located on

the cache tab of the Java™ Plug-in Control Panel applet. This should be done for all clients that connect to RILOE II.

Login name and password problems

If you have connected to the board but it does not accept your login name and password, you must verify that your login information is configured correctly. Connect to the RILOE II using your browser, log in with a user name that has administrative access, and reenter the login name and password that are not being accepted.

NOTE: The login name and password are case sensitive. The RBSU F8 can also be used to correct login problems. After five login attempts, the board times out and it may take a minute for it to reset.

Remote Console mouse control issue

While using Remote Console on a server running Microsoft® Windows® Server 2003, mouse movement can be slow, and it might be difficult to navigate to each of the four corners of the screen. When trying to reach a far corner of the screen, the mouse can disappear completely.

NOTE: This mouse behavior is more pronounced when the Remote Console session is running in a browser applet window that is smaller than the size of the server screen, and scrolling is required to see the full contents of the screen, which are not displayed.

To resolve this issue:

1. Select **Start>Settings>Control Panel>Mouse Properties** from the Windows® Server 2003 desktop applet.
2. Disable the Enhance pointer precision parameter.

If mouse movement is still sluggish:

1. Select **Start>Settings>Control Panel>Display>Settings>Advanced>Troubleshooting>** from the Windows® Server 2003 desktop applet.
2. Set the slider control to full hardware acceleration.

For more information, refer to the "Optimizing performance for graphical Remote Console (on page 37)" section.

Resetting the RILOE II to Factory Default Settings

1. Log into the RILOE II web agents.
2. Select **Tasks>Remote Management>Remote Insight Options.**
3. Click **Reset RILOE II.**

Resetting RILOE II to the factory defaults erases all existing user account, password, and security settings. Be sure the default user account and password information is available.

Virtual Floppy media applet is unresponsive

RILOE II Virtual Floppy media applet can become unresponsive if the physical floppy diskette contains media errors.

To prevent the virtual floppy media applet from becoming unresponsive, run CHKDSK.EXE (or a similar utility) to check the physical floppy diskette media for errors. If the physical media contains errors, reload the floppy diskette image onto a new physical floppy diskette.

Video Problems

The RILOE II contains an integrated VGA controller. When the RILOE II is first installed, the server detects this controller and attempts to use it by switching video from the embedded video controller of the server. To avoid this problem, be sure that your monitor is connected to the RILOE II. Refer to "Monitor Cable Connection" for more information.

Some servers contain PCI-based VGA controllers. These controllers must be removed to configure the VGA controller on the RILOE II board.

Be sure the RILOE II is installed in a supported PCI slot. Refer to the Server PCI Slot and Cable Matrix (on page 174) to determine the correct slot for the server. If the server is not listed, refer to the HP website (http://www.hp.com/servers/lights-out) for an updated table.

Some servers require disabling of the embedded video before installing the RILOE II board. You can disable the embedded video controller by powering off the server and setting the system configuration maintenance switch 1 to ON.

The following servers require that the embedded video be disabled:

- ProLiant ML330 server
- ProLiant ML350 server

Troubleshooting the host server

The RILOE II provides features for proactive system management and efficient troubleshooting of server problems.

In addition to the Remote Console, you have access to overall server status information, video replay of previous server resets, and other information gathered by the Survey utility.

The RILOE II maintains a complete set of logs for troubleshooting server problems. These logs are the Remote Insight Event Log and the Integrated Management Log.

Full integration with Systems Insight Manager provides warning of potential problems through SNMP trap alerts displayed on an Systems Insight Manager. This integration is achieved by installing and configuring HP Insight agents on the remote server.

Additional information on the state of the host server

The **Server Status** option provides comprehensive status information about the following items:

- Server information
- POST diagnostic results

Information logs

The **System Status** tab gives you access to two types of information logs that are useful when troubleshooting host server problems:

- **Integrated Management Log (IML)**

  The IML allows you to view logged remote server events. Logged events include all server-specific events recorded by the system health driver, including operating system information and ROM-based POST codes.

