HP Integrated Lights-Out 2 User Guide

HP Part Number: 394326-403
Published: June 2012
Edition: 1



© Copyright 2012 Hewlett-Packard Development Company, L.P

Notices

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

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Microsoft, Windows, Windows Server, Windows Vista, Windows NT, and Windows XP are U.S. registered trademarks of Microsoft Corporation. AMD is a trademark of Advanced Micro Devices, Inc. Intel is a trademark of Intel Corporation in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates.

Intended audience

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

1 Overview....11
New in this release of iLO 2....11
iLO 2 Overview....11
Differences between iLO 2 and iLO....12
HP Insight Control server deployment....12
Server management through IPMI version 2.0 compliant applications....13
WS-Management compatibility overview....13
iLO 2 browser interface overview....14
Supported browsers and client operating systems....15
Supported server operating system software....15
2 Setting up iLO 2....17
Quick setup....17
Preparing to set up iLO 2....17
Connecting to the network....18
Configuring the IP address....19
Logging in to iLO 2 for the first time....20
Setting up user accounts....20
Setting up iLO 2 using iLO 2 RBSU....20
Setting up iLO 2 with the browser-based option....21
Activating iLO 2 licensed features with a browser....21
Installing iLO 2 device drivers....21
Microsoft device driver support....22
Linux device driver support....22
Novell NetWare device driver support....22
3 Configuring iLO 2....24
iLO 2 configuration overview....24
Upgrading iLO 2 firmware....24
Upgrading iLO 2 with a browser....25
Updating the firmware using the maintenance CD....25
Recovering from a failed iLO 2 firmware update....26
Downgrading the iLO 2 firmware....26
Licensing....26
User administration....28
Adding a new user....29
Viewing or modifying existing user settings....31
Deleting a user....31
Group administration....32
Configuring iLO 2 access....33
Services options....33
Terminal Services Passthrough option....35
Terminal Services client requirements....35
Enabling the Terminal Services Passthrough option....36
Terminal Services warning message....37
Terminal Services Passthrough option display....37
Remote Console and Terminal Services clients....37
Terminal Services troubleshooting....38
Access options....38
iLO 2 Remote Console and Remote Serial Console access....41
Security....41
General security guidelines....41

Password guidelines....42
Securing RBSU....42
iLO 2 Security Override Switch administration....42
Trusted Platform Module support....43
User accounts and access....43
Privileges....44
Login security....44
SSH key administration....44
SSL certificate administration....45
Two-factor authentication....46
Setting up two-factor authentication for the first time....47
Setting up a user for two-factor authentication....48
Two-factor authentication login....49
Using two-factor authentication with directory authentication....50
Directory settings....51
Configuring directory settings....51
Directory tests....53
Encryption....53
Encryption settings....54
Connecting to the iLO 2 using AES/3DES encryption....54
HP SIM single sign-on (SSO)....55
Setting up iLO 2 for HP SIM SSO....55
Adding HP SIM trusted servers....56
Setting up HP SIM SSO....57
Remote Console Computer Lock....58
Network....60
Network Settings....60
iLO 2 subsystem name limitations....61
iLO 2 Shared Network Port....61
iLO 2 Shared Management Port features and restrictions....62
Enabling the iLO 2 Shared Network Port feature....62
Re-enabling the dedicated iLO 2 management port....63
DHCP/DNS Settings....64
SNMP/Insight Manager settings....65
Enabling SNMP alerts....65
SNMP generated trap definitions....66
Configuring Insight Manager integration....67
Static IP bay configuration....68
Configuring a ProLiant BL p-Class blade enclosure....68
Configuring static IP bay settings....69
ProLiant BL p-Class standard configuration parameters....69
ProLiant BL p-Class advanced configuration parameters....69
Enabling iLO 2 IP address assignment....70
HP BladeSystem setup....70
The iLO 2 firmware configuration screen....71
Verify Server RAID Configuration screen....71
Connect Virtual Media screen....72
Install Software screen....72
iLO 2 diagnostic port configuration parameters....72
4 Using iLO 2....74
System status and status summary information....74
System Information Summary....75
Fans....76
Temperatures....76

Power....77
Processors....77
Memory....77
NIC....77
iLO 2 Log....77
IML....78
Diagnostics....79
Insight Agents....80
iLO 2 Remote Console....80
Remote Console overview and licensing options....81
Remote Console settings....81
Remote console hot keys....83
Supported hot keys....84
Hot keys and international keyboards....85
Hot keys and Virtual Serial Port....85
IRC Fullscreen....85
Integrated Remote Console option....85
Optimizing mouse performance for Remote Console or Integrated Remote Console....88
High Performance Mouse settings....88
Multi-user access to the Integrated Remote Console....89
Using Console Capture....90
Using HP iLO Video Player....90
iLO Video Player user interface....91
iLO Video Player controls....92
Acquiring the Remote Console....92
Remote Console....93
Remote Console features and controls....94
Recommended client settings....94
Recommended server settings....95
Microsoft Windows Server 2003 settings....95
Red Hat Linux and SUSE Linux server settings....95
Text-based remote console overview....95
Text-based console during POST....95
Text-based console after POST....96
Using the iLO 2 Text Console....97
Customizing iLO 2 Text Console....97
Using a Linux session....99
Virtual serial port and remote serial console....99
Remote Serial Console....100
Virtual Serial Port enhancements....101
Windows EMS Console....102
Virtual media....104
Using iLO 2 Virtual Media devices....104
Virtual Media and Windows 7....105
iLO 2 Virtual Floppy/USBKey....105
Virtual Floppy/USB Key operating systems notes....106
Operating system USB support....107
Mounting USB Virtual Floppy/USBKey in NetWare 6.5....107
Mounting USB Virtual Media/USBKey in Linux....108
Changing diskettes....109
iLO 2 Virtual CD/DVD-ROM....109
Virtual Media CD/DVD-ROM operating system notes....110
Mounting USB Virtual Media CD/DVD-ROM in Linux....110
Creating iLO 2 disk image files....111
Virtual folder....111

Virtual folder operating system notes....112
Power management....112
Server power settings....113
Server power data....115
Processor states....116
Power efficiency....117
Graceful shutdown....118
Brown-Out recovery....119
ProLiant BL p-Class Advanced management....119
Rack View....120
Blade configuration and information....121
Enclosure information....122
Power enclosure information....122
Network component information....123
iLO 2 control of ProLiant BL p-Class server LEDs....123
Server POST tracking....123
Insufficient power notification....124
ProLiant BL p-Class alert forwarding....124
ProLiant BladeSystem HP Onboard Administrator....124
iLO 2 BL c-Class tab....124
Enclosure bay IP addressing....125
Dynamic power capping for server blades....127
iLO 2 Virtual Fan....128
iLO option....128
Web Administration....128
BL p-Class and BL c-Class features....129
5 Directory services....130
Overview of directory integration....130
Benefits of directory integration....130
Advantages and disadvantages of schema-free directories and HP schema directory....131
Schema-free directory integration....131
Setting up Schema-free directory integration....132
Active Directory preparation....132
Introduction to certificate services....132
Installing certificate services....132
Verifying certificate services....133
Configuring Automatic Certificate Request....133
Schema-free browser-based setup....133
Schema-free scripted setup....133
Schema-free HPLOMIG-based setup....134
Schema-free setup options....134
Schema-free nested groups....135
Setting up HP schema directory integration....136
Features supported by HP schema directory integration....136
Setting up directory services....136
Schema documentation....137
Directory services support....137
Schema required software....137
Schema installer....138
Schema Preview....138
Setup....138
Results....139
Management snap-in installer....140
Directory services for Active Directory....140

Active Directory installation prerequisites....140
Installing Active Directory on Windows Server 2008....141
Directory services preparation for Active Directory....141
Snap-in installation and initialization for Active Directory....142
Example: Creating and configuring directory objects for use with iLO 2 in Active Directory....143
Directory services objects....145
Active Directory snap-ins....146
Active Directory role restrictions....147
Active Directory Lights-Out management....148
Directory services for eDirectory....149
eDirectory installation prerequisites....149
Snap-in installation and initialization for eDirectory....150
Creating and configuring directory objects for use with LOM devices in eDirectory....150
Directory Services objects for eDirectory....152
Role managed devices....152
Members....153
eDirectory Role Restrictions....154
Time restrictions....154
Enforced client IP address or DNS name access....154
eDirectory Lights-Out Management....155
User login using directory services....156
Directory-enabled remote management....156
Introduction....156
Creating roles to follow organizational structure....157
Using existing groups....157
Using multiple roles....157
How directory login restrictions are enforced....158
Restricting roles....158
Role time restrictions....159
Role address restrictions....159
User restrictions....159
User address restrictions....159
How user time restrictions are enforced....160
Creating multiple restrictions and roles....160
Using bulk import tools....161
HPLOMIG directory migration utility....162
Introduction to HPLOMIG utility....162
Compatibility....162
HP Lights-Out directory package....163
Using HPLOMIG....163
Finding management processors....163
Upgrading firmware on management processors....165
Selecting a directory access method....166
Naming management processors....167
Configuring directories when HP Extended schema is selected....168
Configuring directories when schema-free integration is selected....169
Setting up management processors for directories....170
Directory services schema....171
HP Management Core LDAP OID classes and attributes....171
Core classes....172
Core attributes....172
Core class definitions....172
hpqTarget....172
hpqRole....172
hpqPolicy....173

Core attribute definitions....173
hpqPolicyDN....173
hpqRoleMembership....173
hpqTargetMembership....173
hpqRoleIPRestrictionDefault....173
hpqRoleIPRestrictions....174
hpqRoleTimeRestriction....174
Lights-Out Management specific LDAP OID classes and attributes....175
Lights-Out Management classes....175
Lights-Out Management attributes....175
Lights-Out Management class definitions....175
hpqLOMv100....175
Lights-Out Management attribute definitions....175
hpqLOMRightLogin....175
hpqLOMRightRemoteConsole....176
hpqLOMRightVirtualMedia....176
hpqLOMRightServerReset....176
hpqLOMRightLocalUserAdmin....176
hpqLOMRightConfigureSettings....177
6 HP Systems Insight Manager integration....178
Integrating iLO 2 with HP SIM....178
HP SIM functional overview....178
Establishing SSO with HP SIM....178
HP SIM identification and association....179
HP SIM status....179
HP SIM links....179
HP SIM systems lists....180
Receiving SNMP alerts in HP SIM....180
HP SIM port matching....181
Reviewing Advanced Pack license information in HP SIM....181
7 Troubleshooting iLO 2....182
iLO 2 POST LED indicators....182
Event log entries....183
Hardware and software link-related issues....186
JVM support....186
Login issues....187
Login name and password not accepted....187
Directory user premature logout....187
iLO 2 Management Port not accessible by name....187
iLO 2 RBSU unavailable after iLO 2 and server reset....188
Inability to access the login page....188
Inability to access iLO 2 using Telnet....188
Inability to access virtual media or graphical remote console....188
Inability to connect to iLO 2 after changing network settings....188
Inability to connect to the iLO 2 Diagnostic Port....188
Inability to connect to the iLO 2 processor through the NIC....189
Inability to log in to iLO 2 after installing the iLO 2 certificate....189
Firewall issues....189
Proxy server issues....190
Two-factor authentication error....190
Troubleshooting alert and trap issues....190
Inability to receive HP SIM alarms (SNMP traps) fromiLO 2....191
iLO 2 Security Override switch....191
Authentication code error message....191

Troubleshooting directory issues....191
Domain/name format login issues....191
ActiveX controls are enabled and I see a prompt but the domain/name login format does not work....192
User contexts do not appear to work....192
Directory user does not logout after the directory timeout has expires....192
Troubleshooting Remote Console issues....192
Remote Console applet has a red X when running Linux client browser....192
Inability to navigate the single cursor of the Remote Console to corners of the Remote Console window....192
Remote Console no longer opens on the existing browser session....193
Remote console text window not updating properly....193
Remote Console turns gray or black....193
Remote Serial Console troubleshooting....193
Troubleshooting Integrated Remote Console issues....194
Internet Explorer 7 and a flickering remote console screen....194
Configuring Apache to accept exported capture buffers....194
No console replay while server is powered down....195
Skipping information during boot and fault buffer playback....195
Out of Memory error starting Integrated Remote Console....195
Session leader does not receive connection request when IRC is in replay mode....195
Keyboard LED does not display correctly....195
Inactive IRC....196
IRC Failed to connect to server error message....196
IRC toolbar icons do not update....196
GNOME interface does not lock....197
Repeating keys on the Remote Console....197
Remote Console playback does not work when the host server is powered off....197
Troubleshooting SSH and Telnet issues....197
Initial PuTTY input slow....197
PuTTY client unresponsive with Shared Network Port....197
SSH text support from a Remote Console session....197
Troubleshooting terminal services issues....197
Terminal Services button is not working....197
Terminal Services proxy stops responding....198
Troubleshooting video and monitor issues....198
General guidelines....198
Telnet displays incorrectly in DOS....198
Video applications not displaying in the Remote Console....198
User interface is not displaying correctly....198
Troubleshooting Virtual Media issues....198
Virtual Media applet has a red X and does not display....199
Virtual Floppy media applet is unresponsive....199
Troubleshooting iLO Video Player issues....199
Video capture file does not play....199
Video capture file plays erratically....199
Troubleshooting Remote Text Console issues....199
Viewing the Linux installer in the text console....199
Passing data through an SSH terminal....199
Troubleshooting miscellaneous issues....199
Cookie sharing between browser instances and iLO 2....199
Shared instances....200
Cookie order behavior....200
Displaying the current session cookie....201
Preventing cookie-related user issues....201

Inability to access ActiveX downloads....201
Inability to get SNMP information from HP SIM....201
Incorrect time or date of the entries in the event log....201
Inability to upgrade iLO 2 firmware....201
Diagnostic steps....202
iLO 2 network flash recovery....202
Recovering from a bad iLO 2 flash image using network flash recovery....202
Recovering from a bad iLO 2 flash image using the HP Smart Update Firmware DVD....203
The iLO 2 firmware does not respond to SSL requests....204
Testing SSL....204
Resetting iLO 2....204
Server name still present after ERASE utility is executed....204
Troubleshooting a remote host....205
8 Technical support....206
Support information....206
HP contact information....207
Before you contact HP....207
Acronyms and abbreviations....208
Index....211

1 Overview

The iLO 2 firmware provides multiple ways to configure, update, and operate servers remotely. The *HP Integrated Lights-Out 2 User Guide* describes these features and how to use them with the browser-based interface and RBSU. Some features are licensed features and may only be accessed after purchasing an optional license. For more information, see "Licensing" (page 26).

The *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide* describes the syntax and tools available to use iLO 2 through a command-line or scripted interface. Click the link for the guide http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=135&prodTypeId=18964&prodSeriesId=1146658.

This manual discusses HP Integrated Lights-Out 2 firmware version 2.09 for ProLiant ML/DL servers, as well as ProLiant BladeSystem server blades.

New in this release of iLO 2

The iLO 2 firmware version 2.09 adds:

- iLO 2 Enhanced CLI prompt and Virtual Serial Port Log
- Support for SUSE Linux 10 and 11 (32– and 64–bit)

iLO 2 Overview

The iLO 2 firmware can remotely perform most functions that otherwise require a visit to servers at the data center, computer room, or remote location. The following are just a few of the iLO 2 features.

- Remote Console and virtual power – Enables you to view a stalled remote server with blue screen conditions and restart the server without onsite assistance.
- Remote Console – Enables you to change BIOS settings when necessary.
- Virtual KVM technology – Provides a high-performance remote console that enables you to remotely administer operating systems and applications in everyday situations.
- Virtual CD/DVD or floppy – Enables you to install an operating system or flash system firmware over the network from images on your workstations or on centralized web servers.
- Virtual Folder – Enables you to update operating system drivers or copy system files without physical media or creating a disk image.
- Scripting – Enables you to use virtual power and virtual media in other scripting tools to automate deployment and provisioning.
- Active participation in monitoring and maintaining server health, referred to as embedded health. iLO 2 monitors temperatures in the server and sends corrective signals to the fans to maintain proper server cooling. In addition to temperature monitoring, iLO 2 provides fan status monitoring and monitoring of the status of the power supplies, voltage regulators, and the internal hard drives.

These examples are just a few ways iLO 2 is used to manage HP ProLiant servers from your office, home, or travel location. As you begin using iLO 2 and defining your specific infrastructure requirements, refer to this guide for additional ways to simplify your remote server management needs.

For information about the features available in each version of iLO 2, see "Licensing" (page 26).

Differences between iLO 2 and iLO

The iLO 2 firmware is based on the iLO and shares many common features. However, to use iLO 2 to access a pre-operating system, text-based remote console, you must use the remote serial console. For more information, see "Text-based remote console overview" (page 95).

The following table highlights the differences between iLO 2 and iLO.

Feature	iLO 2	iLO
Standard features		
Text console	Pre-OS	Pre-OS and OS
Remote Serial Console (virtual serial port)	Pre-OS and OS	Pre-OS and OS
Server health monitoring and maintenance	Yes	No
Advanced features		
Text console	Pre-OS and OS	Pre-OS and OS
Remote console	Yes (Virtual KVM)	Yes
Integrated Remote Console	Yes	No
Support for Microsoft JVM	Yes	No
Remote Console Acquire button	Yes	Yes
Terminal Services integration	Yes	Yes
HP schema directory integration	Yes	Yes
Schema-free directory integration	Yes	Yes
Two-factor authentication	Yes	Yes
Power Regulator reporting	Yes	Yes
Virtual Floppy and CD/DVD-ROM	Yes	Yes
USB key virtual media	Yes	Yes
Virtual folder	Yes	No

HP Insight Control server deployment

HP Insight Control server deployment integrates with iLO 2 to enable the management of remote servers and the performance of remote console operations, regardless of the state of the operating system or hardware.

The deployment server provides the capability to use the power management features of iLO 2 to power on, power off, or cycle power on the target server. Each time a server connects to the deployment server, the deployment server polls the target server to determine whether a LOM management device is installed. If installed, the server gathers information including the DNS name, IP address, and user login name. Security is maintained by requiring the user to enter a correct password.

For more information about the HP Insight Control server deployment, see the documentation that ships on the HP Insight Software DVD, or the HP Insight Control webpage at http://www.hp.com/go/insightcontrol.

Server management through IPMI version 2.0 compliant applications

Server management through the IPMI is a standardized method for controlling and monitoring the server. iLO 2 provides server management based on the IPMI version 2.0 specification.

The IPMI specification defines a standardized interface for platform management. The IPMI specification defines the following types of platform management:

- Monitoring of system information, such as fans, temperatures, and power supplies
- Recovery capabilities, such as system resets and power on/off operations
- Logging capabilities, for abnormal events such as over temperature readings or fan failures
- Inventory capabilities, such as identifying failed hardware components

IPMI communications are dependent on the BMC and the SMS. The BMC manages the interface between the SMS and the platform management hardware. iLO 2 emulates the BMC functionality and the SMS functionality can be provided by various industry-standard tools. For additional information, see the IPMI specification on the Intel website at http://www.intel.com/design/servers/ipmi/tools.htm.

The iLO 2 firmware provides the KCS interface, or open interface, for SMS communications. The KCS interface provides a set of I/O mapped communications registers. The default system base address for the I/O mapped SMS Interface is 0xCA2 and is byte aligned at this system address.

The KCS interface is accessible to SMS software that is running on the local system. Examples of compatible SMS software applications include:

- IPMI version 2.0 Command Test Tool is a low-level MS-DOS command line tool that enables hex-formatted IPMI commands to be sent to an IPMI BMC that implements the KCS interface. You can locate this tool on the Intel website at http://www.intel.com/design/servers/ipmi/tools.htm.
- IPMItool is a utility for managing and configuring devices that support the IPMI version 1.5 and version 2.0 specifications and can be used in a Linux environment. You can locate this tool on the IPMItool website at http://ipmitool.sourceforge.net/index.html.

IPMI functionality provided by iLO 2

When emulating a BMC for the IPMI interface, iLO 2 supports all mandatory commands listed in the IPMI version 2.0 specification. See the IPMI version 2.0 specification for a listing of these commands. Also, the SMS uses the methods described in the specification for determining which IPMI features are enabled or disabled in the BMC (for example, using the `Get Device ID` command).

If the server operating system is running and the health driver is enabled, any IPMI traffic through the KCS interface can affect the performance of the health driver and overall health performance of the system. Do not issue any IPMI commands through the KCS interface that might detrimentally affect the monitoring performed by the health driver. These commands include any commands that sets or changes IPMI parameters, such as `Set Watchdog Timer` and `Set BMC Global Enabled`. Any IPMI command that simply returns data is safe to use, such as `Get Device ID` and `Get Sensor Reading`.

WS-Management compatibility overview

The iLO 2 firmware implementation of WS-Management is in accordance with the DTMF *Web Services for Management 1.0.0a* specification.

Authentication:

- The iLO 2 firmware uses basic authentication over SSL, compliant with profile:

  `wsman:secprofile/https/basic`.

- Authenticated users are authorized to execute WS-Management commands in accordance with designated privileges in their local or directory accounts.
- To enable basic authentication on Windows Vista, enter `gpedit.msc` at the command prompt to launch the Group Policy Object Editor. Select **Computer Configuration> Administrative Templates> Windows Components> Windows Remote Management (WinRM)> WinRM Client**. Set Allow Basic authentication to **Enabled**.

Compatibility:

- WS-Management in iLO 2 is compatible with the Windows Vista WinRM utility, Microsoft Operations Manager 3, and the Management Pack provided by HP.
- The full set of WS-Management commands is available on iLO 2 servers that support embedded system health. A greatly reduced subset of these commands is available on servers without embedded systems health support.

Commands:

The following commands are available for remote invocation of the following devices:

- Server power
- UID

Status:

The WS-Management in iLO 2 returns status information for fans, temperatures, power supplies, and VRMs.

iLO 2 browser interface overview

The iLO 2 browser interface groups similar tasks for easy navigation and workflow. These tasks are organized under high-level tabs across the top of the iLO 2 interface. These tabs appear on the browser interface and include System Status, Remote Console, Virtual Media, Power Management, and Administration.

Each high-level iLO 2 tab has a menu on the left side of the interface with various options. When you select a different high-level tab, the menu changes, and displays the options available from that tab. Each menu option displays a page title, which is a description of the information or settings available on that page. This page title might not reflect the name that appears on the menu option.

Assistance for all iLO 2 pages is available from iLO 2 Help. Links on each iLO 2 page provide summary information about the features of iLO 2 and helpful information to optimize its operation. To access page-specific help, click the question mark **(?)** on the right side of the browser window.

Typical user tasks are found under the System Status, Remote Console, Virtual Media, and Power Management tabs of the iLO 2 interface. These tasks are described in "Using iLO 2" (page 74).

The Administration tab is typically used by an advanced or administrative user who must manage users, configure global and network settings, as well as configure or enable the more advanced functions of iLO 2. These tasks are discussed in "Setting up iLO 2" (page 17) and "Configuring iLO 2" (page 24).

Subject-specific areas of iLO 2 functionality and integration are detailed in:

- "Directory services" (page 130)
- "Directory-enabled remote management" (page 156)
- "HPLOMIG directory migration utility" (page 162)
- "HP Systems Insight Manager integration" (page 178)

- "Troubleshooting iLO 2" (page 182)
- "Directory services schema" (page 171)

Supported browsers and client operating systems

- Microsoft Internet Explorer 7, Internet Explorer 8, Internet Explorer 9
  - These browsers are supported on Microsoft Windows products.
  - HP supports Microsoft JVM and SUN Java 1.4.2_13. To download the recommended JVM for your system configuration, see the website at http://h18006.www1.hp.com/products/servers/management/ilo_table.html?jumpid=reg_r1002_usen.
- Mozilla Firefox versions 8, 9, and 10
  - This browser is supported on Red Hat Enterprise Linux Desktop 4 and Novell Linux Desktop 9.
  - HP supports Microsoft JVM and SUN Java 1.4.2_13. To download the recommended JVM for your system configuration, see the HP website at http://h18006.www1.hp.com/products/servers/management/ilo_table.html?jumpid=reg_r1002_usen.

Certain browsers and operating system combinations might not work correctly, depending on the implementation of the required browser technologies.

Supported server operating system software

iLO 2 is an independent microprocessor running an embedded operating system. The architecture ensures that the majority of iLO 2 functionality is available, regardless of the host operating system.

For graceful host operating system shutdown, HP SIM integration requires health drivers and Management Agents or remote console access.

iLO 2 provides two interface drivers:

- The iLO 2 Advanced Server Management Controller Driver (health driver) – Provides system management support, including monitoring of server components, event logging, and support for the Management Agents.
- The iLO 2 Management Interface Driver – Enables system software and SNMP Insight Agents to communicate with iLO 2.

These drivers and agents are available for the following network operating systems:

- Microsoft
  - Windows 2008 Server
  - Windows 2008 Advanced Server
  - Windows Server 2003
  - Windows Server 2003, Web Edition
  - Windows Small Business Server 2003 (ML300 series)
  - Windows Vista
- Red Hat
  - RedHat Enterprise Linux 3 (x86)
  - RedHat Enterprise Linux 3 (AMD64/EM64T)
  - RedHat Enterprise Linux 4 (x86)

- RedHat Enterprise Linux 4 (AMD64/EM64T)
- RedHat Enterprise Linux 5 (x86)
- RedHat Enterprise Linux 5 (AMD64/EM64T)

- SUSE LINUX
  - SUSE LINUX Enterprise Server 9 (x86)
  - SUSE LINUX Enterprise Server (AMD64/EM64T)
  - SUSE LINUX Enterprise Server 10
  - SUSE LINUX 10 (32– and 64–bit)
  - SUSE LINUX 11 (32– and 64–bit)

2 Setting up iLO 2

Quick setup

To quickly set up iLO 2 by using the default settings for iLO 2 Standard and iLO Advanced features, follow these steps:

1. To decide how you want to structure networking and security, see"Preparing to set up iLO 2" (page 17)
2. To connect iLO 2 to the network, see "Connecting to the network" (page 18).
3. If you are not using dynamic IP addressing to configure a static IP address, use the iLO 2 RBSU. See "Configuring the IP address" (page 19).
4. To log into iLO 2 from a supported browser or command line using the default user name, password, and DNS name provided on the iLO 2 Network Settings tag attached to the server, see "Logging in to iLO 2 for the first time" (page 20).
5. Change the default user name and password on the administrator account to your predefined selections.
6. To use the local accounts feature, set up your user accounts, see "Setting up user accounts" (page 20).
7. To activate iLO 2 advanced features, see "Activating iLO 2 licensed features with a browser" (page 21).
8. To install the iLO 2 device drivers, see "Installing iLO 2 device drivers" (page 21).

Preparing to set up iLO 2

Before setting up your iLO 2 management processors, you must decide how to handle networking and security. The following questions can help you configure iLO 2 for your needs:

1. **How should iLO 2 connect to the network?**

   For a graphical representation and explanation of the available connections, see "Connecting to the network" (page 18). Typically iLO 2 is connected to the network using either:

   - A corporate network where both the NIC and the iLO 2 port are connected to the corporate network. This connection enables access to iLO 2 from anywhere on the network and reduces the amount of networking hardware and infrastructure required to support iLO 2. However, on corporate networks, network traffic can impede iLO 2 performance.
   - A dedicated management network with the iLO 2 port on a separate network. A separate network improves performance and security because you can physically control which workstations are connected to the network. A separate network also provides redundant access to the server when a hardware failure occurs on the corporate network. In this configuration, iLO 2 cannot be accessed directly from the corporate network.

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

   To access iLO 2 after connecting it to the network, the management processor must acquire an IP address and subnet mask using either a dynamic or static process:

   - Dynamic IP address is set by default. iLO 2 obtains the IP address and subnet mask from DNS/DHCP servers. This method is the simplest.
   - Static IP address is used to configure a static IP address if DNS/DHCP servers are not available on the network. A static IP address can be configured in iLO 2 using the RBSU.

     If using a static IP, you must have an IP address before starting iLO 2 setup.

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

   The iLO 2 firmware provides several options to control user access. You must select one of the following methods to prevent unauthorized access to corporate IT assets:

   - Local accounts with up to 12 user names and passwords can be stored on iLO 2. This is ideal for small environments such as labs and small- and medium-sized businesses.
   - Directory services use the corporate directory (Microsoft Active Directory or Novell eDirectory) to manage iLO 2 user access. This is ideal for environments with a large number of frequently changing users. If you plan to use Directory services leave at least one local account enabled for alternate access. For more information, see "Security" (page 41).

4. **How do you want to configure iLO 2?**

   The iLO 2 firmware supports various interfaces for configuration and operation. This guide discusses the following interfaces:

   - Using iLO 2 RBSU when the system environment does not use DHCP, DNS, or WINS. For more information, see "Setting up iLO 2 using iLO 2 RBSU" (page 20).
   - Using a browser-based setup when you can connect to iLO 2 on the network using a browser. This method can also reconfigure a previously configured iLO 2. For more information, see "Setting up iLO 2 with the browser-based option" (page 21).
   - Using SMASH CLP when a command line is accessible through Telnet, SSH, or physical serial port. For more information, see the *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide* at http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=135&prodTypeId=18964&prodSeriesId=1146658.

The iLO 2 default settings enable you to use most features with no additional configuration. However, the extensive configuration flexibility of iLO 2 enables customization for multiple enterprise environments. For all available options, see "Configuring iLO 2" (page 24).

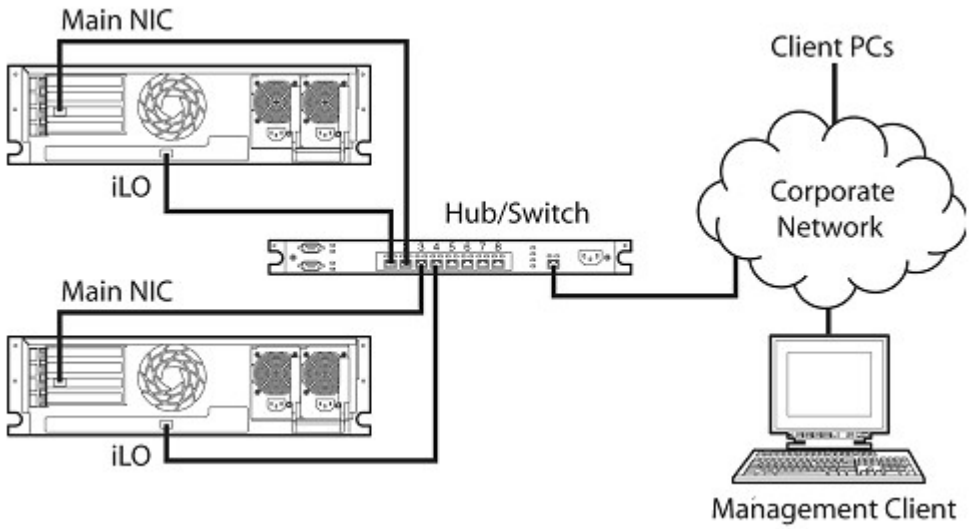
For advanced setup of multiple iLO 2 management processors using scripting commands, the following methods are available. Scripts are text files written in an XML-based scripting language called RIBCL. You can use RIBCL scripts to configure iLO 2 on the network, during initial deployment, or from an already deployed host. Each method is described in the *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide* at http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=135&prodTypeId=18964&prodSeriesId=1146658

- `CPQLOCFG` is a Microsoft Windows utility that sends RIBCL scripts to iLO 2 over the network.
- `HPONCFG` is a local, online, and scripted setup utility that runs on the host and passes RIBCL scripts to the local iLO 2 firmware. This utility has Windows and Linux versions, which require the iLO 2 Management Interface Driver.
- Perl is a scripting language that you use from Linux clients to send RIBCL scripts to the iLO 2 firmware over the network.

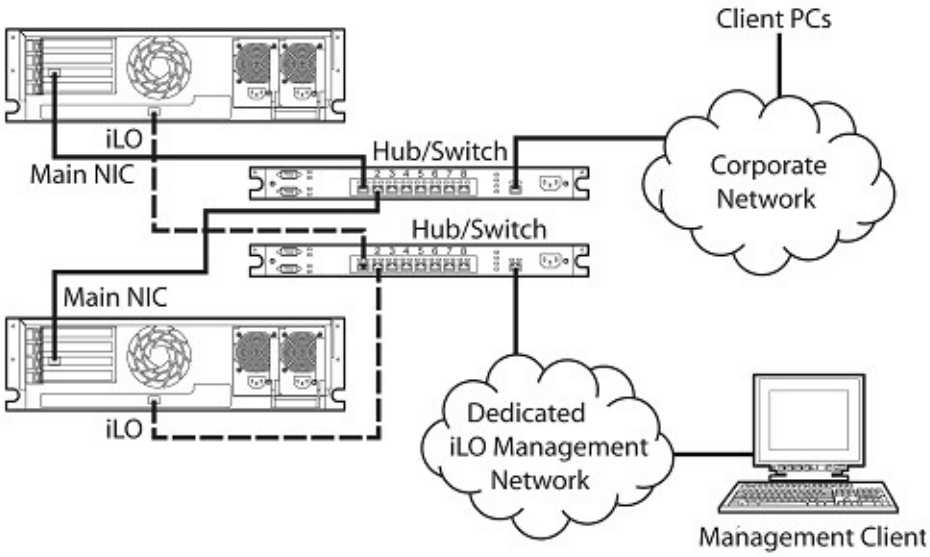
Connecting to the network

Typically, iLO 2 is connected to the network in one of two ways:

- Corporate network, where both ports are connected to the corporate network. In this configuration, the server has two network ports (one server NIC, and one iLO 2 NIC) connected to a corporate network.



- Dedicated management network, where the iLO 2 port is on a separate network.



Configuring the IP address

This step is necessary only if you are using a static IP address. When using dynamic IP addressing, your DHCP server automatically assigns an IP address for iLO 2. To simplify installation, HP recommends using DNS or DHCP with iLO 2.

To configure a static IP address, use the iLO 2 RBSU with the following procedure to disable DNS and DHCP and configure the IP address and the subnet mask:

1. Restart or power the server on.
2. Press the **F8** key when prompted during POST. The iLO 2 RBSU runs.
3. Select **Network>DNS/DHCP**, press the **Enter** key, and then select **DHCP Enable**.
4. Press the spacebar to turn off DHCP. Be sure that DHCP Enable is set to `Off`, and then save the changes.
5. Select **Network>NIC>TCP/IP**, press the **Enter** key, and then enter the appropriate information in the IP Address, Subnet Mask, and Gateway IP Address fields.
6. Save the changes.
7. Exit iLO 2 RBSU. The changes take effect when you exit iLO 2 RBSU.

Logging in to iLO 2 for the first time

The iLO 2 firmware is configured with a default user name, password, and DNS name. Default user information is located on the iLO 2 Network Settings tag attached to the server containing the iLO 2 management processor. Use these values to access iLO 2 remotely from a network client using a standard Web browser.

For security reasons, HP recommends changing the default settings after logging in to iLO 2 for the first time.

The default values are:

- User name – Administrator
- Password – A random, eight-character, alphanumeric string
- DNS Name – ILO*XXXXXXXXXXXX*

  where *XXXXXXXXXXXX* represents the serial number of the server

NOTE: User names and passwords are case sensitive.

If you enter an incorrect user name and password, or a log in attempt fails, then iLO 2 imposes a security delay. For more information on login security, see "Login security" (page 44).

Setting up user accounts

The iLO 2 firmware comes preconfigured with default factory settings, including a default user account and password. For security reasons, HP recommends changing the default settings after logging in to iLO 2 for the first time. These changes can be made using any of the iLO 2 user interfaces. RBSU and browser procedures are explained in this user guide. Other options including the SMASH CLP and scripting methods are described in the *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide* at http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=135&prodTypeId=18964&prodSeriesId=1146658.

If iLO 2 is connected to a network running DNS or DHCP, you can use it immediately without changing any settings.

Setting up iLO 2 using iLO 2 RBSU

HP recommends that you use the iLO 2 RBSU to initially set up iLO 2 and configure iLO 2 network parameters for environments that do not use DHCP and DNS, or WINS. RBSU provides the basic tools to configure iLO 2 network settings and user accounts to get iLO 2 on the network.

You can use RBSU to configure network parameters, global settings, and user accounts. The iLO 2 RBSU is not intended for continued administration. RBSU is available every time the server is booted and can be run remotely using the iLO 2 Remote Console.

The iLO 2 RBSU can be disabled in the Global Settings preferences. Disabling iLO 2 RBSU prevents reconfiguration from the host unless the iLO 2 Security Override Switch is set.

To run iLO 2 RBSU to set up local accounts:

1. Restart or power the server on.
2. Press the **F8** key when prompted during POST. The iLO 2 RBSU runs.
3. If prompted, enter a valid iLO 2 user ID and password with the appropriate iLO 2 privileges (**Administer User Accounts>Configure iLO 2 Settings**). Default account information is located on the iLO 2 Default Network Settings tag attached to the server containing the iLO 2 management processor. If iLO 2 has not been configured to present a login challenge to the RBSU, then no prompt appears.
4. Make and save any necessary changes to the iLO 2 configuration.
5. Exit iLO 2 RBSU.

Setting up iLO 2 with the browser-based option

If you can connect to iLO 2 on the network with a browser, then use the browser-based setup method. You can also use this method to reconfigure a previously configured iLO 2.

Access iLO 2 from a remote network client using a supported browser, and provide the default DNS name, user name, and password. Default DNS name and account information is located on the iLO 2 Network Settings tag attached to the server containing the iLO 2 management processor.

When you successfully log onto iLO 2, you can change the default values of the local user accounts by selecting User Administration under the iLO 2 Administration tab.

Activating iLO 2 licensed features with a browser

The Licensing page enables you to view the current license status and enter a key to activate iLO 2 license features. The iLO 2 version and current license information appears in this section. If a license is installed (including an evaluation license), the license number appears. For more information about iLO 2 license options, see "Licensing" (page 26).

1. Log into iLO 2 through a supported browser.
2. To display the iLO 2 license activation screen, click **Administration>Licensing**.



3. Enter the license key. To move between fields, press the **Tab** key or click inside a field. The Activation Key field advances automatically as you enter data. To clear the fields and reload the page, click **Licensing**.
4. Click **Install**. The EULA confirmation appears. The EULA details are available on the HP website at http://www.hp.com/servers/lights-out and with the license kit.
5. Click **OK**.

The advanced features of iLO 2 are now enabled.

Installing iLO 2 device drivers

The iLO 2 Management Interface Driver enables system software such as SNMP Insight Agents and the Terminal Services passthrough service to communicate with iLO 2.

The device drivers required to support iLO 2 are part of the PSP located on the SmartStart CD, Management CD, or on the HP website at http://www.hp.com/servers/lights-out.

All the support drivers for your server and iLO 2 can be downloaded from the HP website at http://www.hp.com/servers/lights-out.

To download the drivers:

1. Click the iLO 2 graphic.
2. Select **Software and Drivers**.

Microsoft device driver support

The device drivers that support the iLO 2 are part of the PSP that is located on the HP website at 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.

iLO 2 prerequisite files:

- `CPQCIDRV.SYS` – Provides the iLO 2 Management Interface Driver support.
- `CPQASM2.SYS`, `SYSMGMT.SYS`, and `SYSDOWN.SYS` – Provide the iLO 2 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 at 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 at http://www.hp.com/support.
2. Run the `SETUP.EXE` file included in the download, and then follow the installation instructions.

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

Linux device driver support

You can download the LSP files containing the iLO 2 driver, the foundation agents, and health agents from the HP website at http://www.hp.com/support. The instructions on how to install or update the iLO 2 driver are available on the website. The HP Management Agents for Linux are:

- RPM package (`hp-snmp-agents`) combines the health driver, IML viewer, foundation agents, health agent, and standard equipment agent into one package.
- RPM package (`hp-iLO`) combines the RIB driver, rack daemon, RIB agent, and rack agent into one package.

To load the health and iLO 2 driver packages, enter the following commands:

```
rpm -ivh hp-snmp-agents-d.vv.v-pp.Linux_version.i386.rpm
rpm -ivh hp-iLO-d.vv.v-pp.Linux_version.i386.rpm
```

where:

d is the Linux distribution and version

vv.v-pp are version numbers

To remove the health and iLO 2 drivers, enter the following commands:

```
rpm -e hp-snmp-agents
rpm -e hp-iLO
```

For additional information, see the HP Software and Drivers website at http://www.hp.com/support.

Novell NetWare device driver support

The device drivers required to support iLO 2 are part of the PSP that is located on the SmartStart CD and the HP website at http://www.hp.com/support. The PSP for Novell NetWare includes an installer that analyzes system requirements and installs all drivers.

iLO 2 requires the following files:

- The `CPQHLTH.NLM` file provides the Health Driver for Novell NetWare.
- The `CPQCI.NLM` file provides iLO 2 Management Interface Driver support.

When updating iLO 2 drivers, be sure iLO 2 is running the latest version of iLO 2 firmware. You can obtain the latest version as a Smart Component from the HP website at http://www.hp.com/servers/lights-out.

Install the drivers download the PSP from the HP website at 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 ATI ES1000 video driver that is provided by the operating system for best results.

3 Configuring iLO 2

iLO 2 configuration overview

Typically, an advanced or administrative user who must manage users and configure global and network settings configures iLO 2. You can configure iLO 2 using the iLO 2 browser-based GUI or scripting tools such as CPQLOCFG and HPONCFG (described in the *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide* at http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=135&prodTypeId=18964&prodSeriesId=1146658.

The iLO 2 Administration tab enables you to configure and manage user settings, SNMP alerting (through integration with HP SIM), security settings, licensing, certificate administration, directory settings, and network environment settings. The Administration tab includes the following menu options:

- iLO 2 Firmware. See"Upgrading iLO 2 firmware" (page 24).
- Licensing. See "Licensing" (page 26).
- User Admininstration. See "User administration" (page 28)
- Settings
  - Access. See "Configuring iLO 2 access" (page 33)
  - Security. See "Security" (page 41)
  - Network. See "Network" (page 60)
  - Management. See "SNMP/Insight Manager settings" (page 65)

Upgrading iLO 2 firmware

Firmware upgrades enhance the functionality of iLO 2. You can find the latest firmware on the HP website at http://www.hp.com/servers/lights-out. Select your iLO 2 product, and then select **Software & Drivers**. After the software and drivers page appears, select your iLO 2 product and operating system, and then click **Locate Software**. You can also locate your iLO 2 software by selecting the **Operating System and Category** options.

You must have the Configure iLO 2 privilege (configure local device settings) to update the firmware unless, you set the security override switch. For more information, see "iLO 2 Security Override Switch administration" (page 42). If the security override switch is set, any iLO 2 user can update the firmware. You must run firmware updates from an Administrator or root context on the host operating system.

To update the iLO 2 choose one of the following methods:

- Online firmware update – Download the appropriate operating system component and run it from the Administrator or root context of the operating system. The online firmware update software runs on the host operating system and updates the iLO 2 firmware without requiring you to log in to iLO 2.
- Offline firmware update for SmartStart maintenance – Download the iLO 2 firmware image file you plan to install, and see "Upgrading iLO 2 with a browser" (page 25).
- **Firmware Maintenance CD-ROM** – Download the component to create a bootable CD that contains many firmware updates for ProLiant servers and options.
- **Scripting with CPQLOCFG** – Download the `CPQLOCFG` component to get the network-based scripting utility `CPQLOCFG`. `CPQLOCFG` enables you to use RIBCL scripts that perform firmware

updates, iLO 2 configuration, and iLO 2 operations in bulk, securely over the network. HP recommends that Linux users review the HP Lights-Out XML PERL Scripting Samples for Linux.

- **Scripting with HPONCFG** – Download the `HPONCFG` component to get the host-based scripting utility `HPONCFG`. This utility enables you to use RIBCL scripts that perform firmware updates, Lights-Out processor configuration and operations in bulk, from Administrator or root account access on supported host operating systems.
- **HP Directories Support for Management Processors** – Download the HP Directories Support for Management Processors executable file to get the directory support components. One of the components, `HPLOMIG`, can be used to discover iLO 2 processors, and update the firmware. You do not have to use directory integration to take advantage of this functionality.

Upgrading iLO 2 with a browser

You can complete the firmware upgrade from any network client using a supported browser. You must have the Update iLO 2 Firmware privilege to upgrade the iLO 2 firmware. The most recent firmware for iLO 2 is available on the HP website at http://www.hp.com/servers/lights-out. To upgrade the iLO 2 firmware using a supported browser:

1. Log in to iLO 2 with an account that has the Configure iLO 2 Settings privilege.
2. Click **Administration>Upgrade iLO 2 Firmware**. The Upgrade iLO 2 Firmware page appears.



3. Enter the file name in the New firmware image field or browse for the file.
4. Click **Send firmware image**. The firmware upgrade takes a few minutes. A progress bar displays the progress of the firmware upgrade.

Do not interrupt an Upgrade iLO 2 Firmware session. The iLO 2 system automatically resets after a successful firmware upgrade. The iLO 2 system reset does not affect the host operating system and server.

If the firmware upgrade is interrupted or fails, attempt the upgrade again immediately. Do not reset the iLO 2 system before reattempting a firmware upgrade.

Updating the firmware using the maintenance CD

To use HP Smart Update Manager on the Firmware Maintenance CD:

1. Place the Firmware Maintenance CD on a USB key using the USB Key Creator Utility.
2. Copy `CP009768.exe` to the `/compaq/swpackages` directory on the USB Key.
3. Follow HP Smart Update Manager steps to complete firmware update.

Recovering from a failed iLO 2 firmware update

To recover from a failed firmware update using the HP Drive Key Boot Utility:

1. Copy the iLO 2 offline flash component to your USB drive key.
2. Verify that the iLO 2 security override switch is set to disabled.
3. Boot the USB drive key containing the iLO 2 flash component.

   To download the HP Drive Key Boot Utility and for information on how to create a boot USB key, see the HP website at http://www.hp.com/go/support.
4. After the first screen displays, switch to text console by pressing the **Ctrl+Alt+F1** keys.
5. Switch to the directory where the flash component is stored by entering `cd /mnt/usb/components/` at the # prompt.
6. Remove the loaded HP Lights-Out driver by entering the following commands:

   ```
   /etc/init.d/hp-snmp-agents stop
   /etc/init.d/hp-ilo stop
   ```

   or

   ```
   /etc/init.d/hpasm stop
   ```
7. Run the component using the `- -direct` option. For example:

   ```
   ./CP00xxxx.scexe - -direct
   ```
8. Enter **y** at the `Continue (y/n)?` prompt.
9. After programming is successfully completed, set the security override switch to **enabled** and reboot the server.

Downgrading the iLO 2 firmware

If you downgrade the iLO 2 firmware, you must remove the iLO 2 1.30 Remote Console ActiveX applet 1.3.0.19 from your Internet Explorer client browser. To remove the applet:

1. Open Internet Explorer.
2. Select **Tools>Internet Options>Settings>View objects**.
3. To remove `1.30.19`, right-click **iLO2 Remote console 1.3.0.18**.

Licensing

HP iLO Advanced Pack and HP iLO Advanced Pack for Blade System licenses activate optional iLO 2 features that are not bundled with an unlicensed system.

If you purchase the iLO Advanced Pack or the iLO Advanced Pack for BladeSystem with any Insight Control software suite or iLO Power Management Pack, HP provides Technical Support and Update Services. For more information, see "Support information" (page 206).

If you purchase the iLO Advanced Pack or the iLO Advanced Pack for Blade System as a one-time activation of licensed features, you must purchase future functional upgrades. For more information, see "Support information" (page 206).

One iLO Advanced or iLO Advanced Pack for Blade System license is required for each server on which the product is installed and used. Licenses are nontransferable. You cannot license an HP ProLiant ML/DL server with an iLO Advanced for BladeSystem. For additional information, see the EULA.

HP will continue to provide maintenance releases with fixes as well as iLO Standard and iLO Standard Blade Edition feature enhancements at no extra charge.

A 60-day evaluation license key is available for download from the HP website. The evaluation license activates and enables access to iLO 2 Advanced features. You can only install one evaluation license per iLO 2. When the evaluation period expires, the iLO 2 features deactivate.

The following versions of iLO 2 are available:

NOTE: The features annotated with an asterisk (*) are not supported on all systems.

Feature	iLO 2 Advanced	iLO 2 Advanced for BladeSystem	iLO 2 Standard	iLO 2 Standard Blade Edition
Virtual power and reset control	X	X	X	X
Server console access through POST	X	X	X	X
Text console after POST	X	X	– –	– –
Event logs	X	X	X	X
System health* and configuration	X	X	X	X
UID	X	X	X	X
DMTF SMASH standard CLP	X	X	X	X
RIBCL/XML scripting	X	X	X	X
WS Management Scripting	X	X	X	X
Browser access	X	X	X	X
SSH access	X	X	X	X
Shared network port	X	– –	X	– –
Serial access	X	X	X	X
Remote serial console	X	X	X	X
Integrated remote console	X	X	– –	X
Remote console	X	X	– –	X
Virtual media applet	X	X	– –	X
Secure digital card support*	X	X	– –	X
Terminal services passthrough	X	X	– –	X
Virtual media scripting	X	X	– –	– –
Directory integration	X	X	– –	– –
24 hour power reporting*	X	X	X	X
Real-time power reporting*	X	X	– –	– –
Dynamic power capping	X	X	– –	– –
Group power capping	X	X	– –	– –
Two-factor smart card authentication	X	X	– –	– –
HP SIM single sign-on	X	X	– –	– –

Feature	iLO 2 Advanced	iLO 2 Advanced for BladeSystem	iLO 2 Standard	iLO 2 Standard Blade Edition
Kernel debugger for Windows	X	X	– –	– –
Console replay	X	X	– –	– –
Shared remote console	X	X	– –	– –
Boot/fault console capture	X	X	– –	– –
iLO video player (license required for capture)	X	X	X	X
Enhanced CLI prompt	X	X	X	X
Virtual Serial port log	X	X	– –	– –

In addition to the standard iLO 2 single-server licenses, two other licensing options are available:

- The Flexible Quantity License Kit enables you to purchase a single software package, one copy of the documentation, and a single license key to activate the exact number of licenses requested.
- The Activation Key Agreement enables a volume purchase of ProLiant Essentials and Insight Control software over time, typically in conjunction with new ProLiant servers that are acquired on a regular basis.

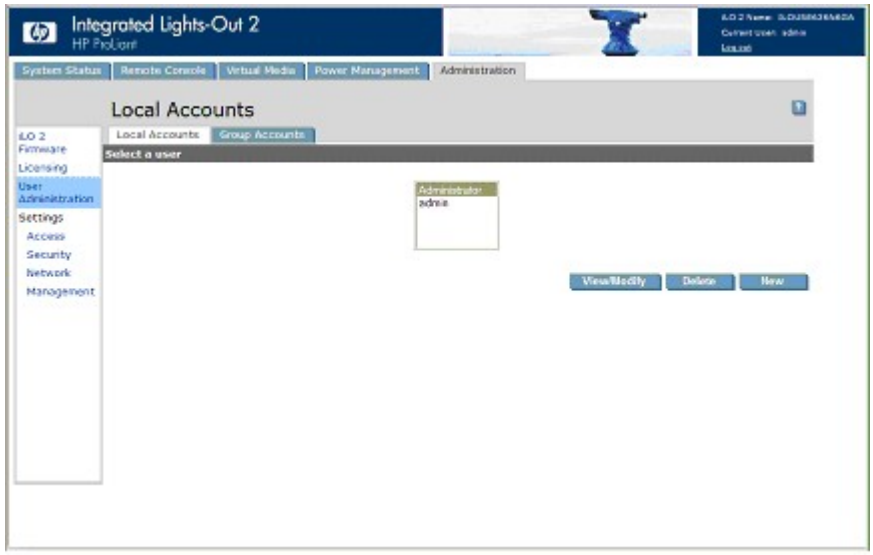
User administration

The iLO 2 firmware enables you to manage user accounts stored locally in the secure iLO 2 memory and directory group accounts. Use MMC or ConsoleOne to manage directory user accounts.

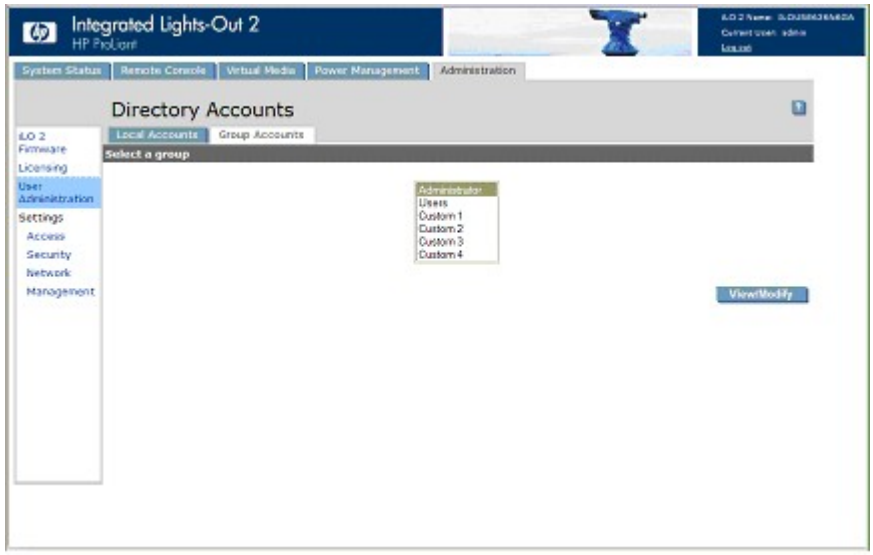
The iLO 2 firmware supports up to 12 users with customizable access rights, login names, and advanced password encryption. Privileges control individual user settings. Users can have privileges customized to their individual access requirements. To support more than 12 users, you must have the Advanced Pack, which enables integration with an unlimited number of directory-based user accounts.

You must have the Administer User Accounts privilege to view iLO 2 users, add new users, and modify or delete existing users. If you do not have this privilege, you can view and modify only your account.