- **Remote Insight Event Log**

  The Remote Insight Event Log ("Event Log Entries" on page 182) is an operating system-independent log that maintains a record of events by date and time. Logged events include major server events,

such as a server power outage or a server reset, and Remote Insight events, such as a loose cable or an unauthorized login attempt.

Integrated Management Log

RILOE II manages the IML of the server, which can be accessed by using a supported browser, even when the server is not operational. This capability can be helpful when troubleshooting remote host server problems.

The IML enables you to view logged remote server events. Logged events include all server-specific events recorded by the system health driver, including operating system information and ROM-based POST codes. For more information, refer to the server guide.

1. Click **Clear Event Log** to clear the event log of all previously logged information.

2. Click **OK** to confirm that you want to clear the event log. A line indicating that the log has been cleared is logged.

Event Log Entries

The following table lists Event Log displays and explanations to help you troubleshoot the RILOE II board. In the table, *USER*, *#*, and *IP address* are used to designate that a specific user, number, or IP address is displayed, as appropriate.

Event Log Display	Event Log Explanation
Server power failed	Appears when the server power fails.
Browser login: IP address	Displays the IP address for the browser that logged in.
Server power restored	Appears when the server power is restored.
Browser logout: IP address	Displays the IP address for the browser that logged out.
Server reset	Appears when the server is reset.
Failed Browser login - IP Address: IP address	Appears when a browser login fails.
Remote Insight Self-Test Error: #	Appears when the Remote Insight board has failed an internal test. The probable cause is that a critical component has failed. Further use of this board is not recommended.
Remote Insight Board reset	Appears when the board is reset.
On-board clock set; was #:#:#:#:#:#	Appears when the onboard clock is set.
Server logged critical error(s)	Appears when the server logs critical errors.
Event log cleared by: USER	Appears when a user clears the event log.
Keyboard cable disconnected	Appears when the keyboard cable is disconnected.
Keyboard cable connected	Appears when the keyboard cable is connected.
Remote Insight Board reset to factory defaults	Appears when the board is reset to the default settings.

Event Log Display	Event Log Explanation
Remote Insight Board reset	Appears when the board is reset.
Remote Insight ROM upgrade to #	Is displayed when the ROM has been upgraded.
Remote Insight Board reset for ROMPAQ upgrade	Appears when the board is reset for the ROM upgrade.
Remote Insight Board reset by user diagnostics	Is displayed when the board is reset by a user diagnostics session.
Power restored to Remote Insight Board	Appears when the power is restored to the board.
Remote Insight Board reset by watchdog	Appears when a noncritical error has occurred in the Remote Insight board, and the board has automatically reset itself. If this action persists, call customer support.
Remote Insight Board reset by host	Appears when the board is reset by the server.
Recoverable Remote Insight Error, code #	Appears when a noncritical error has occurred in the Remote Insight board, and the board has automatically reset itself. If this action persists, call customer support.
SNMP trap delivery failure: IP address	Appears when the SMNP trap does not connect to the specified IP address.
Test SNMP trap alert failed for: IP address	Appears when the SNMP trap does not connect to the specified IP address.
Power outage SNMP trap alert failed for: IP address	Appears when the SNMP trap does not connect to the specified IP address.
Server reset SNMP trap alert failed for: IP address	Appears when the SNMP trap does not connect to the specified IP address.
Illegal login SNMP trap alert failed for: IP address	Appears when the SNMP trap does not connect to the specified IP address.
Keyboard cable SNMP trap alert failed for: IP address	Appears when the SNMP trap does not connect to the specified IP address.
Diagnostic error SNMP trap alert failed for: IP address	Appears when the SNMP trap does not connect to the specified IP address.
Host generated SNMP trap alert failed for: IP address	Appears when the SNMP trap does not connect to the specified IP address.
Remote Insight network link up	Appears when the network is connected to the board.
Remote Insight network link down	Appears when the network is not connected to the board.
Mouse cable SNMP trap alert failed for: IP address	Appears when the SNMP trap does not connect to the specified IP address.
Mouse cable connected	Appears when the mouse cable is connected.
Mouse cable disconnected	Appears when the mouse cable is disconnected.
External power adapter connected	Appears when the external power adapter is connected.

Event Log Display	Event Log Explanation
External power adapter disconnected	Appears when the external power adapter is disconnected.
RIB Firmware upgrade started from browser by: USER	Appears when a user starts a firmware upgrade.
Remote Floppy Inserted by: USER	Is displayed when a user inserts the remote floppy.
Host server reset by: USER	Appears when a user resets the host server.
Host server powered OFF by: USER	Appears when a user powers off a host server.
Host server powered ON by: USER	Is displayed when a user powers on a host server.
Virtual Floppy Inserted by: USER	Appears when a user inserts a Virtual Floppy.
Remote Console login: USER	Is displayed when a user logs on to a Remote Console.
Remote Console Closed	Appears when a Remote Console is closed.
Failed Console login - IP Address: IP address	Displays a failed console login and IP address.
Handheld login: IP address	Appears when a handheld logs in.
Handheld logout: IP address	Appears when a handheld logs out.
Failed Handheld login - IP Address: IP address	Displays a failed handheld login and IP address.
Added User: User	Appears when a user adds a user.
User Deleted by: USER	Appears when a user deletes a user.
Modified User: USER	Appears when a user modifies a user.
XML login: USER	Appears when a user logs on.
Failed XML login: USER	Appears when a user's login fails.
XML: Modified USER	Appears when a user modifies a user.
RIB Firmware upgrade started from XML by: USER	Appears when a firmware upgrade is started.
XML: Added User: USER	Appears when a user adds a user.
XML: User Deleted: USER	Appears when a user deletes a user.
User has been deleted	Appears when a user has been deleted.
System PCI config error, Code	Appears when there is a PCI configuration error.
Subsystem Failure, Code	Displays subsystem failures. For more information, refer to the Subsystem Failure Codes (on page 184) table.

Subsystem Failure Codes

Server failures can cause certain subsystems of the RILOE II to initialize incorrectly. The RILOE II event log will report RILOE II initialization errors, not server initialization errors.

Code		
1	VGA PCI initialization error	• HOST server PCI bus is not functioning correctly • RILOE II PCI bus is not functioning correctly • VGA is not functioning correctly
2	IRC PCI initialization error	• HOST server PCI bus is not functioning correctly • RILOE II PCI bus is not functioning correctly • IRC is not functioning correctly
3	IRC initialization error	IRC is not functioning correctly
4	Video initialization error	Video is not functioning correctly
5	Keyboard system initialization error	Keyboard system is not functioning correctly
6	Telnet system initialization error	Telnet system is not functioning correctly
7	Remote Console system initialization error	Remote Console system is not functioning correctly

Restarting the host server

An administrator can restart the host server by using the options listed on the **Virtual Devices** tab:

- **Turn Server Power ON/OFF**—Turns server power on or off, if the host server Virtual Power Button was enabled.

  Clicking **Turn Server Power ON/OFF** is analogous to pressing the physical power button of the host server.

IMPORTANT: Using the **Virtual Power Button** option does not gracefully shut down the host server operating system. For a graceful shutdown of a server operating system, use HP Insight Manager or the Remote Console before using the **Virtual Power Button** option.

- **Power Cycle Server**—Performs a hardware-level cold boot reset and is available regardless of the condition of the host server or the operating system.

To power cycle a host server:

1. Click **Power Cycle Server** on the **Virtual Power** screen. A confirmation screen is displayed, followed by a warning.
2. Click **Confirm** to begin rebooting the host server.

After the host server reboots, a Remote Console session begins, allowing you to observe ROM-based POST messages and operating system load messages.

Directory Services errors

The following are the most common Directory Services LDAP errors.

- Directory Server Connect Failed
- Invalid Credentials
- Invalid Directory server address or port
- Directory Server Timeout

- Unauthorized, couldn't find RIB object
- Unauthorized, no readable roles
- Unable to read restrictions on object
- Time Restriction Not Satisfied
- IP Restriction Not Satisfied
- Unauthorized

Directory Server connect failed

The RILOE II was not able to connect to the LDAP server. Be sure that the Directory Server Address on the RILOE II Directory Settings Screen is correct, and that the port number corresponds to the LDAP SSL port number used by that directory server, usually port 636. If the directory server address is a DNS name, be sure that the DNS server is properly configured on the RILOE II Network Setting Screen, and that the DNS name of the directory server resolves to the appropriate address using "nslookup" or a similar tool.