To access local accounts, click **Administration>User Administration>Local Accounts**.



iLO 2 Directory Accounts enables you to view iLO 2 groups and modify the settings for those groups. You must have the Administer Directory Groups privilege. To access Directory Accounts, click **Administration>User Administration>Group Accounts**.



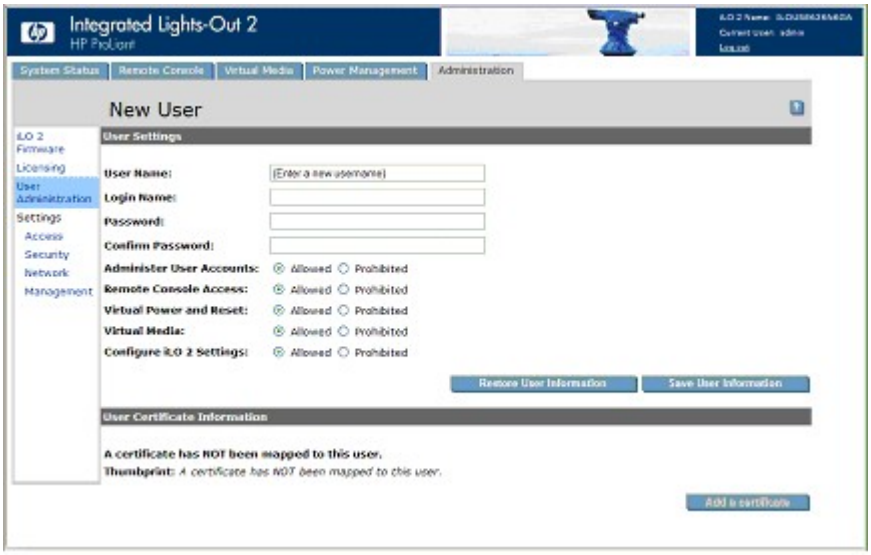
Adding a new user

NOTE: Only users with the **Administer User Accounts** privilege can manage other users on iLO 2.

You can assign a different access privilege to each user. Each user can have a unique set of privileges designed for the tasks that the user must perform. You can grant or deny access to critical functions such as remote access, user management, virtual power, and other features.

To add a new user to iLO 2:

1. Log in to iLO 2 using an account that has the Administer User Accounts privilege.
2. Click **Administration**.
3. Select **User Administration>Local Accounts**.
4. Click **New**.



5. Complete the fields. The following options are available:
   - **User Name** appears in the user list and on the home page. It is not necessarily the same as the Login name. The maximum length for a User Name is 39 characters. The User Name must use printable characters.
   - **Login Name** is the name that you must use when logging in to iLO 2. The maximum length for a login name is 39 characters. The login name can only use printable characters.
   - **Password** and **Confirm Password** fields set and confirm the password that is used when logging in to iLO 2. The minimum length for a password is set in the **Access Options** page. The maximum length for a password is 39 characters. Enter the password twice for verification.
   - **Administer User Accounts** is a user privilege that allows you to add, modify, and delete local iLO 2 user accounts. **Administer User Accounts** also allows you to alter privileges for all users, including granting all permissions to yourself. Without this privilege, you can only view your own settings and change your own password.
   - **Remote Console Access** is a user privilege that allows you to remotely access the host system Remote Console and Remote Serial Console, including video, keyboard and mouse control. You are still required to have access to the remote system to use this capability.
   - **Virtual Power and Reset** is a user privilege that allows you to power-cycle or reset the host platform. Any of these activities interrupts the availability of the system. You can also diagnose the system using the virtual NMI button.
   - **Virtual Media** is a user privilege that allows you to use virtual media on the host platform.
   - **Configure iLO 2 Settings** is a privilege that allows you to configure most iLO 2 settings, including security settings. **Configure iLO 2 Settings** enables you to remotely update iLO 2 firmware. It does not include user account administration. These settings rarely change.

     After correctly configuring iLO 2, revoking this privilege from all users prevents reconfiguration. A user with the Administer User Accounts privilege can enable or disable this privilege. If iLO 2 RBSU is enabled, you can also reconfigure iLO 2.
   - **User Certificate Information** maps a certificate to a user. User certificates are only required for two-factor authentication. If a certificate is not mapped to the user account, then the following message displays `A certificate has NOT been mapped to this user`, along with the **Add a Certificate** button. Click this button to map a certificate to the user. After a certificate is mapped to the user account, a 40-digit thumbprint of the certificate appears, along with the **Remove this Certificate** button, which can be used to remove the certificate. If Two-Factor Authentication is enabled, map a different certificate

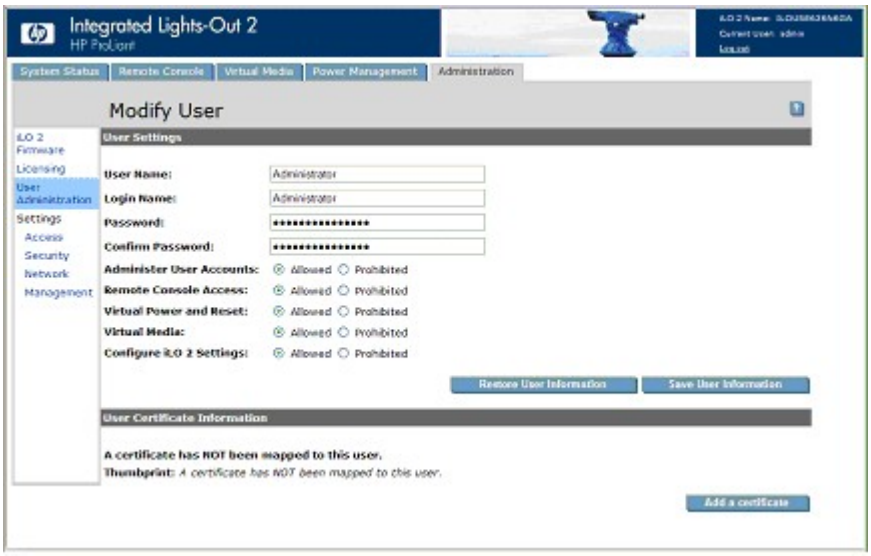
to each user. A user who presents a certificate when connecting to iLO 2 is authenticated as the user to whom the certificate is mapped. Two-Factor Authentication must be enabled to authenticate using a certificate.

6. When the user profile is complete, return to the User Administration screen by clicking **Save User Information**. To clear the user profile while entering a new user, click **Restore User Information**.

Viewing or modifying existing user settings

1. Log in to iLO 2 using an account that has the Administer User Accounts privilege.

   You must have the Administer User Accounts privilege to manage other users on iLO 2. All users can change their own password using the View/Modify User feature.
2. Click **Administration>User Administration**, and select the name of the user whose information you want to modify.
3. Click **View/Modify**.



4. Change user information as required.
5. After changing the fields, return to the User Administration screen by clicking **Save User Information**. To recover the original user information, click **Restore User Information**. All changes made to the profile are discarded.

Deleting a user

NOTE: Only users with the Administer User Accounts privilege can manage other users on iLO 2.

To delete existing user information:

1. Log in to iLO 2 using an account that has the Administer User Accounts privilege.
2. Click **Administration**.
3. Click **User Administration** and select from the list the name of the user whose information you want to change.
4. Click **Delete User**.

   A pop-up window displays:

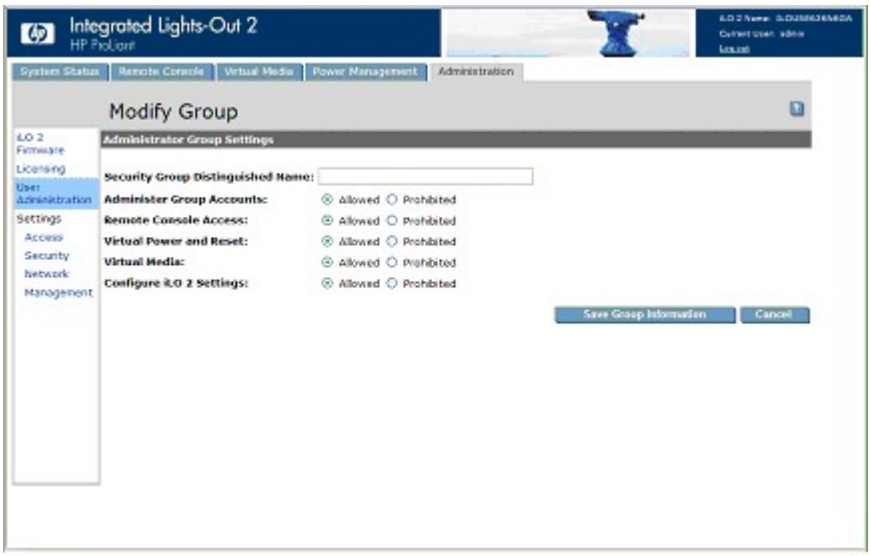
   ```
   Are you sure you want to delete the selected user?
   ```
5. Click **OK**.

Group administration

The iLO 2 firmware enables you to view iLO 2 groups and modify settings for those groups. You must have the Administer Directory Groups privilege. To view or modify a group:

1. Click **Administration>User Administration>Group Accounts**.
2. Select the group, and click **View/Modify Group**. The Modify Group page appears.

   Click **Cancel** to return to the Group Administration page.



The following settings are available:

- Security Group Distinguished Name is the distinguished name of a group within the directory. All members of this group are granted the privileges set for the group. The group specified in the Security Group Distinguished Name must exist within the directory, and users who need access to iLO 2 must be members of this group. Complete this field with a Distinguished Name from the directory (for example, `CN=Group1,OU=Managed Groups, DC=domain, DC=extension`).
- Administer Group Accounts enables users who belong to this group to alter privileges for any group.
- Remote Console Access enables you to remotely access the host system Remote Console, including the Remote Serial Console. You must have access to the remote system to use this capability.
- Virtual Power and Reset enables you to power cycle or reset the host platform. These activities interrupt the availability of the system. If selected, this option also allows you to diagnose the system using the virtual NMI button.
- Virtual Media enables you to use virtual media on the host platform.
- Configure iLO 2 Settings enables you to configure most iLO 2 settings, including security settings. If selected, you can remotely update iLO 2 firmware. This setting does not include group account administration. These settings rarely change.

  After iLO 2 is correctly configured, revoking this privilege from all groups prevents reconfiguration. Users with the Administer Group Accounts privilege can enable or disable this privilege. The iLO 2 firmware can also be reconfigured if iLO 2 RBSU is enabled.

To save updated information, click **Save Group Information**, or to discard changes and return to the Group Administration page, click **Cancel**.

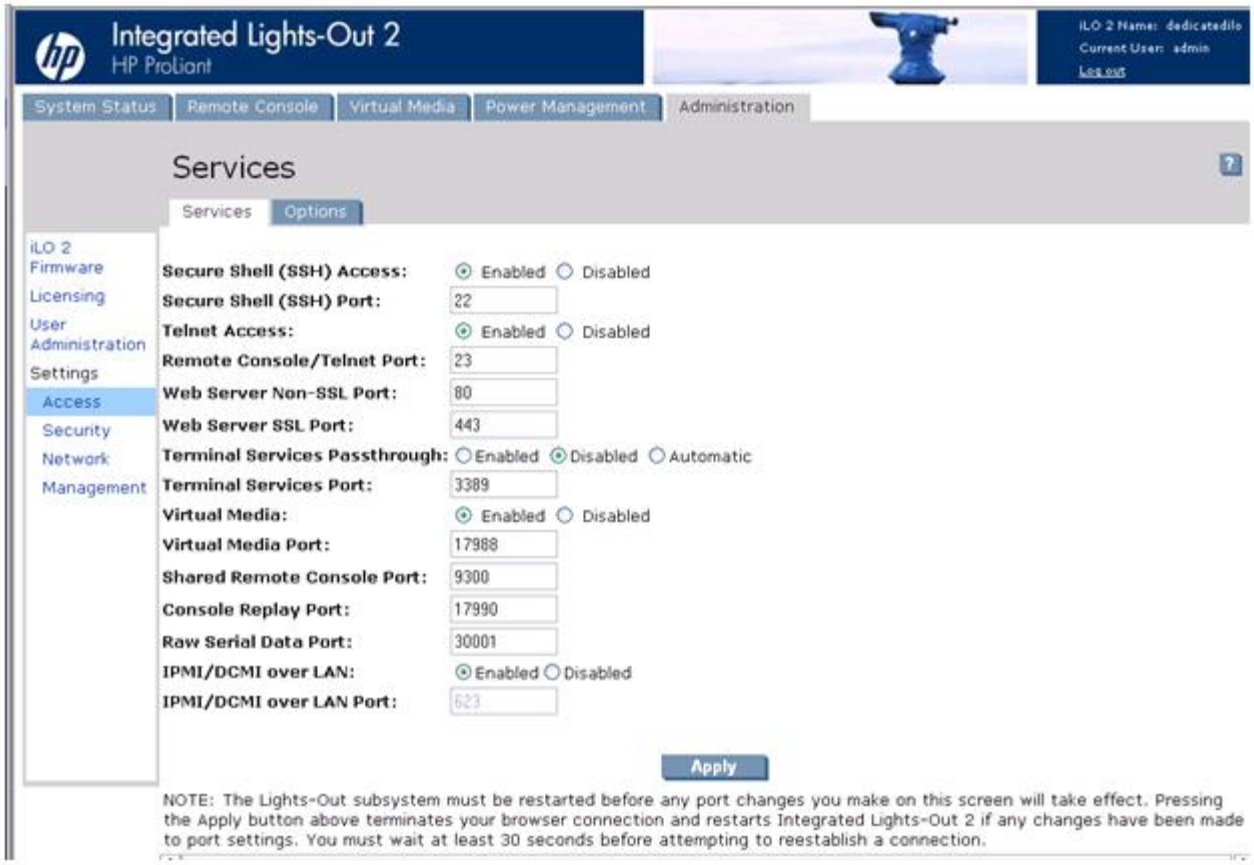
Configuring iLO 2 access

The iLO 2 firmware enables you to configure which services are enabled on iLO 2 and user access to iLO 2. To configure iLO 2 services options, click **Administration>Access.** The Services page (tab) appears. To configure iLO 2 access options), click **Administration>Access>Options** (tab). You must have the Configure iLO 2 Settings privilege to modify iLO 2 services and access options. For more information, see "Access options" (page 38).

Services options

The Services tab enables you to select which services you want to enable on iLO 2, including SSH, SSL, Remote Console, Telnet, and Terminal Services. The Services tab also enables you to set the ports for each selected option. Settings on the Services page apply to all iLO 2 users. You must have the Configure iLO 2 Settings privilege to modify settings on this page.

To access Services, click **Administration>Access>Services**. Click **Apply** to save updated information. You must restart iLO 2 before any changes take effect. If any changes have been made to enable or disable Lights-Out functionality, clicking **Apply** terminates your browser connection and restarts iLO 2. You must wait at least 30 seconds before attempting to reestablish a connection.



The Services tab includes the following settings:

Parameter	Default value	Description
Secure Shell (SSH) Access	Enabled	This setting enables you to specify whether the SSH feature on the iLO 2 is enabled or disabled.
Secure shell (SSH) Port	22	This setting enables you to configure the iLO 2 SSH port to be used for SSH communications.

Parameter	Default value	Description
Telnet Access	Disabled	This setting enables you to connect a Telnet client to the Remote Console/Telnet port, providing access to the iLO 2 CLP. The following settings are valid: • Enabled – iLO 2 enables Telnet clients to connect to the Remote Console/Telnet port. Network port scanners can detect that iLO 2 is listening on this port. Unencrypted communication is allowed between the iLO 2 CLP and Telnet clients. • Disabled – iLO 2 does not allow Telnet clients to connect to the Remote Console/Telnet port. Network port scanners will not normally detect if this port is open on iLO 2. iLO 2 listens on this port for a few seconds when the Remote Console is opened, but Telnet connections are not accepted. Communication between the iLO 2 and Remote Console is always encrypted.
Remote Console/Telnet Port	23	This setting enables you to specify which port the iLO 2 Remote Console uses for remote console communications.
Web Server Non-SSL Port	80	This setting enables you to specify which port the embedded web server in iLO 2 uses for unencrypted communications.
Web Server SSL Port	443	This setting enables you to specify which port the embedded web server in iLO 2 uses for encrypted communications.
Terminal Services Passthrough	Disabled	This setting enables you to control the ability to support a connection through iLO 2 between a Microsoft Terminal Services client and Terminal Services server running on the host. The following settings are valid: • Automatic – When remote console is started, the Terminal Services client is launched. • Enabled – The passthrough feature is enabled and can connect the Terminal Services client directly to the iLO 2 without logging-into the iLO 2. • Disabled – The passthrough feature is off.
Terminal Services Port	3389	This setting enables you to specify the Terminal Services Port that the iLO 2 uses for encrypted communications with Terminal Services passthrough software on the server. If the Terminal Services port is configured to anything other than the default, you must manually change the port number.
Virtual Media	Enabled	This setting enables you to specify whether the virtual media port on the iLO 2 is enabled or disabled. The following settings are valid: • Enabled – iLO 2 enables the Virtual media port. • Disabled – iLO 2 disables the Virtual media port.
Virtual Media Port	17988	This setting enables you to specify the port for virtual media support in iLO 2 communications.
Shared Remote Console Port	9300	This setting enables you to specify the Shared Remote Console Port. The Shared Remote Console Port is opened on the client to allow additional users to connect to remote console in a peer-to-peer fashion. This port is only open when Shared Remote Console is in use.
Console Replay Port	17990	This setting enables you to specify the Console Replay Port. The Console Replay Port is opened on the client to enable the transfer of internal capture buffers to the client for replay. This

Parameter	Default value	Description
		port is only open when a capture buffer is being transferred to the client.
Raw Serial Data Port	3002	This setting specifies the Raw Serial Data port address. The Raw Serial Data port is only open while the `WiLODbg.exe` utility is being used to debug the host server remotely.

Terminal Services Passthrough option

Terminal Services is provided by the Microsoft Windows operating systems. The iLO 2 Terminal Services Passthrough 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 Passthrough option is enabled, the iLO 2 firmware enables a socket, listening by default on port 3389. All data received from Terminal Services on this port is forwarded to the server and all data Terminal Services receives from the server is forwarded back to the socket. The iLO 2 firmware reads anything received on this port as an RDP packet. RDP packets are exchanged between the iLO 2 firmware and the server Terminal Services (RDP) server through the local host address on the server. The service provided facilitates communications between the iLO 2 firmware and the RDP server. The RDP server interprets the service as an established external RDP connection. For more information on RDP services, see "Windows RDP Passthrough service" (page 36).

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 iLO 2 Remote Console provides a view of the host system console. For more information on Remote Console and Terminal Services, see "Remote Console and Terminal Services clients" (page 37).

To configure the Terminal Services Passthrough option, see the "Terminal Services client requirements" (page 35) and "Terminal Services Passthrough installation" (page 36).

Terminal Services client requirements

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

- Windows Server 2003

  On Windows Server 2003 servers, the Terminal Services client and RDP connection is built-in. The client is part of the operating system and is activated using Remote Desktop sharing. To activate desktop sharing, 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 Server 2008

  On Windows Server 2008 servers, the Terminal Services client and RDP connection is built-in. The client is part of the operating system and is activated using Remote Desktop sharing. To activate desktop sharing, select **My Computer>Properties>Remote>Remote Desktop**. The Terminal Services client in Windows Server 2008 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 part of the operating system and is activated using Remote Desktop sharing. To activate desktop sharing, select **Start>Programs>Accessories>Communications>Remote Desktop**. The Terminal Services client in Windows XP provides command-line options and launches from the remote console applet.

Windows RDP Passthrough service

To use the iLO 2 Terminal Services Passthrough feature, you must install a passthrough service on the host system. This service displays the name of the iLO 2 Proxy in the host list of available services. The service utilizes Microsoft .NET framework security and reliability. After the service is started, the service polls iLO 2 to detect if an RDP connection with the client is established. If an RDP connection with the client is established, the service establishes a TCP connection with local host and begins exchanging packets. The port used to communicate with the local host is read from the Windows registry at:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\
Wds\rdpwd\Tds\tcp\PortNumber
```

The port is typically port 3389.

Terminal Services Passthrough installation

The following section describes how to install Terminal Services Passthrough on Windows Server 2008, Windows Server 2003, and Microsoft Windows XP.

- Windows Server 2003 and Windows Server 2008

  Windows servers require Microsoft .NET Framework to support the use of iLO 2 Terminal Services. The Terminal Services Passthrough service and the iLO 2 Management Interface driver for Windows Server 2008 and Windows Server 2003 must be installed on the server that has the iLO 2.

  1. Install the iLO 2 Management Interface driver.
  2. Install the passthrough service. To install the service, launch the component installer and follow the directions in the installation wizard.

     If the service is already installed, then you must manually restart or reboot the server when the driver is installed.
  3. Activate the Terminal Services client.

     On Windows Server 2003 and Windows Server 2008, you can activate Remote Desktop sharing by clicking the **Remote** tab under My Computer and Properties.

  If the iLO 2 installation is complete, and if iLO 2 Terminal Services passthrough option is set to automatic, then Terminal Services launches when the installation is complete.

- Microsoft Windows XP

  On Windows XP, the Remote Desktop Connection is built-in and has no other installation requirements.

Errors that occur during installation and execution of the passthrough service are logged in the server Application Event Log. You can remove the passthrough service using Add or Remove Programs in the Control Panel.

Enabling the Terminal Services Passthrough option

By default, the Terminal Services Passthrough feature is disabled and can be enabled on the **Administration>Access>Services** page. The Terminal Services button in the Remote Console is deactivated until the Terminal Services passthrough feature is enabled.

To use of the Terminal Services Passthrough feature, install the latest Lights-Out Management Interface Driver and then install Terminal Services passthrough service for Microsoft Windows on the server.

When the Terminal Services Passthrough option is set to Enabled or Automatic on the **Administration>Access>Services** 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 you click the **Terminal Services** button, 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 iLO 2, or both.

Terminal Services warning message

Terminals Services users operating on Windows 2003 Server might notice the following when using the Terminal Services passthrough feature of iLO 2. If a Terminal Services session is established through iLO 2 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 Passthrough option display

The iLO 2 firmware might not accurately display the Terminal Services Passthrough option. The Terminal Services Passthrough option might appear active even if the operating system is not Terminal Services enabled (for example, if the host operating system is Linux, which does not support Terminal Services operation).

Remote Console and Terminal Services clients

Using the management network connection to the iLO 2, an iLO 2 Remote Console session can be used to display a Terminal Services session to the host. When the iLO 2 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 Remote Console cannot automatically launch the Terminal Services client.

If Terminal Services passthrough is enabled, and the Terminal Services server is available, switching between iLO 2 Remote Console and the Terminal Services client will be seamless as the server progresses from pre-operating system environment to operating system-running environment, to operating system-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 passthrough option with Windows Server 2003 and Windows Server 2008, a 30-second delay occurs after the CTRL-ALT-DEL dialog box appears before the Terminal Services client launches. 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 iLO 2 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 launch the Terminal Services client directly from the Terminal Services client menu. Launching directly from the client menu enables 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 iLO 2 firmware to reset. Resetting the iLO 2 firmware interrupts any open connections to iLO 2.

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 iLO 2.

The iLO 2 firmware 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 events:

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

Terminal Services troubleshooting

To resolve issues with iLO 2 Terminal Services Passthrough:

1. Verify that Terminal Services is enabled on the host by selecting

   My Computer>Properties>Remote>Remote Desktop.
2. Verify that the iLO 2 passthrough configuration is enabled or automatic in the iLO 2 Global Settings.
3. Verify that iLO Advanced Pack is licensed.
4. Verify that the iLO 2 Management Interface Driver is installed on the host. To verify the driver, select **My Computer>Properties>Hardware>Device Manager>Multifunction Adapters**.
5. Verify that the Terminal Services passthrough service and iLO 2 Proxy are installed and running on the host. To verify these services, select **Control Panel>Administrative Tools>Services** and attempting to restart the service.
6. Verify that the Application Event Log is not full.

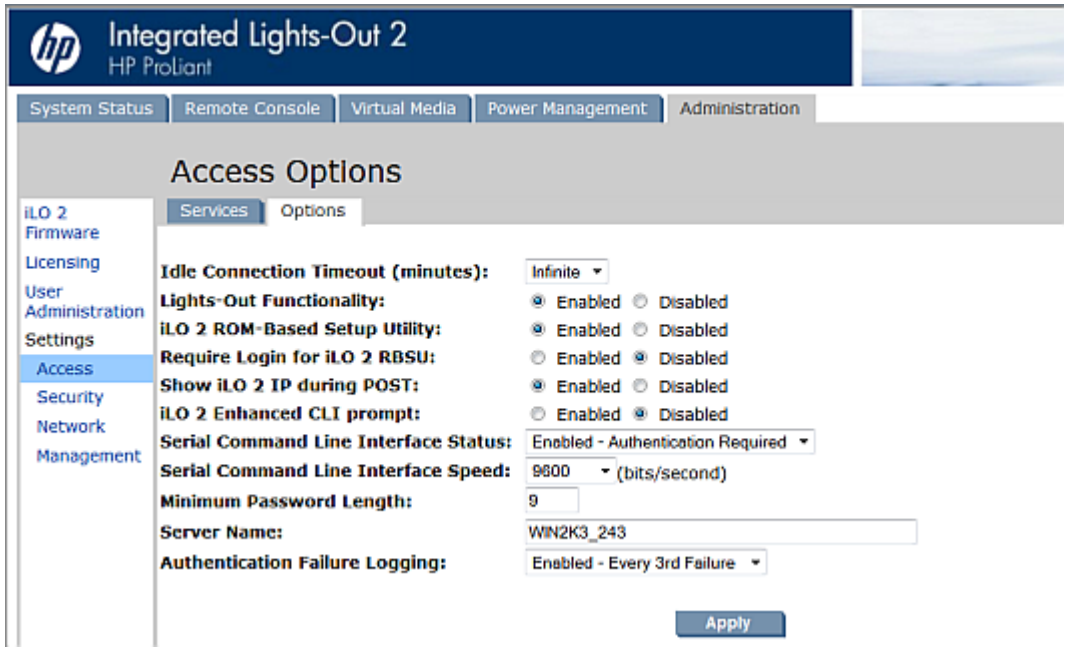
   The Terminal Services passthrough service might experience start-up issues when the operating system Application Event Log is full. To view the event log, select **Computer Management>System Tools>Event Viewer>Application**.
7. Verify that the Terminal Services port assignment is correct.
8. Verify that the Terminal Services client, `mstsc.exe` is located in `\WINDOWS\SYSTEM32`.

   If not, set the passthrough configuration to **Enabled**, and manually activate the terminal services client.

Access options

The iLO 2 firmware enables you to modify iLO 2 access, including connection idle time, iLO 2 functionality, iLO 2 RBSU, login requirements, CLI parameters, minimum password length, and server name. Settings on the Access Options page apply to all iLO 2 users. You must have the Configure iLO 2 Settings privilege to modify settings on this page.

To view or modify iLO 2 access, click **Administration>Access>Options** and click **Apply** to save any updated information. You must restart iLO 2 before your updates take effect. If any changes enable or disable Lights-Out functionality, click **Apply** to terminate your browser connection and restart iLO 2. You must wait at least 30 seconds before attempting to reestablish a connection.



The Options tab includes the following.

Parameter	Default value	Descriptions
Idle Connection Timeout (minutes)	30 minutes	This setting specifies the interval of user inactivity, in minutes, before the web server and Remote Console session automatically terminate. The following settings are valid: 15, 30, 60, 120 minutes, or 0 (infinite). The infinite timeout value does not log out inactive users.
Lights-Out Functionality	Enabled	This setting enables connection to iLO 2. If disabled, all connections to iLO 2 are prevented. The iLO 2 10/100 network and communications with operating system drivers are turned off if Lights-Out functionality is disabled. The iLO 2 Diagnostic Port for an HP ProLiant BL p Class server is also disabled. If iLO 2 functionality is disabled (including the iLO 2 Diagnostic Port), you must use the server Security Override Switch to enable iLO 2. See your server documentation to locate the Security Override Switch and set it to Override. Power the server on and use the iLO 2 RBSU to set Lights-Out Functionality to Enabled.
iLO 2 ROM-Based Setup Utility	Enabled	This setting enables or disables the iLO 2 ROM-Based Setup Utility. Normally, the iLO2 Option ROM prompts you to press **F8** to enter RBSU, but if iLO 2 is disabled or iLO 2 RBSU is disabled, the RBSU prompt is bypassed.
Require Login for iLO 2 RBSU	Disabled	This setting enables RBSU access with or without a user-credentials challenge. If this setting is Enabled and you press **F8** during POST to enter iLO 2 RBSU, a login dialog box appears.
Show iLO 2 during POST	Disabled	This setting enables the display of the iLO 2 network IP address during the host server POST process.
iLO 2 Enhanced CLI prompt	Disabled	The SMASH CLP can be enhanced by including the server name in the “hpiLO” prompt. This button enables the user to enable or disable the enhanced CLI prompt feature. By default, this feature is disabled. The following settings are valid: • Enabled – iLO 2 enables the enhanced CLI prompt feature. • Disabled – iLO 2 disables the enhanced CLI prompt.

Parameter	Default value	Descriptions
Serial Command Line Interface Status	Enabled-Authentication Required	This setting enables you to change the login model of the CLI feature through the serial port. The following settings are valid: • Enabled – Authentication Required • Enabled – No Authentication • Disabled
Serial Command Line Interface Speed	9600	This setting enables you to use the serial port to change the speed of the serial port for the CLI feature. The following speeds (in bits/s) are valid: 9600, 19200, 38400, 57600, and 115200. The serial port configuration must be set to No parity, 8 data bits, and 1 stop bit (N/8/1) for proper operation. The serial port speed that is set by this parameter must match the speed of the serial port set in the System ROM RBSU setup.
Minimum Password Length	8	This setting specifies the minimum number of characters allowed when a user password is set or changed. The character length can be set at a value from 0 to 39.
Server Name		This setting enables you to specify the host server name. This value is assigned when using HP ProLiant Management Agents. If you do not use the agents and the `host unnamed` message appears, you can change it here. If the agents are running, the value you assign can be overwritten. To force the browser to refresh, save this setting, and press **F5**.
Authentication Failure Logging	Enabled-Every 3rd Failure	This setting enables you to configure logging criteria for failed authentications. All login types are supported and every login type works independently. The following are valid settings: • Enabled-Every Failure – A failed login log entry is recorded after every failed login attempt. • Enabled-Every 2nd Failure – A failed login log entry is recorded after every second failed login attempt. • Enabled-Every 3rd Failure – A failed login log entry is recorded after every third failed login attempt. • Enabled-Every 5th Failure – A failed login log entry is recorded after every fifth failed login attempt. • Disabled – No failed login log entry is recorded.
Virtual Serial Port Log	Disabled	This setting enables you to capture the serial port output messages into a circular log buffer. The following settings are valid: • Enabled - Virtual serial Port log feature is enabled. • Disabled - Virtual serial Port log feature is disabled.

When logging in to iLO 2 with Telnet or SSH clients, the number of login name and password prompts offered by iLO 2 matches the value of the Authentication Failure Logging parameter (or 3 when it is disabled.) However, the number of prompts might also be affected by your Telnet and SSH client configurations. Telnet and SSH logins also implement delays after login failure. During the delay, login is disabled so no login failure occurs. As an example, to generate an SSH authentication failure log with a default value (for instance, Enabled-Every 3rd Failure), three consecutive login failures occur as follows (assuming the SSH client is configured with the number of password prompts >= 3):

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

connection terminates, and the second login failure is recorded. The SSH login failure counter is set to 2.

3. Run the SSH client until receiving the login prompt. Log in with an incorrect login name and password. You will receive three password prompts. After the third incorrect password, the connection terminates and the third login failure is recorded. The SSH login failure counter is set to 3.

At this point, iLO 2 firmware records an SSH login failure log entry and sets the SSH login failure counter to 0.

iLO 2 Remote Console and Remote Serial Console access

For iLO 2 Remote Console recommended client settings, server settings, optimizing mouse support, and Remote Serial Console settings, see "iLO 2 Remote Console" (page 80).

Security

The iLO 2 firmware enables you to customize iLO 2 security settings. To access iLO 2 security settings, select **Administration>Security**. iLO 2 security options include:

- "SSH key administration" (page 44)
- "SSL certificate administration" (page 45)
- "Two-factor authentication" (page 46)
- "Directory settings" (page 51)
- "Encryption" (page 53)
- "HP SIM single sign-on (SSO)" (page 55)
- "Remote Console Computer Lock" (page 58)

iLO 2 security options enables iLO 2 to provide the following security features:

- User-defined TCP/IP ports
- User actions logged in the iLO 2 Event Log
- Progressive delays for failed login attempts
- Support for X.509 CA signed certificates
- Support for securing RBSU
- Encrypted communication using:
  - SSH key administration
  - SSL certificate administration
- Support for optional LDAP-based directory services

Some of these options are licensed features. To verify your available options, see "Licensing" (page 26).

General security guidelines

The following are general guidelines concerning security for iLO 2:

- For maximum security, iLO 2 must be set up on a separate management network.
- The iLO 2 firmware must 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. Passwords must:

- Never be written down or recorded
- Never be shared with others
- Not be words generally found in a dictionary, or easy to guess words, such as the company name, product names, the user's name, or the user's User ID
- Include at least three of the four 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, password reset, or a locked-out user ID must also conform to these standards. Each password must be a minimum length of zero characters and a maximum length of 39 characters. The default minimum length is set to eight characters. Setting 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.

Securing RBSU

iLO 2 RBSU enables you to view and modify the iLO 2 configuration. RBSU access settings can be configured using RBSU, a web browser, RIBCL scripts, or the iLO 2 Security Override Switch. For more information, see "Access options" (page 38). RBSU has three levels of security:

- RBSU Login Not Required (default)

  Anyone with access to the host during POST can enter the iLO 2 RBSU to view and modify configuration settings. This is an acceptable setting if host access is controlled.

- 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 Disabled (most secure)

  If iLO 2 RBSU is disabled, user access is prohibited. This prevents modification using the RBSU interface.

iLO 2 Security Override Switch administration

The iLO 2 Security Override Switch allows the administrator full access to the iLO 2 processor. This access might be necessary for any of the following conditions:

- The iLO 2 firmware must be re-enabled after it has been disabled.
- All user accounts with the Administer User Accounts privilege have been locked out.
- A bad configuration keeps the iLO 2 from displaying on the network and RBSU has been disabled.
- The boot block must be flashed.

Ramifications of setting the Security Override Switch include:

- All security authorization checks are disabled while the switch is set.
- The iLO 2 firmware RBSU runs if the host server is reset.
- The iLO 2 firmware is not disabled and might display on the network as configured.

- The iLO 2 firmware, if disabled while the Security Override Switch is set, does not log the user out and complete the disable process until the power is cycled on the server.
- The boot block is exposed for programming.

NOTE: The iLO 2 Security Override Switch is located inside the server and cannot be accessed without opening the server enclosure.

A warning message appears on iLO 2 browser pages indicating that the iLO 2 Security Override Switch is currently in use. An iLO 2 log entry records the use of the iLO 2 Security Override Switch. An SNMP alert can also be sent upon setting or clearing the iLO 2 Security Override Switch.

Setting the iLO 2 Security Override Switch also enables you to flash the iLO 2 boot block. HP does not anticipate you needing to update the iLO 2 boot block. If an iLO 2 boot block update is required, you must perform the update at the server, then and reset iLO 2. The boot block update cannot be done remotely. The boot block is exposed until iLO 2 is reset. For maximum security, HP recommends that you disconnect the iLO 2 from the network until you complete the reset.

To set the iLO 2 Security Override Switch:

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

Reverse the procedure to clear the iLO 2 Security Override Switch.

Depending on the server, the iLO 2 Security Override Switch might be a single jumper or a specific switch position on a dip switch panel. To access and locate the iLO 2 Security Override Switch, see the server documentation. The iLO 2 Security Override Switch can also be located using the diagrams on the server access panel.

Trusted Platform Module support

TPM is a hardware based system security feature. It is a computer chip that securely stores artifacts used to authenticate the platform. These artifacts can include passwords, certificates, or encryption keys. You can also use a TPM to store platform measurements to help ensure that the platform remains trustworthy. iLO 2 provides support for the TPM mezzanine module in ProLiant 100, 300, and 500 series servers.

On a supported system, iLO 2 decodes the TPM record and passes the configuration status to iLO 2, CLP, and XML interface. The System Status page displays the TPM configuration status. If the host system or System ROM does not support TPM, TPM Status is not displayed in **Status Summary** page. The Status Summary displays the following TPM status information:

- Not Present – A TPM module is not installed.
- Present – when:
  - A TPM module is installed but it is disabled.
  - A TPM module is installed and enabled.
  - A TPM module is installed, enabled, and Expansion ROM measuring is enabled. If Expansion ROM measuring is enabled, the Update iLO 2 Firmware page displays a legal warning message when you click **Send firmware image**.

User accounts and access

The iLO 2 firmware supports the configuration of up to 12 local user accounts. Each of these accounts can be managed through the use of the following features:

- “Privileges” (page 44)
- “Login security” (page 44)

The iLO 2 firmware iLO 2 can be configured to use a directory to authenticate and authorize its users. This configuration enables a virtually unlimited number of users, and easily scales to the number of Lights-Out devices in an enterprise. Additionally, the directory provides a central point of administration for Lights-Out devices and users, and the directory can enforce a stronger password policy. iLO 2 enables you to use local users, directory users, or both.

Two configuration options are available:

- To use a directory that has been extended with HP Schema, see "Setting up HP schema directory integration" (page 136).
- To use the directory default schema (schema-free), see "Setting up Schema-free directory integration" (page 132).

Privileges

The iLO 2 firmware enables the administrator to control user account access to iLO 2 functions through the use of privileges. When a user attempts to use a function, the iLO 2 system verifies that the user has the privilege before the user is allowed to perform the function.

Each feature available through iLO 2 can be controlled through privileges, including Administer User Accounts, Remote Console Access, Virtual Power and Reset, Virtual Media, and Configure iLO 2 Settings. Privileges for each user can be configured on the User Administration page of the Administration tab.

Login security

iLO 2 provides several login security features. After an initial failed login attempt, iLO 2 imposes a delay of five seconds. After a second failed attempt, iLO 2 imposes a delay of 10 seconds. After the third failed attempt, and any subsequent attempts, iLO 2 imposes a delay of 60 seconds. All subsequent failed login attempts cycles through these values. An information page appears during each delay. This continues until a valid login is completed. This feature assists in defending against possible dictionary attacks against the browser login port.

The iLO 2 firmware saves a detailed log entry for failed login attempts, which imposes a delay of 60 seconds.

SSH key administration

The iLO 2 firmware enables you to authorize up to four SSH keys at one time on the SSH Key tab. The SSH Key tab also displays the owner (if any keys are authorized) of each authorized SSH key. Multiple keys can belong to a single user.

To add an authorized key to iLO 2, the public key path must be submitted to iLO 2. The key file must contain the user name after the end of the key. iLO 2 associates each key with a local user account. If the local account does not exist or if it is deleted, the key is invalid (the key is not listed if the local account does not exist).

Alternatively, you can authorize SSH keys for an HP SIM server by running the mxagentconfig tool from the HP SIM server and specifying the address and user credentials for iLO 2. See your HP SIM documentation for more details.

To authorize a new key:

1. In the iLO 2 interface, click **Administration>Security>SSH Key**.
2. Click **Browse**, and locate the key file.
3. Click **Authorize Key**.

You can view or delete any previously authorized key by selecting the key, and clicking **View Selected Key** or **Delete Selected Key**. The **View Selected Key** and **Delete Selected Key** buttons only appear when SSH keys are installed.

SSL certificate administration

The iLO 2 firmware enables you to create a certificate signing request (CSR) with custom subject information or default settings, import a certificate, and view certificate administration information associated with a stored certificate. Certificate information is encoded in the certificate by the CA and is extracted by iLO 2.

By default, iLO 2 creates a self-signed certificate for use in SSL connections. This certificate enables iLO 2 to work without any additional configuration steps. The security features of the iLO 2 can be enhanced by importing a trusted certificate. For more information on certificates and certificate services, see "Introduction to certificate services" (page 132) and "Installing certificate services" (page 132).

To access certificate information, click **Administration>Security>SSL Certificate**. The SSL Certificate tab displays the following information:

- The Issued To field lists the entity to which the certificate was issued.
- The Issued By field lists the CA that issued the certificate.
- The Valid From field lists the first date that the certificate is valid.
- The Valid Until field lists the date that the certificate will expire.
- The Serial Number field lists the serial number assigned to the certificate by the CA.
- The Domain Name button to choose between the fully qualified domain name and the shortname as CSR Common Name (CN).
- The SSL Key Length button to choose between 2048 or 1024 bit private key length for CSR.
- The Customized CSR radio button to choose between CSR with custom or default subject fields.
- The Country field for configuring the CSR subject country name.
- The State or Province field for configuring the CSR subject state name.
- The Organization Name field for configuring the CSR subject organization name.
- The Organization Unit field for configuring the CSR subject organization unit name.
- The City or Locality field for configuring the CSR subject city or locality name.
- The Common Name field for configuring the CSR subject common name.

The following options are available on the SSL Certificate tab:

- Apply Button – When you click the Apply button, custom CSR data is validated and stored in iLO2. During the certificate generation request, the stored CSR settings are used by iLO2.
- Create Certificate Request – Use this button to create a certificate request. When you click this button, a CR is created (in PKCS #10 format) that can be sent to a CA. This certificate request is Base64-encoded. A CA processes this request and returns a response (X.509 certificate) that can be imported into iLO 2.

  The CR contains a public/private key pair that validates communications between the client browser and iLO 2. The generated CR is held in memory until a new CR is generated, iLO 2 is reset, or a certificate is imported by the generation process. You can generate the CR and copy it to the client clipboard, leave the iLO 2 website to retrieve the certificate, and then return to import the certificate.

  When submitting the request to the CA, be sure to perform the following tasks:

  1. Use the iLO 2 name as listed on the System Status screen as the URL for the server.
  2. Request that the certificate is generated in the RAW format.
  3. Include the `Begin` and `End` certificate lines.

  Every time you click **Create Certificate Request,** a new certificate request is generated, even though the iLO 2 name is the same. Generally SSL keys pairs are pre-generated. The CSR is

generated immediately on clicking the Create Certificate Request button. However, the certificate request generation button is grayed out while the key generation is in progress. In this scenario, you can close all active Remote Console sessions and try again later (around 2 minutes for a 1024-bit key, and 10 minutes for 2048-bit key).

- **Import Certificate** – Use this button when you are returning to the Certificate Administration page with a certificate to import. Click **Import Certificate** to go directly to the Certificate Import screen without generating a new CR. A certificate only works with the keys generated for the original CR from which the certificate was generated. If iLO 2 has been reset, or another CR was generated since the original CR was submitted to a CA, then a new CR must be generated and submitted to the CA.

You can customize and create a CR or import an existing certificate using RIBCL XML commands. These commands enable you to script and automate certificate deployment on iLO 2 servers instead of manually deploying certificates through the browser interface. For more information, see *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide* at http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=135&prodTypeId=18964&prodSeriesId=1146658.

Two-factor authentication

Access to iLO 2 requires user authentication. This firmware release provides an enhanced authentication scheme for iLO 2 using two factors of authentication: a password or PIN, and a private key for a digital certificate. Using two-factor authentication requires that you verify your identity by providing both factors. You can store your digital certificates and private keys wherever you choose, for example, on a smart card, USB token, or hard drive.

The Two-Factor Authentication tab enables you to configure security settings and review, import, or delete a trusted CA certificate. The Two-Factor Authentication Enforcement setting controls whether two-factor authentication is used for user authentication during login. To require two-factor authentication, click **Enabled**. To turn off the two-factor authentication requirement and allow login with user name and password only, click **Disabled**. You cannot change the setting to Enabled if a trusted CA certificate is not configured. To provide the necessary security, the following configuration changes are made when two-factor authentication is enabled:

- Telnet Access: Disabled
- Secure Shell (SSH) Access: Disabled
- 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 iLO 2 with Telnet, SSH, or Serial CLI.

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

A trusted CA certificate is required for two-factor authentication to function. You cannot change the Two-Factor Authentication Enforcement setting to Enabled if a trusted CA certificate is not configured. Also, you must map a client certificate to a local user account if local user accounts are used. If iLO 2 is using directory authentication, client certificate mapping to local user accounts is optional.

To change two-factor authentication security settings for iLO 2:

1. Log in to iLO 2 with an account that has the Configure iLO 2 Settings privilege.
2. Click **Administration>Security>Two-Factor Authentication**.
3. Change the settings by entering your selections in the fields.
4. To save the changes, click **Apply**s.

The Certificate Revocation Checking setting controls whether iLO 2 uses the certificate CRL distribution points attribute to download the latest CRL and verify revocation of the client certificate. If the client certificate is contained in the CRL, or if you cannot download the CRL, access is denied. The CRL distribution point must be available and accessible to iLO 2 when Certificate Revocation Checking is set to `Yes`.

The Certificate Owner Field setting specifies which attribute of the client certificate to use when authenticating with the directory. Only use the Certificate Owner Field setting if directory authentication is enabled. Configuration of the Certificate Owner Field depends on the version of directory support used, the directory configuration, and the certificate issuance policy of your organization. If SAN is specified, iLO 2 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). For example, if the subject name is `/DC=com/DC=domain/OU=organization/CN=user`, iLO 2 will derive `CN=user,OU=organization,DC=domain,DC=com`.

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 "Two-factor authentication" (page 46).

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 iLO 2.
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 it by pressing the **Ctrl+C** keys.
6. Log in to iLO 2, and browse to the Two-Factor Authentication Settings page.
7. Click **Import Trusted CA Certificate**. The Import Root CA Certificate page appears.
8. Click inside 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 iLO 2, 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 inside 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. Select **Enabled** for the Two-Factor Authentication option.
18. Select **Disabled** for the Certificate Revocation Checking option. This value is the default.

19. Click **Apply** to reset iLO 2. When iLO 2 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 might 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 contact your certificate authority.
20. Select the certificate that was added to the user in iLO 2. 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 iLO 2.

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 Base64-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 iLO 2, and browse to the **Two-Factor Authentication Settings** page.
5. Click **Import Trusted CA Certificate**. Another page appears.
6. Click inside 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 Certificate Revocation Checking to `No (default)`.
10. Change Certificate Owner Field to `SAN`. For more information, see "Two-factor authentication" (page 46).
11. Click **Apply**. iLO 2 is reset. When iLO 2 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 iLO 2. Click **OK**.
13. If prompted to do so, insert your smart card, or enter your PIN or password. The login page appears 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 iLO 2. For more information on configuring directory users and privileges, see "Directory settings" (page 51).

Setting up a user for two-factor authentication

To authenticate a user with a local iLO 2 account, 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, the following message displays, as well as a button that starts the certificate import process:

```
Thumbprint: A certificate has NOT been mapped to this user
```

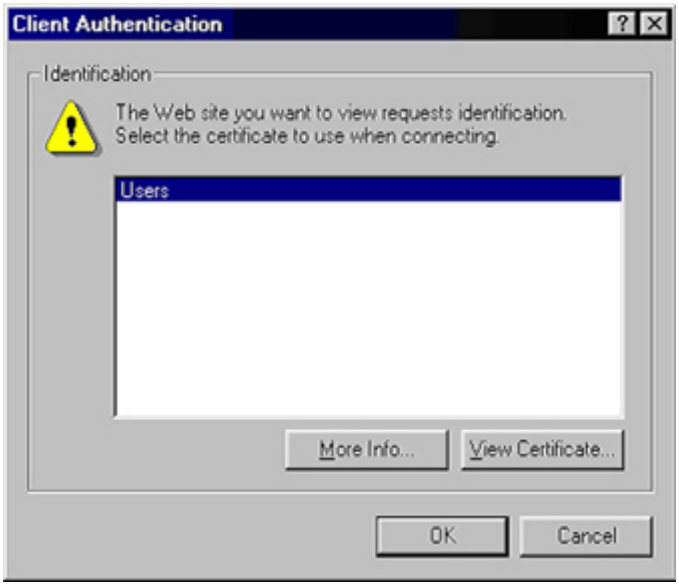
To set up a user for two-factor authentication and add a user certificate:

1. Log in to iLO 2 using an account that has the Configure iLO 2 Settings privilege.
2. Click **Administration>User Administration**. 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 "Setting up two-factor authentication for the first time" (page 47).

Two-factor authentication login

When you connect to iLO 2 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 iLO 2, 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 iLO 2 to ensure it was issued by a trusted CA by checking the signature against the CA certificate configured in iLO 2. iLO 2 determines if the certificate has been revoked and if it maps to a user in the iLO 2 local user database. If all of these tests pass, then the normal iLO 2 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 then try connecting again. If directory authentication is enabled, and local user authentication fails, iLO 2 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). iLO 2 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. iLO 2 can use HP Extended schema or Default Directory schema to integrate with directory services. To ensure security when two-factor authentication is enforced, iLO 2 uses an attribute from the client certificate as the directory user's login name. Which client certificate attribute iLO 2 uses is determined by the Certificate Owner Field configuration setting on the Two-Factor Authentication Settings page. If Certificate Owner Field is set to SAN, iLO 2 obtains the directory user's login name from the UPN attribute of the SAN. If the Certificate Owner Field setting is set to Subject, iLO 2 obtains the directory user's distinguished name from the subject of the certificate.

Which Certificate Owner Field setting to choose depends on the directory integration method used, the directory architecture, and what information is contained in the 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 iLO 2 with `username:john.doe@MyCompany.com` and password works 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 is **not** 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. The Directory User field on the login page is then populated with the user's actual distinguished name, as follows:

`CN=John Doe,OU=IT,DC=MyCompany,DC=com`

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 iLO 2 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. Because this is the correct distinguished name for the user, iLO 2 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 authenticating using the HP Extended Schema method, HP recommends selecting the SAN option on the Two-factor Authentication Settings page.

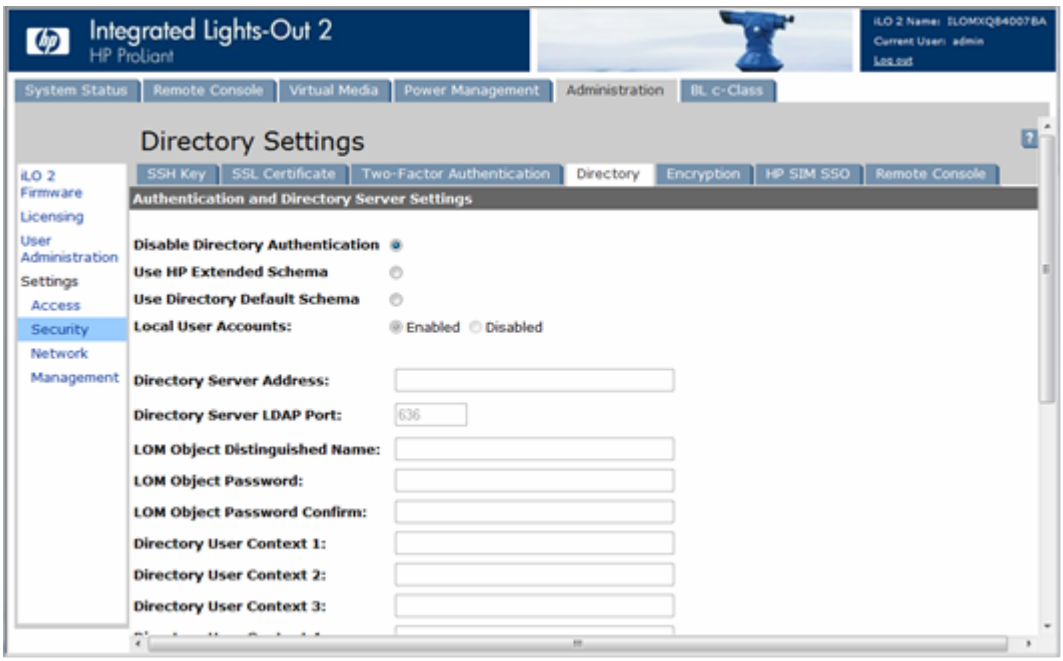
Directory settings

iLO 2 connects to Microsoft Active Directory, Novell e-Directory, and other LDAP 3.0-compliant directory services for user authentication and authorization. You can configure iLO 2 to authenticate and authorize users using the HP schema directory integration or the schema-free directory integration. iLO 2 only connects to directory services using SSL-secured connections to the directory server LDAP port. The default secure LDAP port is 636. Directory services support is a licensed feature available with the purchase of optional licenses. For more information, see "Licensing" (page 26) and "Directory services" (page 130).

Locally-stored user accounts (found on the User Administration page) can be active while iLO 2 directory support is enabled. This support enables both local- and directory-based user directory-based user accesses. Typically, an administrator can delete local user accounts (except required accounts, such as an emergency access account) after iLO 2 is successfully configured to access the directory service. You can also disable access to these accounts if directory support is enabled.

Configuring directory settings

iLO 2 enables administrators to centralize user account administration using directory services. You must have the Configure iLO 2 Settings privilege to configure and test the iLO 2 directory services. To access Directory Settings, click **Administration>Security>Directory**.



iLO 2 directory settings enable you to control directory-related behavior for the iLO 2 directory you are logged in to. These settings include:

- Disable Directory Authentication – Enables you to activate or deactivate directory support on this iLO 2 directory.
  - If directory authentication is enabled and configured properly, users can log in using directory credentials.
  - If directory authentication is disabled, user credentials are not validated using the directory.
- Use HP Extended Schema – Selects directory authentication and authorization using directory objects created with HP schema. Select this option if the directory has been extended with HP schema, and you plan to use it.
- Use Directory Default Schema – Selects directory authentication and authorization using user accounts in the directory. Select this option if the directory is not extended with HP schema.

User accounts and group memberships are used to authenticate and authorize users. After entering the directory network information, to grant users access to iLO 2, click **Administer Groups**, and enter one or more valid directory distinguished names and privileges.

- Enable Local User Accounts – Enables you to limit access to local users.
  - If Local User Accounts are enabled, a user can login using locally stored user credentials.
  - If Local User Accounts are disabled, user access is limited to valid directory credentials only.

  Access using Local User Accounts is enabled if Directory Support is disabled and/or the iLO 2 Select or iLO 2 Advanced License is revoked. You cannot disable local user access if you are logged in using a local user account.

iLO 2 directory server settings enables you to identify the directory server address and port. These settings include:

- Directory Server Address – Enables you to specify the network DNS name or IP address of the directory server. You can specify multiple servers, separated by a comma (,) or space ( ). If Use Directory Default Schema is selected, enter a DNS name in the Directory Server Address field to allow authentication with user ID. For example:

  ```
  directory.hp.com
  192.168.1.250, 192.168.1.251
  ```

- Directory Server LDAP Port – Specifies the port number for the secure LDAP service on the server. The default value for this port is 636. However, you can specify a different value if your directory service is configured to use a different port.
- iLO 2 Directory Properties – Identifies the LOM object in the directory tree. This information is used to determine user access rights. You can configure iLO 2 with the password to the LOM object at this time however, this information is not used until directory configuration support is provided.
- LOM Object Distinguished Name – Specifies where this LOM instance is listed in the directory tree. For example: `cn=iLO 2 Mail Server,ou=Management Devices,o=hp`.

  User search contexts are not applied to the LOM Object Distinguished Name when accessing the directory server.
- LOM Object Password – Specifies the password to the iLO 2 object that iLO 2 uses to verify the directory for updates (LOM Object Distinguished Name).
- Confirm Password – Verifies your LOM Object Password. If you alter the LOM Object Password, reenter the new password in this field.
- User Login Search Contexts enables you to specify common directory subcontexts so that users do not need to enter their full distinguished name at login.

  You can identify all objects listed in a directory using unique distinguished names. However, distinguished names can be long and users might not know their distinguished names, or have accounts in different directory contexts. iLO 2 attempts to contact the directory service by distinguishing name, and then applies the search contexts in order until successful.

  Directory User Contexts specify user name contexts that are applied to the login name.

  Example 1:

  Instead of logging in as `cn=user,ou=engineering,o=hp` a search context of `ou=engineering,o=hp` allows login as `user`.

  Example 2:

  If a system is managed by Information Management, Services, and Training, search contexts like:

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

Allow users in any of these organizations to log in by using just their common names. If a user exists in both the IM organizational unit and the Training organizational unit, login is first attempted as `cn=user,ou=IM,o=hp`.

Example 3 (Active Directory only):

Microsoft Active Directory allows an alternate user credential format. Search contexts in this format cannot be tested except by successful login attempt. A user can log in as:

`user@domain.hp.com` in which case a search context of `@domain.hp.com` allows the user to login as `user`.

To test the communication between the directory server and iLO 2, click **Test Settings**. For more information, see "Directory tests" (page 53).

Directory tests

To validate current directory settings for iLO 2, click **Test Settings** on the Directory Settings page. The Directory Tests page appears.

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

To verify your directory settings:

1. Enter the distinguished name and password of a directory administrator. A good choice would be the same credentials used when creating the iLO 2 objects in the directory. These credentials are not stored by iLO 2. They are used to verify the iLO 2 object and user search contexts.
2. Enter a test user name and password. Typically, this account would be intended to access the iLO 2 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 iLO 2.
3. 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. Consult the help link on the page for test details and actions in the event of trouble.

Encryption

iLO 2 provides enhanced security for remote management in distributed IT environments. Web browser data is protected by SSL encryption. SSL encryption of HTTP data ensures that the data is secure as it is transmitted across the network. iLO 2 provides support for two of the strongest available cipher strengths; the Advanced Encryption Standard (AES) and the Triple Data Encryption Standard (3DES). iLO 2 supports the following cipher strengths:

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

iLO 2 also provides enhanced encryption through the SSH port for secure CLP transactions. iLO 2 supports AES128-CBC and 3DES-CBC cipher strengths through the SSH port.

If enabled, iLO 2 enforces the usage of these enhanced ciphers (both AES and 3DES) over the secure channels, including secure HTTP transmissions through the browser, SSH port, and XML port. When AES/3DES encryption is enabled, you must use a cipher strength equal to or greater than AES/3DES to connect to iLO 2 through these secure channels. Communications and connections over less secure channels (such as the Telnet port) are not affected by the AES/3DES encryption enforcement setting.

By default, remote console data uses 128-bit RC4 bi-directional encryption. The CPQLOCFG utility uses a 168-bit Triple DES with RSA and a SHA1 MAC cipher to securely send RIBCL scripts to iLO 2 over the network.

Encryption settings

You can view or modify the current encryption settings using the iLO 2 interface, CLP, or RIBCL.

To view or modify current encryption settings using the iLO 2 interface:

1. Click **Administration>Security>Encryption**.

   The Encryption page appears, displaying the current encryption settings for iLO 2. Both the current negotiated cipher and the encryption enforcement settings appear on this page.

   - Current Negotiated Cipher displays the cipher in use for the current browser session. After logging in to iLO 2 through the browser, the browser and iLO 2 negotiate a cipher setting to use during the session. The Encryption page Current Negotiated Cipher section displays the negotiated cipher.

     Encryption Enforcement Settings displays the current encryption settings for iLO 2. Enforce AES/3DES Encryption (if enabled) enables iLO 2 to only accept connections through the browser and SSH interface that meet the minimum cipher strength. A cipher strength of at least AES or 3DES must be used to connect to iLO 2 if this setting is enabled. Enforce AES/3DES Encryption can be enabled or disabled.

2. To save changes, click **Apply**.

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

To view or modify current encryption settings through the CLP or RIBCL, see the *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide* at http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=135&prodTypeId=18964&prodSeriesId=1146658.

Connecting to the iLO 2 using AES/3DES encryption

After enabling the Enforce AES/3DES Encryption setting, iLO 2 requires you to connect through secure channels (web browser, SSH, or XML port) using a cipher strength of at least AES or 3DES.

To connect to iLO 2 through a browser, the browser must be configured with a cipher strength of at least AES or 3DES. If the web browser is not using AES or 3DES ciphers, iLO 2 displays an error message informing you to close the current connection and select the correct cipher.

See your browser documentation to select a cipher strength of at least AES or 3DES. Different browsers use different methods of selecting a negotiated cipher. You must log out of iLO 2 through the current browser before changing the browser cipher strength. Any changes made to the browser cipher setting while logged in to iLO 2 might enable the browser to continue using a non-AES/3DES cipher.

All client operating systems and browsers supported by iLO 2, support the iLO 2 AES/3DES Encryption feature except when using Windows 2000 Professional with Internet Explorer. By default, Windows 2000 Professional does not support AES or 3DES ciphers. If a client uses Windows 2000 Professional, you must use another browser, or update the operating system.

Internet Explorer does not have a user-selectable cipher strength setting. You must edit the registry to enable Internet Explorer to connect to iLO 2 when the Enforce AES/3DES Encryption setting is enabled. To enable AES/3DES encryption in Internet Explorer, open the registry and set `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy` to 1.

NOTE: 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. For information on how to restore your registry, see the Microsoft Knowledge Base article at http://support.microsoft.com/kb/307545.

To connect to iLO 2 through an SSH connection, see your SSH utility documentation to set the cipher strength.

When connecting through the XML channel, the CPQLOCFG utility uses a secure 3DES cipher by default. CPQLOCFG 2.26 or later displays the following current-connection cipher strength on the XML output. For example:

```
Connecting to Server..
Negotiated cipher: 168-bit Triple DES with RSA and a SHA1 MAC
```

AES encryption is not supported by Internet Explorer on a Windows 2000 Professional client. To use AES encryption with this operating system, use another browser (such as Mozilla).

HP SIM single sign-on (SSO)

HP SIM SSO enables you to browse directly from HP SIM to your LOM processor, bypassing an intermediate login step. To use SSO, a current version of HP SIM is required, and you must configure your LOM processor to accept the links from HP SIM. HP SIM requires the latest updates and patches to function correctly. For more information about HP Systems Insight Manager and available updates, see the HP website at http://www.hp.com/go/hpsim.

HP SIM SSO is a licensed feature available with the purchase of optional licenses. For more information, see "Licensing" (page 26).

The HP SIM SSO page enables you to view and configure SSO settings through the iLO 2 interface. For more information, see "Setting up HP SIM SSO" (page 57).

You can also access HP SIM SSO configuration settings using scripts, text files, and through a command-line using text-based clients such as SSH over the network or from the operating system on the host computer. Scripting SSO enables you to use the same SSO settings on all your LOM processors. For more information, example scripts, and CLP extensions to read, modify, and write HP SIM SSO configuration settings, see the *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide* at http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=135&prodTypeId=18964&prodSeriesId=1146658.

Setting up iLO 2 for HP SIM SSO

Before you start SSO setup, you must have the network address of HP SIM and ensure that a license key is installed. To setup SSO:

1. Enable Single Sign-On Trust Mode by selecting either **Trust by Certificate** (recommended), **Trust by Name**, or **Trust All**.
2. Add the HP SIM certificate of the server to iLO 2.
   a. Click **Add an HP SIM Server.**
   b. Enter the HP SIM server network address.
   c. Click **Import Certificate.**

   The certificate repository is sized to allow five typical iLO 2 certificates. However, certificate sizes can vary if typical certificates are not issued. There is 6KB of combined storage allocated

for certificates and iLO 2 server names. When the allocated storage is used, no more imports are accepted.

After setting up SSO in iLO 2, log in to HP SIM, locate the LOM processor, select **Tools>System Information>iLO as...** HP SIM launches a new browser that is logged in to the LOM management processor.

Adding HP SIM trusted servers

You can install HP SIM server certificates using scripting that is suitable for mass deployment. For more information, see the *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide* at http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=135&prodTypeId=18964&prodSeriesId=1146658. To add HP SIM server records using a browser:

1. Click **Administration>Security>HP SIM SSO**.
2. Click **Add an HP SIM Server**.
3. To authenticate the server, choose one of the following:
   - To add an HP SIM server using Trust by Name authentication, enter the full network name of the HP SIM server in the Add a Trusted HP SIM Server Name section. Click **Add Server Name**.

     Trust by Name authentication uses fully qualified domain names; for example, `sim-host.hp.com` instead of `sim-host`. If you are unsure of the fully qualified domain name, use the `nslookup host` command.
   - To retrieve and import a certificate from a trusted HP SIM server, enter the full network name of an HP SIM Server in the Retrieve and import a certificate from a trusted HP SIM Server section. Click **Import Certificate** to request the certificate from the HP SIM server and automatically import it. This record supports SSO Trust by Name and SSO Trust by Certificate.

     To prevent any certificate tampering directly import an HP SIM server certificate. To directly import an HP SIM server certificate, retrieve the HP SIM certificate date using one of the following options:

     - Using a separate browser window, browse to the HP SIM server at http://<sim network address>:280/GetCertificate.

       Cut and paste the certificate data from HP SIM into iLO 2.
     - Export the HP SIM server certificate from the HP SIM user interface by selecting **Options>Security>Certificates>Server Certificate**. Open the file using a text editor, and copy and paste all the certificate raw data into iLO 2.
     - Using command-line tools on the HP SIM server, the HP SIM certificate can be extracted using the tomcat-coded alias for the HP SIM certificate. For example:

       ```
       mxcert -l tomcat
       ```

       The certificate data resembles:

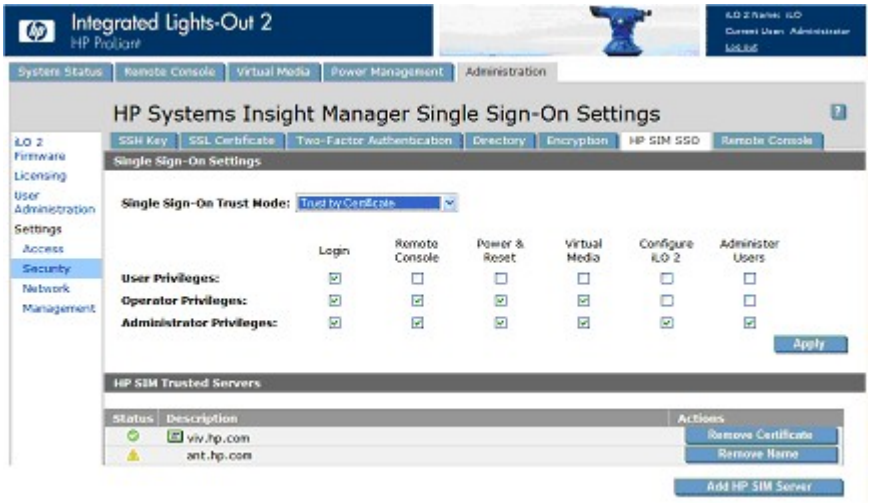
       ```
       -----BEGIN CERTIFICATE-----
       .
       .
       .
       several lines of encoded data
       .
       .
       .
       -----END CERTIFICATE-----
       ```

After pasting the HP SIM server base-64 encoded x.509 certificate data into the Directly import a HP SIM Server Certificate section, click **Import Certificate** to record the data. This type of record supports SSO Trust by Name and SSO Trust by Certificate.

There are other ways to retrieve HP SIM server certificate data. For more information, see your HP SIM documentation.

Setting up HP SIM SSO

The HP SIM SSO page allows you to view and configure the existing iLO 2 Single Sign-On settings. You must have the Configure iLO 2 privilege to alter these settings. To access iLO 2 SSO settings, click **Administration>Security>HP SIM SSO**.



The HP Systems Insight Manager Single Sign-On Settings page includes the following fields and options:

- Single Sign-On Trust Mode – Enables you to control how SSO-initiated connections are accepted:
  - Trust None (default) – Rejects all SSO connection requests.
  - Trust by Certificate (most secure) – Enables only SSO connections from an HP SIM server matching a certificate previously imported into iLO 2.
  - Trust by Name – Enables SSO connections from an HP SIM server matching a DNS name or certificate previously imported into iLO 2.
  - Trust All (least secure) – Accepts any SSO connections initiated from any HP SIM server.

  Users who log in to HP SIM are authorized based upon the role assignment at the HP SIM server. The role assignment is passed to the LOM processor when SSO is attempted. You can configure iLO 2 privileges for each role in the Single Sign-On Settings section. For more information about each privilege, see "User administration" (page 28).

  Using directory-based user accounts, SSO attempts to receive only the privileges assigned in this section. Lights-Out directory settings do not apply. Default privilege assignments are:

  - User – Login only
  - Operator – Login, Remote Console, Power and Reset, and Virtual Media
  - Administrator – Login, Remote Console, Power and Reset, Virtual Media, Configure iLO 2, and Administer Users
- HP SIM Trusted Servers – Enables you to view the status of trusted HP SIM servers configured to use SSO with the current LOM processor. Click **Add a SIM Server** to add a server name,

import a server certificate, or directly install a server certificate. For more information, see "Adding HP SIM trusted servers" (page 56).

The server table displays a list of registered HP SIM servers with the status of each. The actual number of systems allowed depends on the size of the stored certificate data.

Although a system might be registered, SSO might be refused because of the current trust level or certificate status. For example, if an HP SIM server name is registered and the trust level is set to Trust by Certificate, SSO is not allowed from that server. Likewise, if an HP SIM server certificate is imported, but the certificate has expired, SSO is not allowed from that server. Additionally, the records are not used when SSO is disabled. iLO 2 does not enforce SSO server certificate revocation.

- Status – Indicates the status of the record (if any are installed).
- Description – Displays the server name (or certificate subject). A thumbnail of a certificate indicates that the record contains a stored certificate.
- Actions – Displays the actions you can take on a selected record. The actions displayed depend on the type and number of records installed:
  - Remove Name – Removes the server name record.
  - Remove Certificate – Removes the certificate record.

Remote Console Computer Lock

Remote Console Computer Lock enhances the security of an iLO 2 managed server by automatically locking an operating system, or logging out a user when a remote console session terminates or the network link to iLO 2 is lost. Unlike Remote Console or Integrated Remote Console, this feature is standard and does not require an additional license. As a result, if you open a Remote Console Session or an Integrated Remote Console window and have this feature configured, it will lock the operating system when the window is closed even if additional feature licenses are not installed.

You can view and configure the Remote Console Computer Lock settings through the Administration or Remote Console tabs in the iLO 2 interface. The Remote Console Computer Lock feature is disabled by default.

To change the Remote Console Computer Lock settings:

1. Log in to iLO 2 using an account that has the Configure iLO 2 Settings privilege.
2. Click **Administration>Security>Remote Console**. The Computer Lock Settings page appears.



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

You can create a Remote Console Computer Lock key sequence using the keys listed in the following table.

ESC	F4	1	e
L_ALT	F5	2	f
R_ALT	F6	3	g
L_SHIFT	F7	4	h
R_SHIFT	F8	5	i
L-CTRL	F9	6	j
R_CTRL	F10	7	k
L_GUI	F11	8	l
R_GUI	F12	9	m
INS	" " (Space)	:	n
DEL	!	;	o
HOME	"	<	p
END	#	=	q
PG_UP	$	>	r
PG_DN	%	?	s
ENTER	&	@	t
TAB	'	[	u
BREAK	(	\	v
BACKSPACE	)	]	w
NUM PLUS	*	^	x
NUM MINUS	+	_	y
SCRL LCK	,	'	z
SYS RQ	-	a	{
F1	.	b	}
F2	/	c	|
F3	0	d	~

4. Click **Apply** to save changes.

This feature can also be configured using scripting or command lines. For more information, see the *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide* at http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=135&prodTypeId=18964&prodSeriesId=1146658.

Network

The Network Settings and DCHP/DNS tabs of the Network section enable you to view and modify network settings for iLO 2.

Only users with the Configure iLO 2 Settings privilege can change these settings. Users that do not have the Configure iLO 2 Settings privilege can view the assigned settings.

To change network settings for iLO 2:

1. Log in to iLO 2 using an account that has the Configure iLO 2 Settings privilege. Click **Administration>Network**.
2. Select **Network Settings** or **DHCP/DNS**.
3. Change the settings as needed.
4. After completing any parameter changes, click **Apply** to complete the changes.

iLO 2 restarts, and the connection of your browser to iLO 2 terminates. To reestablish a connection, wait 60 seconds before launching another browser session and logging in.

Network Settings

The Network Settings page displays the NIC IP address, subnet mask, and other TCP/IP-related information and settings. From the Network Settings screen, you can enable or disable DHCP and configure a static IP address for servers not using DHCP. All users can view the network settings, but only users with the Configure iLO 2 Settings privilege can change these settings. To access the Network Settings page, click **Administration>Network>Network**. The Network Settings page appears with the following information and settings:

- NIC enables you to set the iLO 2 NIC to Enabled, Disabled, or to Shared Network Port.
  - Enabled – Enables the primary iLO 2 network interface.
  - Disabled – Disables the iLO 2 network interface. You must use the iLO 2 RBSU or other host-based scripting utility to re-enable the network interface.
  - Shared Network Port – Enables networking using the designated host Ethernet port. The port appears as two separate Ethernet MACs and IP addresses on the network. For more information, see "iLO 2 Shared Network Port" (page 61).
- DHCP enables you to select static IP (disabled) or enables the use of a DHCP server to obtain an IP address for the Integrated Lights-Out 2 subsystem.

  You cannot set the iLO 2 IP Address and Subnet Mask if DHCP is enabled. Disabling DHCP enables you to configure the IP address. The IP Address field also appears on the DHCP/DNS Settings page for convenience. Changing the value on either page changes the DHCP setting.
- IP Address is the iLO 2 IP address. If DHCP is used, the iLO 2 IP address is automatically supplied. If not, enter a static IP address. The IP Address field appears on the DHCP/DNS page for convenience. Entering values in the field on either page changes the IP address of the iLO 2.
- Subnet Mask is the subnet mask of the iLO 2 IP network. If DHCP is used, the Subnet Mask is automatically supplied. If not, enter the subnet mask for the network.
- Gateway IP Address displays the IP address of the network gateway. If DHCP is in use, the Gateway IP Address is automatically supplied. If not, enter the network gateway address.

- iLO 2 Subsystem Name is a name used by the iLO 2 subsystem. If DHCP and DNS are configured correctly, this name can be used to connect to the iLO 2 subsystem instead of the IP address. For more information, see "iLO 2 subsystem name limitations" (page 61).
- Link controls the speed and duplex of the iLO 2 network transceiver. The current link speed of the primary dedicated iLO 2 NIC can be highlighted. Link settings include the following:
  - Automatic (default) enables iLO 2 to negotiate the highest supported link speed and duplex when connected to the network.
  - 100Mb/FD forces a 100-Mb connection using full duplex.
  - 100Mb/HD forces a 100-Mb connection using half duplex.
  - 10Mb/FD forces a 10-Mb connection using full duplex.
  - 10Mb/HD forces a 10-Mb connection using half duplex.

NOTE: If autosense is disabled, the network switch must match the iLO 2 settings to prevent iLO 2 access issues.

You are not permitted to modify the NIC speed settings and autosense options on blade servers. These settings are auto negotiated between iLO 2 and the Onboard Administrator.

iLO 2 subsystem name limitations

The iLO 2 subsystem name represents the DNS name of the iLO 2 subsystem. For example, `ilo` instead of `ilo.hp.com`. This name can only be used, if DHCP and DNS are configured properly to connect to the iLO 2 subsystem name instead of the IP address.

- Name service limitations – The subsystem name is used as part of the DNS name and WINS name. However DNS and WINS limitations differ:
  - DNS allows alphanumeric and hyphen. WINS allows alphanumeric, hyphen and underscore.
  - WINS subsystem names are truncated at 15 characters, DNS are not.

If you require underscores, they can be entered in RBSU or using the iLO 2 scripting utility.

NOTE: Name service limitations also apply to the domain name.

To avoid name space issues:

- Do not use the underscore character.
- Limit subsystem names to 15 characters.
- Verify you can ping iLO by IP address and by DNS/WINS name.
- Verify NSLOOKUP correctly resolves the iLO network address and that there are no namespace conflicts.
- Verify DNS and WINS both correctly resolve the name (if you are using both).
- Flush the DNS name if you make any name space changes.

iLO 2 Shared Network Port

The iLO 2 Shared Network Port enables you to choose either the system NIC or dedicated iLO 2 Dedicated Management NIC for server management. When you enable the iLO 2 Shared Network Port, both regular network traffic, and network traffic intended for iLO 2 pass through the system NIC.

iLO 2 provides support for servers that might not have an iLO 2 Dedicated Management NIC. On servers using the iLO 2 Dedicated Management NIC, the standard hardware configuration provides iLO 2 network connectivity only through the iLO 2 Shared Network Port connection. iLO 2 detects the lack of an iLO 2 Dedicated Management NIC and automatically defaults to the Shared Network Port. On some of these servers, an iLO 2 Dedicated Management NIC might be available as a hardware option. If an iLO 2 Dedicated Management NIC is available as a hardware option, iLO 2 defaults to the installed iLO 2 Dedicated Management NIC. On servers using the iLO 2 Dedicated Management NIC, you can enable shared network port operation through the iLO 2 interface.

The iLO 2 Shared Network Port uses the network port labeled NIC 1 on the rear panel of the server. NIC numbering in the operating system can be different from system numbering. The iLO 2 Shared Network Port does not incur an iLO 2 performance penalty. Peak iLO 2 traffic is less than 2 MB (on a NIC capable of 1000-Mb speeds), and average iLO 2 traffic is infrequent and low.

The Shared Network Port is not available on HP ProLiant ML310 G3, ML310 G4, BL20p G4, and all c-Class blade servers.

iLO 2 Shared Management Port features and restrictions

iLO 2 Shared Network Port and the iLO 2 Dedicated Management NIC port are used for iLO 2 server management. You can only use the iLO 2 Shared Network Port and the iLO 2 Dedicated Management NIC port for iLO 2 server management. The iLO 2 Shared Network Port and the iLO 2 Dedicated Management NIC port cannot operate simultaneously. If you enable the dedicated iLO 2 NIC, you will disable the iLO 2 Shared Network Port. If you enable the iLO 2 Shared Network Port, you will disable the dedicated iLO 2 Dedicated Management NIC.

However, disabling the Shared Network Port does not completely disable the system NIC. Regular network traffic still passes through the system NIC. When Shared Network Port network traffic is disabled, any traffic going to or originating from iLO 2 will not pass on to iLO 2 through the Shared Network Port because the Shared Network Port is no longer shared with iLO 2.

The Shared Network Port must not be considered an availability feature. The Shared Network Port is intended to allow managed network port consolidation. The use of this feature can create a single failure point, that is, if the port fails or is unplugged, both the host and iLO 2 become unavailable to the network.

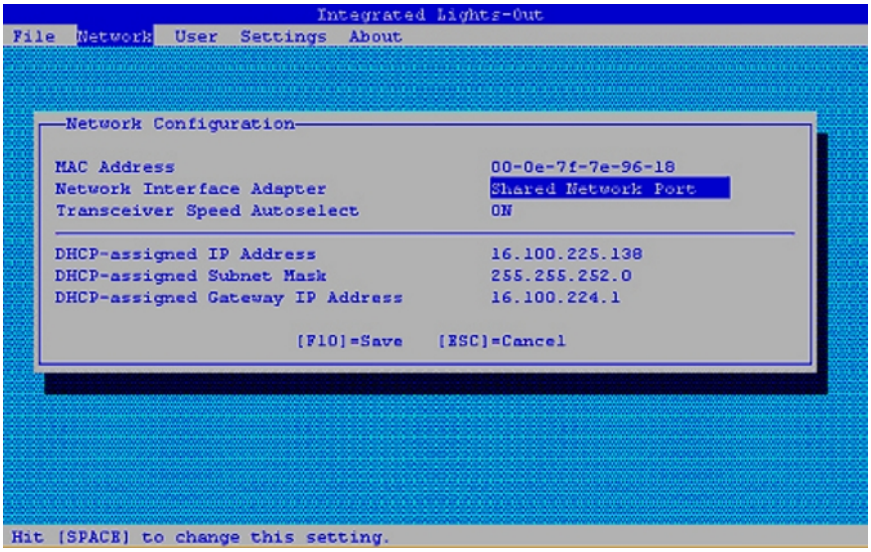
Enabling the iLO 2 Shared Network Port feature

The iLO 2 Shared Network Port feature is disabled by default. This feature can be enabled through one of the following:

- The iLO 2 RBSU
- The iLO 2 web interface
- XML scripting

Enabling the iLO 2 Shared Network Port feature through iLO 2 RBSU

1. Connect the server's NIC port 1 to a LAN.
2. When prompted during POST, press the **F8** key to enter iLO 2 RBSU.
3. Select **Network>NIC>TCP/IP**, and press the **Enter** key.
4. In the Network Configuration menu, toggle the Network Interface Adapter Field to Shared Network Port by pressing the space bar. The Shared Network Port option is only available on supported servers.



5. Press the **F10** key to save the configuration.
6. Select **File>Exit**, and press the **Enter** key.

After iLO 2 resets, the Shared Network Port feature is active. Any network traffic going to or originating from iLO 2 is directed through the system's NIC port 1.

Enabling the iLO 2 Shared Network Port feature through the web interface

1. Connect iLO 2 NIC port 1 to a LAN.
2. Open a browser, and browse to the iLO 2 IP address or DNS name.
3. Select **Administration>Network Settings**.
4. On the Network Settings page, select **Shared Network Port**. The Shared Network feature is available on supported servers only.
5. Click **Apply** at the bottom of the page.
6. Click **Yes** in the warning dialog box, and click **OK**.

After iLO 2 resets, the Shared Network Port feature is active. Any network traffic going to or originating from iLO 2 is directed through the system's NIC port 1.

Only the Shared Network Port or the iLO 2 Dedicated Management NIC is active for server management. They cannot be enabled at the same time.

Re-enabling the dedicated iLO 2 management port

The iLO 2 web interface, RBSU, or XML (described in the scripting and command line reference guide) scripting must be used to re-enable the iLO 2 Dedicated Management NIC. Re-enabling iLO 2 through RBSU requires that the system be rebooted.

To re-enable the iLO 2 Dedicated Management NIC using RBSU:

1. Connect the iLO 2 dedicated management NIC port to a LAN from which the server is managed.
2. Reboot the server.
3. When prompted during POST, press the **F8** key to enter iLO 2 RBSU.
4. Select **Network>NIC>TCP/IP**, and press the **Enter** key.
5. In the Network Configuration menu, toggle the Network Interface Adapter Field to ON by pressing the space bar.
6. Press the **F10** key to save the configuration.
7. Select **File>Exit**, and press the **Enter** key.

After iLO 2 resets, the iLO 2 Dedicated Management NIC port is active.

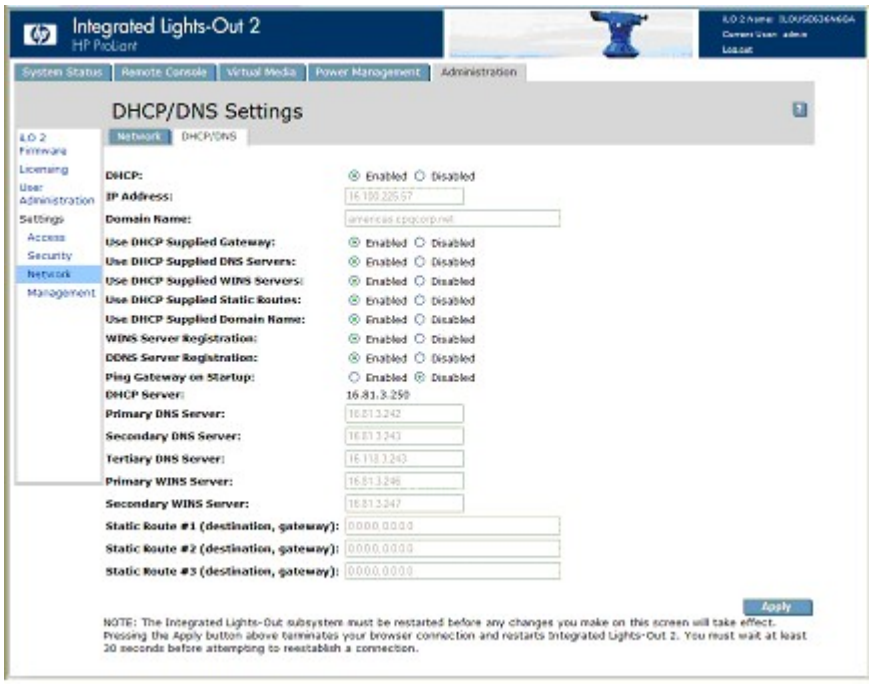
To re-enable the iLO 2 Dedicated Management NIC using iLO 2 interface:

1. Open a browser and navigate to the iLO 2 IP address or DNS name
2. On the Network Settings page, select **Enabled** for the iLO 2 NIC.
3. Click **Apply**. A warning dialog appears.
4. Click **Yes**, and then **OK**.

After iLO 2 resets, the iLO 2 Dedicated Management NIC is active. When using IRC through iLO 2 Dedicated Management NIC port and depending on the network traffic, you might not have sufficient time to press the RBSU keys during POST.

DHCP/DNS Settings

The iLO 2 DHCP/DNS Settings page displays DHCP/DNS configuration information for iLO 2. All users can view the DHCP/DNS settings, but you must have the Configure iLO 2 Settings privilege to change them. These settings can also be changed using the iLO 2 RBSU (F8 during POST). To access DHCP/DNS settings, click **Administration>Network>DHCP/DNS**. The DHCP/DNS Settings page appears.



The following options are available:

- DHCP allows you to select static IP (disabled) or enable the use of a DHCP server to obtain an IP address for the iLO 2 subsystem.

  You cannot set the iLO 2 IP address if DHCP is enabled. Disabling DHCP allows you to configure the IP address. The IP Address field also appears on the Network Settings page for your convenience. Changing the value on either page changes the DHCP setting.

- IP Address is the iLO 2 IP address. If DHCP is used, the iLO 2 IP address is automatically supplied. If not, enter a static IP address. The IP Address field appears on the Network Settings page for your convenience. Changing the value on either page changes the IP address of iLO 2.

- Domain Name is the name of the domain where the iLO 2 subsystem resides. This name is assigned by DHCP (if DHCP is enabled). Enabling DHCP allows you to configure the following DHCP options:
  - Use DHCP Supplied Gateway – Toggles if iLO 2 uses the DHCP server-supplied gateway. If not, enter an gateway address in the Gateway IP Address box.
  - Use DHCP Supplied DNS Servers – Toggles if iLO 2 uses the DHCP server-supplied DNS server list. If not, enter the DNS server address in the Primary, Secondary, and Tertiary DNS Server fields.
  - Use DHCP Supplied WINS Servers – Toggles if iLO 2 uses the DHCP server-supplied WINS server list. If not, enter the WINS server address in the Primary and Secondary WINS Server fields.
  - Use DHCP Supplied Static Routes – Toggles if iLO 2 uses the DHCP server-supplied static route. If not, enter the static route address in Static Route #1, Static Route #2, or Static Route #3 fields.
  - Use DHCP Supplied Domain Name – Toggles if iLO 2 uses the DHCP server-supplied domain name. If not, enter a domain name in the Domain Name box.
- WINS Server Registration toggles if iLO 2 registers its name with a WINS server.
- DDNS Server Registration toggles if iLO 2 registers its name with a DDNS server.
- Ping Gateway on Startup option causes iLO 2 to send four ICMP echo request packets to the gateway when iLO 2 initializes. This option ensures that the ARP cache entry for iLO 2 is up-to-date on the router responsible for routing packets to and from iLO 2.
- DHCP Server is the IP address of the DHCP server. This field cannot be assigned. It is received from DHCP if DHCP is enabled and represents the last known valid DHCP server address.
- Primary, Secondary, and Tertiary DNS Server are the IP addresses of the DNS servers. If supplied by the DHCP server, these fields are automatically populated. Otherwise, enter the IP addresses manually.
- Primary and Secondary WINS Server are the IP addresses of the WINS servers. If supplied by the DHCP server, these fields are automatically populated. Otherwise, enter the IP addresses manually.
- Static Route #1, Static Route #2, and Static Route #3 (destination, gateway) are the network destination gateway addresses. Enter up to three network destination/gateway routing pairs.

SNMP/Insight Manager settings

The Management option of the Administration section displays the SNMP/Insight Manager Settings page. The SNMP/Insight Manager Settings page enables you to configure SNMP alerts, generate a test alert, and configure integration with HP SIM.

Enabling SNMP alerts

iLO 2 supports up to three IP addresses to receive SNMP alerts. Typically, the addresses used are the same as the IP address of the HP SIM server console.

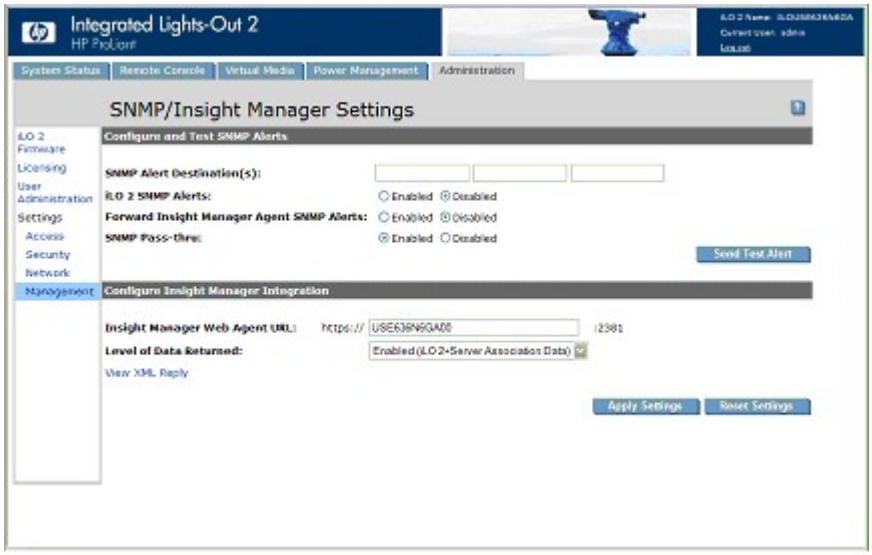
Only users with the Configure iLO 2 Settings privilege can change these settings. Users that do not have the Configure iLO 2 Settings privilege can only view the assigned settings.

The following alert options are available in the SNMP/Insight Manager Settings screen:

- SNMP Alert Destination(s)
- iLO 2 SNMP Alerts
- Forward Insight Manager Agent SNMP Alerts

- SNMP Pass-thru
- p-Class Alert Forwarding (displayed on p-Class servers only)

For more information see to the *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide* at http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=135&prodTypeId=18964&prodSeriesId=1146658.



To configure alerts:

1. Log in to iLO 2 using an account that has the Configure iLO 2 Settings privilege.
2. Select **Management** in the Administration tab. The SNMP/Insight Manager Settings screen appears.
3. In the SNMP Alert Destination(s) fields, enter up to three IP addresses that you want to receive the SNMP alerts and select the alert options you want iLO 2 to support.
4. Click **Apply Settings**.

Test alerts include an Insight Manager SNMP trap and are used to verify the network connectivity of iLO 2 in HP SIM. Only users with the Configure iLO 2 Settings privilege can send test alerts.

Be sure you have saved any changes to the SNMP Alert Destination(s) fields before sending a test alert.

To send a test alert:

1. Select **Management** in the Administration tab. The SNMP/Insight Manager Settings screen appears.
2. Click **Send Test Alert** in the Configure and Test SNMP Alerts section to generate a test alert and send it to the TCP/IP addresses saved in the SNMP Alert Destinations fields.
3. After generating the alert, a confirmation screen appears.
4. Check the HP SIM console for receipt of the trap.

SNMP generated trap definitions

You can generate the following SNMP traps on BL c-Class servers and iLO 2:

- `ALERT_TEST` – Verifies that the SNMP configuration, client SNMP console, and network are operating correctly. You can use the iLO 2 interface to generate this alert to verify receipt of the alert at the SNMP console. You can also generate this alert using the iLO 2 Option ROM to verify SNMP configuration settings.
- `ALERT_SERVER_POWER` – Occurs when the iLO 2 management processor detects an unexpected transition of the host system power, either from ON to OFF, or OFF to ON.

Transitions of the host system power are unexpected when the change takes place because of events unknown to the management processor. This alert is not generated when the system is powered up or down using the iLO 2 interface, CLI, RIBCL or other management feature. If the server is powered down because of the operating system, physical power button presses, or other methods, the alert is generated and sent.

- `ALERT_SERVER_RESET` – Occurs when the iLO 2 management processor is used to perform a cold boot or warm boot of the host system. This alert is also sent when the iLO 2 management processor detects the host system is in reset because of events unknown to the management processor. Certain operating system behavior or actions can cause this type of event to be detected, and the alert transmitted.
- `ALERT_ILLEGAL_LOGIN` – An SNMP alert transmitted when a connection is attempted using an invalid username and password. This alert is transmitted regardless of connection type; web interface, serial port, Telnet, SSH, or RIBCL.
- `ALERT_LOGS_FULL` – An SNMP alert transmitted when the iLO 2 Event Log is full and an attempt to log a new event occurs.
- `ALERT_SELFTEST_FAILURE` – An SNMP alert transmitted when iLO 2 detects an error in any one of the monitored internal components. If an error is detected an SNMP alert is transmitted.
- `ALERT_SECURITY_ENABLED` – Alert is transmitted when the iLO 2 management processor detects a change in the Security Override Switch to enabled.
- `ALERT_SECURITY_DISABLED` – An SNMP alert transmitted when the iLO 2 management processor detects a change in the Security Override Switch to disabled.
- `ALERT_HOST_GENERATED` – An SNMP alert generated when the iLO 2 management processor was asked to transmit a Host (SNMP passthrough) alert and the management processor was unable to transmit the original SNMP alert. iLO 2 attempts to transmit this generic alert in order to notify the SNMP management console that an alert intended to be transmitted from the host system was not transmitted.

Configuring Insight Manager integration

The Insight Manager Web Agent URL (DNS name or IP address) sets the browser destination of the Insight Agent link on iLO 2 pages. Typically, this link is the IP address or DNS name of the management agent running on the host server operating system.

Enter the IP address of the host server. The protocol (`https://`) and port number (`:2381`) are automatically added to the IP address or DNS name to allow access to the Insight Management Web Agents from iLO 2.

If the Insight Manager Web Agent URL is set through another method (for example, CPQLOCFG), click the refresh button of your browser to display the updated URL.

The Level of Data Returned setting controls the content of an anonymous discovery message received by iLO 2. The information returned is used for Insight Manager HTTP identification requests. The following options are available:

- Enabled (default) – Enables Insight Manager to associate the management processor with the host server and provides sufficient data to allow integration with HP SIM.
- Disabled – Prevents iLO 2 from responding to the HP SIM requests.
- View XML Reply – Enables you to examine the data returned at the settings.

  View the response that is returned to Insight Manager when it requests Management Processor identification using this link.

To see the results of changes made, click **Apply Settings** to save the changes. To return the page to its previous state and clear the fields, click **Reset Settings**. The Reset Settings button does not save any changes.

For more information on Insight Agents, click **System Status>Insight Agent**.

Static IP bay configuration

Static IP bay configuration is implemented using the Static IP Bay Settings option on the BL p-Class tab. This option eases the initial deployment of an entire enclosure or the subsequent deployment of blades within an existing enclosure. While the preferred method for assigning IP addresses to the iLO 2 in each blade server is through DHCP and DNS, these protocols are not always available on nonproduction networks.

For example, after configuring Static IP Bay configuration for the blade in bay 1, subsequent blade additions to the enclosure assume subsequent addresses without DHCP. The network addresses are assigned by blade position `bay 1: 192.168.1.1`, `bay 2: 192.168.1.2`, and so on. Deploying subsequent blades does not demand extra configuration, and the network address corresponds to the bay number.

Static IP bay configuration automates the first step of BL p-Class blade deployment by enabling the iLO 2 management processor in each blade slot to obtain a predefined IP address without relying on DHCP. iLO 2 is immediately accessible for server deployment using Virtual Media and other remote administration functions.

Static IP bay configuration uses the Static IP Bay Configuration addressing method, which enables you to assign IP addresses to each iLO 2 based on slot location in the respective server enclosure. By providing a set of IP addresses in the enclosure, you gain the advantages of a static IP bay configuration without requiring each individual iLO 2 to be configured locally.

Using iLO 2 static IP bay configuration:

- Helps avoid the costs of a DHCP infrastructure to support the blade environment
- Provides easier setup with automatic iLO 2 address generation for all or a few selected bays

Static IP Bay Configuration is not supported in G1 BL-series blade enclosures. To view the enclosure generation, click **BL p-Class>Rack View>Details** for a specific enclosure. Static IP Bay configuration is not supported on an enclosure when Enclosure Type details displays the message `BL Enclosure G1`

When a blade is redeployed, Static IP Bay Configuration might not complete as expected. To correct this, verify that the blade is using the current iLO 2 firmware, and then reset the iLO 2 configuration to factory default settings using iLO 2 RBSU.

Configuring a ProLiant BL p-Class blade enclosure

To configure a BL p-Class blade enclosure using static IP bay addressing:

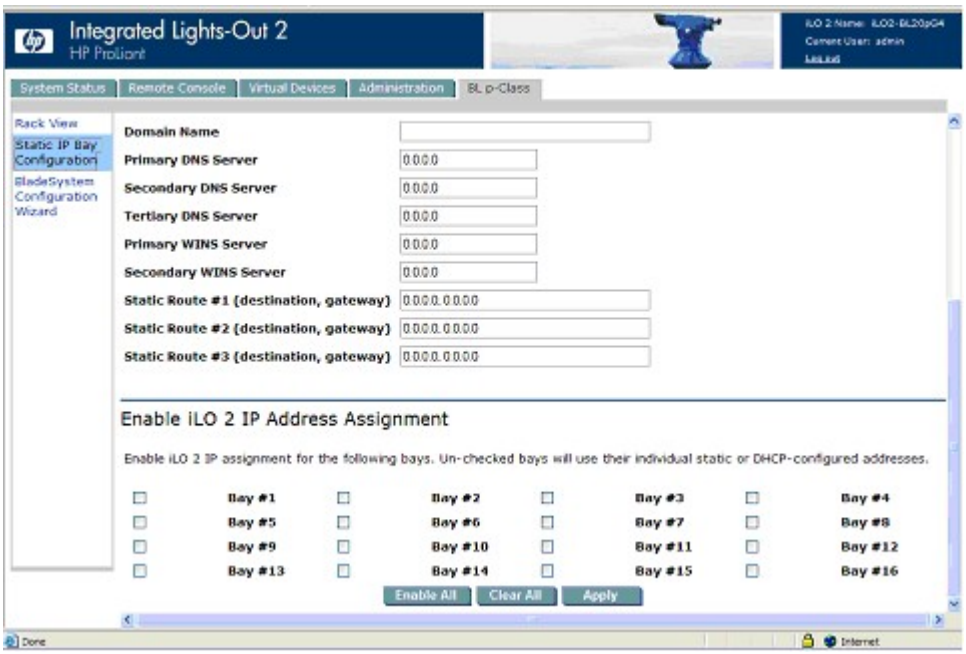
1. Install a server blade in bay 1 of the BL p-Class enclosure. The server blade does not need to be configured or have an operating system installed. The server blade must be configured before installing any additional blades in the enclosure.
2. Connect a client device to the front-panel iLO 2 port of the blade using the local I/O cable. The local I/O cable connects to the I/O port on the front of the server blade. This connection enables the static IP 192.168.1.1 for the iLO 2 Web interface.
3. Configure the enclosure setting. Using the iLO 2 Web interface, select the BL p-Class tab to access the Enclosure Static IP Settings. The BL p-Class tab provides a user interface for configuring the enclosure-level static IP addresses.
4. Select a reasonable starting IP address, with the last digit(s) of the address corresponding to the bay number of each blade (example: `192.168.100.1` through `192.168.100.16`), to build an easy-to-remember numbering system.
5. Reset bay #1, if necessary. The blade in bay #1 must only be reset if you intend the blade to use a Static IP bay Configuration address by marking the feature enable mask for bay #1. Before resetting the blade, browse to the Network Settings page, select **Enable Static IP Settings** and click **Apply** to force the blade to reboot and use the newly assigned enclosure static IP.

If multiple enclosures are deployed at the same time, the process can be repeated easily by moving a single blade to bay #1 of each enclosure to perform the configuration.

Configuring static IP bay settings

Static IP bay settings are available on the BL p-Class tab and enable you to configure and deploy the blade server. When configuring these settings, you must use the blade in bay 1.

The Enable Static IP Bay Configuration Settings checkbox, available on the Network Settings tab (not shown), allows you to enable or disable Static IP Bay Configuration. The new Enable Static IP Bay Configuration Settings option is only available on blade servers. When Static IP Bay Configuration is enabled, all fields except iLO 2 Subsystem Name are disabled. Only Static IP Bay Configuration or DHCP can be enabled at one time. Disabling both Static IP Bay Configuration and DHCP signals iLO 2 to use a user-defined IP address. The Enable Static IP Bay Configuration Settings option remains disabled if the infrastructure does not support Static IP Bay Configuration.



ProLiant BL p-Class standard configuration parameters

Beginning IP Address (Bay 1) – Assigns the starting IP address. All IP addresses must be valid addresses.

Ending IP Address (Bay 16) – Assigns the ending IP address. All IP addresses must be valid addresses.

Subnet Mask – Assigns the subnet mask for the default gateway. This field might be filled in if either Static IP Bay Configuration or DHCP is enabled. The entire IP address range must conform to the subnet mask.

Gateway IP Address – Assigns the IP address of the network router that connects the Remote Insight subnet to another subnet where the management PC resides. This field might be filled in if either Static IP Bay Configuration or DHCP is enabled.

ProLiant BL p-Class advanced configuration parameters

Domain Name – Enables you to assign the name of the domain in which the iLO 2 will participate.

Primary DNS Server – Assigns a unique DNS server IP address on your network.

Secondary DNS Server – Assigns a unique DNS server IP address on your network.

Tertiary DNS Server – Assigns a unique DNS server IP address on your network.

Primary WINS Server – Assigns a unique WINS server IP address on your network.

Secondary WINS Server – Assigns a unique WINS server IP address on your network.

Static Route #1, #2, and #3 (destination gateway) – Assigns the appropriate static route destination and gateway IP address on your network (the default IP values are 0.0.0.0 and 0.0.0.0, where the first IP address corresponds to the destination IP, and the second IP address corresponds to the gateway IP).

Enabling iLO 2 IP address assignment

The bay #1 through bay #16 checkboxes enable you to select which BL p-Class blade servers will be configured. You can Enable All, Clear All, or Apply your selection.

HP BladeSystem setup

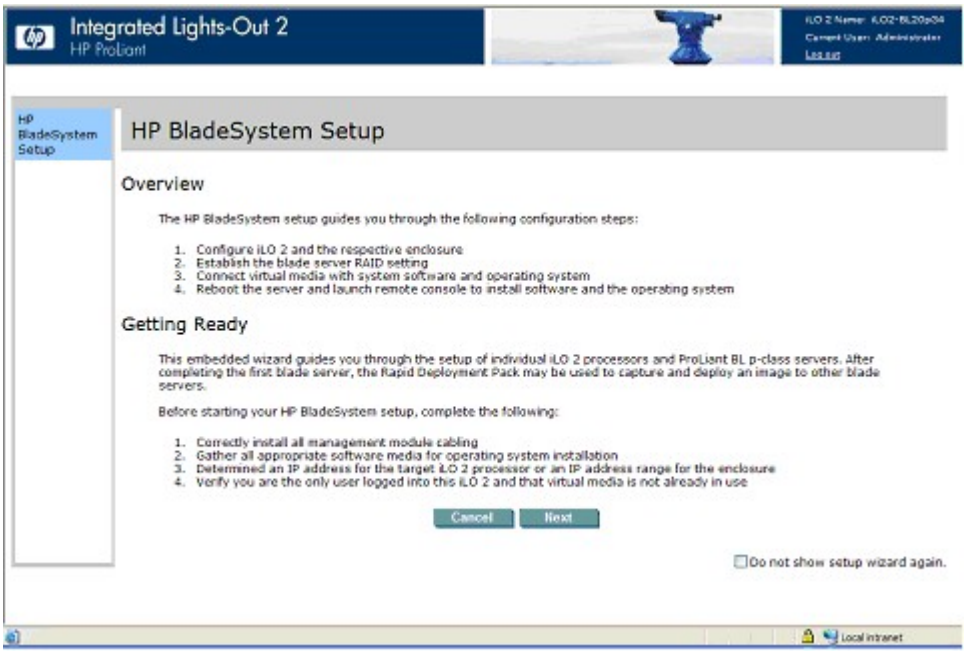
The HP BladeSystem setup wizard provides step-by-step instructions to simplify single blade setup without requiring DHCP or PXE. The HP BladeSystem Setup page launches after you authenticate to iLO 2 from the front port.

The server blade must be properly cabled for iLO 2 connectivity. Connect to the server blade through the server blade I/O port, while the blade is in the rack. This method requires you to connect the local I/O cable to the I/O port and a client PC. Using the static IP address listed on the I/O cable label and the initial access information on the front of the server blade, you can access the server blade through iLO 2 through its standard Web browser interface.

Although any blade can be used for access, if you use a static IP bay configuration to configure iLO 2 network settings, then the first blade in the enclosure must be used for access.

The first page of the wizard automatically launches if:

- This blade is new from the factory, and you have logged into iLO 2 from the front port.
- You did not fully complete the wizard by selecting **Finish** on the final page, and you did not select **Do not show setup wizard again** and clicked **Cancel** on the beginning page.
- You have set iLO 2 back to factory default settings.



Click **Cancel** to close the automated setup wizard. Click **Next** to set up your blade server. The setup wizard will guide you through:

1. iLO 2 configuration
2. Server RAID verification
3. Virtual media connection
4. Software installation

The iLO 2 firmware configuration screen

This screen enables you to change the following settings:

- Administrator password. HP recommends changing the default password.
- Network configuration settings. The following are the default settings:
  - Enable DHCP – Yes
  - Enable Static IP Bay Configuration – No
- If connected to the blade in enclosure slot 1, you can enable Static IP Bay configuration to preconfigure the static address for other iLO 2 processors in the enclosure.

In the default configuration, the iLO 2 being updated gets its IP address through DHCP. Other iLO 2 processors in the enclosure must be configured separately. If these settings are not changed, clicking **Next** displays the next page in the setup wizard. If either of these settings are changed, iLO 2 reboots to invoke the updated settings.

The following configuration combinations are also available (the default setting is in parentheses):

- Enable DHCP (Yes) and Enable Static IP Bay Configuration (Yes)

  This configuration causes the iLO 2 being configured to get its IP address through DHCP. Clicking **Next** displays the Static IP Bay Configuration page, enabling you to specify the IP addresses for other iLO 2s in the enclosure. After you click **Next**, you are prompted to verify that you want to use DHCP for this iLO 2 IP address.

- Enable DHCP (No) and Enable Static IP Bay Configuration (Yes)

  This configuration causes the iLO 2 being configured to set its IP address according to the settings specified through the Static IP Bay Configuration. Clicking **Next** displays the Static IP Bay Configuration page.

- Enable DHCP (No) and Enable Static IP Bay Configuration (No)

  This configuration causes the iLO 2 being configured to set its IP address according to the settings specified through the Network Settings page. Clicking **Next** displays the Network Settings page.

To save any network changes, you must have the Configure iLO 2 privilege.

Click **Next** to save changes and continue.

Verify Server RAID Configuration screen

This step of the installation wizard enables you to verify and accept server RAID configuration settings. Verify the detected RAID level for the hard drives on the blade server displayed on the web page and do one of the following:

- Click **Next** to keep current RAID settings.
- Click **Default Settings** to automatically configure the RAID level based on the number of installed drives. You are prompted to verify that you want to reset the RAID level because this could result in loss of data. Resetting the RAID level requires a server power-on or reboot. iLO 2 displays a page indicating that this action is occurring. The page is refreshed automatically every 10 seconds. After the server reboots, the next page in the installation wizard displays again. If an error occurs during the RAID reset process, the RAID Configuration page will redisplay with an indication of the error. An error is most likely to occur if the server is in

POST. If this is the case, exit any RBSU program you are running, allow POST to complete, and try the operation again.

You can change the RAID level manually through RBSU. If the operating system is already installed, changing the RAID level results in a loss of data.

Connect Virtual Media screen

This step of the installation wizard enables you to verify and accept the drive you will use during the installation of the operating system. Under Settings, select the local drive and media type you intend to use during operating system installation. Click **Launch Virtual Media** to launch the Virtual Media applet.

- Ensure the operating system media is connected. In the Virtual Media applet, a green icon appears next to the media currently selected.
- Verify that the operating system media is in the appropriate local drive.
- Accept security certificates as they appear.

After making your selection, click **Next** to save your settings and continue. The virtual media applet appears. After the applet is available, you can change the selected drive, or select other options not available on the installation wizard page.

Install Software screen

This step of the installation wizard enables you to launch the Remote Console and install the operating system. To start the operating system installation process:

- Click **Launch Software Installation** to launch the Remote Console. iLO 2 automatically initiates a server power-on or reboot to start the operating system installation through the previously selected virtual media.
- Accept security certificates as they appear.

Click **Finish** to complete the setup process.

iLO 2 diagnostic port configuration parameters

The iLO 2 Diagnostic Port on the front of ProLiant BL p-Class servers enables you to access and troubleshoot server issues by using a diagnostic cable. The iLO 2 Diagnostic Port uses a static IP address. It does not use DHCP to obtain an IP address, register with WINS or dynamic DNS, or use a gateway. The diagnostic port cable must not be left plugged in without an active network connection because it will cause degraded network performance on the standard iLO 2 network port.

In Network Settings, you can configure specific diagnostic port information. For more information on using the diagnostic port and the diagnostic cable, see to the setup and installation guide for the blade server.

The following are the fields that can be configured for the Diagnostic Port:

- Enable NIC

  If Enable NIC is set to Yes, the diagnostic port is enabled.
- Transceiver Speed Autoselect
- Speed
- Duplex

- IP Address

  Use this parameter to assign a static IP address to iLO 2 on your network. By default, the IP address is assigned by DHCP. By default, the IP address is `192.168.1.1` for all iLO 2 Diagnostic Ports.

- Subnet Mask
  - Use the subnet mask parameter to assign the subnet mask for the iLO 2 Diagnostic Port. By default, the subnet mask is `255.255.255.0` for all iLO 2 Diagnostic Ports.
  - The use of the Diagnostic Port is automatically sensed when an active network cable is plugged in to it. When switching between the diagnostic and back ports, you must allow 90 seconds for the network switchover to complete before attempting connection through the web browser.

    NOTE: The diagnostic port does not switch over if an active Remote Console session or a firmware update is in progress.

4 Using iLO 2

System status and status summary information

When you first access iLO 2, the interface displays the Status Summary page with system status and status summary information, and provides access to health information, system logs, and Insight Agent information. The options available in the System Status section are: **Summary**, **System Information**, **iLO 2 Log**, **IML**, **Diagnostics**, **iLO 2 User Tips**, and **Insight Agents**.

The Status Summary page displays high-level details about the system and iLO 2 subsystem, as well as links to commonly used features. To access the Status Summary page from other areas of the iLO 2 interface, click **System Status>Summary**.



Status information includes:

- Server Name – Displays the name of the server and is a link to Administration>Options>Access.
- UUID – Displays the ID of the server.
- Server Serial Number/Product ID – Displays the serial number of the server, which is assigned when the system is manufactured. You can change this setting using the system RBSU during POST. Product ID distinguishes between different systems with similar serial numbers. Although the Product ID is assigned when the system is manufactured, you can change this setting using the system RBSU during POST.
- System ROM – Displays the family and version of the active system ROM. If the system supports a backup system ROM, the backup date is also shown.
- System Health – Summarizes the condition of the monitored subsystems including overall status and redundancy (ability to handle a failure) and is a link to **System>Status>System Information Summary**.
- Internal Health LED – Represents the server internal health indicator (if supported). It summarizes issues with fans, temperature sensors, VRMs, and other monitored subsystems in the server. For more information, see "System Information Summary" (page 75).
- TPM Status – Displays TPM status configuration. If the host system or System ROM does not support TPM. TPM Status does not appear in Status Summary page. For more information, see "Trusted Platform Module support" (page 43).
- Server Power – Displays the current power state of the server (ON/STANDBY) when the page was loaded and is a link to Server>Power Management. Users with virtual power and reset privilege can also use the Momentary Press button.

- UID Light – Displays the state of the UID light when the page was loaded. You can control the UID state using the Turn UID On button in addition to the physical UID buttons on the server chassis.

  The UID helps you identify and locate a system, especially in high-density rack environments. Additionally, the UID indicates that a critical operation is underway on the host, such as Remote Console access or firmware update.

CAUTION: Never remove power from a server with a flashing UID.

The current state of the UID (on or off) is the last state chosen using one of these methods. If a new state is chosen while the UID is blinking, the new state becomes the current state and takes effect when the UID stops blinking. While the UID is blinking, the current state of the UID is shown along with the tag flashing. When the UID stops blinking, the tag is removed.

The UID is not supported on the HP ProLiant ML310 G3.

- Last Used Remote Console – Displays the previously launched remote console and its availability, which enables you to quickly launch your preferred Remote Console. You can use the Remote Console if it is available and you have the appropriate user privilege. You can pick a different console by following the Last Used Remote Console link.
- Latest IML Entry – Displays the most recent entry in the IML.
- iLO 2 Name – Displays the name assigned to the iLO 2 subsystem. By default, this is the word iLO added to the system serial number. This value is used for the network name and must be unique.
- License Type – Displays whether the system has a feature license installed and is a link to Administration>Licensing. Some features of iLO 2 cannot be accessed unless licensed.
- iLO 2 Firmware Version – Displays information about the version of iLO 2 firmware currently installed and is a link to the iLO 2 Release Notes page which highlights new capabilities in the current firmware release and in selected previous releases
- IP Address – Displays the network IP address of the iLO 2 subsystem and is a link to Administration>Network Settings.
- Active Sessions – Displays all users currently logged in to iLO 2.
- Latest iLO 2 Event Log Entry – Displays the most recent entry in the iLO 2 Event Log.
- iLO 2 Date – Displays the date (`MM/DD/YYYY`) as indicated by the iLO 2 subsystem internal calendar. The iLO 2 internal calendar is synchronized with the host system at POST and when the Insight Agents run.
- iLO 2Date/Time – Displays the iLO 2 subsystem internal clock. The iLO 2 internal clock is synchronized with the host system at POST and when the Insight Agents run.

System Information Summary

System Information displays the health of the monitored system. Many of the features necessary to operate and manage the components of the HP ProLiant server have migrated from the health driver to the iLO 2 microprocessor. These features are available without installing and loading the health driver for the installed operating system. The iLO 2 microprocessor monitors these devices when the server is powered on during server boot, operating system initialization, and operation. Monitoring continues through an unexpected operating system failure. To access System Information, click **System Status>System Information**. The System Health Summary tab appears. System Information also displays the following embedded health tabs: "Fans" (page 76), "Temperatures" (page 76), "Power" (page 77), "Processors" (page 77), "Memory" (page 77), and "NIC" (page 77).

The Summary tab displays the state of monitored host-platform subsystems status at a glance, summarizing the condition of the monitored subsystems, including overall status and redundancy

(ability to handle a failure). The subsystems can include fans, temperature sensors, power supplies, and voltage regulator modules.

- Fans – Displays the state of the replaceable fans in the server chassis. This data includes the area that is cooled by each fan and current fan speeds.
- Temperatures – Displays the temperature conditions monitored at sensors in various locations in the server chassis, and the processor temperature. The temperature is monitored to maintain the location temperature below the caution threshold. If the temperature exceeds the caution threshold, the fan speed is increased to maximum.
- VRMs – Displays VRM status. A VRM is required for each processor in the system. The VRM adjusts the power to meet the power requirements of the processor supported. A failed VRM prevents the processor from being supported and must be replaced.
- Power Supplies – Displays the presence and condition of installed power supplies.
  - OK – Indicates that the power supply is installed and operational.
  - Unpowered – Indicates that the power supply is installed, but not operational. Verify that the power cord is connected.
  - Not present – Indicates that the power supply is not installed. Power is not redundant in this condition.
  - Failed – Indicates that the power supply must be replaced.

To access the Summary tab from other areas of the iLO 2 interface, click **System Status>System Information>Summary**.

Fans

iLO 2, in conjunction with additional hardware, controls the operation and speed of the fans. Fans provide essential cooling of components to ensure reliability and correct operation. Fan location, placement, design and speed control take into account various temperatures monitored throughout the system to provide appropriate cooling with minimal noise levels.

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

Monitoring the fan sub-system includes the sufficient, redundant, and non-redundant configurations of the fans. Fan failure is a rare occurrence, but to ensure reliability and uptime, ProLiant servers have redundant fan configurations. In ProLiant servers that support redundant configurations, fan or fans might fail and still provide sufficient cooling to continue operation. iLO 2 increases fan control to continue safe operation of the server in the event of fan failure, maintenance operations, or any event that alters cooling of the server.

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

The Fan tab displays the state of the replaceable fans within the server chassis. This data includes the area cooled by each fan and the current fan speed.

Temperatures

The Temperatures tab displays the location, status, temperature, and threshold settings of temperature sensors in the server chassis. The temperature is monitored to maintain the location temperature

below the caution threshold. If one or more sensors exceed this threshold, iLO 2 implements the recovery policy to prevent damage to server components.

- If the temperature exceeds the caution threshold, the fan speed is increased to maximum.
- If the temperature exceeds the critical temperature, a graceful server shutdown is attempted.
- If the temperature exceeds the fatal threshold, the server is immediately turned off to prevent permanent damage.

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

After correcting the excessive temperature conditions additional polices are implemented including returning the fan speed to normal, recording the event in the IML, turning off the LED indicators, and if appropriate, canceling shutdowns in progress.

Power

The VRMs/Power Supplies tab displays the state of each VRM or power supply. VRMs are required for each processor in the system. VRMs adjust the power to meet the needs of the processor supported. A VRM can be replaced if it fails. A failed VRM prevents the processor from being supported.

iLO 2 also monitors power supplies in the system to ensure the longest available uptime of the server and operating system. Power supplies can be affected by the brownouts and other electrical conditions, or AC cords can be accidentally unplugged. These conditions result in a loss of redundancy if redundant power supplies are configured, or result in loss of operation if redundant power supplies are not in use. Additionally, if a power supply failure is detected (hardware failure) or the AC power cord is disconnected, then these events are recorded in the IML and the LED indicators light.

iLO 2 monitors power supplies to ensure that they are correctly installed. This information appears on the System Information page. Reviewing the System Information page and IML will assist you in deciding when to repair or replace a power supply, preventing a disruption in service.

Processors

The Processors tab displays the available processor slots, the type of processor installed in the slot, and a brief status summary of the processor subsystem. If available, installed processor speed in MHz and cache capabilities are displayed.

Memory

The Memory tab displays the available memory slots and the type of memory, if any, installed in the slot.

NIC

The NIC tab displays the MAC addresses of the integrated NICs. This page does not display add-in network adapters.

iLO 2 Log

The iLO 2 Log page displays the iLO 2 Event Log, which is a record of significant events detected by iLO 2. Logged events include major server events such as a server power outage or a server reset and iLO 2 events such as unauthorized login attempts. Other logged events include successful or unsuccessful browser and Remote Console logins, virtual power and power cycle events, clear event log actions, and some configuration changes, such as creating or deleting a user.

iLO 2 provides secure password encryption, tracking all login attempts and maintaining a record of all login failures. Authentication Failure Logging allows you to configure logging criteria for

failed authentications. You can configure tracking failed login attempts for every attempt or every second, third, or fifth attempt, and captures the client name for each logged entry to improve auditing capabilities in DHCP environments, as well as recording account name, computer name, and IP address. When login attempts fail, iLO 2 also generates alerts and sends them to a remote management console.

Events logged by higher versions of iLO 2 firmware might not be supported by earlier versions. If an event is logged by an unsupported firmware, the event is listed as `UNKNOWN EVENT TYPE`. You can clear the event log to eliminate these entries, or update the firmware to the latest supported version.

To access the iLO 2 Log, click **System Status>iLO 2 Log**.

To clear the event log:

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.

IML

The IML page displays the Integrated Management Log, which is a record of historical events that have occurred on the server as reported by various software components. Events are generated by the system ROM and by services like the System Management (health) driver. 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, see to the server guide.

Entries in the IML can assist during issue diagnosis or help identify possible issues before they occur. Preventative action might be recommended to avoid possible disruption of service. iLO 2 manages the IML, which can be accessed using a supported browser, even when the server is off. The ability to view the event log even when the server is off can be helpful when troubleshooting remote host server issues.

You can sort the log by clicking the header of any column of data. After the sort completes, clicking the same column header again sorts the log in reverse of its current order. Very large logs will take several minutes to sort and display. You can clear the events in this log on the server's Insight Manager Web Agents home page.

The iLO 2 processor records the following information to the IML based upon the occurrences in the system.

- Fan inserted
- Fan removed
- Fan failure
- Fan degraded
- Fan repaired
- Fan redundancy lost
- Fans redundant
- Power supply inserted
- Power supply removed
- Power supply failure
- Power supplies redundancy lost
- Power supplies redundant
- Temperature over threshold

- Temperature normal
- Automatic shutdown started
- Automatic shutdown cancelled

Diagnostics

The Diagnostics option on the System Status tab displays the Server and iLO 2 Diagnostics screen. The Server and iLO 2 Diagnostic screen displays iLO 2 self-test results, and provides options to generate an NMI to the system and to reset iLO 2.

NOTE: When connected through the Diagnostics Port, the directory server is not available. You can log in using a local account only.

The Diagnostics page contains the following sections:

- Non-Maskable Interrupt (NMI) button

  The Non-Maskable Interrupt (NMI) button section contains the Generate NMI to System button which enables you to halt the operating system for debugging. This functionality is an advanced function and must only be used for kernel-level debugging. The possible uses of the Generate NMI to System feature include the following:

  — Use the Demonstrate ASR feature only if the System Management (health) driver is loaded and ASR is enabled. The host automatically reboots after an NMI has occurred.

  — Use the Debug feature if a software application hangs the system. The Generate NMI to System button can be used to engage the operating system debugger.

  — Initiate the dump of an unresponsive host if you want to capture the server context.

  The Virtual Power and Reset privilege is required to generate an NMI. An unexpected NMI typically signals a fatal condition on the host platform. A blue-screen, panic, ABEND, or other fatal exception occurs when an unexpected NMI is received by the host operating system, even when the operating system is unresponsive or locked-up. Generating an unexpected NMI can be used to diagnose a catatonic or deadlocked operating system. Generating an NMI crashes the operating system, resulting in lost service and data.

  Generating an NMI must only be used in extreme diagnostic cases in which the operating system is not functioning properly and an experienced support organization has recommended that you proceed with an NMI. Generating an NMI as a diagnostic and debugging tool is primarily used when the operating system is no longer available. Generating an NMI must not be used during normal operation of the server. The Generate NMI to System button does not gracefully shut down the operating system.

- **iLO 2 Self-Test Results**

  The iLO 2 Self-Test Results sections displays the results of iLO 2 internal diagnostics. iLO 2 performs a series of initialization and diagnostic procedures on the subsystems of the iLO 2 system. The results display on the Server and iLO 2 Diagnostics screen. All tested subsystems display `Passed` under normal circumstances. Each test displays one of three results: Passed, Fault, or N/A.

  The status of these self-tests is indicated by the test results and is intended to identify issue areas. If a Fault test condition is indicated, follow information noted on the screen. The specific tests that are run is system-dependant. Not all tests are run on all systems. See the iLO 2 Diagnostics page to verify which tests are automatically performed on your system.

- **Reset Integrated Lights-Out 2**

  The Reset Integrated Lights-Out 2 section contains the Reset button which enables you to reboot the iLO 2 processor. Using Reset does not make any configuration changes. Reset disconnects any active connections to iLO 2 and completes any firmware updates in progress. You must

have the Configure iLO 2 privilege (configure local device settings) to reset iLO 2 using this option.

Insight Agents

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

The agents can automatically provide the link to iLO 2, or you can manually enter the link using Administration/Management.

For more information, see "HP Systems Insight Manager integration" (page 178), and the HP web site at http://www.hp.com/servers/manage.

iLO 2 Remote Console

iLO 2 Remote Console redirects the host server console to the network client browser, providing full text (standard), graphical mode video, keyboard, and mouse access to the remote host server (if licensed). iLO 2 uses virtual KVM technology to improve remote console performance comparable with other KVM solutions.

With remote console access, 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 consoles (if licensed) enable you to view and control the host server screen throughout the installation process.

Remote console access provides you complete control over a remote host server as if you were in front of the system, including access to the remote file system and network drives. Remote Console enables you to change hardware and software settings of the remote host server, install applications and drivers, change remote server screen resolution, and gracefully shut down the remote system.

Up to 10 users are allowed to simultaneously log in to iLO 2. However, only four users can access a shared Integrated Remote Console. If you attempt to open the Remote Console while it is already in use, a warning message appears, indicating that it is in use by another user. To view the remote console session already in progress, see "Multi-user access to the Integrated Remote Console" (page 89). To take control of the session, use the Remote Console Acquire feature, see "Acquiring the Remote Console" (page 92).

The Remote Console Information page provides access links to the different remote console access options. After deciding which console option you want to use, click the appropriate link. iLO 2 provides the following remote console access options:

- "Integrated Remote Console option" (page 85) – Provides access to the system KVM, allowing control of Virtual Power and Virtual Media from a single console using Microsoft Internet Explorer.
- "IRC Fullscreen" (page 85) – Resizes the Integrated Remote Console to the same display resolution as the remote host.

  The Integrated Remote Console and Integrated Remote Console Fullscreen uses ActiveX and requires Microsoft Internet Explorer.
- "Remote Console" (page 93) – Provides access to the system KVM through a Java applet-based console. Remote Console is the familiar Remote Console support carried forward from the original iLO product. Remote Console support requires that Java be installed on the client

system. Remote Console operates with all operating systems and browsers supported by iLO 2.

- "Remote Serial Console" (page 100) – Provides access to a VT320 serial console through a Java applet-based console connected to the iLO 2 Virtual Serial Port. The Remote Serial Console is available without an additional license and is suitable for host operating systems that do not require access to the graphical console.

Standard iLO 2 provides server console access from server power-on through POST. Integrated Remote Console, Integrated Remote Console Fullscreen, and Remote Console are graphical remote consoles that turn a supported browser into a virtual desktop, allowing you full control over the display, keyboard, and mouse of the host server. The operating-system-independent console supports graphic modes that display remote host server activities, including shutdown and startup operations (if licensed).

Remote console access to the host server after server POST is a licensed feature available with the purchase of optional licenses. For more information, see "Licensing" (page 26). To access iLO 2 Remote Console, click **Remote Console.** The Remote Console Information page appears.

Remote Console overview and licensing options

Remote Console and Integrated Remote Console connections are graphical and must be rendered using a client program that can process iLO 2 graphics commands. Two clients are provided to render the iLO 2 graphics:

- Java-based Remote Console
- Windows Active X-based Integrated Remote Console

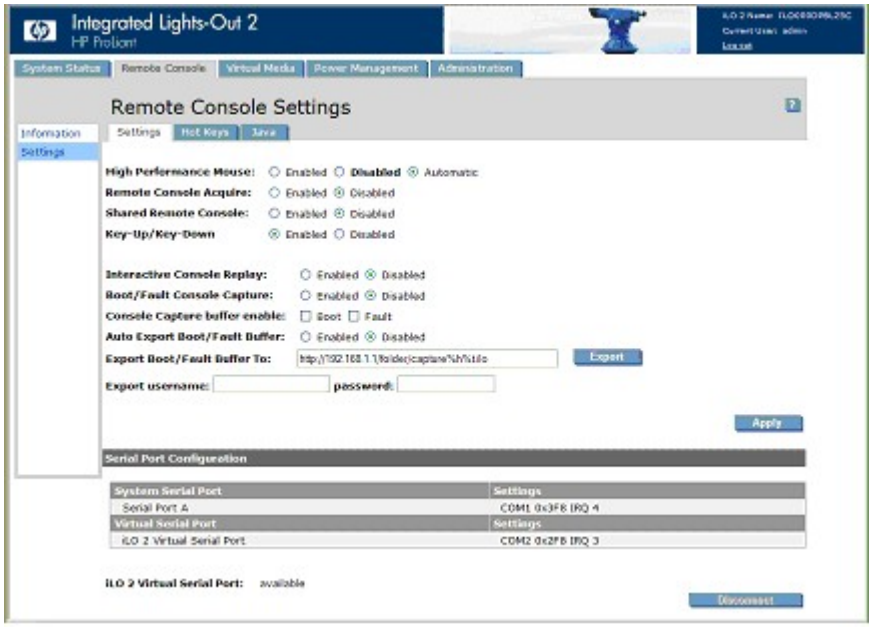
For those clients that do not understand iLO 2 graphics, SSH and Telnet, you must use the iLO 2 Remote Serial Console or purchase an iLO Advanced license to use the text-based console after POST.

ESX consoles, in particular ESX console 1, do not fully support iLO 2 Remote Console and Integrated Remote Console. ESX does not support Remote Serial Console.

iLO 2 blades ship with the iLO 2 Standard Blade Edition, which includes the Remote Console. However, the HP ProLiant ML and HP ProLiant DL models ship with the iLO Standard license, which does not include the Remote Console or Integrated Remote Console. As soon as the server starts to boot an operating system, the iLO 2 Standard on the HP ProLiant ML and ProLiant DL models displays a message that indicates the need for the iLO 2 Advanced license. For more information, see "Licensing" (page 26).

Remote Console settings

The iLO 2 Remote Console settings and options are configured on the Remote Console Settings page. To access the Remote Console Settings page, click **Remote Console>Settings**.



The Remote Console Settings page includes three tabs:

Settings

- High Performance Mouse settings can help alleviate remote console mouse synchronization issues, but this feature is not supported on all operating systems. The effects of changing the settings take place when remote console is started or restarted. The following options are available:
  - Disabled – Enables the mouse to use the relative coordinates mode which is compatible with most host operating systems.
  - Enabled – Enables the mouse to use the absolute coordinates mode, eliminating synchronization issues on supported operating systems.
  - Automatic – Enables iLO 2 to select the appropriate mouse mode when the iLO 2 driver is loaded on the host operating system. The selected mode is persistent unless a different mode is indicated when the operating system driver is loaded or if you choose another setting.
- Remote Console Acquire enables one user to take the remote console session away from another user. This setting enables or disables the acquire functionality.
- Shared Remote Console enables multiple users to view and control the server console at the same time. This setting enables or disables the shared functionality.
- Interactive Console Replay allows you to replay the captured console video of boot and fault sequences along with user-initiated manual console captures.
- The Key-Up/Key-Down setting allows you toggle between using the HID report keyboard model and the ASCII and ESC codes keyboard model in the IRC. The HID report keyboard model is enabled by default but might cause repeating characters on high latency networks. If you experience repeating characters when using IRC, set Key-Up/Key-Down to **Disabled**.
- Boot/Fault Console Capture enables you to capture console video to internal buffers of any boot and fault sequences. Internal buffer space is limited to the capture of the most recent boot or fault sequence. Buffer space is limited. The more dynamic and the higher the graphical resolution of the server console, the less amount of data that can be stored in the buffer. Select which type of video to capture using the following options:
  - Console Capture buffer allows you to select which type of console sequence to capture. You can enable either buffer or enable both buffers at the same time. The buffers share the same internal data area, so enabling both reduces the amount of console video that

can be captured. You can change the enabled buffers at any time to maximize buffer utilization. When the buffer configuration is changed, both buffers are reset and information currently in the buffers at that time is lost.

— Auto Export/Fault Buffer allows you to enable or disable automatically exporting captured console data.

- Export Boot/Fault Buffer enables you to specify the URL location of a web server that accepts a PUT or POST Method data transfer. For example: `http://192.168.1.1/images/capture%h%t.ilo` transfers the internal-capture buffers to a web server at the IP address 192.168.1.1, and stores the data in the `images` folder using the filename `captureServerNameDateTime-Boot(or Fault).ilo`.

  Where:

  — `%h` specifies the addition of the server name to the filename

  — `%t` specifies that a time stamp will be included in the filename

  — `Boot or Fault` is automatically added to denote the buffer type as either a boot-sequence or fault-sequence event

  For more information about web server configuration, and how to configure an Apache web server to accept exported capture buffers, see "Configuring Apache to accept exported capture buffers" (page 194).

  ◦ Export enables you to trigger an export manually.

  ◦ Export username is the username for the web server that is specified in the URL.

  ◦ Password is the password of the web server that is specified in the URL.

  After making changes, click **Apply**.

- Serial Port Configuration displays the current settings of the system serial ports and the Virtual Serial Port. The Settings for the system and virtual serial ports are also displayed, showing the COM ports in use and IRQ numbers.
- iLO 2 Virtual Serial Port displays the current status of the Virtual Serial Port connection. The possible modes available are: in use raw mode, or in use normal mode. If the connection is in use, the Disconnect button is available and can be used to disconnect a Virtual Serial Port connection. Raw mode indicates that a client is connected using the WiLODbg.exe utility which is used for remote Windows kernel debugging.

Hot Keys enable you to define keystroke sequences that are transmitted to the remote host server by pressing a hot key. Remote Console hot keys allow specific key sequences such as **Alt+Tab** and **Alt+SysRq** to be passed to the server from the Remote Console Java session. For more information, see "Remote console hot keys" (page 83).

Java displays the Java requirements for each supported operating system and a link to download Java. For more information, see "Supported browsers and client operating systems" (page 15).

Remote console hot keys

The Program Remote Console Hot Keys page enables you to define up to six multiple key combinations assigned to each hot key. When a hot key is pressed in the Remote Console, on client systems, the defined key combination (all keys pressed at the same time) are transmitted in place of the hot key to the remote host server. To access AltGr symbols on international keyboards, use hot keys to define these symbols. For a list of support hot keys, see ("Supported hot keys" (page 84).

Remote console hot keys are active during a Remote Console session through the IRC, Remote Console applet, and during a text Remote Console session through a Telnet client. When using the IRC, keyboard LED states for NumLock, CapsLock and ScrollLock on the client keyboard do

not necessarily reflect the state of the server keyboard. However, pressing any of the locking keys will change that Lock state on the server.

To define a Remote Console hot key:

1. Click **Remote Console>Hot Keys**.
2. Select the hot key you want to define, and use the drop-down 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 Program Remote Console Hot Keys page also contains a Reset Hot Keys option. This option clears all entries in the hot key fields. Click **Save Hot Keys** to save the cleared fields.

Supported hot keys

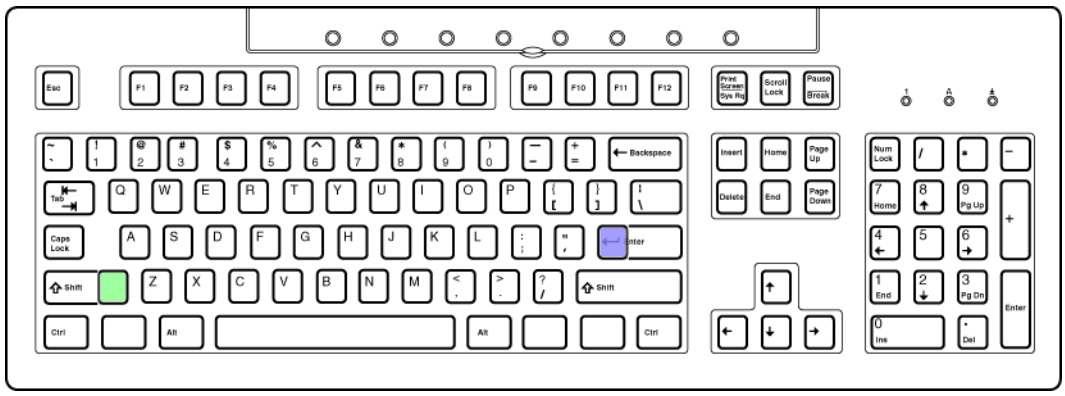
The Program Remote Console Hot Keys page allows you to define up to 6 different sets of hot keys for use during a Remote Console session. Each hot key represents a combination of up to 5 different keys which are sent to the host machine whenever the hot key is pressed during a Remote Console session. The selected key combination (all keys pressed at the same time) are transmitted in its place. For more information, see "Remote console hot keys" (page 83). 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	

Hot keys and international keyboards

To set up hot keys on an international keyboard, select keys on your keyboard in the same position on a US keyboard. To create a hot key using the international AltGR key, use R_ALT in the key list. Use the US keyboard layout shown to select your keys.



Shaded keys do not exist on a US keyboard.

- The green shaded key is known as the Non-US \ and | keys on an international keyboard.
- The purple shaded key is known as the Non-US # and ~ key on an international keyboard.

Hot keys and Virtual Serial Port

When connected to the Virtual Serial Port feature of iLO 2 using Telnet, the key sequence **CTRL+P+!** (CTRL key, P key, SHIFT key, and 1 key pressed simultaneously) normally causes the remote server to reboot.

To power the remote server off, use the key sequence **CTRL+P 6**. To power the remote server on, use the key sequence **CTRL+P 1**.

If iLO 2 becomes unresponsive, close the Virtual Serial Port session. iLO 2 automatically resets in approximately three minutes and returns to normal operation.

IRC Fullscreen

Integrated Remote Console Fullscreen allows you to re-size the IRC to the same display resolution as the remote host. To return to your client desktop, exit the console.

Integrated Remote Console Fullscreen causes your client to resize to the same resolution as the remote server. Integrated Remote Console Fullscreen attempts to pick the best client display settings for that resolution; however, some monitors might have trouble with the highest screen refresh rates supported by the video adapter. If this occurs, check your desktop properties by right-clicking on the **Desktop** and selecting **Properties>Settings>Advanced>Monitor** and select a lower screen refresh rate.

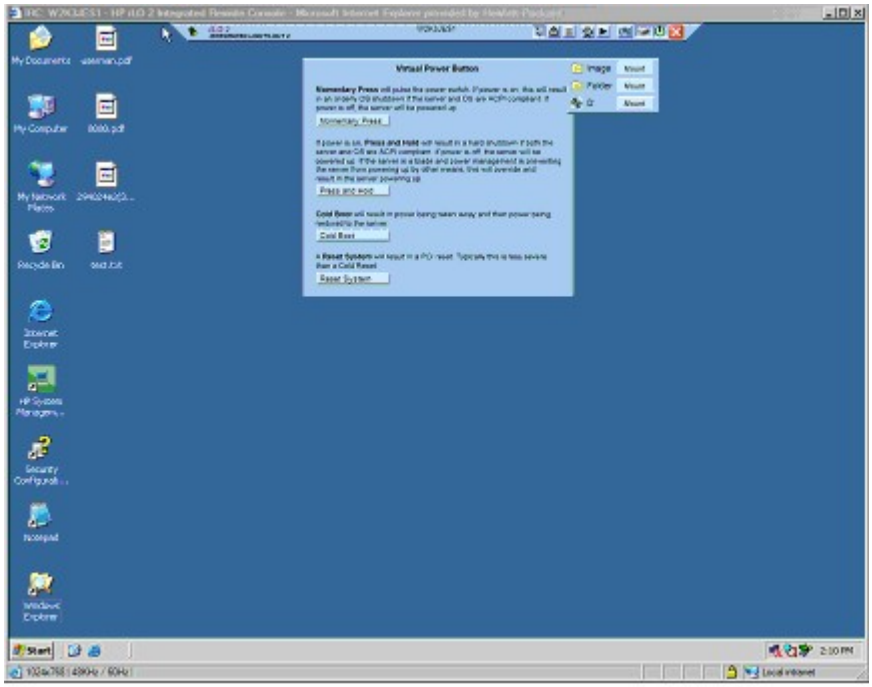
For more information on the Integrated Remote Console Full screen display, see "Integrated Remote Console option" (page 85).

Integrated Remote Console option

The Integrated Remote Console offers a high-performance remote console interface for Windows clients, combining KVM, Virtual Power, and Virtual Media functionality. The Integrated Remote Console option is an ActiveX control that runs from Microsoft Internet Explorer. Integrated Remote

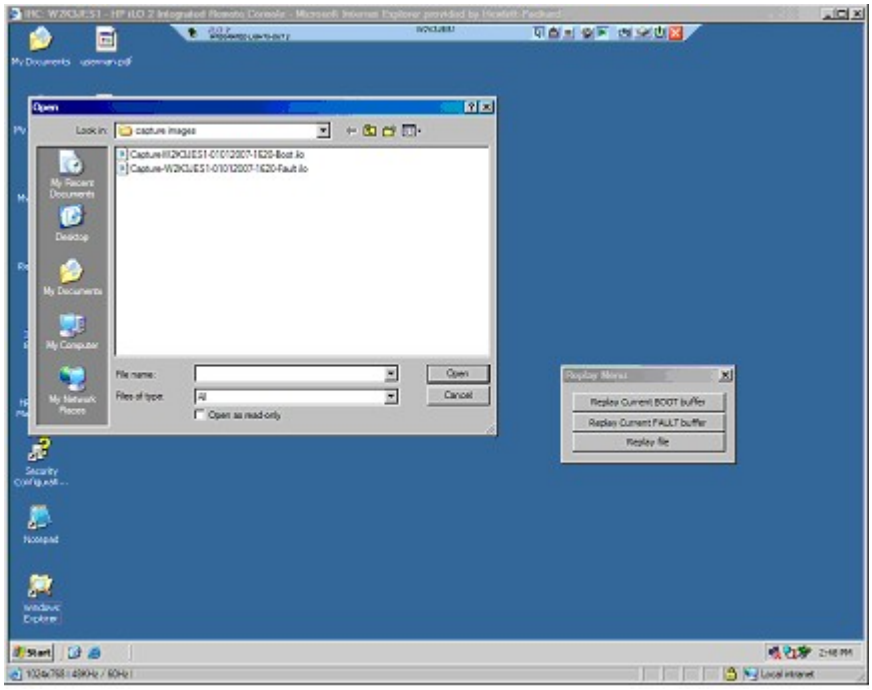
Console is a licensed feature available with the purchase of optional licenses. For more information, see "Licensing" (page 26).

The Integrated Remote Console supports four simultaneous remote console sessions with the same server if enabled through the Remote Console Settings screen, SMASH CLI (OEM), or RIBCL. For more information about using multiple remote console sessions, see "Multi-user access to the Integrated Remote Console" (page 89).

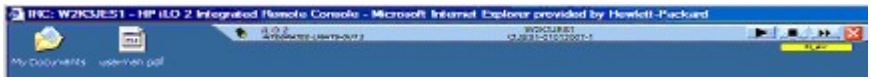


Integrated Remote Console and Integrated Remote Console Fullscreen display a menu bar and buttons rendered on the screen. The menu bar has the following options:

- Remote Console Replay (play icon) – Displays the Replay Menu dialog (if Boot/Fault Console Capture is enabled) or starts the Open File dialog box if Boot/Fault Console Capture is not enabled.
  - Replay Current BOOT buffer and Replay Current FAULT buffer – Enables you to transfer the internally captured buffers to the client using the Console Replay port specified on the Administration>Access tab. Click **Replay Current BOOT buffer** or **Replay Current FAULT buffer** to change the Remote Console menu to the Replay Console menu.
  - Replay file – Displays an Open dialog box enabling you to view a previously saved file. After you select a file and click **Open,** the Remote Console menu changes to the Replay Console menu.



- Replay (play icon on the main menu) – Displays the Replay Console. The Replay Console provides playback control of the selected data buffer and displays elapsed playback time.



The Replay Console has the following options:

  - Click **Play** to start the playback. After you click Play, you can:
    - Click **Pause** to stop the playback and hold the current position. To resume playback, click **Play** from the paused state and the playback resumes from the current position.
    - Click **Stop** to halt the playback and reset the playback to the beginning of the data buffer.
    - Click **Fast-forward** to increases the playback rate 2x, 4x, or 8x of normal speed.
  - Close appears when playback is complete. Click **Close** to exit the Replay Console and display the Remote Console menu bar.

- Record (camera icon) – Enables you to manually record current server console video. Press **Record** to display a Save dialog box enabling you to specify the file name and the location to save the current recording session. During a recording session, Record will appear depressed and change to green. While enabled, any server console activity appearing on the Integrated Remote Console is saved to the file specified. If you click **Record** during a recording session, the recording session stops and returns the Record button to the normal unpressed state. To replay the recording, click **Replay.**
- Control – Enables the session leader to reclaim full control if control was authorized for a satellite client.
- Lock – Enables you to prevent any additional satellite client requests from appearing on the session leader console.
- Client List – Displays the user name and DNS name (if available) or IP address of the current satellite clients.
- Drive – Displays all available media.

- Power (green power icon) – Displays the power status and allows you to access the power options. The power button is green when the server is powered up. When you press **Power** the Virtual Power Button screen appears with four options: Momentary Press, Press and Hold, Cold Boot, and Reset System.

  When either the Drives or Power button is pressed, the menu displayed remains open even when the mouse is moved away from the menu bar.
- CAD – Enables you to start a dialog to send the Ctrl-Alt-Del keys (or any one of the six hotkeys) to the server.
- Thumb tack – Enables you to keep the Remote Console main menu open or to retract the main menu when the mouse is moved away.
- Exit (red X icon) – Enables you to close and exit the remote console.

Internet Explorer 7 security enhancements display the address bar in any recently opened windows. If you want to remove the address bar from the IRC, you must change the Security setting from the default level. To remove the address bar, set **Set Allow websites to open windows without address or status bars** to **Enable**.

Optimizing mouse performance for Remote Console or Integrated Remote Console

In some Microsoft Windows configurations the mouse acceleration must be set correctly for remote console mouse to behave properly.

SLES 9

Determine which mouse device is the Remote Console mouse by using the `xsetpointer -l` command to list all mice.

1. Determine which mouse you want to modify by cross-referencing the output of `xsetpointer` with the X configuration (either `/etc/X11/XF86Config` or `/etc/X11/xorg.conf`)
2. Select the remote console mouse as the mouse you want to modify. For example:

   ```
   xsetpointer Mouse[2]
   ```
3. Set the acceleration parameters. For example:

   ```
   xset m 1/1 1
   ```

Red Hat Enterprise Linux

Set the acceleration parameters using:

```
xset m 1/1 1
```

Windows mouse synchronization

The default High Performance mouse setting on the Global Setting page is designed to use the best setting based on the server operating system. To function correctly requires the HP ProLiant Lights-Out Management Interface Driver is loaded and the server has been rebooted after the driver installation. If you experience mouse synchronization issues under Windows, change the High Performance Mouse setting to `Yes`.

High Performance Mouse settings

When using the Remote Console, you can enable the High Performance Mouse feature. This feature greatly improves pointer performance and accuracy on supported operating systems. iLO 2 High Performance Mouse is a pointing device that provides absolute position coordinates to describe its location similar to a USB tablet mouse. A conventional mouse sends relative position information (such as the mouse has moved 12 pixels to the right). The host computer can modify relative position information to enable features like mouse acceleration. When using the Remote Console, the client is not aware of these modifications. Therefore, synchronization between the client and host mouse cursors fails.

Both the Integrated Remote Console and the Remote Console applets send absolute and relative mouse cursor coordinates to iLO 2. When iLO 2 is in High Performance Mouse mode, it discards the relative coordinates and sends the absolute coordinates to the USB tablet mouse emulator. The result is that the server "sees" the mouse move as if the coordinate information had originated from a local USB tablet mouse. When iLO 2 is not in High Performance Mouse mode, the absolute coordinates are discarded and the relative coordinates are sent to the USB relative mouse emulator.

High-Performance Mouse is supported only on operating systems that support USB tablet mouse. Windows users must enable the High Performance Mouse option on the Remote Console Settings screen. Linux users must enable the High Performance mouse option once the iLO 2 High Performance Mouse for Linux driver is installed. Other operating system servers experiencing Remote Console mouse trouble must disable the High Performance Mouse option.

When using Integrated Remote Console from iLO 2 and SmartStart, the local mouse and remote mouse do not stay aligned. The High Performance Mouse setting must be disabled while in SmartStart. If the local mouse and remote mouse get out of alignment while you are using the High Performance Mouse feature, you can use the right Ctrl key to realign them. Alternatively, you can use the Java Remote Console instead of Integrated Remote Console.

The High Performance Mouse option alleviates all mouse synchronization issues on supported host operating systems. You can select this mode on the Remote Console Settings page before starting a Remote Console. However, it might not be supported by all operating systems, particularly during installation. For best performance:

- Select a lower remote server screen resolution to improve the performance of the Remote Console. The maximum supported resolution is 1280 x 1024 pixels.
- Set the client screen resolution higher than the remote server resolution to maximize Remote Console visibility.
- The color quality of the remote server has no effect on the performance of the remote console. The Remote Console is rendered in 4096 (12-bit) colors.
- Use a non-animated mouse pointer on the remote system.
- Disable mouse trails on the remote system.

To configure the host server adjust the following settings in the Control Panel:

1. Select **Mouse>Pointers>Scheme>Windows Default scheme.** Click **OK**.
2. From the Mouse>Pointers page, select **Enable pointer shadow**. Click **OK**.
3. Select **Display>Settings>Advanced>Troubleshoot>Hardware Acceleration>Full.** Click **OK**.
4. Select **System>Advanced>Performance Settings>Visual Effects>Adjust for best performance**. Click **OK**.

Alternatively, the HP online configuration utility (HPONCFG) can automatically adjust these settings. You can also edit High Performance Mouse settings using the XML command `MOD_GLOBAL_SETTINGS`. For more information about using the RIBCL command `MOD_GLOBAL_SETTINGS`, see the *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide* at http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=135&prodTypeId=18964&prodSeriesId=1146658.

Multi-user access to the Integrated Remote Console

Shared Remote Console is an iLO 2 feature that allows the connection of up to four sessions on the same on the same server. This feature does not replace the Acquire feature described in "Acquiring the Remote Console" (page 92), or allow full-access clients (read/write) to control power. Shared Remote Console does not support passing server host designation to another user or a failed user connection to reconnect after failure. You must restart the remote console session to allow user access after failure.

Shared Remote Console is a licensed feature available with the purchase of optional licenses. For more information, see "Licensing" (page 26).

Shared Remote Console and Forced Switch mode are disabled by default. You must enable and configure these features through the browser, SMASH CLI (OEM), or RIBCL. All console sessions are encrypted by authenticating the client first, and then the session leader decides whether to allow the new connection.

The first user to initiate a Remote Console session connects to the server normally and is designated as the session leader (session host.) Any subsequent user requesting Remote Console access initiates an access request, requesting a satellite client connection, calling the session leader. A pop-up for each satellite client request appears on the session leader's desktop, identifying the requester's user name and DNS name (if available) or IP address.

Session hosts have the option to grant or deny access. A list of users and session host names appears within the remote console browser frame. Satellite client sessions terminate when the session host is terminated.

Shared sessions do not operate well with the Console Capture and replay features of iLO 2. If a satellite session is viewing a captured session, during the playback time, the satellite session will not receive session leader control messages. If the session host starts to view captured video data during a shared session, the video appears on all satellite Remote Console sessions.

Using Console Capture

Console Capture is a Remote Console feature that enables you to record and replay a video stream of events such as booting, ASR events, and sensed operating system faults. You can also manually start and stop the recording of console video. Console Capture is only available through the iLO 2 user interface and cannot be accessed through XML scripting or the CLP. Console Capture is a licensed feature available with the purchase of optional licenses. For more information, see "Licensing" (page 26).

A buffer area is set aside in the management processor to store captured video data. This buffer area is shared with the firmware update buffer, so any information captured is lost when you start the firmware update process. You cannot capture video data during the firmware update process.

Buffer space is limited. Only one of each type of event is stored in the buffer area at a time. You can transfer captured data buffers to a client running the IRC for replay. You can also configure iLO 2 to automatically send captured video data to a web server on the same network as the iLO 2 when an event occurs. The web server must accept POST-method data transfers. You can select Boot buffer only, Fault buffer, or combine them both as one large buffer to have more room to capture Linux boot sequences.

Exported buffer data is given a unique name to easily identify the data for playback. Playback requires a licensed iLO 2 on the network. Some operating systems (such as Linux) can fill the buffer quickly. If you leave the system console in text mode, it helps maximize the amount of information captured. Also, closing or reducing the number of active graphical console elements helps optimize internal buffer space.

You can manually capture video of the server console using the IRC Record feature. All manually captured data is stored in a local file on the client for later playback.

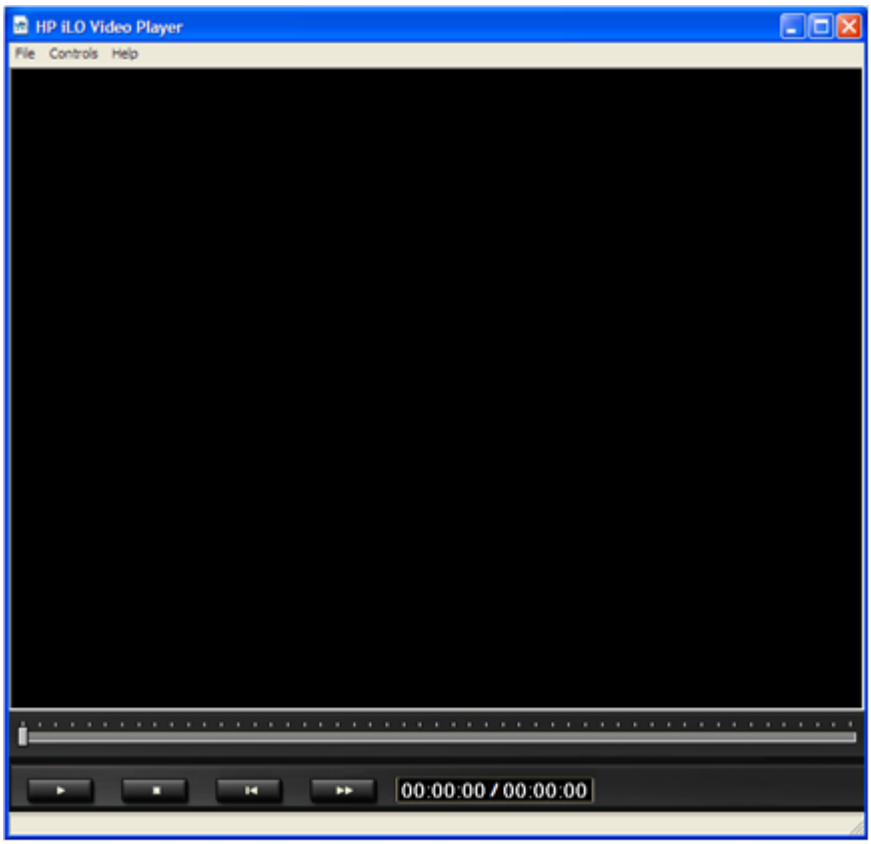
Using HP iLO Video Player

HP iLO Video Player enables you to playback iLO 2 console capture files without installing iLO 2 on your local system. iLO Video Player is designed as a typical media player with similar controls. You can run iLO Video Player as a standalone application on either a server or client. Typically, the application is located on the client. iLO 2 capture files are created using iLO 2 Console Capture feature, see "Using Console Capture" (page 90).

To use iLO Video Player, you must have a Microsoft Windows 2000, Windows XP, or Windows Vista operating systems, and Internet Explorer (version 7 or later) installed on your system.

iLO Video Player user interface

When you launch HP iLO Video Player, the user interface appears and serves as the control point for all playback functions.



iLO Video Player menu options:

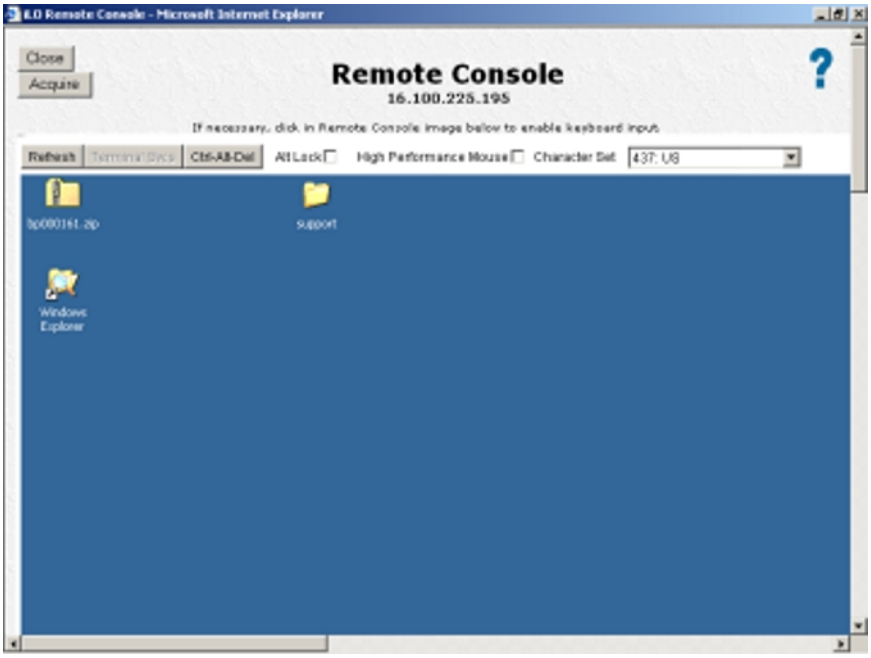
- File
  - Open – Opens a video capture file.
  - Exit – Closes the iLO Video Player.
- Controls
  - Play – Plays or restart the current video capture file.
  - Stop – Stop playback of the current video capture file.
  - Skip to Start – Restarts playback of the current video capture file.
  - Change Speed – Changes playback speed of the current iLO video capture file.
- Help
  - Help Topics – Opens the iLO Video Player help file.
  - About – Opens the iLO Video Player About page.

iLO Video Player controls

Control	Name	Function
	Play/Pause	Starts playback if the currently selected file is not playing or is paused. If playback is in progress, it pauses the file. If no file is selected, the button is disabled.
	Stop	Stops playback. If no file is selected, the button is disabled.
	Skip to Start	Restarts playback from the beginning of the file. If no file is selected, the button is disabled.
	Seek	Moves the playback video forward or backward. If no file is selected, the button is disabled.
	Change Speed	Changes the playback speed of the currently selected file. The available playback speeds are 1x, 2x, 4x, 8x, and 16x. The speeds are cycled through with successive presses in the following order: 2x, 4x, 8x, 16x, and 1x. If no file is selected, the button is disabled.
	File Position	Displays the time parameters of the currently selected file and appears as in a `HH:MM:SS` format. • The left time on the left indicates the current playback position of the file. • The time on the right indicates the total playback time of the file.

Acquiring the Remote Console

When the Remote Console Acquire setting on the Remote Console Settings screen is enabled, the Remote Console page displays the Acquire button. If you have opened the Remote Console page and are notified that another user is currently using Remote Console, clicking the Acquire button ends the other user's Remote Console session and starts a Remote Console session in your current window.



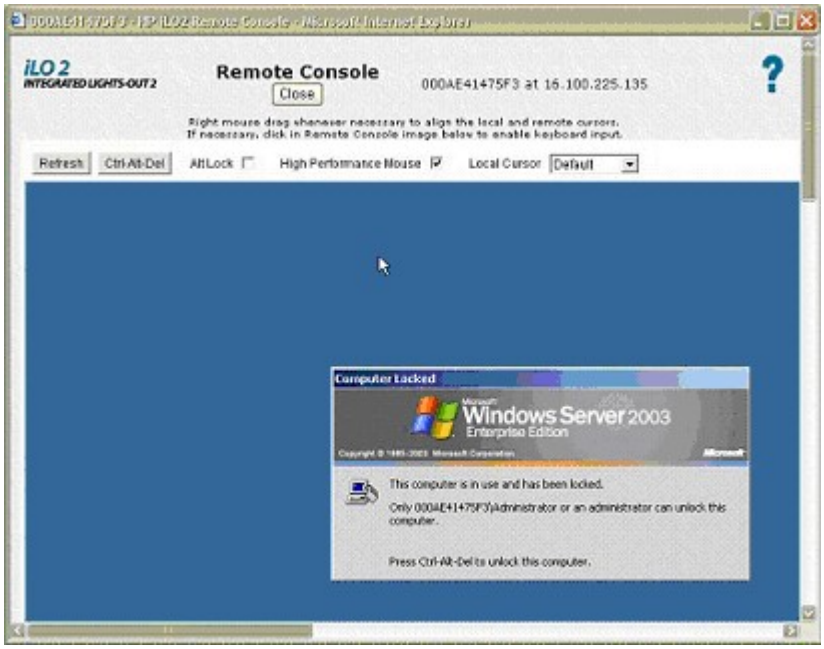
When you click **Acquire**, you are prompted to verify that you want to interrupt the other user's Remote Console session. The other user receives a notification that another user has acquired the Remote Console session after losing the connection. No prior warning is given. After you confirm you want to proceed with the acquire operation, you are notified by an alert window that the operation could take 30 seconds or longer to complete. The **Acquire** button becomes disabled after it is clicked and the acquire operation is started. On browsers that support it, the button changes to light gray to indicate it is disabled. Other browsers might not visibly indicate that the button is disabled.

Only one acquire command is allowed every five minutes for all users. If another user has recently acquired the Remote Console, clicking the **Acquire** button can result in a page informing you that the five-minute acquire-disabled period is in effect. Close the window and re-launch Remote Console again. The **Acquire** button is disabled in the new page until the acquire-disabled period expires. When the **Acquire** button is enabled (this operation happens automatically, and you do not have to refresh the page), you can attempt to acquire the Remote Console session again. On browsers that support it, the button appears light gray to indicate it is disabled during this five-minute time period. On other browsers, there may be no visible indication that the button is disabled. Therefore you do not receive a visual indication when the timeout period expires.

Only one acquire attempt can be made per Remote Console session window. If you have successfully acquired the Remote Console, and someone subsequently acquires it from you, you must open a new Remote Console window to attempt to acquire the Remote Console session again.

Remote Console

Remote Console is a Java applet that renders the remote console with broad browser compatibility including Windows and Linux browsers. Supported browsers are listed in "Supported browsers and client operating systems" (page 15). Remote Console is a licensed feature available with the purchase of optional licenses. For more information, see "Licensing" (page 26).



Remote Console uses dual cursors to help you distinguish between the local and remote mouse pointers. The client computer's mouse cursor appears in the Remote Console as a crosshair symbol. For best performance, be sure to configure the host operating system display as described in "Recommended client settings" (page 94)and "Recommended server settings" (page 95).

To synchronize the remote and local cursors if they drift apart, do one following:

- Right-click, drag, and move the local crosshair cursor to align with the mouse cursor of the remote server.
- Press and hold the right **Ctrl** key, and move the local crosshair cursor to align with the mouse cursor of the remote server.

The local cursor takes the shape of the remote cursor. The cursor appears as a single cursor if the local cursor and the remote cursor are perfectly aligned and the hardware acceleration is set to Full on the managed server.

Remote Console features and controls

The Remote Console applet contains buttons that provide iLO 2 with enhanced features and control. These options are:

- Refresh causes iLO 2 to refresh the screen.
- Terminal Svcs launches the Microsoft Terminal Services client installed on the system. This button is deactivated if Terminal Services is disabled or is not installed on the server.
- Ctrl-Alt-Del enters the key sequence Ctrl+Alt+Del in the Remote Console.
- Alt Lock, when selected, sends any key pressed to the server as if you pressed the Alt key and another key simultaneously.
- Character Set changes the default character set used by the Remote Console. Modifying the Remote Console character set ensures the correct display of characters.
- Close ends the Remote Console session and closes the Remote Console window.

Recommended client settings

Ideally, the remote server operating system display resolution must 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.

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 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`.

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.

Text-based remote console overview

iLO and its predecessors support a true text-based remote console. Video information is obtained from the server and the contents of the video memory are sent to the management processor, compressed, encrypted, and forwarded to the management client application. iLO uses a screen-frame buffer, which detects changes in text information, encrypts the changes, and sends the characters (including screen positioning information) to text-based client applications. This method provides compatibility with standard text-based clients, good performance, and simplicity. However, you cannot display non-ASCII or graphical information, and screen positioning information (displayed characters) might be sent out of order.

The Remote Console uses Virtual KVM and does not provide a true text-based console. iLO 2 uses the video adapter DVO port to access video memory directly. This method significantly increases iLO 2 performance. However, the digital video stream does not contain useful text data. Data obtained from the DVO port represents graphical data (non-character-based), and is not comprehensible ASCII or text data. This video data cannot be rendered by a text-based client application such as Telnet or SSH.

Text-based console during POST

The standard iLO 2 text-based remote console remains available on iLO 2 until the operating system POST is complete. iLO 2 standard firmware continues to use the virtualized serial-port functionality of the management processor. On the iLO 2 firmware, the virtual serial port was renamed Remote Serial Console. iLO 2 uses the Remote Serial Console to access a pre-operating system, text-based

remote console. The iLO 2 Remote Serial Console applet appears as a text-based console, but the information is rendered using graphical video data. iLO 2 displays this information through the remote console applet while in the server pre-operating system state, enabling a non-licensed iLO 2 to observe and interact with the server during POST activities.

For an iLO 2 blade (and an iLO blade running Linux in a graphical format), enter `getty()` on the server's serial port, and then use iLO 2 Remote Serial Console or iLO Virtual Serial Port (CLP command `start /system1/oemhp_vsp1`) to view a login session to the Linux operating system through the serial port.

A non-licensed iLO 2 cannot use Remote Console access after the server completes POST and begins to load the operating system. To use Remote Console and iLO Text Console after POST, you must have an iLO 2 Advanced or iLO 2 Advanced for BladeSystem.

Text-based console after POST

The iLO 2 Text Console after POST feature is a text-based console accessible from Telnet or SSH after POST. When using SSH, the data stream, including authentication credentials, is protected by the encryption method supported by the SSH client and iLO 2. HP recommends using SSH to connect to the iLO 2 Text Console.

iLO 2 also supports using Telnet to connect to the iLO 2 Text Console. However, the data stream is not encrypted when using a normal Telnet connection. As part of the default security policy, using Telnet is disabled. You must enable Telnet to allow access to the CLI, and iLO 2 Text Console.

For more information about the security of the communication methods used by iLO 2, see the *Integrated Lights-Out security technology brief* on the HP website at http://h20000.www2.hp.com/bc/docs/support/SupportManual/c00212796/c00212796.pdf.

The presentation of colors, characters, and screen control depends upon the client you are using and can be any standard Telnet (if enabled) or SSH client compatible with iLO 2. The iLO 2 Text Console is enabled by default on iLO 2 firmware version 1.50 and later. Features and support include:

- Displaying text mode screens that are 80 x 25 (standard color configurations) when the system is on including:
  - System boot process (POST)
  - Standard Option ROMS
  - Text boot-loaders (LILO or GRUB)
  - Linux operating system in VGA 80x25 mode
  - DOS
  - Other text-based operating systems

  Text mode screen support does not include graphics, other VGA text resolutions (132 x 48, 80 x 48), or other text resolutions implemented through a driver (implemented graphically).
- Remote Console hot keys
- International language keyboards (if the server and client system are configured similarly)
- Line-drawing characters when correct font and code-page are selected in the client application

To use the iLO 2 Text Console feature successfully, you must update the HOST ROM. iLO 2 supports iLO 2 Text Console on the following HP ProLiant servers:

- ML350 G5
- ML370 G5
- DL360 G5
- DL380 G5
- DL580 G5
- SE316 M1
- SE326 M1
- DL320 G6
- ML330 G6
- ML/DL 370 G6
- DL785 G6
- ML350 G6
- DL380 G6
- DL360 G6
- BL2x220c G6
- BL460c G1
- BL480c G1
- BL680c G5
- BL685c G6
- BL280c G6
- BL460c G6

Using the iLO 2 Text Console

To start an iLO 2 Text Console session:

1. Start an SSH or Telnet session.

   Be sure the terminal application character encoding is set to Western (ISO-8859-1).
2. Log in to iLO 2.
3. At the prompt, enter `Textcons`.

   A message indicating that the iLO 2 Text Console software is initiating appears.

To exit a iLO 2 Text Console and return to the CLI session, press the **ESC (** keys simultaneously.

Customizing iLO 2 Text Console

When starting iLO 2 Text Console, use the `Textcons` command options and arguments to customize the operation of the display. In general, you do not need to change these options.

- Controlling rate of sampling

  You can use the `Textcons speed` option to indicate in milliseconds the between sampling periods. A sampling period is where the iLO 2 firmware examines screen changes and updates the iLO 2 Text Console. Adjusting the speed can alleviate unnecessary traffic on long or slow network links, reduce the bandwidth used, and reduce iLO 2 CPU time consumed. Reasonable values are between 1 and 5000 (1ms to 5 seconds). For example:

  ```
  Textcons speed 500
  ```

- Controlling smoothing

  iLO 2 attempts to only transmits data when it changes and becomes stable on the screen. If a line of the text screen is constantly changing faster than iLO 2 can sample the change, the line is not be transmitted until it becomes stable. For example, during an `ls -R` of a large file-system, the physical monitor displays text more rapidly than it can be interpreted. The same is true for a iLO 2 Text Console session. In this case, the data appears rapidly, and is essentially indecipherable. In this case however, the data is transmitted by iLO 2 across the network and consuming bandwidth. The default behavior is smoothing (delay 0) which only transmits data when the changes become stable on the screen. You can control or disable smoothing feature using the delay option. For example:

  ```
  Textcons speed 500 delay 10
  ```

- Controlling international keyboard support

  When using iLO 2 Text Console, iLO 2 can emulate character mapping between the client, Telnet, and the server. The default mapping is the USB 101-keyboard translation (or no translation).

To control the translation, use the `xlt` option with the appropriate reference number. For example to set iLO 2 Text Console to a sampling rate of 50 ms using the translation of a British keyboard, enter:

```
Textcons speed 50 xlt 41
```

To translate to another language, use one of the following:

Keyboard	Reference number
United States	0
British	1
Belgian	2
Danish	3
Finnish	4
French	5
French Canadian	6
German	7
Italian	8
Latin American	9
Norwegian	10
Portuguese	11
Spanish	12
Swedish	13
Swiss - French	14
Swiss - German	16

- Configuring Remote Console hot keys

  To use special key sequences that you cannot duplicate in the remote console client, the Remote Console hot keys configured for Remote Console operate in iLO 2 Text Console. For more information, see "Remote console hot keys" (page 83).

- Configuring character mapping

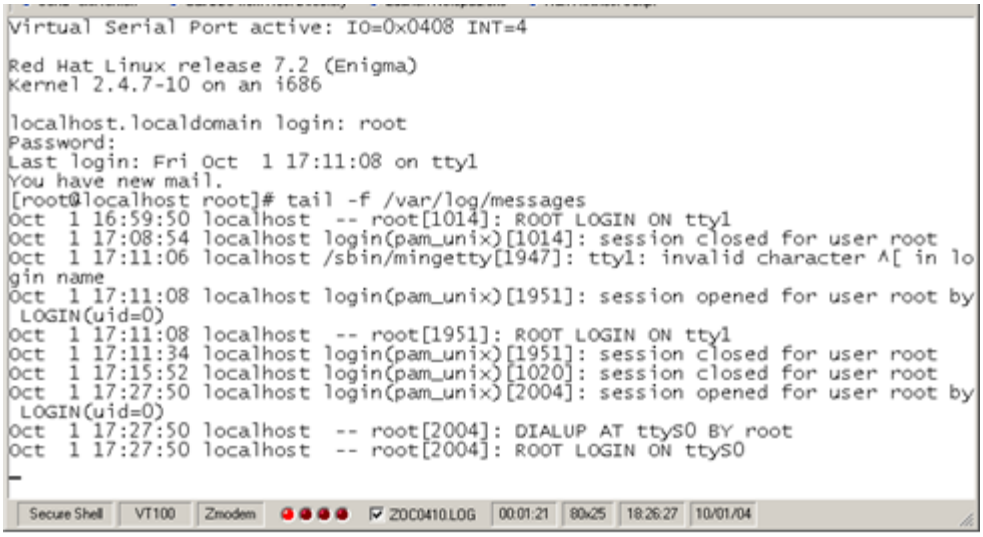
  In general, under the ASCII character set, CONTROL (ASCII characters than 32) are not printable and cannot be displayed. These characters can be used to represent items such as arrows, stars, or circles. Some of these characters are mapped to equivalent ASCII representations. The following are supported equivalents:

Character value	Description	Mapped equivalent
0x07	Small dot	*
0x0F	Sun	*
0x10	Right pointer	>
0x11	Left pointer	<
0x18	Up arrow	^
0x19	Down arrow	v
0x1A	Left arrow	>

Character value	Description	Mapped equivalent
0x1B	Right arrow	>
0x1E	Up pointer	^
0x1F	Down pointer	v
0xFF	Shaded block	blank space

Using a Linux session

You can run an iLO 2 virtual serial port on a Linux system, if the system is configured to present a terminal session on the serial port. This feature enables you to use a remote logging service. You can remotely log on to the serial port and redirect output to a log file. Any system messages directed to the serial port are logged remotely.



Some Linux text modes are actually graphical modes and cannot be displayed using the iLO 2 Text console. For example, SLES terminals are text on graphics mode even though they appear to be text-based it does not display correctly in iLO 2 Text Console. If you attempt to use an unsupported mode, iLO 2 Text Console display a message indicating that the server is using a graphical mode.

Some keyboard character sequences required by Linux in the text mode might not be passed through to iLO 2 Text Console. For example, the alt + tab keyboard combination might be intercepted by the client. To work around these issues, configure a hot key for the keyboard combination. For more information, see "Remote console hot keys" (page 83).

Virtual serial port and remote serial console

The management processor contains serial-port hardware that can replace the physical serial port on the server's motherboard. Using an electronic switch, the iLO 2 firmware disconnects the server's physical serial port and commands its own serial-port hardware to connect. The iLO 2 serial-port hardware establishes a connection between the server and the management processor network. The firmware encapsulates the characters sent by the server to the serial port into network packets and sends the network packets to the remote serial console applet or application (the application can be a Telnet or SSH client). Characters sent by the remote applet or application are encapsulated into network packets and sent to the iLO 2 firmware, which then extracts the characters and feeds them to the server. The iLO 2 remote serial console provides a bi-directional serial communication path between the remote user and the server.

Using the iLO 2 remote serial console, the remote user is able to perform operations such as interacting with the server POST sequence and operating system boot sequence; establishing a login session with the operating system, interacting with the operating system; and executing and interacting with applications on the server operating system. Users of the Microsoft Windows Server 2003 operating system have the ability to execute the EMS subsystem through the remote serial console. EMS is useful for debugging operating system boot and issues at the operating system kernel level.

Remote Serial Console

The Remote Serial Console enables you to access a VT320 serial console from a Java applet-based console connected to the iLO 2 Virtual Serial Port through a browser. Launching the Remote Serial Console enables you to exchange text data with the host. The Remote Serial Console option is compatible with both Windows and Linux host operating systems and requires JVM.

The flow of data is a bi-directional stream sent to the server serial port. Three types of data can appear on a HP ProLiant server serial port:

- Windows EMS console
- Linux user session through serial tty (ttyS0)
- System POST dialog (if BIOS serial console redirection is enabled)

The current configuration appears on the Remote Console Information page when you click the Remote Console tab. You can alter the current settings using the host system RBSU, accessed during a server reset.



Configuring Remote Serial Console

To successfully use the Remote Serial Console, the server software and firmware must be configured correctly. To configure the server POST firmware, the server System RBSU must be invoked to set the serial port parameters. You must configure the RBSU to enable BIOS Serial Console Redirection mode. This mode instructs the server system ROM to send data to, and receive data from, the server serial port. When the iLO 2 firmware enters Remote Serial Console mode, iLO 2 enables a serial port in place of the server serial port, intercepts and retransmits outgoing data to the Remote Serial Console client, receives incoming data (from the Remote Serial Console client), and retransmits it to the system ROM.

After the server completes POST, the server system ROM transfers control to the operating system boot loader. If you are using Linux, you can configure the operating system boot loader to interact with the server serial port instead of the keyboard, mouse, and VGA console. This configuration enables you to view and interact with the operating system boot sequence through the Remote Serial console. For an example of a Linux operating system boot loader, see "Linux configuration example" (page 101).

After the operating system boot loader completes, the operating system continues to load. If you are using a Linux operating system, you can configure the operating system to provide a login session to the system through the serial port, enabling the Remote Serial Console to prompt you for the system user login ID and password. Using this configuration enables you to interact with the operating system as an operating system user or as a system administrator.

Although additional configuration steps are required to use Remote Serial Console (as compared to using the remote console or IRC), the Remote Serial Console allows Telnet or SSH users to interact with the server remotely and without requiring an iLO 2 Advanced license and is the only way a true text-based remote console is presented by iLO 2.

Linux configuration example

The boot loader is the application that loads from the bootable device when the server system ROM finishes POST. For Linux operating systems, the boot loader that is usually used is GRUB. To configure GRUB to use the Remote Serial Console, modify the GRUB configuration file to look like the following (Red Hat Linux 7.2 sample shown):

```
serial -unit=0 -speed=115200
terminal -timeout=10 serial console
default=0
timeout=10
#splashimage=(hd0,2) /grub/splash.zpm.gz
title Red Hat Linux (2.4.18-4smp)
root (hd0,2)
kernel /vmlinuz-2.4.18-4smp ro root=/dev/sda9 console=tty0 console=ttyS0,115200
initrd /initrd-2.4.18-rsmp.img
```

After Linux is fully booted, a login console can be redirected to the serial port. The `/dev/ttyS0` and `/dev/ttyS1` devices, if configured, enable you to obtain serial `tty` sessions through the Remote Serial Console. To begin a shell session on a configured serial port, add the following line to the `/etc/inittab` file to start the login process automatically during system boot (this example invokes the login console on `/dev/ttyS0`):

```
Sx:2345:respawn:/sbin/agetty 115200 ttyS0 vt100
```

For more information about configuring Linux for use with the Remote Serial Console, see the technical publication *Integrated Lights-Out Virtual Serial Port configuration and operation HOWTO* on the HP website at http://www.hp.com/servers/lights-out.

Virtual Serial Port enhancements

iLO 2 firmware 1.35 implements a dynamic flag that instantly informs the server system ROM of an iLO 2 Remote Serial Console connection. After the system ROM POST code recognizes the Remote Serial Console connection, the system begins redirecting the console input and output to the server serial port and the Remote Serial Console. You can establish a Remote Serial Console session at any time before or during the system POST sequence, and you can view and modify the POST. After disconnecting the Remote Serial Console session, the iLO 2 firmware resets the dynamic flag to inform the server system ROM that the session is no longer active. Then, the server system ROM cancels the redirection to the server serial port.

The system ROM RBSU setup must be configured to use iLO 2 Virtual Serial Port for this enhancement to be operational. For more information, see "Configuring Remote Serial Console" (page 100).

Windows EMS Console

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

iLO 2, however, enables you to use EMS over the network through a Web browser. Microsoft EMS enables you to display running processes, change the priority of processes, and halt processes. The EMS console and the iLO 2 Remote Console can be used at the same time.

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 iLO 2 system automatically detects whether the EMS port is enabled or disabled, and the selection of the COM port.

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

For more information on using the EMS features, see the Windows Server 2003 documentation.

Virtual serial port raw mode

You can use the virtual serial port capability of iLO 2 to connect a Windows Kernel Debugger from a remote client using `WiLODbg.exe`. `WiLODbg.exe` bypasses the decoding of bytes by the iLO 2 firmware. After bypassing the decoding of bytes, the virtual serial port is in RAW mode (unprocessed) and sent directly to the serial port.

The `WiLODbg.exe` utility is executed on a client system with the Microsoft application WinDBG.exe or KD.exe installed. When you execute `WiLODbg.exe`, it establishes a virtual serial port connection to iLO 2 and enables RAW mode. `WiLODbg.exe` also automatically launches `WinDBG.exe` with the appropriate switches necessary for `WinDBG.exe` to connect to the remote iLO 2 device.

To configure the server, you must configure the System RBSU:

1. To enable a virtual serial port, assign Virtual Serial Port a COM port from the System Options menu.
2. Set BIOS Serial Console Port and EMS Console to **Disable,** or set it to the same port as an embedded serial port.
3. Set the Microsoft Windows debug port to the same port as the virtual serial port. You can use the `bootcfg` command or modify the `boot.ini` file.

   Example using the `bootcfg` command:

   At the command prompt on a Windows server, issue the following command:

   ```
   Bootcfg /debug on /port com2 /baud 115200 /id 1
   ```

   Example of a modified boot.ini file:

   ```
   [boot loader]
   timeout=5
   default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
   [operating systems]
   multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows
   Debug (com2)" /fastdetect /debug /debugport=com2 /baudrate=115200
   ```

   If the server is configured to boot into debug mode, and a normal virtual serial port connection is established while the server is booting, several bytes of debug data are sent to the virtual serial port client. To avoid this, do not boot the server into debug mode while a normal virtual serial port connection is in use.

Serial Port Configuration displays server configuration information, available serial ports, and virtual serial port status. Status appears as:

- Available – The virtual serial port is not in use
- In use – Normal mode when the virtual serial port is connected normally
- In use – Raw mode when the WiLODbg.exe utility is used to connect

When the virtual serial port is in use, the Disconnect button is enabled and can be used to terminate any type of virtual serial port connection. Using the Disconnect features to terminate a virtual serial port connection that was established using SSH completely disconnects the SSH connection and does not return to the </>hpiLO-> prompt. A similar disconnect occurs if the virtual serial port connection is established using Telnet. If a remote serial connection applet is used to make the connection from a browser, the applet is disconnected. The applet window must be closed and reopened to reestablish the remote serial connection.

Using a remote Windows Kernel Debugger

To start a Windows Kernel Debugger, you must launch the WiLODbg.exe utility on a client system that has Microsoft WinDBG.exe or KD.exe installed, and then reboot the remote server into debug mode to attach the debugger. WiLODbg automatically launches WinDBG.exe or KD.exe. For example:

```
WiLODbg <IP Address>[ -c CommandLine][ -e][ -k][ -p Password][ -s SocketNumber]
[ -t][ -u Username]
If a parameter has whitespace in it, enclose it in quotes.
```

Required Parameters:

`IP Address = <String>` is the IP Address in dot format or full UNC name. `<String>` is a series of characters. Required parameters must occur in the order shown in the example.

Optional Parameters:

- `-c CommandLine = <String>` Provides additional command line parameters to the selected debugger. If there are embedded spaces or dashes (-) enclose them in quotation marks. <String> = A series of characters.
- `-e = <Boolean>` Turns on encryption for the communications link. Encryption only works with the Telnet option in this version. Default is disabled.
- `-k = <Boolean>` Use KD instead of WinDbg. Default is to use WinDbg.
- `-p Password = <String>` Sets the Password to use for iLO 2 login. If not provided, password is requested. `<String>` Is a series of characters.
- `-s SocketNumber = <Integer>` Sets the socket number for connection to iLO 2. SocketNumber must match the Raw Serial Data Port setting on the iLO 2 you are connecting to. Socket 3002 is the default. `<Integer> = [sign]digits.`
- `-t = <Boolean>` Uses a Telnet connection indirectly through this utility from the debugger. Socket connection to socket 3002 is the default setting.
- `-u Username = <String>` Sets the Username for iLO 2 login. If not provided username is requested. <String> is a series of characters. Options can occur in any order.

Example command lines:

- To connect to iLO 2 at 16.100.226.57, validate the user with the user name of `admin` with the password `mypass`, and start `WinDBG.exe` with the additional command line:

  ```
  wilodbg 16.100.226.57 -c "-b" -u admin -p mypass
  ```

This example starts `WinDBG.exe` with an additional command line of `-b` and uses a direct socket connection from `WinDBG.exe` to iLO 2 on port 3002.

- To connect to iLO 2 at `16.100.226.57` and validate the iLO 2 user with the username of **`admin`** and password **`mypass`**, and start `kd` with an additional command line for `kd` of **`-b`**:

  ```
  wilodbg 16.100.226.57 -k -c "-b" -u admin -p mypass -s 7734
  ```

  This example starts `kd` with an additional command line for `kd` of `-b`, and uses a direct socket connection from `kd` to iLO 2 on port 7734. To use this example, you must configure iLO 2 to use port 7734.

- To connect to iLO 2 at 16.100.226.57 and request a user name and password:

  ```
  wilodbg 16.100.226.57 -c "-b" -t -e
  ```

  This example starts `WinDBG.exe` with an additional command line of `-b` and uses an encrypted Telnet connection from `WiLODbg` to iLO 2 and passes `WinDBG.exe` data through the utility to the Telnet encrypted connection.

Virtual media

Virtual Media is a licensed feature, if Virtual Media is not licensed, the message `iLO 2 feature not licensed` appears. For more information, see "Licensing" (page 26). The ability to use iLO 2 Virtual Media is granted or restricted through iLO 2 user privileges. You must have the Virtual Media privilege to select a virtual media device and connect it to the host server.

The iLO 2 Virtual Media option provides you with a Virtual Floppy disk drive and CD/DVD-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. iLO 2 Virtual media devices connect to the host server using USB technology. USB enables new capabilities for the iLO 2 Virtual Media devices when connected to USB-supported operating systems. Different operating systems provide various 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/DVD-ROM capability is enabled, the CD/DVD-ROM drive cannot be accessed from the client operating system.

△ **CAUTION:** To prevent file and data corruption, do not access the local media when using local media as virtual media.

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

To access iLO 2 Virtual Media devices using the browser-based interface, click **Virtual Media>Virtual Media Applet**. An applet loads in support of the Virtual Floppy or Virtual CD/DVD-ROM device.

You can also access virtual media through the Integrated Remote Console. The Integrated Remote Console enables you to access the system KVM and control Virtual Power and Virtual Media from a single console under Microsoft Internet Explorer. For more information on accessing Virtual Power and Virtual Media using the Integrated Remote Console, see "Integrated Remote Console option" (page 85).

Using iLO 2 Virtual Media devices

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 iLO 2 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/DVD-ROM device.

Virtual Media and Windows 7

By default, Windows 7 powers off the ILO virtual hub when no virtual media devices are enabled or connected during boot. To prevent this issue, manually override the power management feature in the Windows 7 through the Control Panel so the virtual hub does not power down.

1. Open **Device Manager**.
2. Click **View**.
3. From the menu, select **Devices by connection**.
4. To display the USB devices including the Generic USB Hub, select and expand **Standard Universal PCI to USB Host Controller**. The Generic USB Hub option is the ILO 2 virtual USB hub controller.
5. Right-click **Generic USB Hub** and select **Properties**.
6. Select the **Power Management** tab.
7. Clear the **Allow the computer to turn off this device to save power** check box.

iLO 2 Virtual Floppy/USBKey

The iLO 2 Virtual Floppy disk is available at server boot time for all operating systems. Booting from the iLO 2 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.

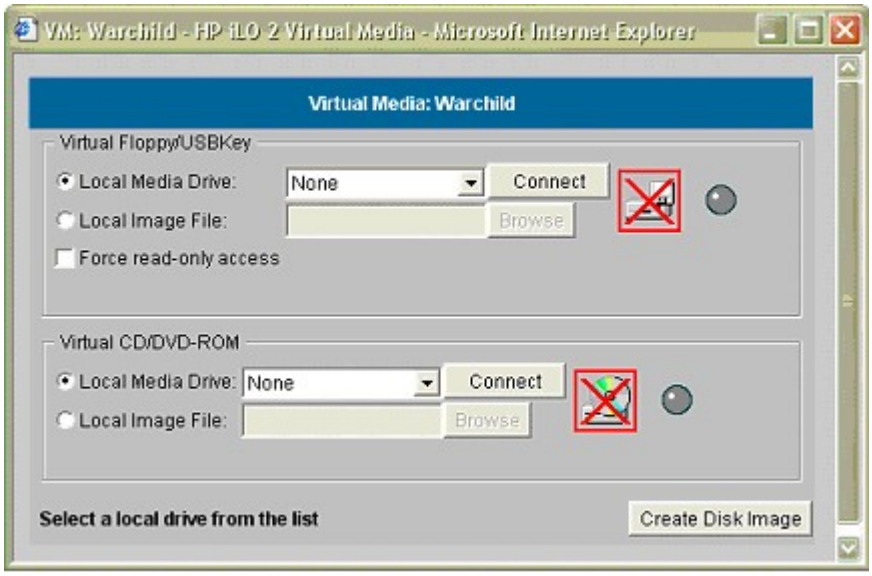
If the host server operating system supports USB mass storage devices or secure digital devices, then the iLO 2 Virtual Floppy/USBKey is also available after the host server operating system loads. You can use the iLO 2 Virtual Floppy/USBKey when the host server operating system is running to upgrade 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 issue with the NIC driver.

The Virtual Floppy/USBKey device can be the physical floppy, USB key, or secure digital drive on which you are running the web browser, or an image file stored on your local hard drive or network drive. For maximum performance, HP recommends using the 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 or USB key drive in your client PC:

1. From the Virtual Floppy/USBKey section, select **Local Media Drive**.
2. From the menu, select the drive letter of the desired local floppy or USB key drive on your client PC. 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. From the Virtual Floppy/USBKey section of the Virtual Media applet, select **Local Image File** .
2. To locate the image file using the Choose Disk Image File dialog box, enter the path or file name of the image in the text-box, or click **Browse**. 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 will change state to reflect the current status of the Virtual Floppy, USB key drive, or secure digital device. When connected, the devices are available to the host server until you close the Virtual Media applet. When you are finished, 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.

The iLO 2 Virtual Floppy/USBKey is available to the host server at run time if the operating system on the host server supports USB floppy or key drives. For information on which operating systems support USB mass storage at the time of the publication of this manual, see "Operating system USB support" (page 107).

To your operating system, iLO 2 Virtual Floppy/USBKey appears just like any other drive. When using iLO 2 for the first time, the host operating system might prompt you to complete a New Hardware Found wizard.

When you are finished using iLO 2 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/USB Key operating systems notes

- MS-DOS

  During boot and MS-DOS sessions, the Virtual Floppy device appears as a standard BIOS floppy drive. This device appears as drive A. If a physically attached floppy drive exists, is

obscured and unavailable during this time. You cannot use a physical local floppy drive and the Virtual Floppy simultaneously.

- Windows Server 2008 or later and Windows Server 2003

  Virtual Floppy and USB key drives appear 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 as a driver diskette, disable the integrated diskette drive in the host RBSU which forces the Virtual Floppy to appear as drive A.

  To use Virtual USBKey during a Windows installation as a driver diskette, change the boot order of the USB key drive in the system RBSU. HP recommends placing the USB key drive first in the boot order.

- Windows Vista

  Virtual media does not work correctly on Windows Vista using Internet Explorer 7 with Protected Mode enabled. If you attempt to use virtual media with Protected Mode enabled, various error messages appear, including `could not open cdrom (the parameter is incorrect.` To use virtual media, click **Tools/Internet Options/Security,** clear **Enable Protected Mode,** then click **Apply**. After disabling Protected Mode, you must close all open browser instances and restart the browser.

- NetWare 6.5

  NetWare 6.5 supports the use of USB diskette and key drives. For step-by-step instructions, see "Mounting USB Virtual Floppy/USBKey in NetWare 6.5" (page 107).

- Red Hat and SUSE Linux

  Linux supports the use of USB diskette and key drives. For step-by-step instructions, see "Mounting USB Virtual Media/USBKey in Linux" (page 108).

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 Server 2008, Windows 2003, Red Hat Enterprise Linux 3, Red Hat Enterprise Linux 4, Red Hat Enterprise Linux 5, SUSE SLES 9, and SUSE SLES 10 support USB devices. Other operating systems can 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: Red Hat Enterprise Linux 3 does not allow you to provide a driver diskette using virtual media.

Mounting USB Virtual Floppy/USBKey in NetWare 6.5

1. Access iLO 2 through a browser.
2. Select **Virtual Media** in the Virtual Devices tab.
3. Insert the media into the local floppy drive, select a diskette drive, and click **Connect**. Alternatively, select a diskette image to be used and click **Connect.**

In NetWare 6.5, use the `lfvmount` command on the server console to assign the device a drive letter.

The NetWare 6.5 operating system will pick the first available drive letter for the Virtual Floppy drive. The `volumes` command can now be used by the server console to show the mount status of this new drive.

When the drive letter shows as mounted, the drive will now be accessible through the server GUI as well as the system console.

When the Virtual Floppy Drive is mounted, if the media is changed in the local floppy drive, you must reissue the `lfvmount` command on the server console to see the new media in the NetWare 6.5 operating system.

Mounting USB Virtual Media/USBKey in Linux

1. Access iLO 2 through a browser.
2. Select **Virtual Media** in the Virtual Devices tab.
3. Select a diskette drive or diskette image.
   a. For a floppy drive or image, select a Local Media Drive or Local Image File and click **Connect**.
   b. For a USB key drive or image, select a Local Image File and click **Connect**.

      For a physical USB key drive, enter `/dev/sda` in the Local Image File text box.
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 drive.
   - To mount the diskette drive, use the following command:

     ```
     mount /dev/sda /mnt/floppy -t vfat
     ```
   - To mount the USB key drive, use the following command:

     ```
     mount /dev/sda1 /mnt/keydrive
     ```

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

The floppy and key drive 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
```

To enable the various mtools commands to access the Virtual USBKey device, modify the existing /etc/mtools.conf file and add the following line:

```
drive v: file="/dev/sda1" exclusive
```

To list the Virtual USBKey device partition table to find the desired partition, use the following command:

```
fdisk -l /dev/sda
```