Many SSL problems are reported with this error; be sure your directory server is properly configured for LDAP SSL connections. Refer to the installation prerequisites for Active Directory ("Active Directory installation prerequisites" on page 83) or eDirectory for more information on testing LDAP SSL configurations.

Invalid credentials

The directory server has denied the authentication request. If configured, check the searchable contexts to be sure the user exists in one of those contexts, or try specifying a fully distinguished name. Directory servers will deny the authentication request if the user account has been disabled, locked out, or is otherwise prevented from authenticating due to network address or time restrictions placed on the account.

This error is common on eDirectory when periods are used to separate the name components, or the components are partially specified. LDAP distinguished name components are separated by commas, not periods, and must be preceded by cn=, or appropriate naming attribute name.

NOTE: The short form of the login name by itself does not tell the directory which domain you are trying to access. You must provide the domain name or use the LDAP distinguished name of your account.

Invalid Directory Server address or port

The specified Directory Server address was empty, or the port number was set to 0. Specify the correct server address or port.

Directory Server timeout

The server did not acknowledge the bind request within a reasonable amount of time, normally 20 seconds. The server may be under heavy load or otherwise unwilling to process the request. Try again later.

This error can also occur if the Directory Server address and port correspond to a service other than LDAP SSL.

Unauthorized, couldn't find RILOE II object

An error occurred while trying to read the RILOE II object. Be sure that the distinguished name specified in the Directory Settings screen matches the location of the object within the directory. The distinguished name must be a fully distinguished LDAP name.

Unauthorized, no readable roles

An error occurred while reading a ROLE object. The object does not exist, or the current user is not authorized to read it. This error is common for users that are not members of all the roles that are managing the RILOE II.

Unable to read restrictions on object

A ROLE object had no readable value for the Time Restriction attribute. The role was subsequently invalidated. This error is common for users that are not members of all the roles that are managing the RILOE II.

Time restriction not satisfied

No roles that manage the RILOE II were granted sufficient rights to authenticate, and at least one of the roles was invalidated because the Time Restriction was not set or specifically disallowed the current time. If the RILOE II host server has never booted or has an incorrect clock, then the RILOE II clock will also be incorrect. Time Restrictions are always applied in RILOE II local time. Be sure that the RILOE II is in the appropriate time zone.

IP restriction not satisfied

A ROLE was invalidated because the IP restrictions demanded it. If a client has been excluded or included on a role on the basis of a DNS name, be sure that the DNS server used by the RILOE II returns the correct hostname.

Unauthorized

None of the roles found were granted the LOGIN right. Correct the roles associated with the RILOE II.

Directory Services schema

HP Management Core LDAP OID classes and attributes

Changes made to the schema during the schema setup process include changes to the:

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 defines 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 using 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 using 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 using 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 defines 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 hpqTarget objects to which this object belongs.
Syntax	Distinguished Name—1.3.6.1.4.1.1466.115.121.1.12
Options	Multi Valued
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	Multi Valued
Remarks	None

hpqRoleIPRestrictionDefault

OID	1.3.6.1.4.1.232.1001.1.1.2.4
Description	A Boolean representing access by unspecified clients which 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, then IP restrictions will be satisfied for unexceptional network clients. If this attribute is FALSE, then 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, domain, address ranges, and subnets which 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	Multi Valued
Remarks	This attribute is only used on role objects. IP restrictions are satisfied when the address matches and general access is denied, and unsatisfied when the address matches and general access is allowed. Values are an identifier byte followed by a type-specific number of bytes specifying 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 a * (ASCII 0x2A), to indicate they should match all names which 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 seven 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 only used on ROLE objects.
	Time restrictions are satisfied when the bit corresponding to the current local side real 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 12 midnight to Sunday 12:30 AM.
	• Each more significant bit and sequential byte corresponds to the next consecutive half-hour blocks within the week.
	• The most significant (8th) bit of the 42nd byte corresponds to Saturday at 11:30 PM to Sunday at 12 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	1.3.6.1.4.1.232.1001.1.8.2.1
hpqLOMRightRemoteConsole	1.3.6.1.4.1.232.1001.1.8.2.2
hpqLOMRightVirtualMedia	1.3.6.1.4.1.232.1001.1.8.2.3
hpqLOMRightServerReset	1.3.6.1.4.1.232.1001.1.8.2.4
hpqLOMRightLocalUserAdmin	1.3.6.1.4.1.232.1001.1.8.2.5
hpqLOMRightConfigureSettings	1.3.6.1.4.1.232.1001.1.8.2.6

Lights-Out Management class definitions

The following 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 defines the Lights-Out Management core class attributes.

hpqLOMRightLogin

OID	1.3.6.1.4.1.232.1001.1.8.2.1
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	1.3.6.1.4.1.232.1001.1.8.2.2
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 only used on ROLE objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightVirtualMedia

OID	1.3.6.1.4.1.232.1001.1.8.2.3
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	1.3.6.1.4.1.232.1001.1.8.2.4
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 only used on ROLE objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightLocalUserAdmin

OID	1.3.6.1.4.1.232.1001.1.8.2.5
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 only used on ROLE objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightConfigureSettings

OID	1.3.6.1.4.1.232.1001.1.8.2.6
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 only used on ROLE objects. If this attribute is TRUE, members of the role are granted the right.

Technical support

In this section

Before you contact HP

Be sure to have the following information available before you call HP:

- Technical support registration number (if applicable)
- Product serial number
- Product model name and number
- Applicable error messages
- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level

HP contact information

For the name of the nearest HP authorized reseller:

- In the United States, refer to the HP US service locator webpage (http://www.hp.com/service_locator).
- In other locations, refer to the HP website (http://www.hp.com).

For HP technical support:

- In North America:
  - Call 1-800-HP-INVENT (1-800-474-6836). This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored.
  - If you have purchased a Care Pack (service upgrade), call 1-800-633-3600. For more information about Care Packs, refer to the HP website (http://www.hp.com).
- Outside North America, call the nearest HP Technical Support Phone Center. For telephone numbers for worldwide Technical Support Centers, refer to the HP website (http://www.hp.com).

Regulatory compliance notices

In this section

Federal Communications Commission notice

Part 15 of the Federal Communications Commission (FCC) Rules and Regulations has established Radio Frequency (RF) emission limits to provide an interference-free radio frequency spectrum. Many electronic devices, including computers, generate RF energy incidental to their intended function and are, therefore, covered by these rules. These rules place computers and related peripheral devices into two classes, A and B, depending upon their intended installation. Class A devices are those that may reasonably be expected to be installed in a business or commercial environment. Class B devices are those that may reasonably be expected to be installed in a residential environment (for example, personal computers). The FCC requires devices in both classes to bear a label indicating the interference potential of the device as well as additional operating instructions for the user.

Class A equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at personal expense.

Class B equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit that is different from that to which the receiver is connected.

- Consult the dealer or an experienced radio or television technician for help.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Hewlett-Packard Company may void the user's authority to operate the equipment.

Declaration of conformity for products marked with the FCC logo, United States only

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For questions regarding this product, contact us by mail or telephone:

- Hewlett-Packard Company
  P. O. Box 692000, Mail Stop 530113
  Houston, Texas 77269-2000
- 1-800-HP-INVENT (1-800-474-6836). (For continuous quality improvement, calls may be recorded or monitored.)

For questions regarding this FCC declaration, contact us by mail or telephone:

- Hewlett-Packard Company
  P. O. Box 692000, Mail Stop 510101
  Houston, Texas 77269-2000
- 1-281-514-3333

To identify this product, refer to the part, series, or model number found on the product.