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
```

Changing diskettes

When using the iLO 2 Virtual Floppy or USB key drive, and the physical diskette drive on the client machine is a USB diskette drive, disk change operations will not be recognized. For example, in this configuration, if a directory listing is obtained from a floppy diskette and the diskette is changed, a subsequent directory listing will show the listing for the first diskette. If disk changes are necessary when using iLO 2 Virtual Floppy/USBKey, be sure the client machine contains a non-USB diskette drive.

iLO 2 Virtual CD/DVD-ROM

The iLO 2 Virtual CD/DVD-ROM is available at server boot time for operating systems specified in "Operating system USB support" (page 107). Booting from the iLO 2 Virtual CD/DVD-ROM enables you to deploy an operating system from network drives and perform disaster recovery of failed operating systems, among other tasks.

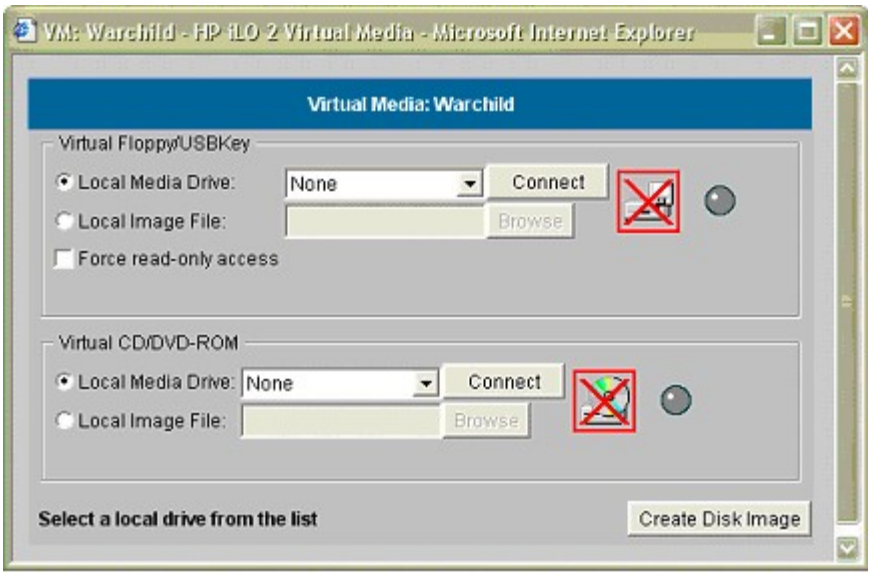
If the host server operating system supports USB mass storage devices, then the iLO 2 Virtual CD/DVD-ROM is also available after the host server operating system loads. You can use the iLO 2 Virtual CD/DVD-ROM when the host server operating system is running to upgrade device drivers, install software, and perform other tasks. Having the Virtual CD/DVD-ROM available when the server is running can be especially useful if you must diagnose and repair an issue with the NIC driver.

The Virtual CD/DVD-ROM can be the physical CD/DVD-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/DVD-ROM drive in your client PC:

1. Select **Local Media Drive** within the Virtual CD/DVD-ROM section.
2. Select the drive letter of the desired physical CD/DVD-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/DVD-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 will change state to reflect the current status of the Virtual CD/DVD-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/DVD-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.

The iLO 2 Virtual Media CD/DVD-ROM is available to the host server at run time if the operating system on the host server supports USB floppy drives. For more information, see "Operating system USB support" (page 107).

The iLO 2 Virtual Media CD/DVD-ROM appears to your operating system just like any other CD/DVD-ROM. When using iLO 2 for the first time, the host operating system might prompt you to complete a New Hardware Found wizard.

When you are finished using iLO 2 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/DVD-ROM operating system notes

- MS-DOS

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

- Windows Server 2008 and Windows Server 2003

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

- Linux

  - Red Hat Linux

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

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

    ```
    mount /mnt/cdrom1
    ```

  - SLES 9

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

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

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

  For step-by-step instructions, see "Mounting USB Virtual Media CD/DVD-ROM in Linux" (page 110).

Mounting USB Virtual Media CD/DVD-ROM in Linux

1. Access iLO 2 through a browser.
2. Select **Virtual Media** in the Virtual Devices tab.

3. Select the CD/DVD-ROM to be used and click **Connect**.
4. Mount the drive using the following command:

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

   For SLES 9:

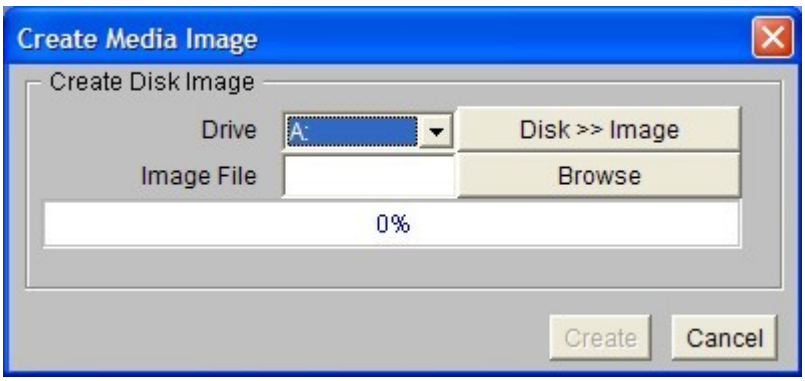
   ```
   mount /dev/scd0 /media/cdrom1
   ```

Creating iLO 2 disk image files

The iLO 2 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 iLO 2 virtual media is faster when image files are used. The utility to create iLO 2 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 is 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.

Virtual folder

The iLO 2 Virtual Folder emulates a USB device, dynamically creating a media image of a selected folder or directory. After creating a virtual image of a folder or directory, the server connects to the created image as a USB storage device, enabling you to browse to the server and transfer the files from the iLO 2 generated image to any location on the server.

The Virtual Folder feature is only available within the IRC. The virtual folder is non-bootable, read-only, and the mounted folder is static. Changes to the client file are not replicated in the mounted folder.

Virtual Folder is a licensed feature available with the purchase of iLO 2 Advanced or iLO 2 Select. The virtual folder feature enables you to access, browse, and transfer files from a client to a managed server. The virtual folder feature supports the ability to mount and dismount a directory

on a local or networked directory that is accessible through the client, mounted and dismounted as a Virtual Media device.

Virtual folder operating system notes

- MS-DOS

  During boot and MS-DOS sessions, the Virtual Folder device appears as a standard BIOS floppy drive. This device appears as drive A. If a physically attached floppy drive exists, it is obscured and unavailable during this time. You cannot use a physical local floppy drive and the Virtual Folder simultaneously.

- Windows

  Virtual Folder appears automatically after Microsoft Windows recognizes the mounting of the virtual USB device. You can use the folder as you would a locally attached device. Virtual Folder is non-bootable. Attempting to boot from the folder might prevent the server from booting.

- NetWare 6.5

  NetWare 6.5 supports the use of Virtual Folder as USB diskette and key drive. For step-by-step instructions, see "Mounting USB Virtual Floppy/USBKey in NetWare 6.5" (page 107).

- Red Hat and SLES Linux

  Linux supports the use of Virtual Folder. Virtual Folder uses a FAT 16 file system format. For more information, see "Mounting USB Virtual Media/USBKey in Linux" (page 108).

Power management

iLO 2 Power Management enables you to view and control the power state of the server, monitor power usage, monitor the processor, and modify power settings. The Power Management page has four menu options: Server Power, Power Meter, Processor States, and Settings. When you select **Power Management**, the Server Power Controls page appears. The Server Power Controls page has two sections: Virtual Power Button and Power Configuration Settings.



The Virtual Power Button section displays the current power state of the server as well as remote server power control options. The displayed power state is the state of the server power when the page is first opened. The server can be On, Off, or Reset. Use the browser refresh feature to keep the status of the power indicator current.

To change the current server power state using the Virtual Power Button options, you must have the Virtual Power and Reset privilege. Some of the power control options do not gracefully shut

down the operating system. An operating system shutdown must be initiated using the Remote Console before using the Virtual Power Button options. The following options are available:

- Momentary Press button provides behavior identical to pressing the physical power button.
- Press and Hold is identical to pressing the physical power button for five seconds and then releasing it. This option provides the ACPI-compatible functionality that is implemented by some operating systems. These operating systems behave differently depending upon a short press or long press. The behavior of this option might circumvent any graceful shutdown features of the operating system.
- Cold Boot of the system immediately removes power from the system. The system will restart after approximately six seconds. This option is not available when the server is powered down. This option circumvents graceful operating system shutdown features.
- Reset System initiates a system reset. This option is not available when the server is powered down. The behavior of this option might circumvent any graceful shutdown features of the operating system.

The Power Configuration Settings section enables you control how the remote server powers up when power is applied. The following options are available:

- Automatically Power On Server enables iLO 2 to turn on a server when power is applied, such as when the server is plugged in, or when a UPS is activated after a power outage. You must have Virtual Power and Reset privilege to alter this setting.

  If power is unexpectedly lost while the server is powering up, the server always powers back on, even if Automatically Power On Server is set to `No`.

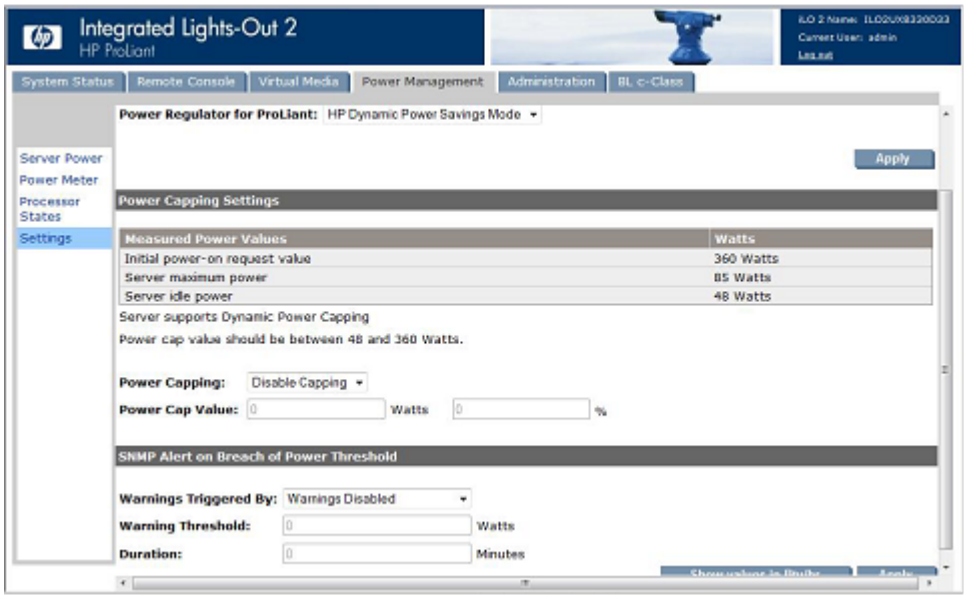
- Power On Delay is used to stagger server power-on in a data center. Blade servers are governed by the rack infrastructure and do not support a power-on delay. Power On Delay does not interfere with the power button.

  The delay occurs before the server is powered-on by iLO 2, including automatic power-on and power restore. Some servers cannot enforce the delay under the power restore case. iLO 2 firmware requires roughly 10 seconds before server power on can take effect. You must have Virtual Power and Reset privilege to alter this setting.

Server power settings

The Power Regulator for ProLiant feature enables iLO 2 to dynamically modify processor frequency and voltage levels based on operating conditions to provide power savings with minimal effect on performance. Processors that support this feature have predefined voltage and frequency states, known as *p-states*. The software can dynamically switch the processor from one p-state to another. P-0 is the highest frequency/voltage combination supported by the processor. Modifying the processor p-state based on CPU utilization enables significant power savings with minimal performance degradation by reducing the voltage and frequency on the processor when the system is idle, and increasing the voltage and frequency on the processor when needed.

The Power Management Settings page enables you to view and control the power regulator mode of the server. You must have the Configure iLO 2 Settings privilege to change this setting.



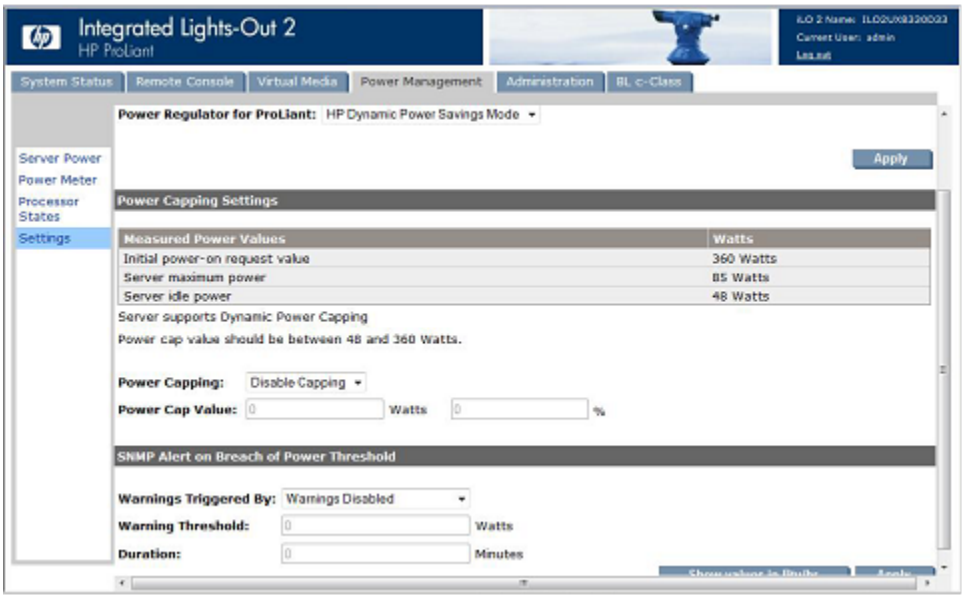
- The Power Regulator for ProLiant section has the following options:
  - Enable HP Dynamic Power Savings Mode sets the processor to dynamically set the power level based on usage.
  - Enable HP Static Low Power Mode sets the processor to minimum power.
  - HP Static High Performance Mode sets the processor to the highest supported processor state and forces it to stay in that state.
  - Enable OS Control Mode sets the processor to maximum power.

  After selecting a Power Regulator for ProLiant option, click **Apply** to save the setting. The server requires a reboot for the change to take effect. These settings cannot be changed while the server is in POST. If the settings do not change after clicking **Apply**, the server might be in the boot process or require rebooting. Exit any RBSU program you are running, allow POST to complete, and then try the operation again.
- The Power Capping Settings section enables you to view measured power values, set a power cap, and disable power capping.

  Measured power values include the server power supply maximum value, the server maximum power, and the server idle power. The power supply maximum power value refers to the maximum amount of power that the server power supply can provide. The server maximum and idle power values are determined by two power tests run by the ROM during POST.

  Power Cap Setting enables you to set a power cap on the server. After a power cap is set, the average power reading of the server over time must be at or below the cap value. You can set the power cap by entering either a watt or Btu/hr value (click **Show values in Btu/hr**) or a percentage. The percentage refers to the difference between the maximum and idle power values. The cap value cannot be set below the server idle power.

  Power Capping Settings are disabled when the server is part of an Enclosure Dynamic Power Cap. These values are set and modified using either Onboard Administrator or Insight Power Manager.



- If the server has the hardware and software to support dynamic power capping, the message `System supports Dynamic Power Capping` appears. Dynamic power capping provides electrical circuit breaker protection.
- If the message `System supports Dynamic Power Capping` does not appear, the server supports normal power capping. Normal power capping does not react fast enough to provide electrical circuit breaker protection.

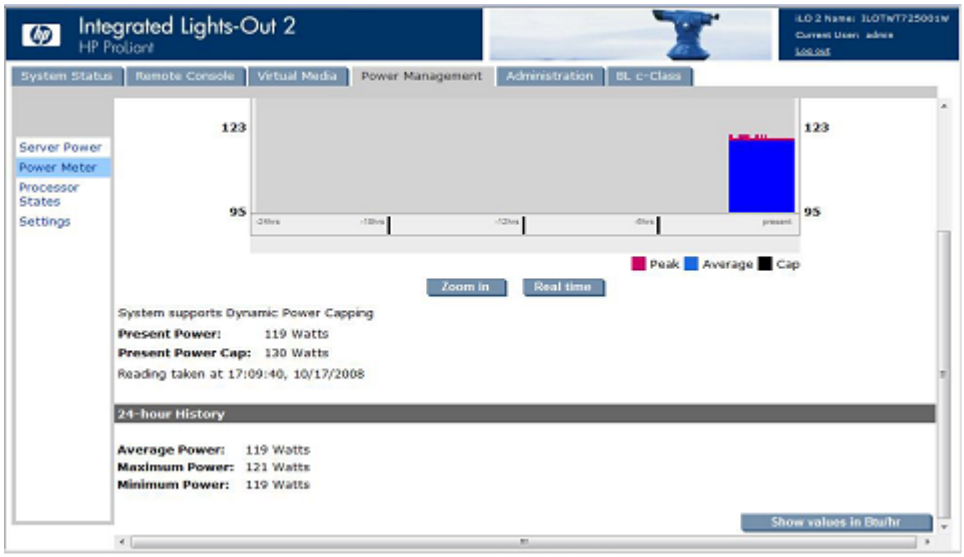
For more information on dynamic power capping, see "Dynamic power capping for server blades."

- SNMP Alert on breach of power threshold section enables the sending of SNMP warnings when power consumption exceeds a defined threshold. You can set the following:
  - Warnings Triggered By – Determines if warnings are based on peak power consumption, average power consumption, or disabled.
  - Warning Threshold – Sets the threshold at which power consumption must remain above in order to trigger an SNMP alert.
  - Duration – Sets the length of time, in minutes, that power consumption must remain above the warning threshold before an SNMP alert is triggered. The maximum duration allowed is 240 minutes and must be a multiple of 5.

To use your selected settings, click **Apply**. Some servers allow modification of the processor power level through the system RBSU. See your system user guide for more information.

Server power data

iLO 2 enables you to graphically view server power usage. The Power Meter Readings page displays server power utilization as a graph. To access Power Meter Readings, select **Power Management**, and click **Power Meter**. The Power Meter Readings page has two sections: Power Meter Readings, and 24-Hour History.



The Power Meter Readings section displays the following:

- The data graph displays the power usage of the server over the previous 24 hours. iLO 2 collects power usage information from the server every 5 minutes. For each five-minute interval, the peak and average power usage is stored in a circular buffer. These two values appear in the form of a bar graph, with the average values in blue and the peak values in red. This data resets whenever either the server or iLO 2 is reset.
  - To increase visibility, click **Zoom in**, which increases the horizontal width of the data bars on the Power Data Graph. A slider appears in this mode to enable inspection of the data in the same size window.
  - To view current power utilization, click **Real Time**. The Real Time data graph displays power consumption information over the previous 20 minutes, including peak power, average power, and the power cap. This button is only available when power cap is enabled.
- Current support for Dynamic Power Capping
- Present Power value displays the current power reading from the server.
- Present Power Cap displays the current power cap setting.

The 24-Hour History section displays the following:

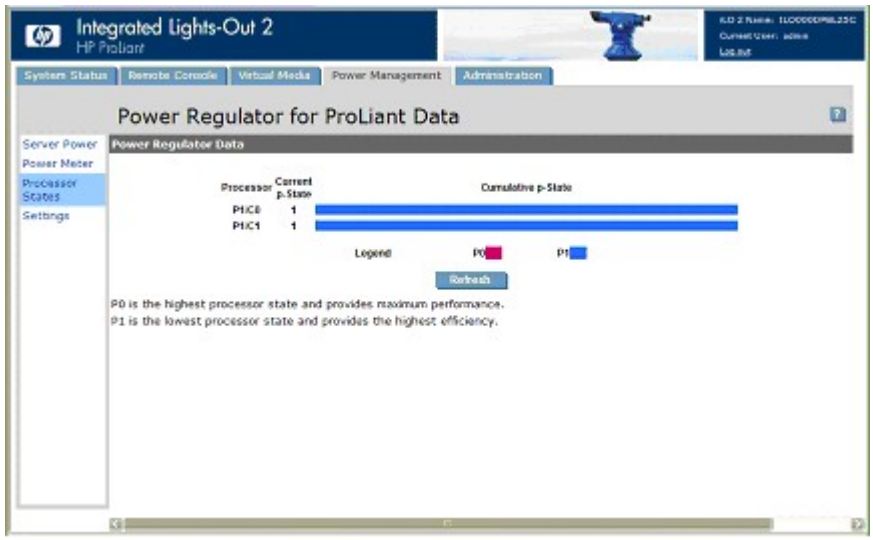
- Average Power Reading displays the average of the power readings from the server over the last 24-hour period. If the server has not been running for 24 hours, the value is the average of all the readings since the server was booted.
- Maximum Power displays the maximum power reading from the server over the last 24-hour period. If the server has not been running for 24 hours, the value is the maximum of all the readings since the server was booted.
- Minimum Power displays the minimum power reading from the server over the last 24-hour period. If the server has not been running for 24 hours, the value is the minimum of all the readings since the server was booted.
- Show value in BTUs changes the displayed data from watts to BTUs.

Processor states

The Power Regulator for ProLiant Data page enables you to view processor states (p-state) and a running average of the percentage of time each logical processor has spent in each p-state over the previous 24-hours. Click **Refresh** to update the p-state data graph.

You must have the Configure iLO 2 Settings privilege to view the Power Regulator for ProLiant Data page. Power Regulator for ProLiant Data is a licensed feature available with the purchase of optional licenses. For more information, see "Licensing" (page 26).

To access the Power Regulator for ProLiant Data page, click **Power Management>Processor States**.



The Power Regulator Data page displays the collected p-state data, starting from host power up once a second and then refreshes for display once every 5 minutes. The system ROM reads the current status of each logical processor. The status register in Intel-based platforms reflects the current operating frequency and voltage. Because of multiple processor dependencies, the status might or might not reflect an absolute p-state. The frequency might be at one p-state and the voltage at a higher p-state. The system ROM updates the p-state count of the p-state for the current frequency and not the current voltage.

Data is displayed using a bar graph, with the total bar length representing 100% of the time covered by the data. One data graph is displayed for each processor or core. Data graphs for multiple threads on a processor or core that supports Hyper-Threading are not displayed. A portion of the bar is colored differently for each p-state the processor was in, with each colored portion scaled to represent the percentage of the total time the processor spent in that p-state. Pausing the mouse over the bar graph displays a tool tip that indicates the numeric percentage that portion of the bar represents.

Power efficiency

iLO 2 enables you to implement improved power usage using a High Efficiency Mode (HEM). HEM improves the power efficiency of the system by placing the secondary power supplies into step-down mode. When the secondary supplies are in step-down mode, the primary supplies provide all the DC power to the system. The power supplies are more efficient (more DC output Watts for each Watt of AC input) at higher power output levels, and the overall power efficiency improves.

When the system begins to draw more than 70% capacity of the maximum power output of the primary supplies, the secondary supplies return to normal operation (out of step-down mode). When the power use drops below 60% capacity of the primary supplies, the secondary supplies return to step-down mode. HEM enables you to achieve power consumption equal to the maximum power output of the primary and the secondary supplies, while maintaining improved efficiency at lower power usage levels.

HEM does not affect power redundancy. If the primary supplies fail, then the secondary supplies immediately begin supplying DC power to the system, preventing any downtime.

You can configure HEM only through the RBSU. You cannot modify these settings through iLO. Settings for HEM are Enabled or Disabled (also called Balanced Mode), and Odd or Even supplies as primary. These settings are visible in the High Efficiency Mode & Standby Power Save Mode section of the System Information>Power tab. This section displays the following information:

- If HEM is enabled or disabled
- Which power supplies are primary (if HEM is enabled)
- Which power supplies do not support HEM



Graceful shutdown

The ability of the iLO 2 microprocessor to perform a graceful shutdown requires cooperation from the operating system. In order to perform a graceful shutdown, the health driver must be loaded. iLO 2 communicates with the health driver, and the appropriate operating system method of safely shutting the system down to ensure data integrity is performed.

In cases where the health driver is not loaded, the iLO 2 processor attempts using the operating system to perform a graceful shutdown through the power button. iLO 2 emulates a physical power button press in order to prompt the operating system to shutdown gracefully. The behavior of the operating system is dependent on its configuration and settings for a power button press.

The EAAS configuration of the HOST ROM RBSU allows for the disabling of this automatic shutdown feature. This configuration allows for the disabling of the automatic shutdown event except for in the most extreme conditions where physical damage would result.

Starting with Windows Server 2003, the computer group policy disables a graceful shutdown of the system using a momentary press unless an Administrator is logged in to the operating system. To change this setting and enable a graceful shutdown, do the following:

1. From a command prompt, issue the command:

   ```
   gpedit.misc
   ```

2. Set **Computer Configuration>Windows Settings>Security Settings>Local Policies>Security Options>Shutdown**. Allow the system to be shut down without having to log on to **Enabled**.

Brown-Out recovery

A brown-out condition occurs when power momentarily is lost to the server. A brown-out interrupts the operating system, but does not interrupt the iLO firmware. Under brown-out conditions the iLO service remains uninterrupted for about 4 seconds (longer power interruptions result in black-outs).

Support has been added to iLO to detect and recover from power brown-outs. If iLO detects that a brown-out has occurred, server power is restored after the power-on delay. After the brown-out recovery, iLO firmware records a `Brown-out recovery` event in the event log.

NOTE: The brown-out recovery service is available on the HP ML and DL servers. BL c-Class blade servers and SL-class servers are not affected.

ProLiant BL p-Class Advanced management

iLO 2 Advanced is a standard component of ProLiant BL p-Class server blades that provides server health and remote server blade manageability. Its features are accessed from a network client device using a supported Web browser. In addition to other features, iLO 2 Advanced provides keyboard, mouse, and video (text and graphics) capability for a server blade, regardless of the state of the host operating system or host server blade.

iLO 2 includes an intelligent microprocessor, secure memory, and a dedicated network interface. This design makes iLO 2 independent of the host server blade and its operating system. iLO 2 provides remote access to any authorized network client, sends alerts, and provides other server blade management functions.

Using a supported Web browser, you can:

- Remotely access the console of the host server blade, including all text mode and graphics mode screens with full keyboard and mouse controls.
- Remotely power up, power down, or reboot the host server blade.
- Remotely boot a host server blade to a virtual diskette image to perform a ROM upgrade or install an operating system.
- Send alerts from iLO 2 Advanced regardless of the state of the host server blade.
- Access advanced troubleshooting features provided by iLO 2 Advanced.
- Launch a Web browser, use SNMP alerting, and diagnose the server blade using HP Systems Insight Manager.
- Configure static IP bay settings for the dedicated iLO 2 management NICs on each server blade in an enclosure for faster deployment.

The server blade must be properly cabled for iLO 2 connectivity. Connect to the server blade with one of the following methods:

- Through an existing network (in the rack) – This method requires you to install the server blade in its enclosure and assign it an IP address manually or using DHCP.
- Through the server blade I/O port
  - In the rack – This method requires you to connect the local I/O cable to the I/O port and a client PC. Using the static IP address listed on the I/O cable label and the initial access information on the front of the server blade, you can access the server blade with the iLO 2 Advanced Remote Console.
  - Out of the rack, with the diagnostic station – This method requires you to power the server blade with the optional diagnostic station and connect to an external computer using the static IP address and the local I/O cable. For cabling instructions, refer to the documentation that ships with the diagnostic station or to the Documentation CD.
  - Through the server blade rear panel connectors (out of the rack, with the diagnostic station) – This method enables you to configure a server blade out of the rack by powering

the blade with the diagnostic station and connecting to an existing network through a hub. The IP address is assigned by a DHCP server on a network.

The BL p-Class tab enables you to control specific settings for the ProLiant BL p-Class blade server rack. iLO 2 also provides Web-based status for the ProLiant BL p-Class server rack.

Rack View

The Rack View page presents an overview of all the enclosures and the contained blade servers, network components, and power supplies. A component, when present in the rack appears and a selectable component on the Rack View page. Blank or empty bays are not selectable. Component-specific information, such as blade name, IP address, and product type, appears as you move the mouse cursor over each component. Clicking the component displays additional information and configuration options in the adjacent screen.



The following fields are available on the Rack View screen:

- Rack name
- Logged-in iLO Location

  This section annotates the blade you are logged in to. You can only configure blade settings for this blade.

- Selected Bay Location

  This section annotates the currently selected bay. You can view information for many different types of components, including blades, power supplies, network components, and enclosures.

- Enclosure Details

  Information about a particular enclosure is viewed by selecting **Details** located on the enumerated enclosure headers.

A Refresh button is available to obtain current Rack View information. Click **Refresh** to force the entire graphical representation of the rack to be redrawn. This operation takes a few moments.

If the rack view information cannot be properly obtained, an error message appears in place of the rendered components. The Refresh button can be used to make another attempt to obtain the proper rack view data. Rack View functionality requires version 2.06 or later of the Server Blade and Power Management Module firmware to display correctly.

Blade configuration and information

The blade configuration option provides information regarding the identity, location, and network address of the blade selected on the Rack View page. To view these settings, select a blade component and select **Configure** on the "Rack View" (page 120) page. You can change some of the settings for the blade in which you are currently logged in. To save changes, click **Apply**.



The following fields are available:

- Identification Information
  - Bay Name
  - Bay Number
- Power On Control
  - Power Source
  - Enable Automatic Power On
  - Enable Rack Alert Logging (IML)

Enclosure information



Enclosure information is specific to the selected enclosure. Information about a particular enclosure is viewed by selecting **Details** located on the enumerated enclosure headers. A limited amount of rack information is available, including the name and serial number

A basic set of information is available for the enclosures that do not contain the blade that you are logged in to. This information includes the name, serial number, and enclosure type.

An advanced set of details is available for the enclosure that contains the bay you are logged into. These details include the following:

- Name
- Serial number
- Enclosure type
- Firmware revision
- Hardware revision
- Enclosure temperature
- Management Module UID

Certain fields can be changed and updated by clicking **Apply**.

Power enclosure information

The Power Enclosure Information page provides diagnostic information regarding the power management module and the power components contained in the power enclosure. This information provides an overview on the health and condition of the power enclosure and components.



The following fields are available:

- Rack name
- Rack serial number
- Enclosure name
- Enclosure serial number
- Enclosure type
- Firmware revision
- Hardware revision
- Load balance wire
- Enclosure temperature
- Enclosure temperature side A and B
- Management Module UID

Certain fields can be changed and updated by clicking **Apply**.

Network component information

Network component information displays the status of the patch panel or interconnect switch that has been selected. The information displayed includes Fuse A, Fuse B, and Network Component Type.

iLO 2 control of ProLiant BL p-Class server LEDs

iLO 2 can monitor BL p-Class servers through POST tracking and the Server Health LED.

Server POST tracking

Feedback is limited while the server is booting because of the headless nature of the ProLiant BL p-Class servers. iLO 2 provides boot-time feedback by flashing the Server Health LED green during server POST. The LED is set to solid amber if the boot is unsuccessful. The LED is set to solid green at the end of a successful boot.

After a successful boot, control of the Server Health LED is returned to the server, which can turn the LED off or set it to some other color to represent the health of the server hardware.

Insufficient power notification

iLO 2 turns the Server Health LED solid red if iLO 2 cannot power on the server because insufficient power is in the rack infrastructure.

ProLiant BL p-Class alert forwarding

iLO 2 supports blade infrastructure SNMP traps on a passthrough basis. Reporting of blade infrastructure status by iLO 2 does not require operating system support. The alerts (traps) originate from the Enclosure Manager and Power Supply Manager and are transmitted to iLO 2. iLO 2 p-Class firmware forwards infrastructure alerts as SNMP traps to a correctly configured management console. These alerts allow the monitoring of p-Class alerts to take place in an SNMP management console.

p-Class alert forwarding is disabled by default and can be enabled from the SNMP/Insight Manage Settings web page.

The following alerts are identified and forwarded by iLO 2:

Alert ID	Description
22005	Enclosure temperature failure
22006	Enclosure temperature degradation
22007	Enclosure temperature OK
22008	Enclosure fan failed
22009	Enclosure fan degraded
22010	Enclosure fan OK
22013	Rack power failure
22014	Rack power degraded
22015	Rack power supply OK
22023	Rack server failed; not enough power

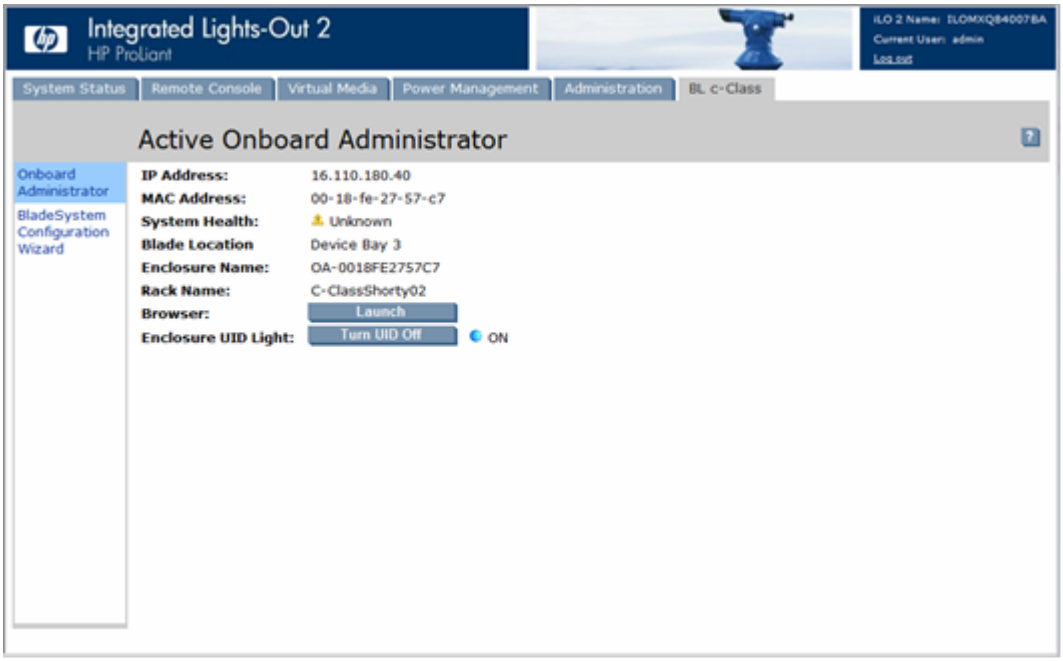
ProLiant BladeSystem HP Onboard Administrator

HP BladeSystem Onboard Administrator is the enclosure management processor, subsystem, and firmware base used to support the HP BladeSystem and all the managed devices contained within the enclosure.

You can access iLO 2 through the HP Onboard Administrator "iLO option" (page 128), using the "Web Administration" (page 128), or directly. To log in to iLO 2 directly, see "Logging in to iLO 2 for the first time" (page 20).

iLO 2 BL c-Class tab

The BL c-Class tab of the iLO 2 web interface enables you to access the Onboard Administrator and the BladeSystem Configuration Wizard. For more information on the BladeSystem Configuration Wizard, see the *HP BladeSystem Onboard Administrator User Guide*.



The Onboard Administrator option enables you to view a brief overview of the server system health as well as launch a browser (which launches the HP Onboard Administrator Rack View screen) or turn the UID Light on or off.

Enclosure bay IP addressing

During completion of the First Time Setup Wizard, you are asked to set up your enclosure bay IP addressing. For more information about the complete wizard setup process, see the *HP BladeSystem Onboard Administrator User Guide*.

The server blade iLO 2 ports and interconnect module management ports can obtain IP addresses on the management network in three ways: DHCP address, static IP address or EBIPA. If your network has an external DHCP service or if you want to manually assign static IP addresses one by one to the server blades and interconnect modules, click **Skip** to bypass this step.

- DHCP addresses – The server blade iLO 2 defaults to DHCP addressing, obtained through the network connector of the active Onboard Administrator. Interconnect modules that have an internal management network connection to the Onboard Administrator might also default to DHCP address.

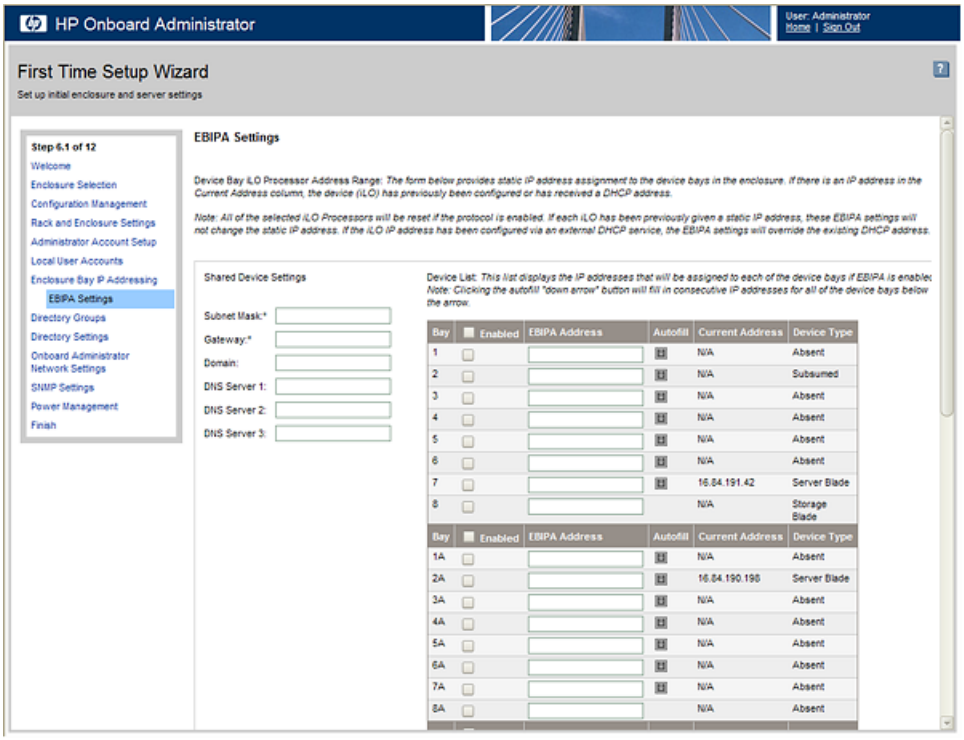
  The Onboard Administrator GUI lists the IP address for the server blade iLO 2 port and interconnect module management port

- Static IP
  - Manual – If your facility prefers static IP address assignment, you can individually change each of the server blade iLO 2 ports and interconnect module management ports to unique static addresses or use EBIPA to assign a range of static IP addresses to individual server blade and interconnect module bays.
  - EBIPA – When a server blade or interconnect module is inserted into a bay that has EBIPA enabled, that management port will get the specific static IP address from the Onboard Administrator if that device is configured for DHCP.

The administrator sets an independent range for server blade bays and interconnects module bays using the Onboard Administrator EBIPA setup wizard. The first address in a range is assigned to the first bay and then consecutive bays through the range.

For example, if you set the server bay EBIPA range to 16.100.226.21 to 16.100.226.36, the iLO 2 in device bay #1 is assigned 16.100.226.21 and the iLO 2 in device bay #12 is assigned

16.100.226.32. If you set the interconnect bay EBIPA range to 16.200.139.51 to 16.209.139.58, the interconnect module management port in interconnect bay #1 is assigned 16.200.139.51 and the interconnect module management port in interconnect bay #7 is assigned 16.200.139.57.



To enable EBIPA settings for the server bays in this enclosure, select **Enable Enclosure Bay IP Addressing for Server Bay iLO 2 Processors**, then enter the following information.

Field	Possible value	Description
Beginning Address	###.###.###.### where ### ranges from 0 to 255	Beginning IP address for the device or interconnect bays. Click the arrow next to the Beginning Address field, and click **Update List** to update the Device List or Interconnect List.
Subnet Mask	###.###.###.### where ### ranges from 0 to 255	Subnet mask for the device or interconnect bays
Gateway	###.###.###.### where ### ranges from 0 to 255	Gateway address for the device or interconnect bays
Domain	A character string, including all alphanumeric characters and the dash (-)	The domain name for the device or interconnect bays
DNS Server 1	###.###.###.### where ### ranges from 0 to 255	The IP address for the primary DNS server
DNS Server 2	###.###.###.### where ### ranges from 0 to 255	The IP address for the secondary DNS server
DNS Server 3	###.###.###.### where ### ranges from 0 to 255	The IP address for the tertiary DNS server
NTP Server 1	###.###.###.### where ### ranges from 0 to 255	The IP address of the primary server used to synchronize time and date using the NTP protocol
NTP Server 2	###.###.###.### where ### ranges from 0 to 255	The IP address of the secondary server used to synchronize time and date using the NTP protocol

Dynamic power capping for server blades

Dynamic power capping is an iLO 2 feature available for c-Class server blades and accessed through HP Onboard Administrator. For more information on all the power setting options for c-Class server blades, see the *HP BladeSystem Onboard Administrator User Guide*.

Dynamic power capping is only available if your system hardware platform, BIOS (ROM), and power micro-controller firmware version support this feature. If your system is capable of performing dynamic power capping, iLO 2 automatically functions in Dynamic Power capping mode.

In Onboard Administrator, there are two Dynamic Power capping options:

- Dynamic Power

  If enabled, Dynamic Power automatically places unused power supplies in standby mode to increase enclosure power supply efficiency, thereby minimizing enclosure power consumption during lower power demand. Increased power demands automatically return standby power supplies to full performance. If Dynamic Power is:

  — Enabled (default setting) – Some power supplies can be automatically placed on standby to increase overall enclosure power subsystem efficiency.

  — Disabled – All power supplies share the load. The power subsystem efficiency varies based on load.

- Enclosure Dynamic Power Cap

  An optional setting that enables you to set a cap on a group of servers in an enclosure. Set the cap between the values shown above the Enclosure Dynamic Power Cap field. These values are based on the enclosure's current configuration.

  As the servers run, the demand for power varies for each server. A power cap for each server is set to provide the server with enough power to meet its workload demands while still conforming to the Enclosure Dynamic Power Cap.

  You can use either the Static Power Limit or the Enclosure Dynamic Power Cap in the following situations:

  — If the facility power is limited to the enclosure, you can enter a fixed limit into each enclosure. For example, if the hosted location limits the enclosure to 5000 W. In the limit Enclosure Input Watts field, enter **5000**. The Onboard Administrator limits total power allocation to 5000 W, which might result in denying power to some of the server blades.

  — If the facility limits cooling capacity to the enclosure, then divide the limit of Btu/hr available to the enclosure by 3.41 to determine the watts limit for that enclosure. Enter that watts limit to restrict the heat load of the enclosures. For example: If the facility limits individual enclosure to 27,280 Btu/hr, then 27,280 divided by 3.41 yields 8,000 W. Enter the watts limit to restrict that enclosure to 27,280 Btu/hr. This limit can result in denying power to some of the server blades.

  — If you need to restrict an enclosure's electrical load or thermal output, an Enclosure Dynamic Power Cap is better. It enables more blades to power on than a Static Power Limit does. A Static Power Limit is better in the following cases:

    – You do not want caps dynamically adjusted on your server blades.

    – You prefer to not power on a server blade if it cannot be allocated full power (even if it typically consumes less).

    – More than 1/4 of the blades in the enclosure do not meet hardware or firmware requirements for the Enclosure Dynamic Power Cap.

    – You do not have redundant AC power supplies.

    – Do not set a cap on an empty enclosure. This disables both the Static Power Limit and the Enclosure Dynamic Power Cap.

For more information on Static Power Limit, see the *HP BladeSystem Onboard Administrator User Guide*.

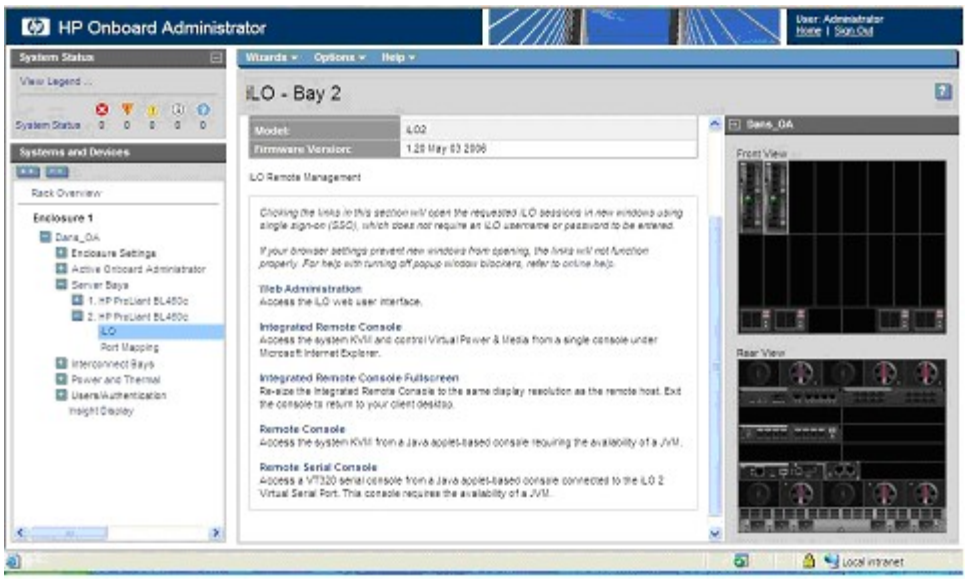
iLO 2 Virtual Fan

In c-Class blade servers, the HP Onboard Administrator controls the enclosure fans. The iLO 2 firmware cannot detect these enclosure fans. Instead, the iLO 2 firmware monitors an ambient temperature sensor located on the blade server. This information displays on the iLO 2 interface and retrieved by the Onboard Administrator periodically. The Onboard Administrator uses the sensor information collected from all iLO 2 management processors in the enclosure to determine enclosure fan speeds.

iLO option

The iLO option of the HP Onboard Administrator allows you to access the "Web Administration" (page 128), the "IRC Fullscreen" (page 85), the "Integrated Remote Console option" (page 85), Remote Console, and "Remote Serial Console" (page 100). Clicking the links in this section opens the requested iLO 2 sessions in new windows using SSO, which does not require an iLO 2 username or password to be entered.

If your browser settings prevent new windows from opening, the links will not function properly. For help with turning off pop-up window blockers, see online help.



Web Administration

The Web Administration link on the HP Onboard Administrator interface accesses the iLO 2 GUI. The System Status page appears, providing an overview of the health of the server.



BL p-Class and BL c-Class features

The HP ProLiant BL p-Class and ProLiant c-Class servers share common features. The differences are highlighted in the following table:

Feature	BL c-Class	BL p-Class
Enclosure communications	Ethernet	i2c
Enclosure-based IP addressing	DHCP	SBIPC
Enclosure authentication to iLO 2	Mutual	Not supported
Server fan	Virtual	Physical
Blade server information and configuration	Unrestricted	Restricted
Power-on override	Not supported	Supported
Front dongle	SUV (no iLO 2)	SUVi
Rack management	Full support through HP Onboard Administrator	Limited support through iLO 2

5 Directory services

Overview of directory integration

iLO 2 can be configured to use a directory to authenticate and authorize its users. Before configuring iLO 2 for directories, you must decide whether or not you want to use the HP Extended schema option.

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 iLO 2.
- RILOE and RILOE II only work with HP Extended schema. (Schema-free will be added to RILOE II at later date.)

iLO 2, RILOE, and RILOE II will only work with eDirectory with HP Extended schema.

For more information, see "Benefits of directory integration" (page 130). "Directory-enabled remote management" (page 156) details how roles, groups, and security is enabled and enforced using directories. There are also white papers available for more information on directory integration on the HP website at http://www.hp.com/servers/lights-out.

Benefits of directory integration

- Scalability – The directory can be leveraged to support thousands of users on thousands of iLO 2s.
- 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 the lack of knowing who performed an operation, instead of knowing what account (or role) was used.
- Role-based administration – 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 at a single role applies to all users and Lights-Out devices associated with that role.
- Single point of administration – You can use native administrative tools like MMC and ConsoleOne to administrate Lights-Out users.
- Immediacy—A single change in the directory rolls-out immediately to associated Lights-Out processors. This eliminates the need to script this 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 – You can create a single role for a single user on a single iLO 2, or you can create a single role for multiple users on multiple iLOs, or you can use a combinations of roles as is suitable for your enterprise.
- Compatibility – Lights-Out directory integration applies to iLO 2, 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.

Advantages and disadvantages of schema-free directories and HP schema directory

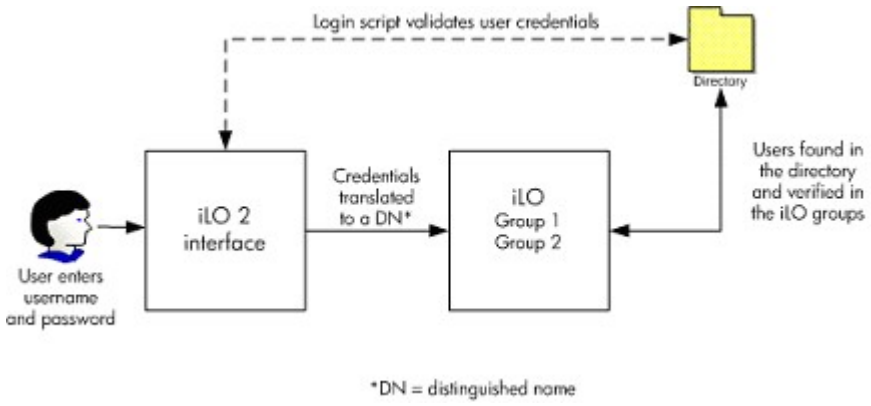
Directories enhance security, enabling you to manage access and rights from a centralized location. Directories also enable flexible configuration. Some directory configuration practices work better with iLO 2 than others. Before configuring iLO 2 for directories, you must decide whether to use the schema-free directory or the HP schema directory integration methods. Answer the following questions to help evaluate your directory integration requirements:

1. Can you apply schema extensions to your directory?
   - No – Are you using Microsoft Active Directory?
   - No – Directory integration might not fit your environment. Consider deploying an evaluation directory server to assess the benefits of directory integration.
   - Yes – Use group-based schema-free directory integration.
   - Yes – Proceed to question 2.
2. Is your configuration scalable?
   - No – Deploy an instance of the schema-free directory integration to evaluate whether or not this directory integration method meets your policy and procedural requirements. If necessary, you can deploy HP schema directory integration later.
   - Yes – Use HP schema directory integration.

   The following questions can help you determine if your configuration is scalable:
   - Are you likely to changes the rights or privileges for a group of directory users?
   - Will you regularly script iLO 2 changes?
   - Do you use more than five groups to control iLO 2 privileges?

Schema-free directory integration

Using the schema-free directory integration method, users and group memberships reside in the directory, but group privileges reside in the individual iLO 2. iLO 2 uses login credentials to read the user object in the directory and retrieve the user group memberships, which are compared to those stored in iLO 2. If there is a match, authorization is granted. For example:



Advantages of using schema-free directory integration:

- There is no need to extend the directory schema.
- When ActiveX controls are enabled in the browser and login, NetBIOS and e-mail formats are supported.
- Little or no setup is required for users in the directory. If there is no setup, the directory uses existing users and group memberships to access iLO 2. For example, if you have a domain

admin named User1; you can copy the distinguished name of the domain admin security group over to iLO 2 and give it full privileges. User1 would then have access to iLO 2.

Disadvantages of using schema-free directory integration

- Supports only Microsoft Active Directory
- Group privileges are administered on each iLO 2. However, this disadvantage is minimized by group privileges rarely changing, and the task of changing group membership is administered in the directory and not on each separate iLO 2. HP provides tools that enable changes to a large number of iLO 2 to be made at the same time.

Setting up Schema-free directory integration

Before setting up the Schema-free option, your system must meet all the prerequisites outlined in "Active Directory preparation" (page 132).

You can set up iLO 2 for directories in three ways:

- Manually using a browser, see "Schema-free browser-based setup" (page 133).
- Using a script, see "Schema-free scripted setup" (page 133).
- Using HPLOMIG, see "Schema-free HPLOMIG-based setup" (page 134).

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. iLO 2 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 at http://support.microsoft.com/.

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

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, iLO 2 cannot connect to the directory server.

Each directory server that you want iLO 2 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.

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 certificate services

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

To verify that certificate services is installed, select **Start>Programs>Administrative Tools>Certification Authority**. 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.

Schema-free browser-based setup

Schema-free can be setup using the iLO 2 browser-based interface.

1. Log on to iLO 2 using an account that has the Configure iLO 2 Settings privilege. Click **Administration**.

   NOTE: Only users with the Configure iLO 2 Settings privilege can change these settings. Users that do not have the Configure iLO 2 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, see "Schema-free setup options" (page 134).
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 at http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=135&prodTypeId=18964&prodSeriesId=1146658.
2. Write a script that configures iLO 2 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 HPLOMIG utility and additional documentation from the HP website at http://www.hp.com/servers/lights-out. HP recommends using HPLOMIG when configuring many LOM processors for directories. For more information on using HPLOMIG, see "HPLOMIG directory migration utility" (page 162).

Schema-free setup options

Setup options are the same regardless of which method (browser, HPLOMIG, 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. This group can be a security group (for example: CN=Administrators,CN=Builtin,DC=HP,DC=com) or any other group as long as the intended iLO 2 users are members of the group.

  With a minimum configuration, you can log in to iLO 2 using your full distinguished name and password. You must be a member of a group that iLO 2 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 iLO 2 tries is `CN=JOHN.SMITH,CN=USERS,DC=HP,DC=COM`.

Maximum Login Flexibility

- Configure iLO 2 as described.
- Configure iLO 2 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 iLO 2 and the client system.
- Enable ActiveX controls in your browser. The iLO 2 login script will attempt to call a Windows control to convert the login name to a distinguished name.

  Configuring iLO 2 with maximum login flexibility enables you to login 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 issue, create another profile and log in to the system.

In some cases, it might not be possible to get the maximum login flexibility option to work. For instance, if the client and iLO 2 are in different DNS domains, one of the two might not be able to resolve the directory server name to an IP address.

Schema-free nested groups

Many organizations have users and administrators arranged into groups. Having this arrangement of existing groups is convenient because you can associate them with one or more Integrated Lights-Out Management role objects. When the devices are associated with the role objects, you can use the administrator controls to access the Lights-Out devices associated with the role by adding or deleting members from the groups.

When using Microsoft Active Directory, you can place one group within another group, creating a nested group. Role objects are considered groups and can include other groups directly. You can add the existing nested group directly to the role and assign the appropriate rights and restrictions. New users can be added to either the existing group or the role.

In previous implementations, only a schema-less user who was a direct member of the primary group was allowed to log in to iLO 2. Using schema-free integration, users who are indirect members (a member of a group which is a nested group of the primary group) are allowed to log in to iLO 2.

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.

Setting up HP schema directory integration

When using the HP schema directory integration, iLO 2 supports both Active Directory and eDirectory. However, these directory services require the schema being extended.

Features supported by HP schema directory integration

iLO 2 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 iLO 2 management processors and iLO 2 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. Plan

   Review the following sections:

   - "Directory services" (page 130)
   - "Directory services schema" (page 171)
   - "Directory-enabled remote management" (page 156)

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 once to extend the schema. For more information, see "Schema installer" (page 138).
   c. Run the management snap-in installer, and install the appropriate snap-in for your directory service on one or more management workstations. For more information, see "Management snap-in installer" (page 140).
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 page in the iLO 2 GUI. For more information, see "Directory settings" (page 51).
4. Manage
   a. Create a management device object and a role object using the snap-in. For more information, see "Directory services objects" (page 145).
   b. Assign rights to the role object, as necessary, and associate the role with the management device object.
   c. Add users to the role object.

For more information on managing the directory service, see "Directory-enabled remote management" (page 156). Examples are available in "Directory services for Active Directory" (page 140) and "Directory services for eDirectory" (page 149).

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, like LDIFDE or VB script, to create complex role associations. For more information, see "Using bulk import tools" (page 161).
   - If you have iLO 2 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 are:

LOM product	Minimum supported firmware
iLO 2	1.1x

After the schema has been extended, you can complete the directory services setup by using HP Lights-Out Directories Migration Utilities. For more information, see "HPLOMIG directory migration utility" (page 162). The migration utilities are included in the HP Lights-Out Directory Package. Version 1.13 and above of the Directories Migration Utility allows Lights-Out import and export and supports different user credentials for each Lights-Out processor.

Schema documentation

To assist with the planning and approval process, HP provides documentation on the changes made to the schema during the schema setup process. To review the changes made to your existing schema, see "Directory services schema" (page 171).

Directory services support

Using HP schema directory integration, iLO 2 supports the following directory services:

- Microsoft Active Directory
- Microsoft Windows Server 2003 Active Directory
- Microsoft Windows Server 2008 Active Directory
- Novell eDirectory 8.7.3
- Novell eDirectory 8.7.1

iLO 2 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.

iLO 2 supports Microsoft Active Directory running on one of the following operating systems:

- Windows Server 2008
- Windows Server 2003

iLO 2 supports eDirectory running on Novell.

Schema required software

iLO 2 requires specific software, which will extend the schema and provide snap-ins to manage the iLO 2 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 at http://www.hp.com/servers/lights-out.

You cannot run the schema installer on a domain controller that hosts Windows Server 2008 Core. Windows Server 2008 Core does not use a GUI (for security and performance reasons). To use the schema installer, you must install a GUI on the domain controller or use a domain controller that hosts an earlier version of Windows.

Schema installer

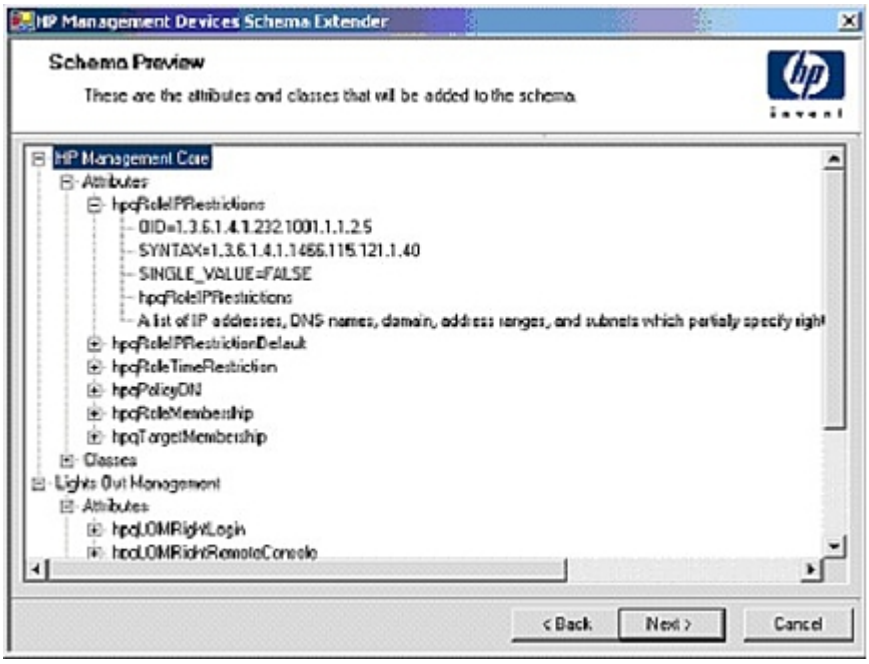
Bundled with the schema installer are one or more .xml files. These files contain the schema that will be added to the directory. Typically, one of these files will contain core schema that is common to all the supported directory services. Additional files contain only product-specific schemas. The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

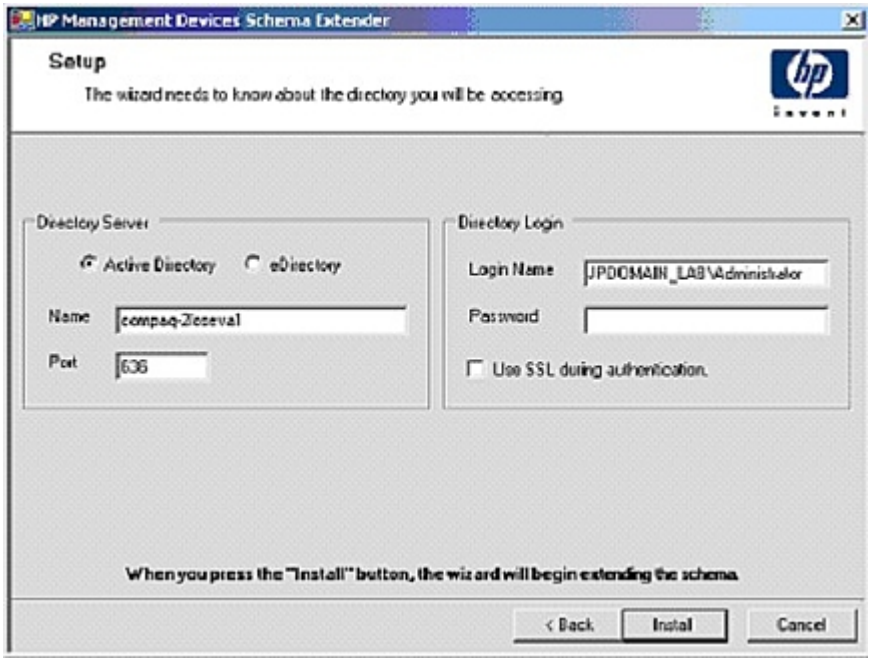
The Setup screen is used to enter the appropriate information before extending the schema.

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.

NOTE: Extending the schema on Active Directory requires that the user be an authenticated Schema Administrator, 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.

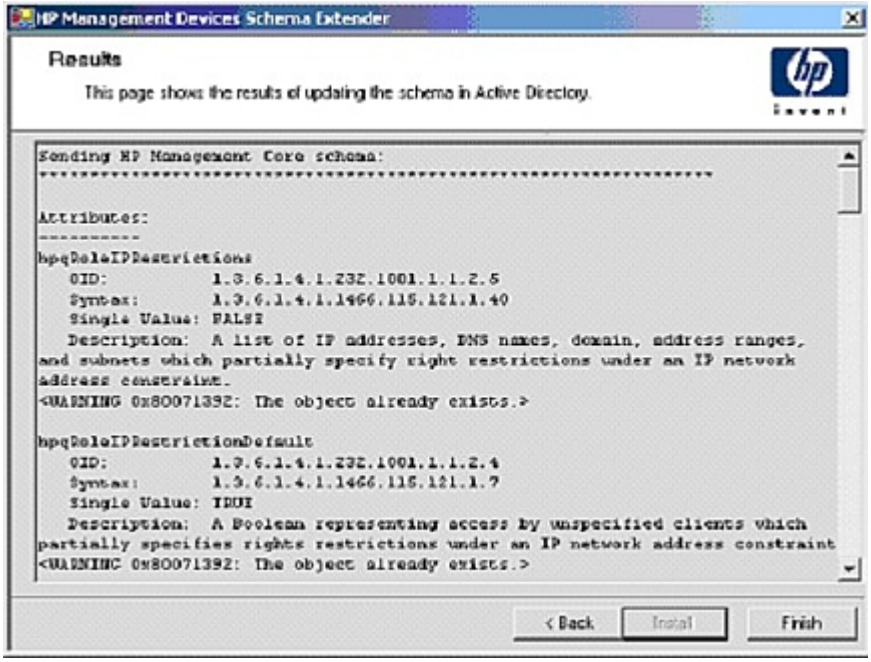
To get write access to the schema on Windows 2000 requires a change to the registry safety interlock. If the user selects the **Active Directory** option, the schema extender will attempt to make the registry change. It will only succeed if the user has rights to do this. Write access to the schema is 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 iLO 2 objects in a Microsoft Active Directory Users and Computers directory or Novell ConsoleOne directory.

iLO 2 snap-ins are used to perform the following tasks in creating an iLO 2 directory:

- Creating and managing the iLO 2 and role objects (policy objects will be supported at a later date).
- Making the associations between iLO 2 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 at http://www.hp.com/servers/lights-out.

Active Directory installation prerequisites

- The Active Directory must have a digital certificate installed to allow iLO 2 to connect securely over the network.
- The Active Directory must have the schema extended to describe Lights-Out object classes and properties.
- The firmware version must be iLO v1.40 or later, or iLO v1.00 or later.
- iLO 2 advanced features must be licensed.

  You can evaluate iLO Advanced with an evaluation license key that you can download from the HP website at http://h10018.www1.hp.com/wwsolutions/ilo/iloeval.html.

Directory Services for iLO 2 uses LDAP over SSL to communicate with the directory servers. Before installing snap-ins and schema for Active Directory, read and have available the following documentation:

NOTE: Installing Directory Services for iLO 2 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 on the Microsoft website at http://msdn.microsoft.com).
- *Installing Active Directory* in the Microsoft Windows 2000 Server Resource Kit
- Microsoft Knowledge Base Articles

  These articles are accessed using the Knowledge Base Article ID Number Search option on the Microsoft website at http://support.microsoft.com/.

  — 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*

  — 299687 *MS01-036: Function Exposed By Using LDAP over SSL Could Enable Passwords to Be Changed*

The iLO 2 firmware requires a secure connection to communicate with the directory service. This requires the installation of the Microsoft CA. Refer to the Microsoft technical reference Knowledge Base Article 321051: *How to Enable LDAP over SSL with a Third-Party Certification Authority.*

Installing Active Directory on Windows Server 2008

For the Default Schema:

1. Disable IPV6, and install Active Directory, DNS, and root CA to Windows Server 2008.
2. Log in to iLO, and access the Directory Settings page. Click **Administration>Security>Directory**.
3. In Directory Settings, enter the settings for your directory.
4. In Directory User Context, enter the settings for you directory.
5. Create the Administer Groups for your iLO users.
6. Click **Administration>Network>DHCP/DNS** and in Domain Name, and Primary DNS server, modify the settings for your environment.

For the Extended Schema:

1. Disable IPV6, and install Active Directory, DNS, and root CA to Windows Server 2008.
2. The iLO LDAP Component requires .Net Framework 1.1_4322. Install .Net Framework.
3. Install the latest iLO LDAP Component (sp31581 or later.)
4. Extend the schema using the HP Management Devices Schema Extender.
5. Install the HP the LDAP component snap-in.
6. Create the HP Device, and HP Role.
7. Log in to iLO, and access the Directory Settings page. Click **Administration>Security>Directory**.
8. Enter the Directory Settings for your directory.
9. Enter the Directory User Context.
10. Click **Administration>Network>DHCP/DNS** and in Domain Name, and Primary DNS server modify, the settings for your environment.

The LDAP component does not work with a Windows Server 2008 core installation.

Directory services preparation for Active Directory

To set up directory services for use with iLO 2 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 (see 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.

   NOTE: 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 iLO 2 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 at 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 at 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 iLO 2 management.

a. Use the management snap-ins from HP to create iLO 2, Policy, Admin, and User Role objects.
b. Use the management snap-ins from HP to build associations between the iLO 2 object, the policy object, and the role object.
c. Point the iLO 2 object to the Admin and User role objects (Admin and User roles automatically point back to the iLO 2 object).

For more information on iLO 2 objects, see "Directory services objects" (page 145).

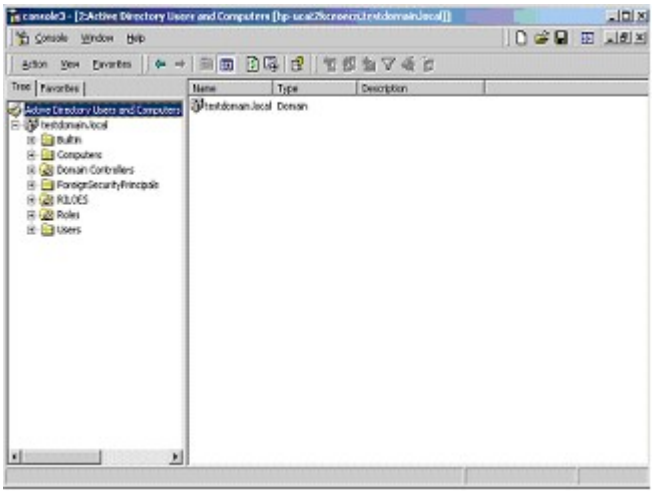
At a minimum, you must create:

- One Role object that contains one or more users and one or more iLO 2 objects.
- One iLO 2 object corresponding to each iLO 2 management processor that will be using the directory.

Example: Creating and configuring directory objects for use with iLO 2 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`.

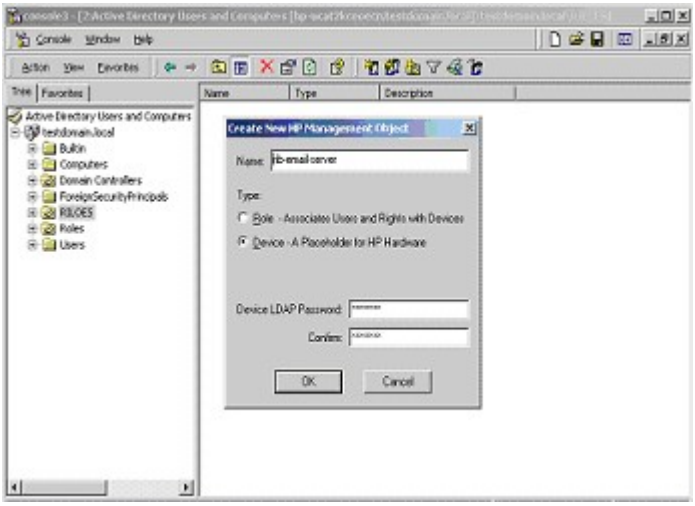
Assume that a company has an enterprise directory including the domain `testdomain.local`, arranged as shown in the following screen.



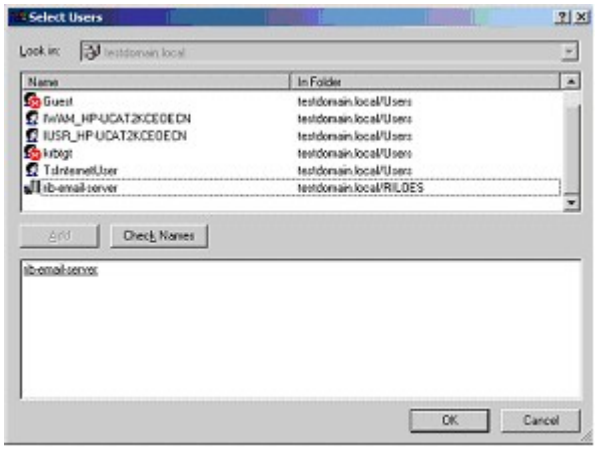
Create an organizational unit, which will contain the Lights-Out Devices managed by the domain. In this example, two organizational units are created called `Roles` and `RILOES`.

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 iLO 2 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 iLO 2 device, `rib-email-server`, is used as the name of the Lights-Out Management object, and the surname is `RILOEII`.

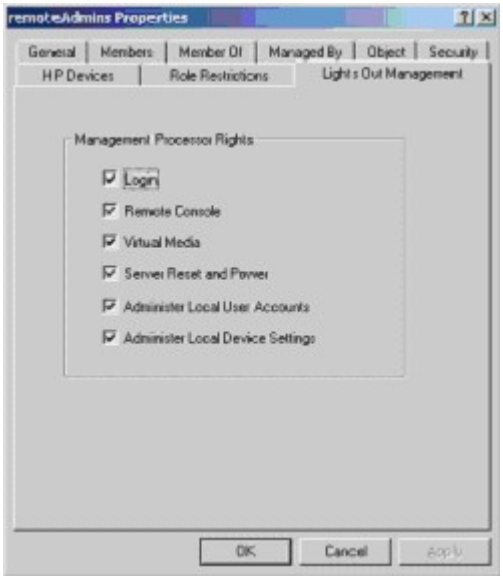
      Enter and confirm a password in the Device LDAP Password and Confirm fields. The device uses this password to authenticate to the directory, and must be unique to the device. This password is the password that is used in the Directory Settings screen of the iLO 2.
   d. Click **OK**.



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 contains users trusted for remote server administration and is 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 iLO 2 devices managed by the role. In this example, the users in the *remoteAdmins* role is given full access to the iLO 2 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 are now able to authenticate and view the server status.

User rights to any iLO 2 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 iLO 2 is a Managed Device. Following the preceding examples, if a user is in both the `remoteAdmins` and `remoteMonitors` roles, they have all the rights, because the `remoteAdmins` role has those rights.

To configure iLO 2 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 iLO 2. Mel would enter `testdomain\moorem`, or `moorem@testdomain.local`, or `Mel Moore`, in the Login Name field of the iLO 2 login screen, and use the 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 iLO 2 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, iLO 2 objects and iLO 2 roles can be created in the directory. Using the Users and Computers tool, the user will:

- Create iLO 2 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

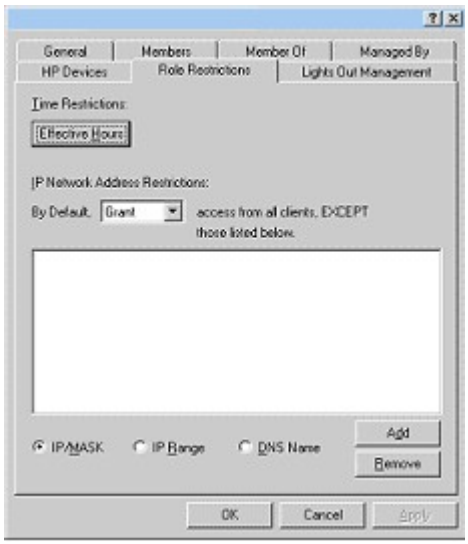
After user objects are created, the Members tab enables you to manage the users within the role. Clicking **Add** enables you to browse to the specific user you want to add. Highlighting an existing user and clicking **Remove** removes the user from the list of valid members.



Active Directory role restrictions

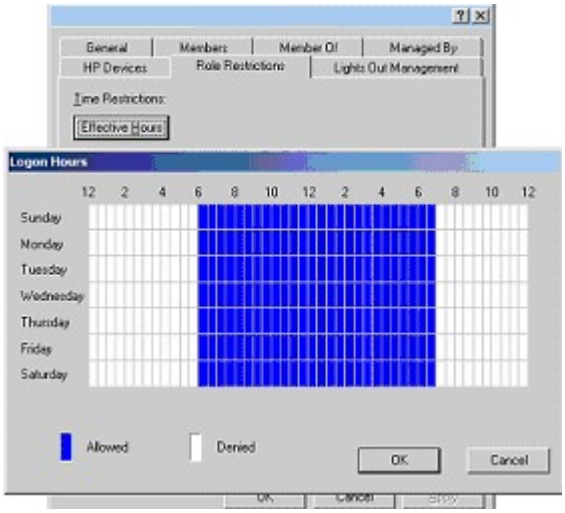
The Role Restrictions subtab allows you to set login restrictions for the role. These restrictions include:

- 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.



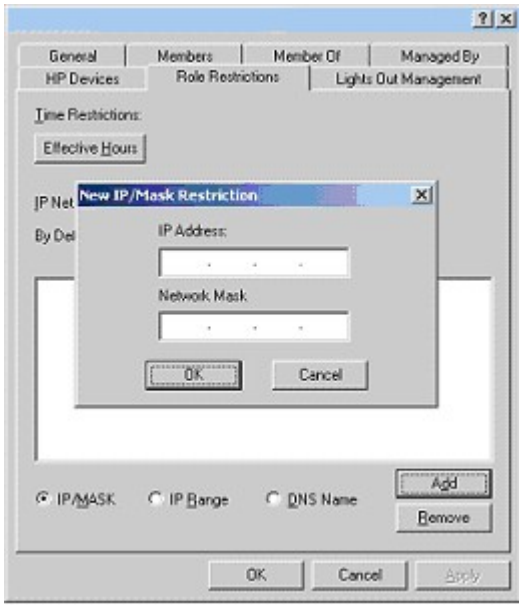
Enforced client IP address or DNS name access

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.

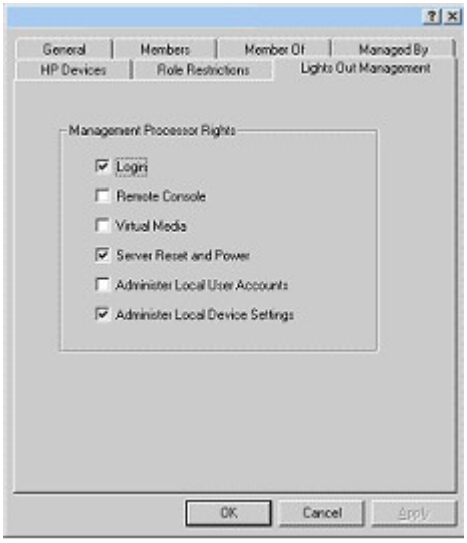
   The DNS Name option allows you to restrict access based on a single DNS name or a subdomain, entered in the form of `host.company.com` or `*.domain.company.com`.
4. Click **OK** to save the changes.

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 iLO 2 virtual media functionality.
- **Server Reset and Power** – This option enables the user access to the iLO 2 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 iLO 2 management processor settings. These settings include the options available on the Global Settings, Network Settings, SNMP Settings, and Directory Settings screens of the iLO 2 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 iLO 2 uses LDAP over SSL to communicate with the directory servers. iLO 2 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 must read and have available the following technical information documents, available on the Novell Support website at http://support.novell.com.

Installing Directory Services for iLO 2 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

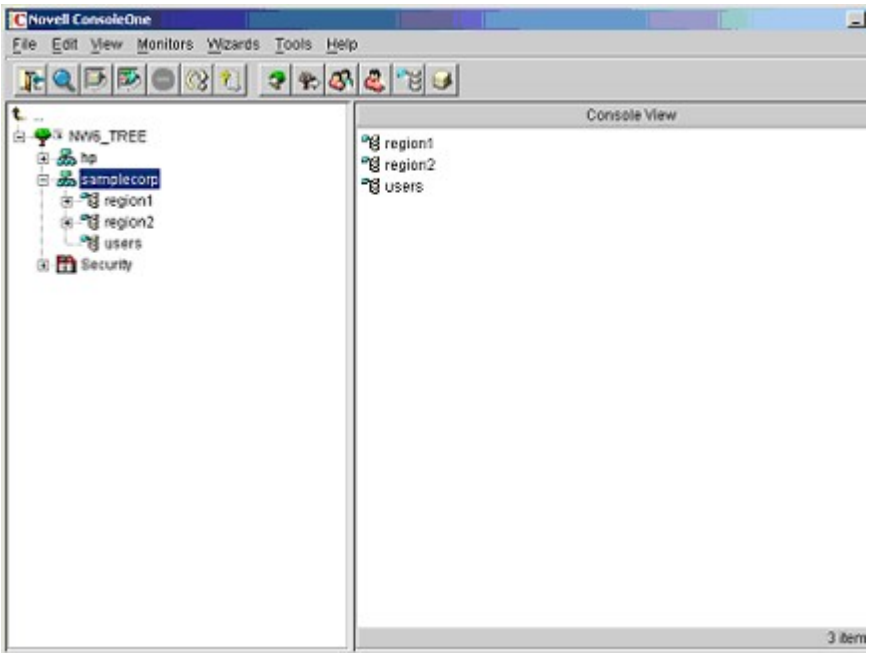
For step-by-step instructions on using the snap-in installation application, see "Snap-in installation and initialization for Active Directory" (page 142).

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

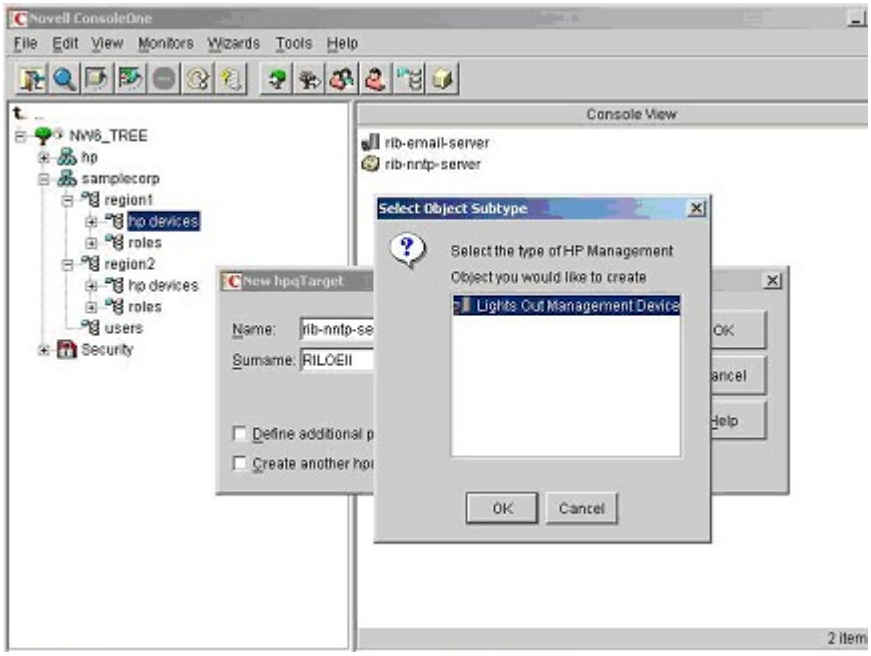
Creating and configuring directory objects for use with LOM devices in eDirectory

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`.

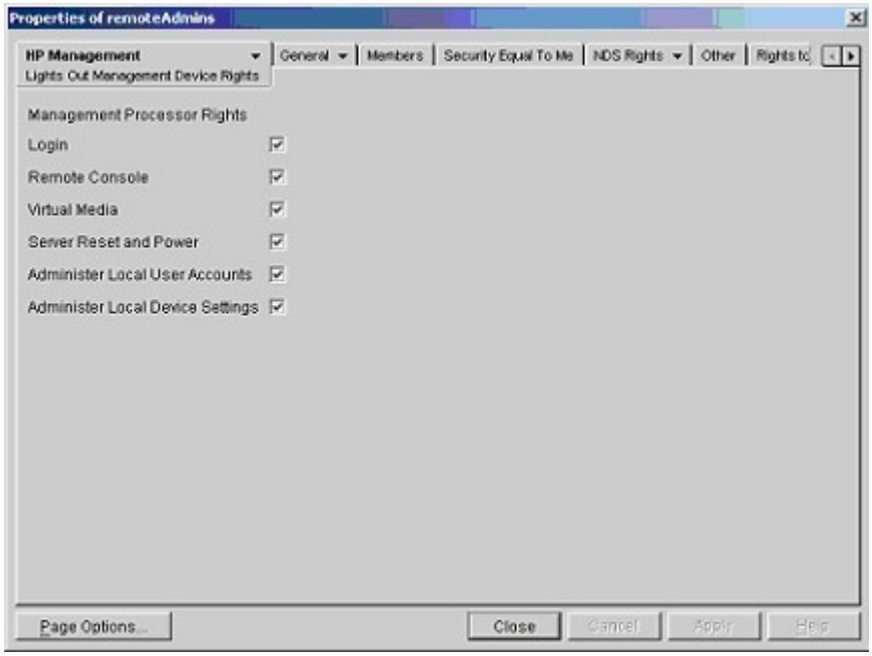
Assume `samplecorp` has an enterprise directory arranged according to the following screen.



1. Create organizational units in each region. Each organizational unit must contain the LOM devices and roles specific to that region. In this example, two organizational units are created, called `roles` and `hp devices`, in each organizational unit, `region1` and `region2`
2. Create LOM objects in the *hp devices* organizational units for several iLO 2 devices using the HP provided ConsoleOne snap-ins tool.
   a. Right-click the **hp devices** organizational unit found in the `region1` organizational unit, and select **New>Object**.
   b. Select **hpqTarget** from the list of classes, and click **OK**.
   c. Enter an appropriate name and surname in the **New hpqTarget** page. In this example, the DNS host name of the iLO 2 device, `rib-email-server` is used as the name of the LOM object, and the surname is `RILOEII`. Click **OK**. The Select Object Subtype page appears.
   d. Select **Lights Out Management Device**, and click **OK**.
   e. Repeat the process for several more iLO 2 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`.



3. Create HP Role objects in the *roles* organizational unit using the HP provided ConsoleOne snap-ins tool.
   a. Right-click the *roles* organizational unit found in the *region2* organizational unit, and select **New>Object**.
   b. Select **hpqRole** from the list of classes, and click **OK**.
   c. Enter an appropriate name on the **New hpqRole** page. In this example, the role will contain users trusted for remote server administration and will be named `remoteAdmins`. Click **OK.** The Select Object Subtype page appears.
   d. Because this role manages 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*.
4. Assign rights to the role and associate the roles with users and devices using the HP provided ConsoleOne snap-ins tool.
   a. Right-click the **remoteAdmins** role in the *roles* organizational unit in the *region1* organizational unit, and select **Properties.**
   b. Select the **Role Managed Devices** tab of the HP Management option and click **Add**.
   c. Using the Select Objects page, browse to the `hp devices` organizational unit in the `region1` organizational unit. Select the three LOM objects created in step 2. Click **OK>Apply**.
   d. Click the **Members** tab, and add users to the role by clicking **Add** on the Select Object page. Devices and users are now associated.
   e. Set the rights for the role using the Lights Out Management Device Rights option on the HP Management tab. All users within the role have the rights assigned to the role on all of the iLO 2 devices managed by the role. In this example, the users in the *remoteAdmins* role are given full access to the iLO 2 functionality. Select the check boxes next to each right, and click **Apply**. To close the property sheet, click **Close**.



5. Using the same procedure as in step 4, edit the properties of the *remoteMonitors* role:
   a. Add the three iLO 2 devices within *hp devices* under *region1* to the **Managed Devices** list on the Role Managed Devices option of the HP Management tab.
   b. Add users to the *remoteMonitors* role using the Members tab.
   c. Select the Login check-box, and click **Apply>Close**. Using the Lights Out Management Device Rights option of the HP Management tab, members of the *remoteMonitors* role can 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 LOM object used in this example, use settings similar to the following on the Directory Settings page.

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
```

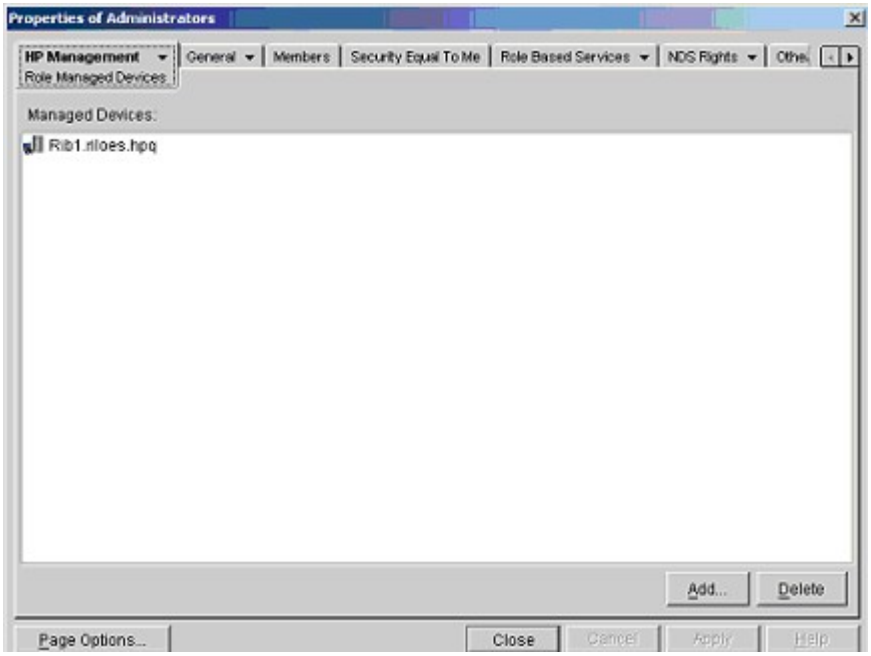
For example, user `CSmith`, located in the *users* organizational unit within the *samplecorp* organization, who is also a member of one of the *remoteAdmins* or *remoteMonitors* roles, would be allowed to log in to the iLO 2. The user enters `csmith` (case insensitive) in the Login Name field of the iLO 2 login screen and uses the 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.

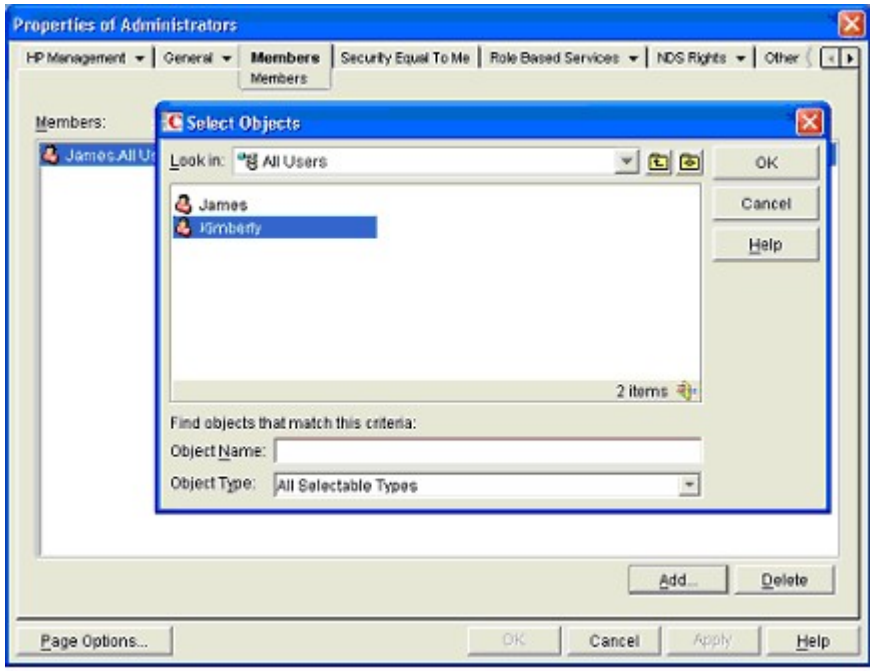
Role managed devices

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** enables you to browse to the specific HP device and add it as a managed device.



Members

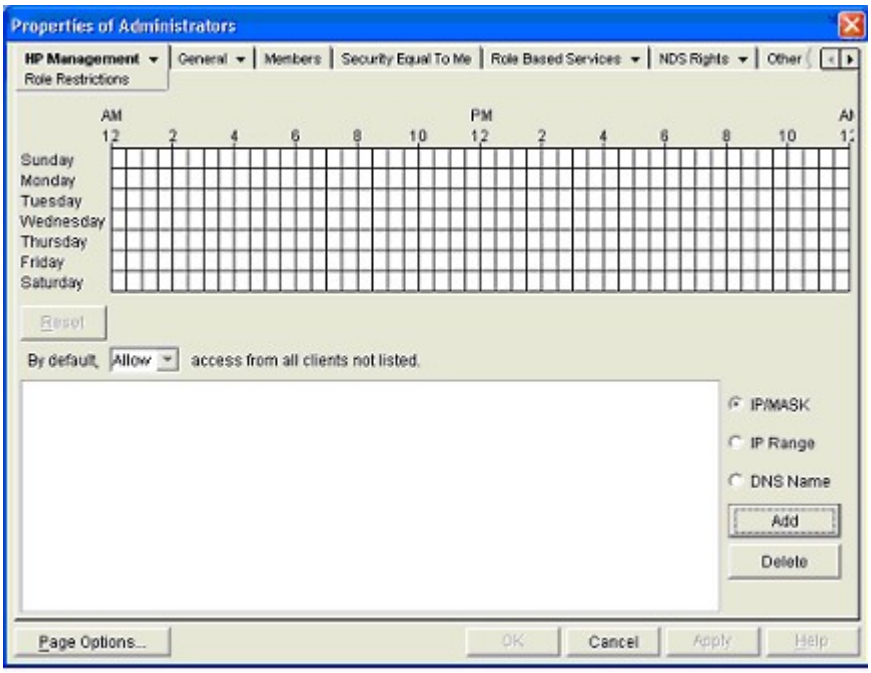
After user objects are created, the Members tab allows you to manage the users within the role. Clicking **Add** enables you to browse to the specific user you want to add. Highlighting an existing user and clicking **Delete** removes the user from the list of valid members.



eDirectory Role Restrictions

The Role Restrictions subtab enables 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.

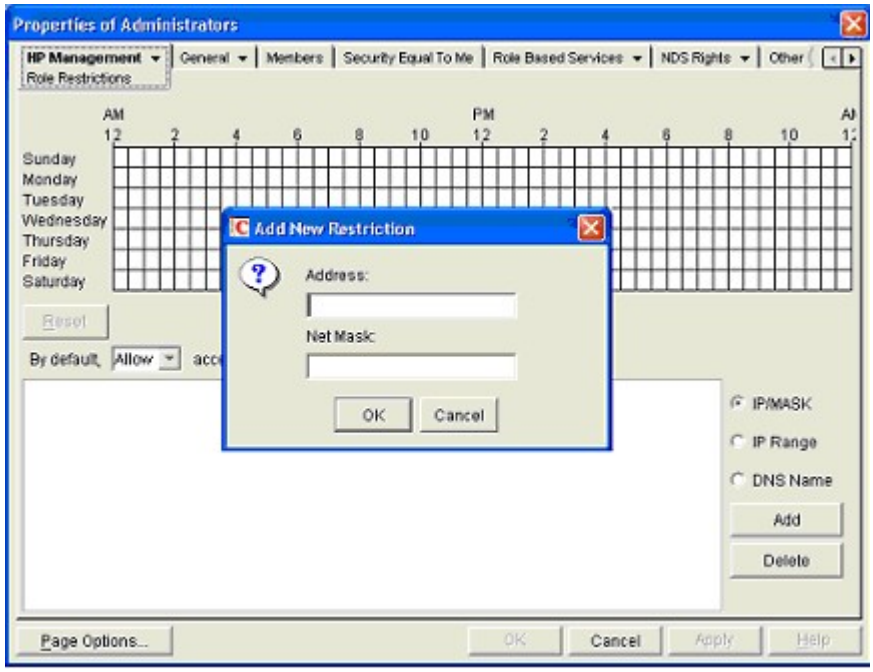
Enforced client IP address or DNS name access

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.

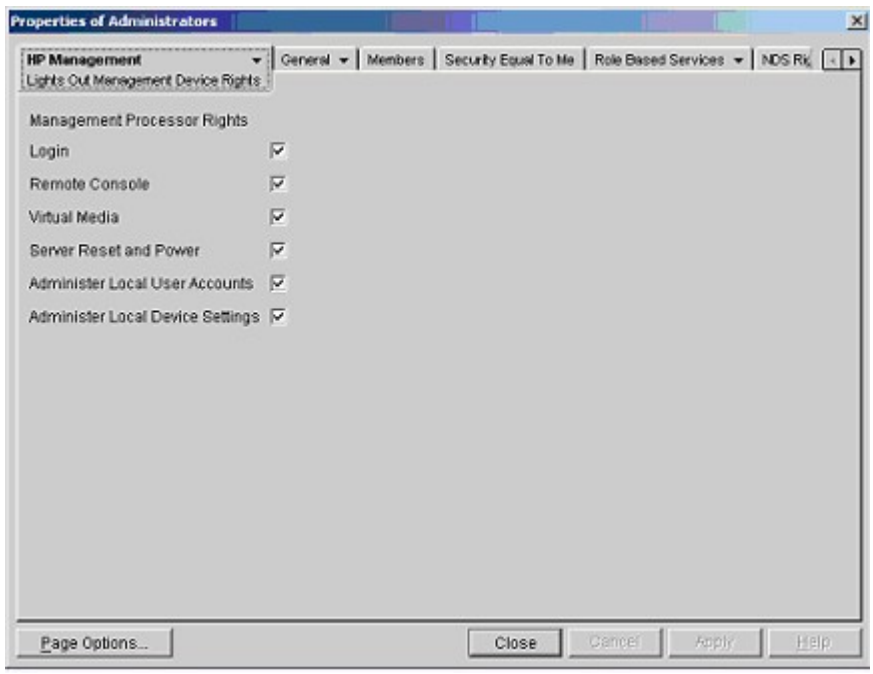
   The DNS Name option allows you to restrict access based on a single DNS name or a subdomain, entered in the form of `host.company.com` or `*.domain.company.com`.
4. Click **Apply** to save the changes.

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



eDirectory 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 log in to the associated devices.

  Login access can be used to create a user who is a service provider and who receives alerts from iLO 2 but does not have login access to iLO 2.
- Remote Console – This option allows the user access to the Remote Console.
- Virtual Media – This option allows the user access to the iLO 2 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 iLO 2 settings. These settings include the options available on the Global Settings, Network Settings, SNMP Settings, and Directory Settings screens of the iLO 2 browser.

User login using directory services

The iLO 2 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 can 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 can be located in one of three searchable contexts, which are configured within Directory Settings.

- Local users – Login-ID

  NOTE: On the iLO 2 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-enabled remote management

Introduction

This section is for administrators who are familiar with directory services and the iLO 2 product and want to use the HP schema directory integration option for iLO 2. You must be familiar with "Directory services" (page 130) 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. For additional information on creating LOM device objects for Active Directory, see "Directory services" (page 130), "Directory services for Active

Directory" (page 140), and "Directory services for eDirectory" (page 149). 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. For details on the specific directory settings, see "Configuring directory settings" (page 51). 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 have users and administrators arranged into groups. In many cases, the organizations can 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.

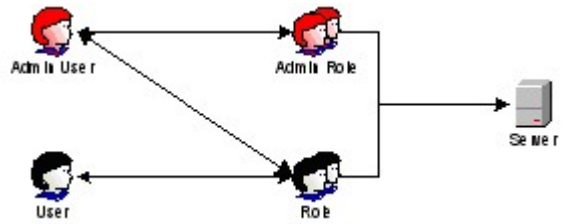
Using multiple roles

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.

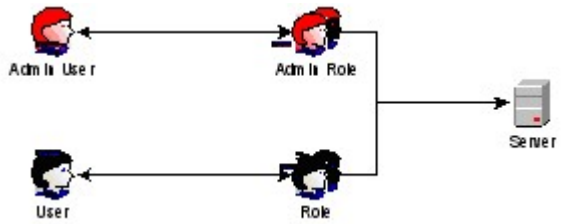
Typically, a directory administrator creates a base role with the minimum number of rights assigned and then creates additional roles to add additional rights. These additional rights are added under specific circumstances or to a specific subset of the base role users.

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.

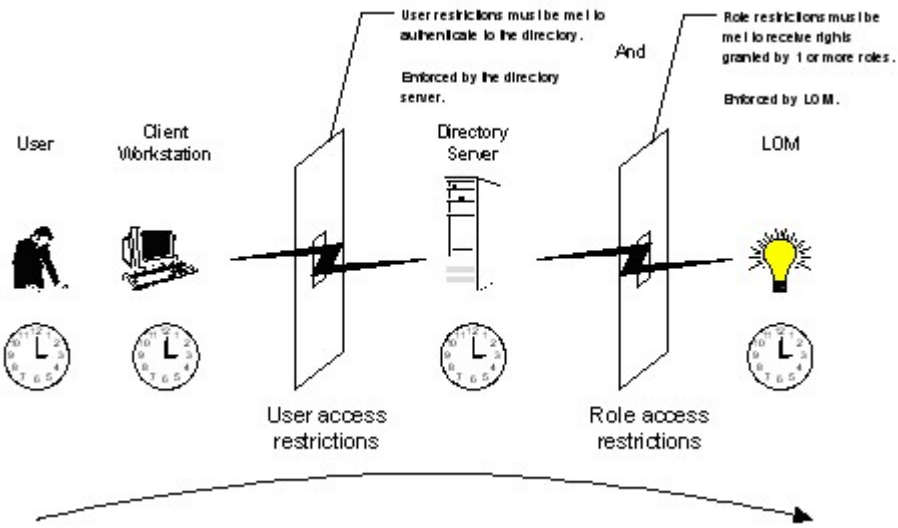


The Admin role assigns all admin rights Server Reset, Remote Console, and Login.



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 can change based on the time of day or network address of the client.

NOTE: When directories are enabled, access to a particular iLO 2 is based on whether the user has read access to a Role object that contains the corresponding iLO 2 object. This includes but is not limited to the members listed in the role object. If the Role is set up to allow inheritable permissions to propagate from a parent, then members of the parent which have read access privileges will also have access to iLO 2. To view the access control list, navigate to Users and Computers, open the properties screen for the Role object and select the **Security** tab.

For step-by-step instructions on how to create network and time restrictions on a role, see "Active Directory role restrictions" (page 147) or "eDirectory Role Restrictions" (page 154).

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.

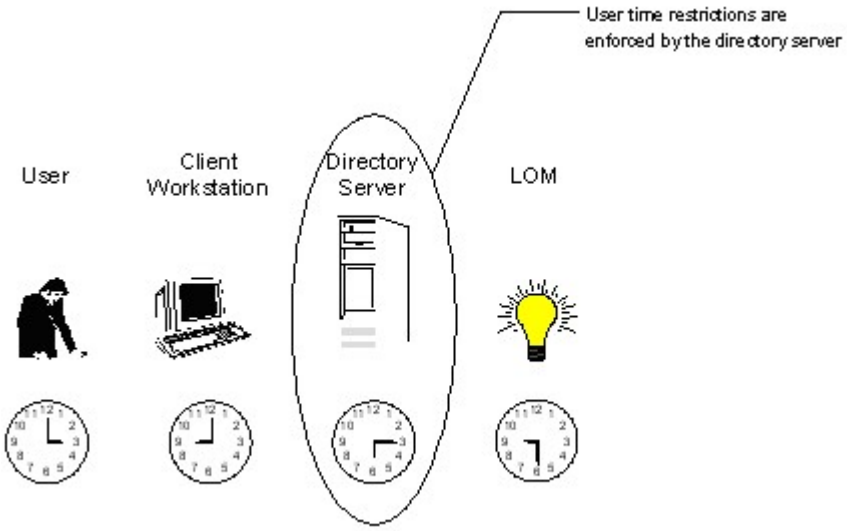
DNS restrictions can cause some ambiguity because a host can be multi-homed. DNS restrictions do not necessarily match one-to-one with a single system.

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 must 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

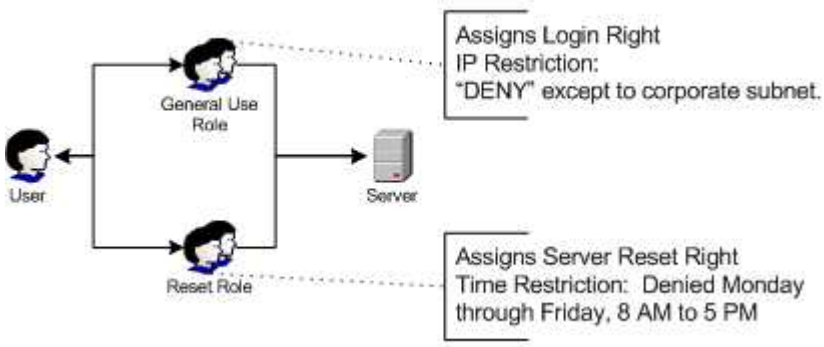
The most useful application of multiple roles includes restricting one or more roles so that rights do not apply in all situations. Other roles provide different rights under different constraints. Using multiple restrictions and roles enables the administrator to create arbitrary, complex rights relationships 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

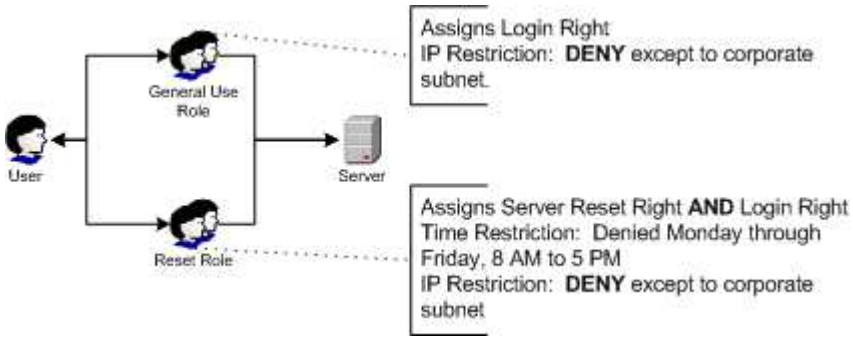
to an after-hours application might allow administrators outside the corporate network to reset the server, which is contrary to most security policies.

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.

- HP Lights-Out Migration utility

  The HP Lights-Out Migration utility, `HPLOMIG.EXE`, imports and configures multiple LOM devices. `HPLOMIG.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, see "HPLOMIG directory migration utility" (page 162).

- 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 HP SIM 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, see "HPLOMIG directory migration utility" (page 162).

- HP SIM utilities:
  - 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, see the *HP Integrated Lights-Out Management Processor Scripting and Command Line Resource Guide* at http://h20000.www2.hp.com/bizsupport/TechSupport/DocumentIndex.jsp?contentType=SupportManual&lang=en&cc=us&docIndexId=64179&taskId=135&prodTypeId=18964&prodSeriesId=1146658.
- 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. For details on attributes and attribute data formats when creating LOM objects, see "Directory services schema" (page 171).

HPLOMIG directory migration utility

Introduction to HPLOMIG utility

The HPLOMIG utility is for customers with previously installed management processors who want to simplify the migration of these processors to management by directories. `HPLOMIG` automates some of the migration steps necessary for the management processors to support Directory Services. `HPLOMIG` can do the following:

- Discover management processors on the network.
- Upgrade the management processor firmware to the version that supports Directory Services or schema-free directories.
- Name the management processors to identify them in the directory.
- Create objects in the directory corresponding to each management processor and associate them to a role.
- Configure the management processors to enable them to communicate with the directory.

Compatibility

The `HPLOMIG` utility operates on Microsoft Windows and requires Microsoft .NET Framework. For additional information and to download .NET framework, see the Microsoft website at http://www.microsoft.com/net. The `HPLOMIG` utility supports the following operating systems:

- Active Directory
  - Windows 2000
  - Windows Server 2003
- Novell eDirectory 8.6.2
  - Windows 2000
  - Windows Server 2003

HP Lights-Out directory package

All of the migration software, as well as the schema extender and management snap-ins, are packaged in an HP Smart Component. To complete the migration of your management processors, you must extend the schema and install the management snap-ins before running the migration tool. The Smart Component is located on the HP Lights-Out management website at http://www.hp.com/servers/lights-out.

To install the migration utilities, click **LDAP Migration Utility** in the Smart Component. A Microsoft MSI installer launches and installs HPLOMIG, the 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. The installer creates a shortcut to `HPLOMIG` on the Start menu and installs a sample XML file.

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

Using HPLOMIG

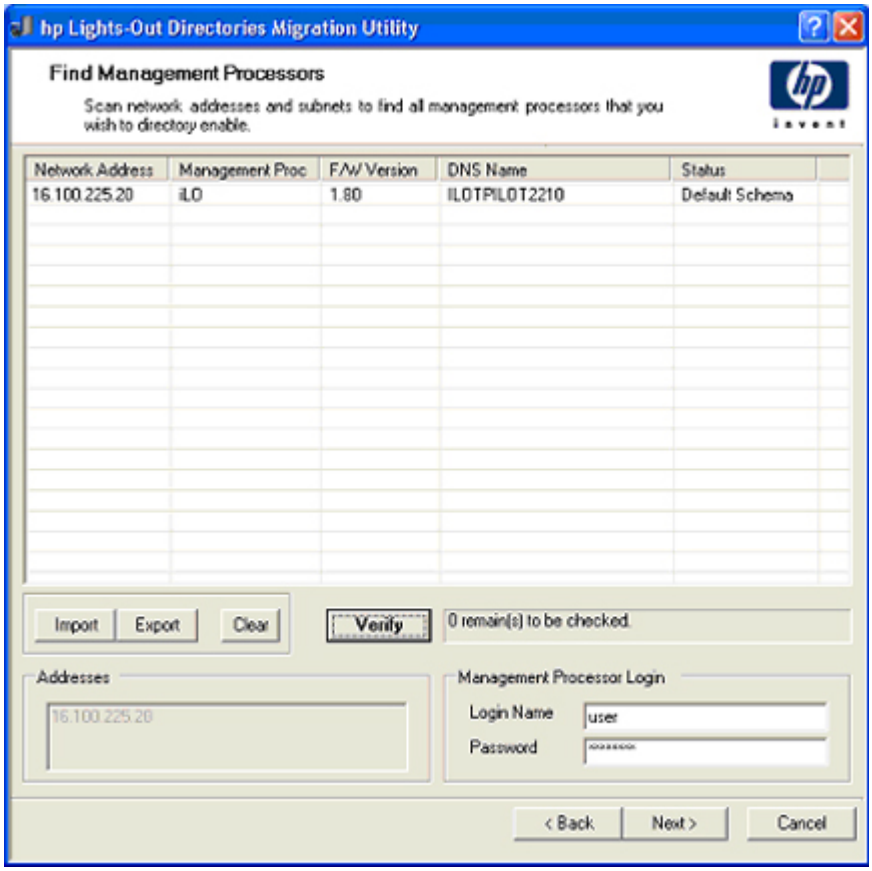
The `HPLOMIG` utility automates the process of migrating management processors by creating objects in the directory corresponding to each management processor and associating them to a role. HPLOMIG has a GUI and provides the user with a wizard approach to implementing or upgrading large amounts of management processors.

Finding management processors

The first step to migrating is to discover all management processors you want to enable for directory services. You can search for management processors using DNS names, IP addresses, or IP address wildcards. The following rules apply to the variables entered in the Addresses field:

- 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 also be specified using a hyphen. For example, 192.168.0.2-10 is a valid range. A hyphen is only supported in the rightmost octet.
- After you click **Find**, HPLOMIG 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**, **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** to start the migration process.
2. Click **Next** to move past the Welcome screen.
3. Enter the variables to perform the management processor search in the Addresses field.
4. Enter your login name and password, and click **Find**. The Find button changes to Verify when the search is complete.

   You can also input a list of management processors by clicking **Import**. The file is a simple text file with one management processor listed per line. The fields are delimited with semicolons. The fields are as follows:

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

   For example, one line could have:

   ```
   16.100.225.20;iLO;1.80;ILOTPILOT2210;user;password;Default Schema
   ```

   If for security reasons the user name and password cannot be in the file, then leave these fields blank, but keep the semicolons.

Upgrading firmware on management processors

The Upgrade Firmware screen enables you to update the management processors to the firmware version that supports directories. This screen also enables you to designate the location of the firmware image for each management processor by either entering the path or clicking **Browse.**

NOTE: 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 at http://www.hp.com/servers/lights-out.

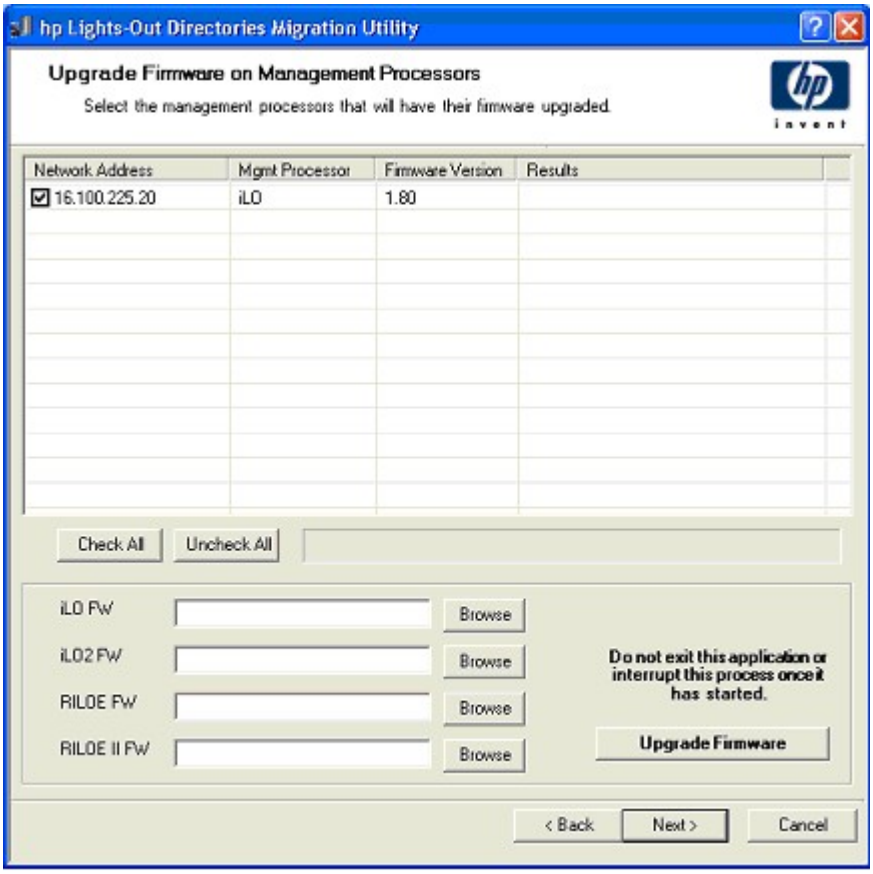
Management processor	Minimum firmware version
iLO 2	1.00

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 `HPLOMIG` continues to upgrade the other discovered management processors.

NOTE: 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.

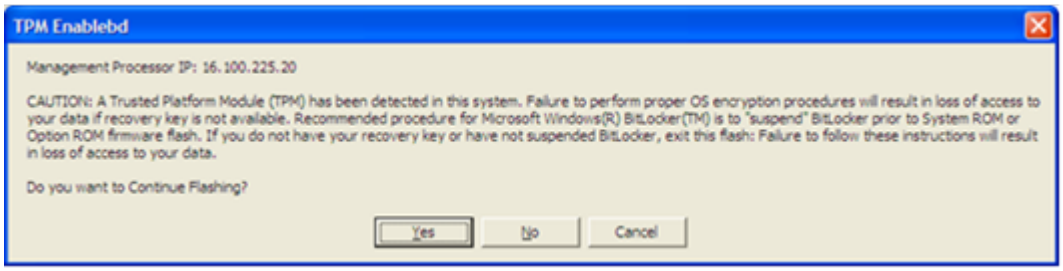
To upgrade the firmware on your management processors:

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 this utility enables you to upgrade hundreds of management processors, only 25 management processors are upgraded simultaneously. Network activity is considerable during this process.
4. After the upgrade is complete, click **Next**.



During the firmware upgrade process, all buttons are deactivated to prevent navigation. You can still close the application using the "X" at the top right of the screen. 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.

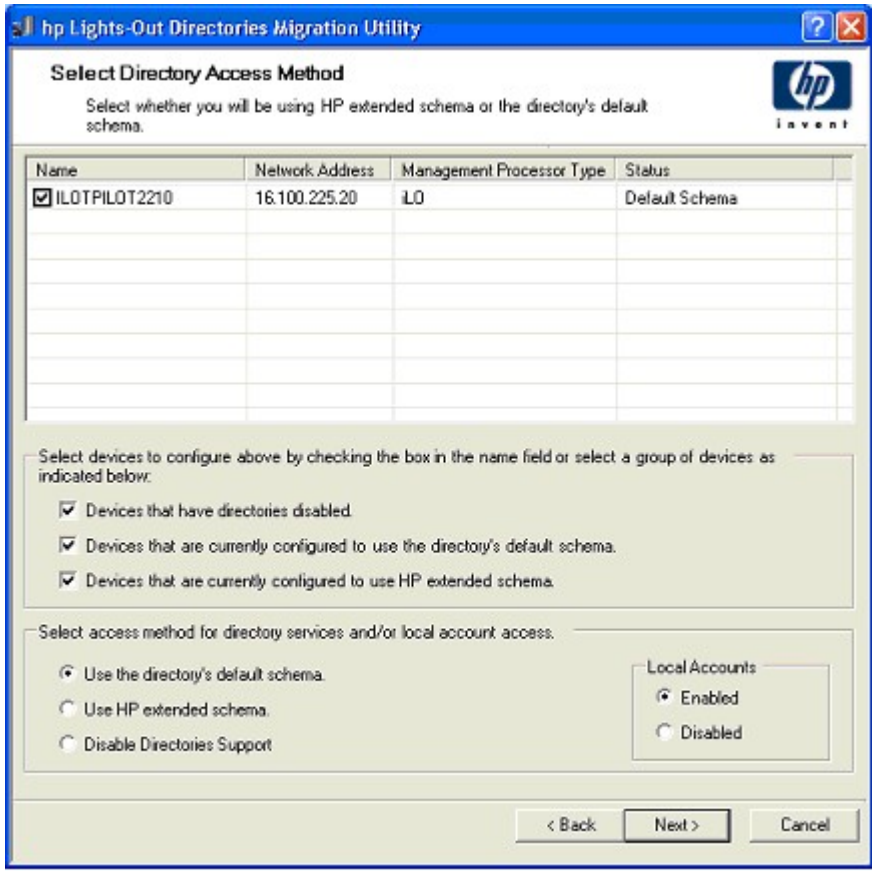
HPLOMIG supports firmware flash on servers with a TPM chip. If a TPM module is present and enabled in the server and Optional ROM measuring is enabled, HPLOMIG displays a warning message (shown below.) If you select Yes, HPLOMIG will continue with the flash process. Otherwise firmware flash on the selected server is skipped. This message displays every time a server with a TPM module is detected during firmware flash.



Selecting a directory access method

After the Firmware Upgrade page, the Select Directory Access Method page displays. You can select which management processors to configure (with respect to schema usage) and how it will be configured. The Select Directory Access Method page helps to prevent an accidental overwrite of iLO 2s already configured for HP schema or those that have directories turned off.

This 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 "Configuring directories when HP Extended schema is selected" (page 168).
- Schema-free (default schema) directories support, see "Setting up Schema-free directory integration" (page 132).

Naming management processors

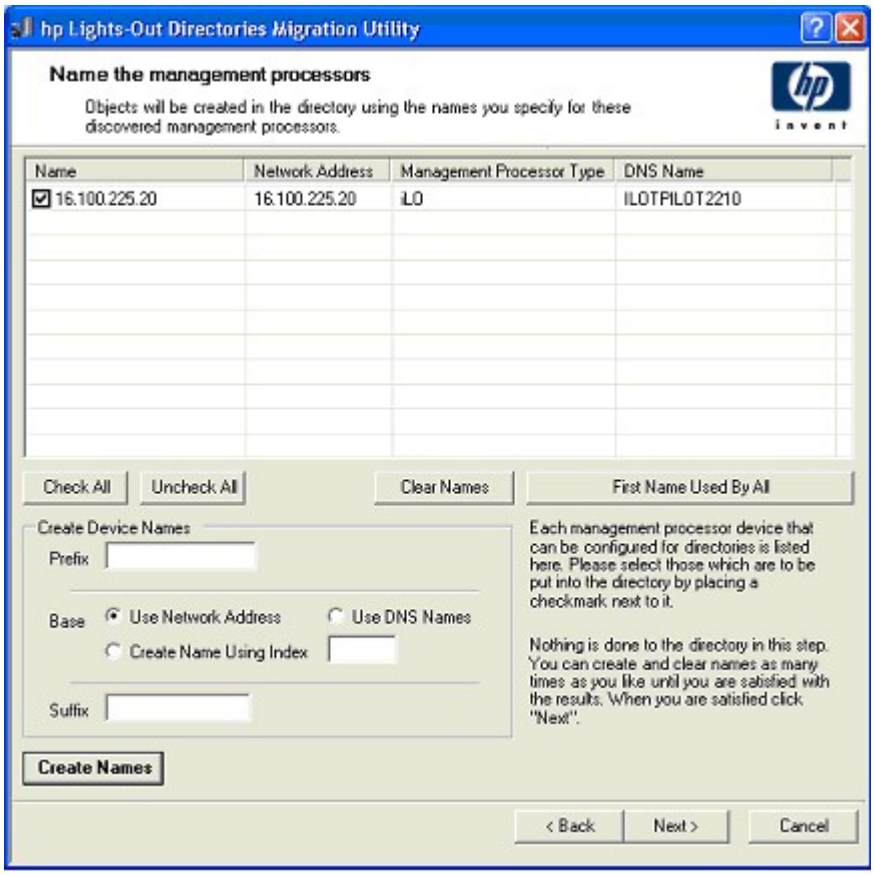
This screen enables you to name Lights-Out management device objects in the directory and create corresponding device objects for all management processors to be managed. You can create names using one or more of the following:

- The network address
- The DNS name
- An index
- Creating the name manually
- Adding a prefix to all
- Adding a suffix to all

To name the management processors, click the **Name** field, and enter the name, or:

1. Select **Use Network Address**, **Use DNS Names**, or **Create Name Using Index**. You can also name each management processor directory object by clicking twice in the name field with a delay between clicks.
2. Enter the text to add (suffix or prefix) to all names (optional).
3. Click **Generate Names**. The names display in the Name column as they are generated. At this point, names are not written to the directory or the management processors. The names are stored until the next page.

4. To change the names (optional), 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

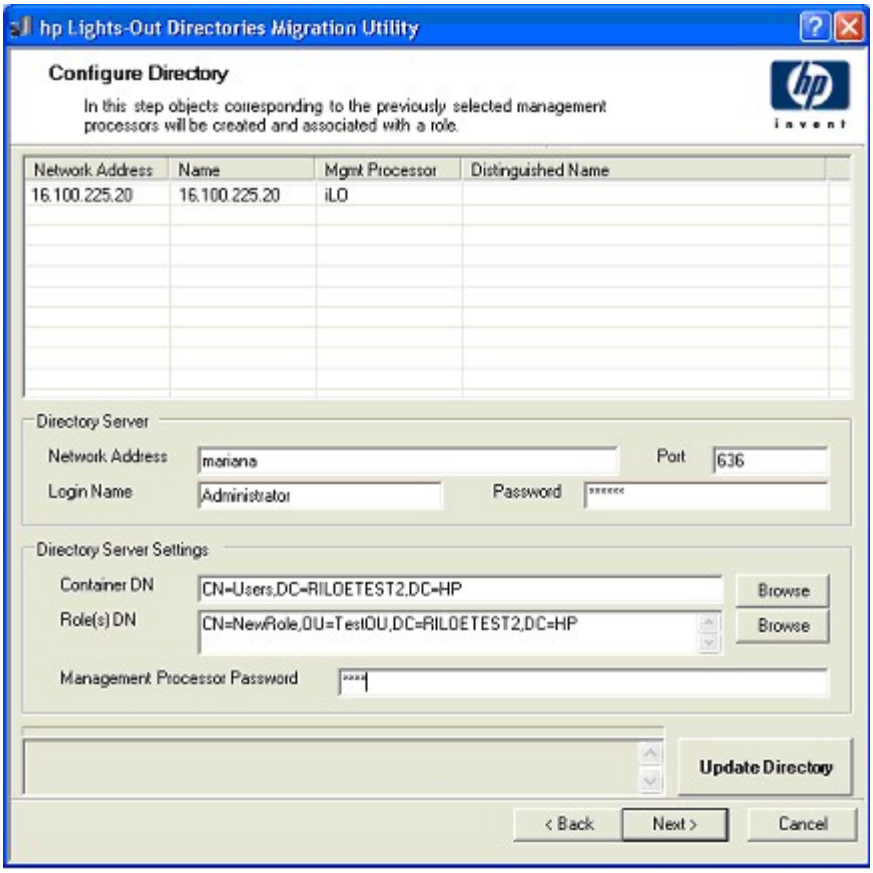
The Configure Directory screen enables you to create a device object for each discovered management processor and to associate the new device object to a previously defined role. For example, the directory defines a user as a member of a role (such as administrator) who has a collection of privileges on a specific device object (such as a RILOE II card).

The fields in the Configure Directory screen are:

- **Network Address** – The network address of the directory server and can either be a valid DNS name or IP address.
- **Port** – The SSL port to the directory. The default entry is 636. Management processors can only communicate with the directory using SSL.
- **Login Name** and **Password** – These fields are used to log in with an account that has domain administrator access to the directory.
- **Container DN** – After you have the network address, port, and login information, you can click **Browse** to navigate for the container and role distinguished name. The container Distinguished Name is where the migration utility will create all of the management processor objects in the directory.
- **Role DN** – The role distinguished name is where the role to be associated with the device objects resides and must be created before to running this utility.

To configure the device objects to be associated with a role:

1. Enter the network address, login name, and password for the designated directory server.
2. Enter the container distinguished name 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 tool connects to the directory, creates the management processor objects, and adds them to the selected roles.
5. After the device objects have been associated with a role, click **Next**.

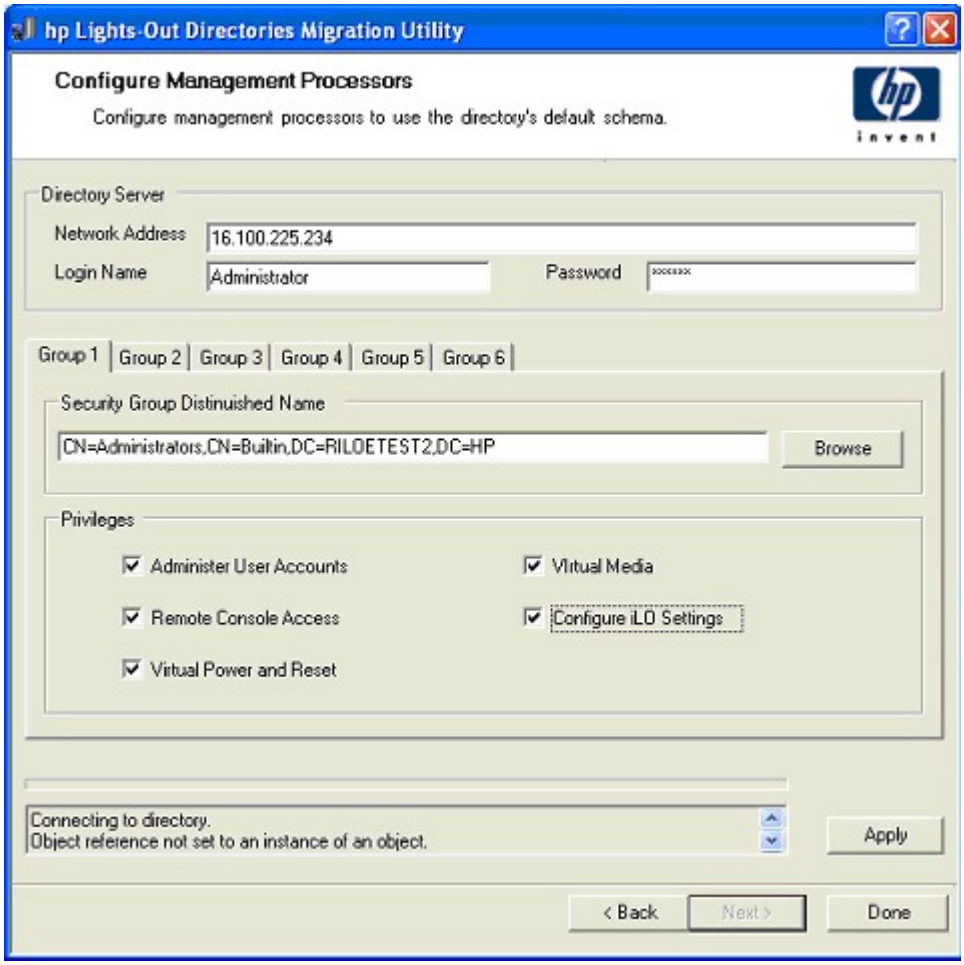


Configuring directories when schema-free integration is selected

The fields in the Configure Management Processors screen are:

- **Network Address** – The network address of the directory server, which can be a valid DNS name or IP address.
- **Login Name** and **Password** – These fields are used to log in with an account that has domain administrator access to the directory.
- **Security Group Distinguished Name** – The distinguished name of the group in the directory that contains a set of iLO 2 users with a common set of privileges. If the directory name, login name, and password are correct, you can click the **Browse** button to navigate to and select the group.
- **Privileges** – The iLO 2 privileges associated with the selected group. The login privilege is implied if the user is a member of the group.

Configure Management Processors settings are stored until the next page in the wizard.



Setting up management processors for directories

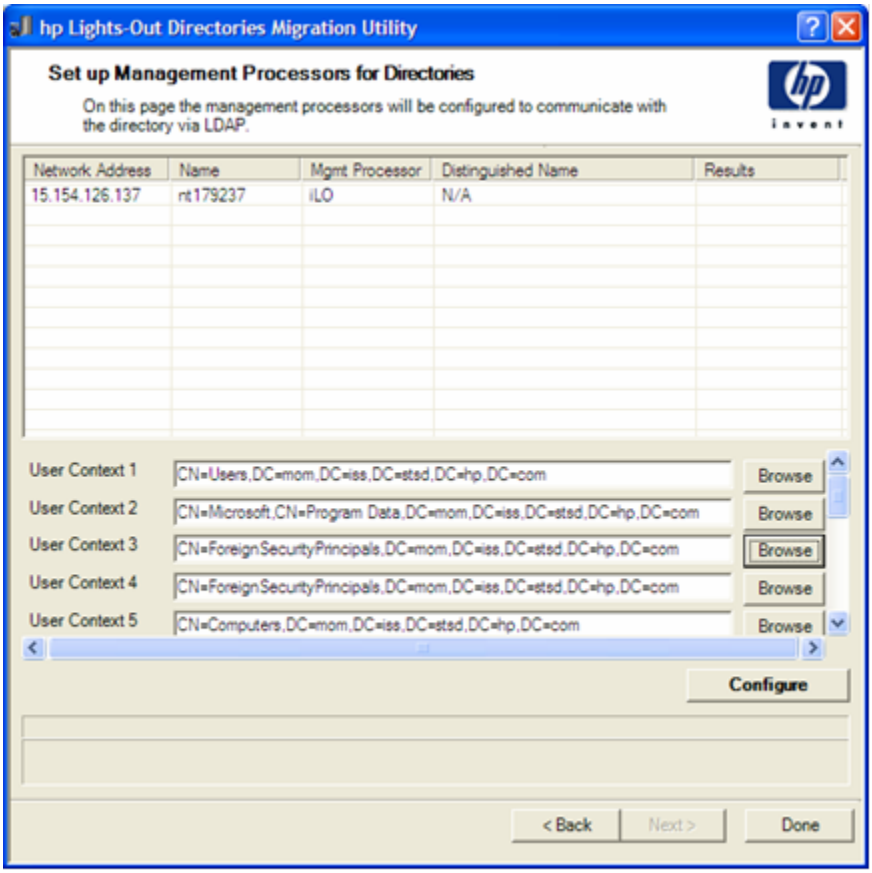
The last step in the migration process is to configure the management processors to communicate with the directory. This screen enables you to create user contexts.