Canadian notice (Avis Canadien)

Class A equipment

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Class B equipment

This Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union regulatory notice

$C\!\in$

This product complies with the following EU Directives:

- Low Voltage Directive 73/23/EEC

- EMC Directive 89/336/EEC

CE Compliance of this product is valid only if powered with the correct HP-provided and CE marked AC adapter.

If this product has telecommunication functionality, it also complies with the essential requirements of:

- R&TTE Directive 1999/5/EC

$$CE (XXXX\text{\textasteriskcentered}) \textcircled{!}$$

*For a notified body number refer to the product regulatory label.

Compliance with these directives implies conformity to harmonized European standards (European Norms) which are listed on the EU Declaration of Conformity issued by Hewlett-Packard for this product or product family.

The telecommunications functionality of this product may be used in the following EU and EFTA countries:

Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, and United Kingdom.

Notice for use in France and Italy

Italy:

Per l'uso del prodotto, è necessaria una concessione ministeriale. Si consiglia di verificare con il distributore di fiducia o direttamente presso la Direzione Generale Pianificazione e Gestione Frequenze.

License required for use. Verify with your dealer or directly with General Direction for Frequency Planning and Management (Direzione Generale Pianificazione e Gestione Frequenze).

France:

L'utilisation de cet equipement (2.4GHz Wireless LAN) est soumise a certaines restrictions: Cet equipement peut etre utilise a l'interieur d'un batiment en utilisant toutes les frequences de 2400 a 2483.5MHz (Chaine 1-13). Pour une utilisation en environement exterieur, vous devez utiliser les frequences comprises entre 2454-2483.5MHz (Chaine 10-13). Pour les dernieres restrictions, voir http://www.art-telecom.fr.

For 2.4 GHz Wireless LAN operation of this product certain restrictions apply: This product may be used indoor for the entire 2400-2483.5 MHz frequency band (channels 1-13). For outdoor use, only 2454-2483.5 MHz frequency band (channels 10-13) may be used. For the latest requirements, see http://www.art-telecom.fr.

Notice for products incorporating 5GHz Wireless LAN devices

Frequency availability for 802.11a or 802.11h Wireless LAN is not currently harmonized throughout the European Union. For compliance requirements, users should verify with their supplier, local HP office or Telecommunications authority.

BSMI notice

警告使用者:

這是甲類的資訊產品，在居住的
環境中使用時，可能會造成射頻
干擾，在這種情況下，使用者會
被要求採取某些適當的對策。

Japanese notice

ご使用になっている装置にVCCIマークが付いていましたら、次の説明文を
お読み下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準
に基づくクラスB情報技術装置です。この装置は、家庭環境で使用すること
を目的としていますが、この装置がラジオやテレビジョン受信機に近接して
使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

VCCIマークが付いていない場合には、次の点にご注意下さい。

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に
基づくクラスA情報技術装置です　この装置を家庭環境で使用すると電波
妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ず
るよう要求されることがあります。

Acronyms and abbreviations

ASCII

American Standard Code for Information Interchange

ASM

Advanced Server Management

CA

certificate authority

CR

Certificate Request

DHCP

Dynamic Host Configuration Protocol

DLL

dynamic link library

DNS

domain name system

EMS

Emergency Management Services

GUI

graphical user interface

HPQLOMGC

HP Lights-Out Migration Command Line

HPQLOMIG

HP Lights-Out Migration

iLO

Integrated Lights-Out

IML

Integrated Management Log

IP

Internet Protocol

LDAP

Lightweight Directory Access Protocol

LED

light-emitting diode

LOM

Lights-Out Management

MMC

Microsoft® Management Console

NIC

network interface controller

PCI

peripheral component interface

PERL

Practical Extraction and Report Language

POST

Power-On Self Test

PSP

ProLiant Support Pack

RBSU

ROM-Based Setup Utility

RDP

Remote Desktop Protocol

RIB

Remote Insight Board

RIBCL

Remote Insight Board Command Language

RILOE

Remote Insight Lights-Out Edition

RSM

Remote Server Management

SNMP

Simple Network Management Protocol

SSL

Secure Sockets Layer

UID

unit identification

USB

universal serial bus

XML

extensible markup language

Index

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com