User contexts enable the user to use short or user object names to log in, rather than the full distinguished name. 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 the configuration as you have specified. `HPLOMIG` supports configuring 15 user contexts. To access the user context fields, use the scroll bar.



When you click Configure, `HPLOMIG` displays the following message:



The message indicates that, all 15 User contexts are applicable to only iLO 2 machines with supported firmware version (1.75 or later.) For all other management processors, only the first three User Context fields are applicable.

4. When the process completes, click **Done**.

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" (page 172)
- "Core attributes" (page 172)

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 are satisfied for unexceptional network clients. If this attribute is FALSE, then IP restrictions are 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 must 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.

6 HP Systems Insight Manager integration

Integrating iLO 2 with HP SIM

iLO 2 fully integrates with HP SIM 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 iLO 2 using HP SIM.

Integration with HP SIM provides:

- Support for SNMP trap delivery to a HP SIM console

  Delivery to a HP SIM console can be configured to forward SNMP traps to a pager or e-mail.

- Support for SNMP management

  HP SIM is allowed to access the Insight Management Agents information through iLO 2.

- Support for a management processor

  HP SIM adds support for a new device type, the management processor. All iLO 2 devices installed in servers on the network are discovered in HP SIM as management processors. The management processors are associated with the servers in which they are installed.

- Grouping of iLO 2 management processors

  All iLO 2 devices can be grouped together logically and displayed on one page. This capability provides access to iLO 2 from one point in HP SIM.

- iLO 2 hyperlinks

  HP SIM provides a hyperlink on the server device page to launch and connect to iLO 2.

- HP Management Agents

  iLO 2, combined with HP Management Agents, provides remote access to system management information through the iLO 2 browser-based interface.

HP SIM functional overview

HP SIM enables you to:

- Identify iLO 2 processors.
- Create an association between iLO 2 and its server.
- Create links between iLO 2 and its server.
- View iLO 2 and server information and status.
- Control the amount of detailed information displayed for iLO 2.
- 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 HP SIM, see the *HP Systems Insight Manager Technical Reference Guide,* provided with HP SIM and available on the HP website (http://www.hp.com/go/hpsim).

Establishing SSO with HP SIM

1. Browse to an iLO 2 and login using Administrator credentials.
2. Select the **Administration** tab
3. In the menu, select **Security**.
4. Select the **HP SIM SSO** tab.
5. Set Single Sign-On Trust Mode to **Trust by Certificate**, and click **Apply**.

6. Click **Add HP SIM Server**. The HP Systems Insight Manager Single Sign-On Settings page displays.
7. In Retrieve and import a certificate from a trusted HP SIM Server, enter the hostname or IP address of the HP SIM Server, and click **Import Certificate**. The server is added to the HP SIM trusted servers list on the HP SIM SSO tab.
8. Log in to the HP SIM you entered in step 7 and discover this `<LOM_server_name>`. After completing the discovery process, SSO is enabled for this iLO 2.

   For more information on Discovery tasks, see your *HP Systems Insight Manager Technical Reference Guide*. For more information on iLO 2 SSO options, see "HP SIM single sign-on (SSO)" (page 55).

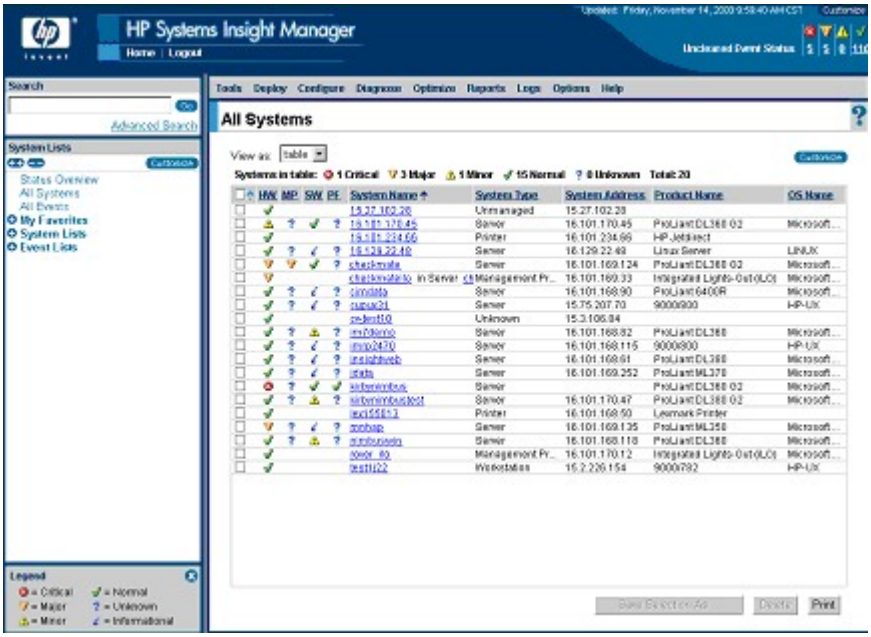
HP SIM identification and association

HP SIM can identify an iLO 2 processor and create an association between iLO 2 and server. The administrator of the LOM device can configure iLO 2 to respond to HP SIM identification requests.

HP SIM status

In HP SIM, iLO 2 is identified as a management processor. HP SIM displays the management processor status within the Systems List.

The iLO 2 management processor appears 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, see the *HP Systems Insight Manager Technical Reference Guide* located on the HP website at http://www.hp.com/go/hpsim.

HP SIM links

For ease of management, HP SIM creates links to the following locations:

- iLO 2 and the host server from any System List
- The server from the System Page of iLO 2
- iLO 2 from the System Page of the server

The Systems List pages display iLO 2, the server, and the relationship between iLO 2 and server. For example, the page can display the server, the iLO 2 name next to the server, and *iLO 2 name* IN *server* in the System Name field for iLO 2.

Clicking a status icon for iLO 2 takes you to the iLO 2 Web interface. Clicking the hardware status icon takes you to the Insight Management Agents for the device. Clicking the iLO 2 or server name takes you to the System Page of the device. Within the System Page are the Identity, Tools & Links, and Event tabs. These tabs provide identity and status information, event information, and links for the associated device.

HP SIM systems lists

iLO 2 management processors can be viewed within HP SIM. A user with full configuration rights can create and use customized system collections to group management processors. Foadditional details, see the *HP Systems Insight Manager Technical Reference Guide* provided with HP SIM and available on the HP website at http://www.hp.com/go/hpsim.

Receiving SNMP alerts in HP SIM

You can configure iLO 2 to forward alerts from the host operating system management agents and to send iLO 2-generated alerts to HP SIM.

HP SIM provides support for full SNMP management, and iLO 2 supports SNMP trap delivery to HP SIM. You can view the event log, select the event, and view the additional information about the alert.

Configuring receipt of SNMP alerts in HP SIM is a two-step process. The process requires HP SIM to discover iLO 2 and configuring iLO 2 to enable SNMP alerts.

1. To enable iLO 2 to send SNMP traps click **SNMP/Insight Manager Settings** on the Administration tab of the iLO 2 navigation frame to enable SNMP alerting and to provide an SNMP trap IP address to iLO 2. This IP address must be the address of the computer running HP SIM. For more information, see "Enabling SNMP alerts" (page 65).
2. To discover iLO 2 in HP SIM configure iLO 2 as a managed device for HP SIM. Adding iLO 2 to HP SIM allows the NIC interface on iLO 2 to function as a dedicated management port, isolating management traffic from the remote host server NIC interface.
   a. Start HP SIM.
   b. Select **Options>Discovery>Automatic Discovery**.
   c. Select the discovery task to run, and click **Edit**.
   d. Select **IP range pinging**. If the IP address is not in the Ping inclusion ranges, templates, or hosts files section, enter the IP address.
   e. Click **OK**.
   f. To add iLO 2 to HP SIM, do one of the following:
      - Click **Save and Run**. After the discovery process is complete, additional queries display the device as a management processor.

        You might have to edit the SNMP read community string (for example, by changing it to `public`) so that iLO 2 appears in the list of monitored systems. You can change the SNMP read community string by accessing the Systems Protocol Settings page. To access these settings, select **Options>Protocol Settings>System Protocol Settings.**
      - Click **Options>Protocol Settings>Global Protocol Settings**, and set community strings for use during discovery under Default SNMP Settings. When set, you can use steps a through e to run discovery process.

For major events not cleared, iLO 2 traps appear in All Events. Click **Event Type** to obtain further information about the event.

NOTE: HP Insight Agents for iLO 2 must be installed on the remote host server to enable management of iLO 2. Refer to "Installing iLO 2 Device Drivers" for additional details about installing and configuring agents.

HP SIM port matching

HP SIM is configured to start an HTTP session to check for iLO 2 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 HP SIM.

To change the port number in HP SIM, add the port to the `config\identification\additionalWsDisc.props` file in the directory where HP SIM is installed. The entry must start with the HTTP port for iLO 2. No entry needs to be in this file for iLO 2 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 iLO 2 is to be discovered at port 55000 (this must all be on one line in the file):

55000`=iLO 2,,true,false,com.hp.mx.core.tools.identification.mgmtproc.MgmtProcessorParser`

Reviewing Advanced Pack license information in HP SIM

HP SIM displays the license status of the iLO 2 management processors. You can use this information to determine how many and which iLO 2 devices are licensed for the iLO Advanced Pack.

To view license information, click **Deploy>License Manager>Manage Keys**. To be sure the data is current, run the identify systems task for your management processors. For additional details about initiating tasks, see the HP SIM documentation.

7 Troubleshooting iLO 2

iLO 2 POST LED indicators

During the initial boot of iLO 2, the POST LED indicators flash to display the progress through the iLO 2 boot process. After the boot process is complete, the HB LED flashes every second. LED 7 also flashes intermittently during normal operation.

The LED indicators (1 through 6) light up after the system has booted to indicate a hardware failure. If a hardware failure is detected, reset iLO 2. For the location of the LED indicators, refer to the server documentation.

A runtime failure of iLO 2 is indicated by HB and LED 7 remaining in either the On or Off state constantly. A runtime failure of iLO 2 can also be indicated by a repeated flashing pattern on all eight LEDs. If a runtime error occurs, reset iLO 2.

A sequential flashing pattern on LEDs, 1, 2, 3, 4, 5, 6, 7, and 8, repeating indefinitely, indicates iLO 2 has experienced a failed flash (firmware upgrade) and is in the flash recovery mode. Refer to the "iLO network flash recovery" section for more information.

The LED indicators have the following assignments:

HB	7	6	5	4	3	2	1

LED indicator	POST code (activity completed)	Description	Failure indicated
None	00	Set up chip selects.	
1 or 2	02 Normal operation	Determine platform.	
2 and 1	03	Set RUNMAP bit.	
3	04	Initialize SDRAM controller.	
3 and 2	06	Activate the I cache.	
3, 2, and 1	07	Initialize (only) the D cache.	
4	08	Copy secondary loader to RAM.	Could not copy secondary loader.
4 and 1	09	Verify secondary loader.	Did not execute secondary loader.
4 and 2	0a	Begin secondary loader.	SDRAM memory test failed.
4, 2, and 1	0b	Copy ROM to RAM.	Could not copy boot block.
4 and 3	0c	Verify ROM image in RAM.	Boot block failed to execute.
4, 3, and 1	0d	Boot Block Main started.	Boot block could not find a valid image.
None		Start C Run time initialization.	
4, 3, and 2	0e	Main() has received control.	Main self-test failed.
Varies	Varies	Each subsystem might self-test.	
4, 3, 2, and 1	0f	Start ThreadX.	RTOS startup failed.

LED indicator	POST code (activity completed)	Description	Failure indicated
None	00	Main_init() completed.	Subsystem startup failed.
HB and 7		Flashes as the iLO 2 processor executes firmware code. It does not change the value of the lower six LEDs.	

The iLO 2 microprocessor firmware includes code that makes consistency checks. If any of these checks fail, the microprocessor executes the FEH. The FEH presents information using the iLO 2 POST LED indicators. The FEH codes are distinguished by the alternating flashing pattern of the number 99 plus the remainder of the error code.

FEH code	Consistency check	Explanation
9902	TXAPICHK	An RTOS function was called with an inappropriate value or from an inappropriate caller.
9903	TXCONTEXT	The saved context of one or more threads has been corrupted.
9905	TRAP	A stack probe failed, the return address is invalid, or an illegal trap instruction has been detected.
9966	NMIWR	An unexpected write to low memory has occurred.
99C1	CHKNULL	The reset vector has been modified.

Event log entries

Event log display	Event log explanation
Server power failed	Displays when the server power fails.
Browser login: *IP address*	Displays the IP address for the browser that logged in.
Server power restored	Displays when the server power is restored.
Browser logout: *IP address*	Displays the IP address for the browser that logged out.
Server reset	Displays when the server is reset.
Failed Browser login—IP Address: *IP address*	Displays when a browser login fails.
iLO 2 Self Test Error: #	Displays when iLO 2 has failed an internal test. The probable cause is that a critical component has failed. Further use of iLO 2 on this server is not recommended.
iLO 2 reset	Displays when iLO 2 is reset.
On-board clock set; was #:#:#:#:#:#	Displays when the onboard clock is set.
Server logged critical error(s)	Displays when the server logs critical errors.
Event log cleared by: *User*	Displays when a user clears the event log.
iLO 2 reset to factory defaults	Displays when iLO 2 is reset to the default settings.
iLO 2 ROM upgrade to #	Displays when the ROM has been upgraded.
iLO 2 reset for ROM upgrade	Displays when iLO 2 is reset for the ROM upgrade.
iLO 2 reset by user diagnostics	Displays when iLO 2 is reset by user diagnostics.
Power restored to iLO 2	Displays when the power is restored to iLO 2.

Event log display	Event log explanation
iLO 2 reset by watchdog	Displays when an error has occurred in iLO 2 and iLO 2 has reset itself. If this issue persists, call customer support.
iLO 2 reset by host	Displays when the server resets iLO 2.
Recoverable iLO 2 error, code #	Displays when a non-critical error has occurred in iLO 2 and iLO 2 has reset itself. If this issue persists, call customer support.
SNMP trap delivery failure: *IP address*	Displays when the SMNP trap does not connect to the specified IP address.
Test SNMP trap alert failed for: *IP address*	Displays when the SNMP trap does not connect to the specified IP address.
Power outage SNMP trap alert failed for: *IP address*	Displays when the SNMP trap does not connect to the specified IP address.
Server reset SNMP trap alert failed for: *IP address*	Displays when the SNMP trap does not connect to the specified IP address.
Illegal login SNMP trap alert failed for: *IP address*	Displays when the SNMP trap does not connect to the specified IP address.
Diagnostic error SNMP trap alert failed for: *IP address*	Displays when the SNMP trap does not connect to the specified IP address.
Host generated SNMP trap alert failed for: *IP address*	Displays when the SNMP trap does not connect to the specified IP address.
Network resource shortage SNMP trap alert failed for: *IP address*	Displays when the SNMP trap does not connect to the specified IP address.
iLO 2 network link up	Displays when the network is connected to iLO 2.
iLO 2 network link down	Displays when the network is not connected to iLO 2.
iLO 2 Firmware upgrade started by: *User*	Displays when a user starts a firmware upgrade.
Host server reset by: *User*	Displays when a user resets the host server.
Host server powered OFF by: *User*	Displays when a user powers off a host server.
Host server powered ON by: *User*	Displays when a user powers on a host server.
Virtual Floppy in use by: *User*	Displays when a user begins using a Virtual Floppy.
Remote Console login: *User*	Displays when a user logs on a Remote Console session.
Remote Console Closed	Displays when a Remote Console session is closed.
Failed Console login - IP Address: *IP address*	Displays a failed console login and IP address.
Added User: *User*	Displays when a local user is added.
User Deleted by: *User*	Displays when a local user is deleted.
Modified User: *User*	Displays when a local user is modified.
Browser login: *User*	Displays when a valid user logs on to iLO 2 using an Internet browser.
Browser logout: User	Displays when a valid user logs off iLO 2 using an Internet browser.
Failed Browser login—IP Address: *IP address*	Displays when a browser login attempt fails.
Remote Console login: *User*	Displays when an authorized user logs on using the Remote Console port.

Event log display	Event log explanation
Remote Console Closed	Displays when an authorized Remote Console user is logged out or when the Remote Console port is closed following a failed login attempt.
Failed Console login—IP Address: *IP address*	Displays when an unauthorized user has failed three login attempts using the Remote Console port.
Added User: *User*	Displays when a new entry is made to the authorized user list.
User Deleted by: *User*	Displays when an entry is removed from the authorized user list. The User section displays the user who requested the removal.
Event Log Cleared: *User*	Displays when the user clears the Event Log.
Power Cycle (Reset): *User*	Displays when the power has been reset.
Virtual Power Event: *User*	Displays when the Virtual Power Button is used.
Security Override Switch Setting is On	Displays when the system is booted with the Security Override Switch set to On.
Security Override Switch Setting Changed to Off	Displays when the system is booted with the Security Override Switch changed from On to Off.
On-board clock set; was previously "[NOT SET]"	Displays when the on-board clock is set. Will display the previous time or "NOT SET" if there was not a time setting previously.
Logs full SNMP trap alert failed for: *IP address*	Displays when the logs are full and the SNMP trap alert failed for a specified IP address.
Security disabled SNMP trap alert failed for: *IP address*	Displays when the security has been disabled and the SNMP trap alert failed for a specified IP address.
Security enabled SNMP trap alert failed for: *IP address*	Displays when the security has been enabled and the SNMP trap alert failed for a specified IP address.
Virtual Floppy connected by *User*	Displays when an authorized user connects the Virtual Floppy.
Virtual Floppy disconnected by *User*	Displays when an authorized user disconnects the Virtual Floppy.
License added by: *User*	Displays when an authorized user adds a license.
License removed by: *User*	Displays when an authorized user removes a license.
License activation error by: *User*	Displays when there is an error activating the license.
iLO 2 RBSU user login: *User*	Displays when an authorized user logs in to iLO 2 RBSU.
Power on request received by: *Type*	A power request was received as one of the following types: Power Button Wake On LAN Automatic Power On
Virtual NMI selected by: *User*	Displays when an authorized user selects the Virtual NMI button.
Virtual Serial Port session started by: *User*	Displays when a Virtual Serial Port session is started.
Virtual Serial Port session stopped by: *User*	Displays when a Virtual Serial Port session is ended.
Virtual Serial Port session login failure from: *User*	Displays when there is a login failure for a Virtual Serial Port session.

Hardware and software link-related issues

iLO 2 uses standard Ethernet cabling, which includes CAT5 UTP with RJ-45 connectors. Straight-through cabling is necessary for a hardware link to a standard Ethernet hub. Use a crossover cable for a direct PC connection.

The iLO 2 Management Port must be connected to a network that is connected to a DHCP server, and iLO 2 must be on the network before power is applied. DHCP sends a request soon after power is applied. If the DHCP request is not answered when iLO 2 first boots, then it will reissue the request at 90-second intervals.

The DHCP server must be configured to supply DNS and WINS name resolution. iLO 2 can be configured to work with a static IP address either in the F8 option ROM setup or from the Network Settings Web page.

The default DNS name appears on the network settings tag and can be used to locate iLO 2 without knowing the assigned IP address.

If a direct connection to a PC is used, then a static IP address must be used because there is no DHCP server on the link.

Within the iLO 2 RBSU, to view the status of iLO 2 DHCP requests, you can press the **F1** key inside the DNS/DHCP page for advanced options.

JVM support

To ensure that the iLO 2 Remote Console applet and Virtual Media applet operate as expected, install Java Runtime Environment, Standard Edition 1.4.2_13. The iLO 2 firmware now supports 64-bit Java for browsers and JVM/JRE. To locate the link to the latest supported version of JRE, from the iLO 2 browser interface, select **Remote Console>Settings>Java.**

The iLO 2 Remote Console, Remote Serial Console, and Virtual Media applets require that JVM be installed on the client server. If the Remote Console and Virtual Media applets are accessed using a version of Java Runtime Environment Standard Edition that is later than 1.4.2_13, the applets can function incorrectly. If you are using another JVM version, you might experience the following:

- If the Remote Console applet is opened with Java Runtime Environment Version 1.5.x or 1.6.x, you might experience the following:
  - The message Automation server cannot create object appears. If you click **OK,** the message disappears and the applet functions normally.
  - The TAB key does not function properly. The TAB key moves around the various portions of the Remote Console applet window, instead of moving inside the applet itself.
- If the Virtual Media applet is opened with Java Runtime Environment Version 1.5.x or Version 1.6.x, you might experience the following:
  - When you click the **Create Disk Image** button, another window appears. The window might appear with the Create and Cancel buttons missing, or appear as only text. If the window is closed and reopened, the buttons eventually appear correctly.
  - When you select an image file in the applet, a file select window appears. After you select a file, the window closes and returns to the regular applet window. However, the image file area is not updated, and the applet appears unresponsive. To update the original Virtual Media applet window and enable it to retain focus in the system, click a separate window. The applet appears unresponsive until the Virtual Media applet window is closed and reopened.

Login issues

Use the following information when attempting to resolve login issues:

- Try the default login, which is located on the network settings tag.
- If you forget your password, an administrator with the Administer User Accounts privilege can reset it.
- If an administrator forgets his or her password, the administrator must use the Security Override Switch or establish an administrator account and password using HPONCFG.
- Check for standard issues, such as:
  - Is the password complying with password restrictions? For example, are there case-sensitive characters in the password?
  - Is an unsupported browser being used?

Login name and password not accepted

If you have connected to iLO 2 but it does not accept your login name and password, you must verify that your login information is configured correctly. Have a user who has the Administer User Accounts privilege log in and change your password. If you are still unable to connect, have the user log in again and delete and re-add your user account.

NOTE: The RBSU can also be used to correct login issues.

Directory user premature logout

Network errors can cause iLO 2 to conclude that a directory connection is no longer valid. If iLO 2 cannot detect the directory, iLO 2 terminates the directory connection. Any additional attempts to continue using the terminated connection redirects the browser to the Login page.

Redirection to the Login page can appear to be a premature session timeout. A premature session timeout can occur during an active session if:

- The network connection is severed.
- The directory server is shut down.

To recover from a premature session timeout, log back in and continue using iLO 2. If the directory server is unavailable, you must use a local account.

iLO 2 Management Port not accessible by name

The iLO 2 Management Port can register with a WINS server or DDNS server to provide the name-to-IP address resolution necessary to access the iLO 2 Management Port by name. The WINS or DDNS server must be up and running before the iLO 2 Management Port is powered on, and the iLO 2 Management Port must have a valid route to the WINS or DDNS server.

In addition, the iLO 2 Management Port must be configured with the IP address of the WINS or DDNS server. You can use DHCP to configure the DHCP server with the necessary IP addresses. You can also enter the IP addresses through RBSU or by selecting **Network Settings** on the Administration tab. The iLO 2 Management Port must be configured to register with either a WINS server or DDNS server. These options are turned on as factory defaults and can be changed through RBSU or by selecting the **Network Settings** option on the Administration tab.

The clients used to access the iLO 2 Management Port must be configured to use the same DDNS server where the IP address of the iLO 2 Management Port was registered.

If you are using a WINS server and a non-dynamic DNS server, the access to the iLO 2 Management Port might be significantly faster if you configure the DNS server to use the WINS server for name resolution. Refer to the appropriate Microsoft documentation for more information.

iLO 2 RBSU unavailable after iLO 2 and server reset

If the iLO 2 processor is reset and the server is immediately reset, there is a small chance that the iLO 2 firmware will not be fully initialized when the server performs its initialization and attempts to invoke the iLO 2 RBSU. In this case, the iLO 2 RBSU is unavailable or the iLO 2 Option ROM code is skipped altogether. If this situation occurs, reset the server a second time. To avoid this issue, wait a few seconds before resetting the server after resetting the iLO 2 processor.

Inability to access the login page

If you cannot access the login page, you must verify the SSL encryption level of your browser is set to 128 bits. The SSL encryption level in iLO 2 is set to 128 bits and cannot be changed. The browser and iLO 2 encryption levels must be the same.

Inability to access iLO 2 using Telnet

If you cannot access iLO 2 using Telnet, you must verify the Remote Console Port Configuration and Remote Console Data Encryption on the Global Settings screen. If Remote Console Port Configuration is set to Automatic, the Remote Console applet enables port 23, starts a session, and then closes port 23 when the session is completed. Telnet cannot automatically enable port 23, so it fails.

Inability to access virtual media or graphical remote console

Virtual media and graphical Remote Console are only enabled by licensing the optional iLO Advanced Pack. A message appears, informing the user that the features are not available without a license. Although up to 10 users are allowed to log in to iLO 2, only one user can access the remote console. A warning message appears indicating that the Remote Console is already in use.

Inability to connect to iLO 2 after changing network settings

Verify that both sides of the connection, the NIC and the switch, have the same settings for transceiver speed autoselect, speed, and duplex. For example, if one side is autoselecting the connection, then the other side must as well. The settings for the iLO 2 NIC are controlled in the Network Settings screen.

Inability to connect to the iLO 2 Diagnostic Port

If you cannot connect to the iLO 2 Diagnostic Port through the NIC, be aware of the following:

- The use of the diagnostic port is automatically sensed when an active network cable is plugged in to it. When switching between the diagnostic and back ports, allow one minute for the network switchover to be complete before attempting to connect through the web browser.
- If a critical activity is in progress, the diagnostic port cannot be used until the critical activity is complete. Critical activities include the following:
  - Firmware upgrade
  - Remote Console session
  - SSL initialization
- If you are using a client workstation that contains more than one enabled NIC, such as a wireless card and a network card, a routing issue might prevent you from accessing the diagnostic port. To resolve this issue:

1. Have only one active NIC on the client workstation. For example, disable the wireless network card.
2. Configure the IP address of the client workstation network to match the iLO 2 Diagnostic Port network so that the following conditions are met:
   - The IP address setting is 192.168.1.*X*, where *X* is any number other than 1, because the IP address of the diagnostic port is set at `192.168.1.1`.
   - The subnet mask setting is `255.255.255.0`.

Inability to connect to the iLO 2 processor through the NIC

If you cannot connect to the iLO 2 processor through the NIC, try any or all of the following troubleshooting methods:

- Confirm that the green LED indicator (link status) on the iLO 2 RJ-45 connector is on. This condition indicates a good connection between the PCI NIC and the network hub.
- Look for intermittent flashes of the green LED indicator, which indicates normal network traffic.
- Run the iLO 2 RBSU to confirm that the NIC is enabled and verify the assigned IP address and subnet mask.
- Run the iLO 2 RBSU and use the F1-Advanced tab inside of the DNS/DHCP page to see the status of DHCP requests.
- Ping the IP address of the NIC from a separate network workstation.
- Attempt to connect with browser software by entering the IP address of the NIC as the URL. You can see the iLO 2 Home page from this address.
- Reset iLO 2.

NOTE: If a network connection is established, you might have to wait up to 90 seconds for the DHCP server request.

ProLiant BL p-Class servers have a Diagnostic Port available. Connecting a live network cable to the diagnostic port causes iLO 2 to automatically switch from the iLO 2 port to the diagnostic port. When switching between the diagnostic and back ports, allow one minute for the network switchover to be complete before attempting connection through the browser.

Inability to log in to iLO 2 after installing the iLO 2 certificate

If the iLO 2 self-signed certificate is installed permanently into some browsers and the iLO 2 is reset, you might not be able to log back in to iLO 2 because iLO 2 generates a new self-signed certificate every time it is reset. When a certificate is installed in the browser, it is indexed by the name contained in the certificate. This name is unique to each iLO 2. Every time iLO 2 resets, it generates a new certificate with the same name.

To avoid this issue, do not install the iLO 2 self-signed certificate in the browser certificate store. If you want to install the iLO 2 certificate, a permanent certificate must be requested from a CA and imported into the iLO 2. This permanent certificate can then be installed in the browser certificate store.

Firewall issues

The iLO 2 firmware communicates through several configurable TCP/IP ports. If these ports are blocked, the administrator must configure the firewall to allow for communications on these ports. See the Administration section of the iLO 2 user interface to view or change port configurations.

Proxy server issues

If the Web browser software is configured to use a proxy server, it will not connect to the iLO 2 IP address. To resolve this issue, configure the browser not to use the proxy server for the IP address of iLO 2. For example, in Internet Explorer, select **Tools>Internet Options>Connections>LAN Settings>Advanced**, and then enter the iLO 2 IP address or DNS name in the Exceptions field.

Two-factor authentication error

When attempting to authenticate to iLO 2 using two-factor authentication, you might receive the message `The page cannot be displayed`. This message might appear for the following reasons:

- No user certificates are registered on the client system. To correct this issue, register the necessary user certificate on the client system, which might require software provided by the smart card vendor.
- The user certificate is stored on a smart card or USB token that is not connected to the client system. To correct this issue, connect the appropriate smart card or USB token to the client system.
- The user certificate is not issued by the trusted CA. The trusted CA's certificate is configured in iLO 2 on the Two-Factor Authentication settings page. The certificate configured as the trusted CA, must be the public certificate of the CA that issues certificates in your organization. To correct this issue, configure the appropriate certificate as the trusted CA on the iLO 2 Two-Factor Authentication settings page, or use a user certificate that is issued by the trusted CA which is already configured.
- The user certificate is expired or not yet valid. Regardless of whether the expired certificate maps to a local user, or whether it corresponds to a directory user account, iLO 2 does not allow authentication with a certificate that has expired or that is not yet valid. Check the validity dates of the certificate to verify that this is the cause of the `The page cannot be displayed` message. To correct this, issue a valid certificate to the user. Map the certificate to the local iLO 2 user account if you are authenticating local iLO 2 users and verify the iLO 2 time clock is set correctly.
- The user certificate was not digitally signed with the same certificate that is specified as the trusted CA. Even though the name on the trusted CA certificate might match the issuer of the user certificate, the user certificate might have been digitally signed by a different certificate. View the certification path of the user certificate, and ensure that the public key of the issuing certificate is the same as the public key of the trusted CA certificate. To correct this issue, configure the appropriate certificate as the trusted CA on the iLO 2 Two-Factor Authentication settings page, or use a user certificate that was issued by the trusted CA.

Troubleshooting alert and trap issues

Alert	Explanation
Test Trap	This trap is generated by a user through the Web configuration page.
Server Power Outage	Server has lost power.
Server Reset	Server has been reset.
Failed Login Attempt	Remote user login attempt failed.
General Error	This is an error condition that is not predefined by the hard-coded MIB.
Logs	Circular log has been overrun.
Security Override Switch Changed: On/Off	The state of the Security Override Switch has changed (On/Off).

Alert	Explanation
Rack Server Power On Failed	The server was unable to power on because the BL p-Class rack indicated that insufficient power was available to power on the server.
Rack Server Power On Manual Override	The server was manually forced by the customer to power on despite the BL p-Class reporting insufficient power.
Rack Name Changed	The name of the ProLiant BL p-Class rack was changed.

Inability to receive HP SIM alarms (SNMP traps) fromiLO 2

A user with the Configure iLO 2 Settings privilege must connect to iLO 2 to configure SNMP trap parameters. When connected to iLO 2, be sure that the correct alert types and trap destinations are enabled in the SNMP/Insight Manager Settings screen of the iLO 2 console application.

iLO 2 Security Override switch

The iLO 2 Security Override switch allows emergency access to the administrator with physical control over the server system board. Setting the iLO 2 Security Override switch allows login access, with all privileges, without a user ID and password.

The iLO 2 Security Override switch is located inside the server and cannot be accessed without opening the server enclosure. To set the iLO 2 Security Override switch, the server must be powered off and disconnected from the power source. Set the switch and then power on the server. Reverse the procedure to clear the iLO 2 Security Override switch.

A warning message appears on the iLO 2 Web pages, indicating that the iLO 2 Security Override switch is currently in use. An iLO 2 log entry is added recording the use of the iLO 2 Security Override switch. An SNMP alert can also be sent upon setting or clearing the iLO 2 Security Override switch.

In the unlikely event that it is necessary, setting the iLO 2 Security Override switch also enables you to flash the iLO 2 boot block. The boot block is exposed until iLO 2 is reset. HP recommends that you disconnect iLO 2 from the network until the reset is complete.

Depending on the server, the iLO 2 Security Override switch might be a single jumper or it might be a specific switch position on a dip switch panel. To access the iLO 2 Security Override switch, refer to the server documentation.

Authentication code error message

Within a Mozilla browser, you might receive an incorrect message authentication code error message, which indicates that the public or private key pair and certificate used to initiate the browser SSL session has changed. This error message can occur when you do not use a customer provided certificate, because iLO 2 generates its own self-signed certificate each time it is rebooted.

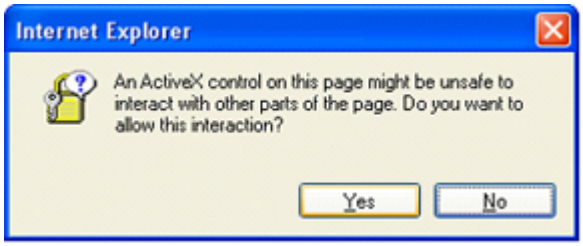
To resolve this, close and restart the Web browser, or install your own certificates into iLO 2.

Troubleshooting directory issues

The following sections discuss troubleshooting directory issues.

Domain/name format login issues

To login using the domain/name format, ActiveX controls must be enabled. To verify that your browser is letting the login script call ActiveX controls open Internet Explorer and set ActiveX controls to **Prompt**.



ActiveX controls are enabled and I see a prompt but the domain/name login format does not work

1. Log in with a local account and determine the directory server name.
2. Verify the directory server name is a name and not an IP address.
3. Verify you can ping the directory server name from your client.
4. Run directory setup tests. Verify the ping was received successfully. For more information on testing directory settings, see "Directory tests" (page 53).

User contexts do not appear to work

Check with your network administrator. The full distinguished name of your user object must be in the directory. Your login name is what appears after the first CN=. The remainder of the distinguished name appears in one of the user context fields. User contexts are not case-sensitive. However, anything else, including spaces are part of the user context.

Directory user does not logout after the directory timeout has expires

If you set the iLO 2 timeout to Infinite timeout, the remote console periodically pings the firmware to verify that the connection exists. When this ping occurs, the iLO 2 firmware queries the Directory for user permissions. This periodic query keeps the Directory connection active, preventing a timeout and logging the user.

Troubleshooting Remote Console issues

The following sections discuss troubleshooting Remote Console issues. In general:

- Pop-up blockers prevent Remote Console and Virtual Serial Port from starting.
- Pop-up blocking applications that are set to prevent the automatic opening of new windows prevent Remote Console and Virtual Serial Port from running. Disable any pop-up blocking programs before starting Remote Console or Virtual Serial Port.

Remote Console applet has a red X when running Linux client browser

Mozilla browsers must be configured to accept cookies.

1. Open the Preferences menu, and select **Privacy & Security>Cookies**.
2. On the Level of Privacy screen, select **Allow cookies based on privacy settings** and click **View**.
3. On the Cookies screen, select **Allow cookies based on privacy settings**.

The level of privacy must be set to **Medium** or **Low**.

Inability to navigate the single cursor of the Remote Console to corners of the Remote Console window

In some cases, you might be unable to navigate the mouse cursor to the corners of the Remote Console window. If so, right-click and drag the mouse cursor outside the Remote Console window and back inside.

If the mouse still fails to operate correctly, or if this situation occurs frequently, verify that your mouse settings match those recommended in "Optimizing mouse performance for Remote Console or Integrated Remote Console" (page 88).

Remote Console no longer opens on the existing browser session

With the addition of the Terminal Services passthrough function, the behavior of the Remote Console applet is slightly different from previous versions of iLO 2 firmware. If a Remote Console session is already open and the Remote Console link is clicked again, then the Remote Console session does not restart. The Remote Console session might appear frozen.

For example, if the following steps are executed:

1. From Client-1, log in to iLO 2 and open a remote console session.
2. From Client-2, log in to iLO 2 and try to open a Remote Console session. The following message displays:

   ```
   Remote console is already opened by another session
   ```

   This is expected because only one Remote Console session is supported at a time.
3. Return to Client-1 and close the Remote Console session.
4. From Client-2, click the **Remote Console** link with the old Remote Console applet still open. The remote console session does not refresh and the old message discussed in step 2 is still displayed.

Although this behavior is different than in previous versions of iLO firmware, this is expected behavior in this version of the iLO firmware. To avoid issues of this nature, always close an open remote console session prior to trying to reopen it.

Remote console text window not updating properly

When using the Remote Console to display text windows that scroll at a high rate of speed, the text window might not update properly. This error is caused by video updates occurring quicker than the iLO 2 firmware can detect and display them. Typically, only the upper left corner of the text window updates while the rest of the text window remains static. After the scrolling is complete, click **Refresh** to properly update the text window.

One known example of this issue is during the Linux booting and posting process, in which some of the POST messages can be lost. A possible result is that a keyboard response is requested by the boot process and might be missed. To avoid this issue, the booting and posting process must be slowed down by editing the Linux startup script to allow more time for keyboard responses.

Remote Console turns gray or black

The Remote Console screen turns gray or black when the server is rebooted from the Terminal Services client. The screen remains gray or black for 30 seconds to one minute. The client closes because the Terminal Services server is not available. The iLO 2 remote console takes over, but the Remote Console screen turns gray or black. When the screen returns, the Remote Console functions normally.

Remote Serial Console troubleshooting

The Remote Serial Console option relies on the Virtual Serial Port. The Virtual Serial Port must be correctly enabled and configured in the host RBSU. You can access the Virtual Serial Port using SSH or Telnet (if enabled). You can access the CLP from a host serial session if the UART and Virtual Serial Port share the same settings. To access the CLP from a host serial session enter **Esc-(** (escape left-parentheses) to switch to the command-line interpreter.

Pop-up blocking applications will prevent the Remote Serial Console option from running. Disable any pop-up blocking programs before starting the Remote Serial Console option.

Troubleshooting Integrated Remote Console issues

Issues with Integrated Remote Console include:

- Issues with Internet Explorer 7
- Apache web server setup for export
- No console playback while server is powered down
- Skipping information during boot and fault buffer playback

Internet Explorer 7 and a flickering remote console screen

Using Internet Explorer 7 with the remote screen can cause the remote console screen to flicker and become difficult to read. Setting the system hardware acceleration to a lower level will help to alleviate the flicker. To change the hardware acceleration level select **Control Panel>Display**, and then select the **Settings** tab. In the Settings section, click **Advanced**. When the Advanced page appears, select the **Troubleshoot** tab. Adjust **Hardware Acceleration** down until the flicker goes away.

Configuring Apache to accept exported capture buffers

To enable the Console Replay Export feature to work correctly, you must configure a web server to accept the buffer data. The following is an example of configuration changes made to Apache version 2.0.59 (Win32) on a server running Microsoft Windows Server 2003.

You must select a location to store the exported data, set Apache permissions to write to this location, and configure authentication. To configure authentication, you must run `htpasswd.exe` to create the user names and passwords for Apache to authenticate against when an access request to the export location is received by Apache. For more information about how to configure users, see the Apache Software Foundation website at http://httpd.apache.org/docs/2.0/howto/auth.html.

WebDAV provides a collaborative environment for you to edit and manage files on web servers. Technically, DAV is an extension to the http protocol. You must make changes to the configuration file to enable WebDAV by loading the Dynamic Shared Object support modules for it. The following two lines must be added to the list of modules in the `http.conf` file: `LoadModule dav_module modules/mod_dav.so` and `LoadModule dav_fs_module modules/mod_dav_fs.so`

You must also enable authentication by loading the `LoadModule auth_module modules/mod_auth.so`and `LoadModule auth_digest_module modules/mod_auth_digest.so` modules.

If a directory for the DavLock database does not exist, then you must create a directory. A DAV directory under Apache2 is all that is necessary. This directory is referenced in the configuration file. The following is an example of the changes to `http.conf` to add this support:

```
# Davlock database location
DavLockDb "C:/apache/Apache2/Apache2/dav/davlock"
# location of data being exported
Alias /images/ "C:/images/"
# Configuration of the directory to support PUT method with authentication
<Directory "C:/images">
  AllowOverride FileInfo AuthConfig Limit
  AuthType Digest
# if digest is not supported by your configuration use the following
# AuthType Basic
# location of the usernames and passwords used for authentication
AuthUserFile "C:/Program Files/apache group/Apache2/passwd/passwords"
# specifies the user that is required for authentication, can be a group
# For group change to the following after creating the appropriate group
# Require group GroupName
  Require user Administrator
  Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
```

```
  Dav On
  <Limit GET PUT OPTIONS PROPFIND>
     Order allow,deny
     Allow from all
  </Limit>
</Directory>
```

No console replay while server is powered down

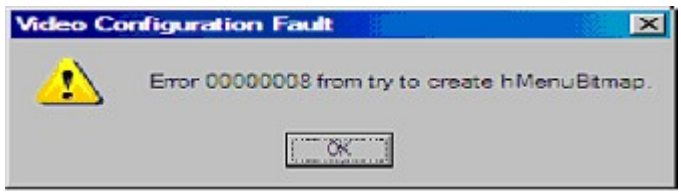
Playback of capture buffers and recorded console sessions are not available any time the server is powered down. You can play back the captured buffers by exporting the buffers to a web server and playing the files on another server IRC console. Manually export the buffer with the export button located on the Remote Console>Settings page after configuring the web server and export location.

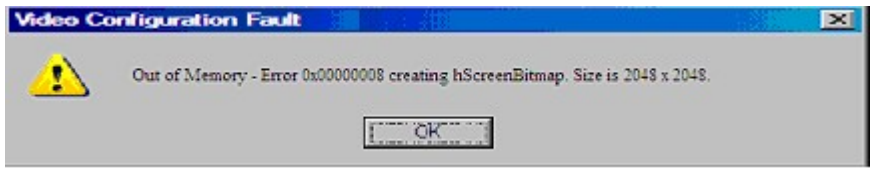
Skipping information during boot and fault buffer playback

Some loss of screen information is normal and might be seen during play back of boot and fault buffers. To help alleviate the issue, ensure that the IRC is active during boot and fault. If you continue to experience data loss, try a manual capture of these sequences. To manually capture a server sequence, start the IRC, and click **Record**.

Out of Memory error starting Integrated Remote Console

The client system can run out of memory if too many IRC sessions are opened at one time. Every IRC session requires at least 16 MB of memory for screen buffer space and Virtual Folder can use about 100 MB. If a message box appears when starting the IRC, not enough memory is available on the client to buffer the screen data. For example:





To correct these types of errors, close some IRC sessions or add memory to the client machine to allow more sessions to be open simultaneously.

Session leader does not receive connection request when IRC is in replay mode

As a session leader, when you play back capture video data, the IRC will not display the `Deny or Accept` warning message when another user attempts to access or share the IRC. Instead, the new IRC session will wait and eventually time-out. If you require access to the IRC, attempt to access the IRC and time-out, use the Acquire feature to take control of the IRC.

Keyboard LED does not display correctly

The client keyboard LED does not reflect the true state of the various keyboard lock keys. However, the Caps Lock, Num Lock and Scroll Lock keys are fully functional when using the Key Up/Down keyboard option in IRC.

Inactive IRC

The iLO 2 IRC might become inactive or disconnected during periods of high activity. The issue is indicated by an inactive IRC. IRC activity slows before becoming inactive. Symptoms of an affected IRC include:

- The IRC display does not update.
- Keyboard and mouse activity are not recorded.
- Shared Remote Console requests do not register.
- The Virtual Media connection displays an empty (blank) virtual media device.

Although you can replay a captured file on an inactive IRC, the active state of the IRC is not restored.

This issue might occur when multiple users are logged into iLO 2, a Virtual Media session is connected and is performing a continuous copy operation, or an IRC session is open. The Virtual Media continuous copy operation takes priority, and, consequently, the IRC loses synchronization. Eventually, the Virtual Media connection resets multiple times and causes the operating system USB media drive to lose synchronization with the Virtual Media client.

To work around this issue, reconnect to the IRC and the Virtual Media. If possible, reduce the number of simultaneous user sessions to iLO 2. If necessary, reset iLO 2 (the server does not need to be reset).

IRC Failed to connect to server error message

iLO 2 might issue the message `Failed to connect to server` when attempting to establish an IRC session. Verify an available Telnet connection.

The iLO 2 IRC client waits a specified amount of time for an IRC connection to be established with iLO 2. If the client server does not receive a response in this amount of time, it issues an error message.

Possible causes for this message include:

- The network response is delayed.
- A shared remote console session is requested, but the remote console session leader delays sending an acceptance or denial message.

To work around this issue, retry the IRC connection. If possible, correct the network delay and retry the IRC connection. If the request was for a shared remote console session, attempt to contact the session leader and retry the request. If the remote console Acquire function is enabled, use the Acquire button rather than requesting a shared remote console session.

IRC toolbar icons do not update

When connecting to the IRC on iLO 2 version 1.30, an IRC object (iLO 2 Remote Console applet) is installed in the browser. The object includes toolbar icons for new features included in iLO2 version 1.30. When browsing to iLO 2 version 1.29 or earlier, the IRC object is not replaced by the version included with the earlier firmware. As a result, toolbar icons appear for features included in iLO2 version 1.30 that are not available in earlier versions. If you click on an icon, an error message might appear.

To manually remove the IRC object:

1. From an Internet Explorer browser, click **Tools>Internet Options**.
2. Select **Temporary Internet files>Settings**
3. Click **View Objects**.
4. Right-click **iLO 2 Remote Console Applet** and click **Remove**.
5. Click **OK** to remove the object, and then click **OK** to close.

GNOME interface does not lock

Terminating an iLO 2 Remote Console or losing iLO 2 network connectivity does not lock the GNOME interface when iLO 2 and the GNOME interface are configured for the Remote Console Lock feature.

The GNOME keyboard handler requires time to process key sequences that contain modifier keystrokes. This issue does not occur when key sequences are entered manually through the IRC, but it becomes an issue when the key sequence is sent by iLO 2. The key sequence with keystroke modifier is sent by iLO 2 faster than the GNOME keyboard handler can process it.

A work around for this issue is to use the Linux KDE GUI instead of GNOME. The KDE keystroke handler does not take an excessively long time to process key sequences that contain modifier keys. Both KDE and GNOME interfaces ship with all distributions of Linux.

Repeating keys on the Remote Console

When using the Remote Console under certain conditions of network latency, you can register multiple key presses for a single key press. For more information, see "Remote Console settings" (page 81).

Remote Console playback does not work when the host server is powered off

When attached to a host server that is powered off, Remote Console playback does not operate. To access recorded Remote Console files, power-on the server or attach to another iLO 2 in a powered on server.

Troubleshooting SSH and Telnet issues

The following sections discuss troubleshooting SSH and Telnet issues.

Initial PuTTY input slow

During initial connection using a PuTTY client, input is accepted slowly for approximately 5 seconds. This can be addressed by changing the configuration options in the client under the Low-level TCP connection options, uncheck the **Disable Nagle's algorithm** option. Under Telnet options, set Telnet negotiation mode to **Passive**.

PuTTY client unresponsive with Shared Network Port

When using PuTTY client with the Shared Network Port, the PuTTY session might become unresponsive when a large amount a data is transferred or when using a Virtual Serial Port and Remote Console. To correct the issue, close the PuTTY client, and restart the session.

SSH text support from a Remote Console session

The Telnet and SSH access from text Remote Console supports the standard 80 x 25 configuration of the text screen. This mode is compatible for text Remote Console for the majority of available text mode interfaces in current operating systems. Extended text configuration beyond the 80 x 25 configuration is not displayed correctly when using Telnet or SSH. HP recommends configuring the text application in 80 x 25 mode or use the iLO 2 Remote Console applet provided by the web interface.

Troubleshooting terminal services issues

The following sections discuss troubleshooting terminal services issues.

Terminal Services button is not working

The Terminal Services option does not function if the Deny option is selected on the Java security warning popup. When the Deny option is selected, you are telling the browser that the Remote

Console applet is not trustworthy. The Remote Console cannot execute any code requiring a higher level of trust. If the Deny option is select, the Remote Console cannot launch the code required to activate the Terminal Services button. If you look in the Java Console, the following error message appears: `"Security Exception - Access denied"`.

Terminal Services proxy stops responding

Any time iLO 2 is reset (such as changing network settings or global settings), Terminal Services passthrough is unavailable for two minutes from the beginning of the reset. iLO 2 requires 60 seconds to complete the reset and POST with a 60-second buffer before continuing. After two minutes, the status changes to Available and Terminal Services passthrough is available for use.

Troubleshooting video and monitor issues

The following sections discuss items to be aware of when attempting to resolve video and monitor issues.

General guidelines

- The client screen resolution must be greater than the screen resolution of the remote server.
- The iLO 2 Remote Console only supports the ATI Rage XL video chip that is integrated in the system. The Remote Console functionality of iLO 2 does not work if you install a plug-in video card. All other iLO 2 functionality is available if you choose to use a plug-in video card.
- Only one user at a time can access the Remote Console. Check to see if another user is logged into iLO 2.

Telnet displays incorrectly in DOS

When using the iLO 2 Telnet session to display text screens involving a maximized DOS window, the Telnet session is unable to represent anything except the upper portion of the screen if the server screen is larger than 80x25.

To correct this adjust the DOS windows properties to limit its size to 80x25, before maximizing the DOS window.

- On the title bar of the DOS window, right-click the mouse and select **Properties**, then select **Layout**.
- On the Layout tab, change the Screen Buffer Size height to **25**.

Video applications not displaying in the Remote Console

Some video applications, such as Microsoft Media Player, do not display, or do not display incorrectly, in the Remote Console. This issue is most often seen with applications that use video overlay registers. Typically, applications that stream video use the video overlay registers. iLO 2 is not intended for use with this type of application.

User interface is not displaying correctly

On ProLiant servers using Red Hat EL 4.0 and some other Linux systems and iLO 2, the text on the buttons of the user interface might be cut off along the bottom of the button. This error occurs because Mozilla Firefox does not display the text size that iLO 2 specifies for the buttons. To display the text correctly, select **View>Text Size>Decrease** until the text appears correctly.

Troubleshooting Virtual Media issues

The following sections discuss troubleshooting Virtual Media issues.

Virtual Media applet has a red X and does not display

The Virtual Media applet might produce a red X if an unsupported browser or JVM is used, or if **Enable All Cookies** is not enabled. To correct this issue, ensure you are using a supported browser and JVM on your client by reviewing the support matrix found in "Supported browsers and client operating systems" (page 15). Also be sure **Enable All Cookies** is selected on the browser Preferences or Options menu. Some browsers do not enable cookies by default.

Virtual Floppy media applet is unresponsive

iLO 2 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.

Troubleshooting iLO Video Player issues

The following sections discuss troubleshooting iLO Video Player issues.

Video capture file does not play

Verify that the file is a valid HP iLO 2 capture and is not corrupted.

Video capture file plays erratically

iLO 2 capture files are recordings of screen activity. During long periods of screen inactivity, the recorded inactivity is truncated to reduce file size and improve playback performance. This can cause the playback to appear to start and stop, or play erratically.

Troubleshooting Remote Text Console issues

The following sections discuss items to be aware of when attempting to resolve Remote Text Console issues.

Viewing the Linux installer in the text console

When installing Linux using the text console, the initial install screen might not display because the screen is in graphics mode. To correct this and proceed with the installation, do one the following:

- For most versions of Linux, enter `linux text nofb`. The characters you enter will not display. If enter the command correctly, the screen changes from graphics mode to text mode, displaying the screen.
- For SLES 9 and SLES 10, blindly press **F2** and the ⇓(down arrow) from the text console. If done correctly, the text mode is selected and the screen appears.

Passing data through an SSH terminal

If you use an SSH terminal to access the text console, SSH might intercept keystroke data and not pass the action to the text console. When this occurs, it appears as if the keystroke did not perform its function. To correct this issue, disable any SSH terminal short-cuts.

Troubleshooting miscellaneous issues

The following sections discuss troubleshooting miscellaneous hardware or software issues.

Cookie sharing between browser instances and iLO 2

iLO 2 uses browser session cookies in part to distinguish separate logins. Each browser window displays as a separate user login, while actually sharing the same active session with the iLO 2.

These multiple logins can confuse the browser. This confusion can appear as an iLO 2 issue; however, this is a manifestation of typical browser behavior.

Several processes can cause a browser to open additional windows. Browser windows opened from within an open browser represent different aspects of the same program in memory. Consequently, each browser window shares properties with the parent, including cookies.

Shared instances

When iLO 2 opens another browser window, for example, Remote Console, Virtual Media, or Help, this window shares the same connection to iLO 2 and the session cookie.

The iLO 2 Web server makes URL decisions based on each request received. For example, if a request does not have access rights, it is redirected to the login page, regardless of the original request. Web server based redirection, selecting **File>New>Window** or pressing the **Ctrl+N** keys, opens a duplicate instance of the original browser.

Cookie order behavior

During login, the login page builds a browser session cookie that links the window to the appropriate session in the firmware. The firmware tracks browser logins as separate sessions listed in the Active Sessions section of the iLO 2 Status page.

For example, when User1 logs in, the Web server builds the initial frames view, with current user: User1 in the top pane, menu items in the left pane, and page data in the lower-right pane. As User1 clicks from link to link, only the menu items and page data are updated.

While User1 is logged in, if another user, User2, opens another browser window on the same client and logs in, the second login overwrites the cookie generated in the original User1 session. Assuming that User2 is a different user account, a different current frame is built, and a new session is granted. The second session appears in the Active Sessions section of the iLO 2 Status page as current user: User2.

The second login has effectively orphaned the first session (User1) by wiping out the cookie generated during User1's login. This behavior is the same as closing User1's browser without clicking the Log Out link. User1's orphaned session is reclaimed when the session timeout expires.

Because the current user frame is not refreshed unless the browser is forced to refresh the entire page, User1 can continue navigating using his or her browser window. However, the browser is now operating using User2's session cookie settings, even though it is not readily apparent.

If User1 continues to navigate in this mode (User1 and User2 sharing the same process because User2 logged in and reset the session cookie), the following can occur:

- User1's session behaves consistently with the privileges assigned to User2.
- User1's activity keeps User2's session alive, but User1's session can time out unexpectedly.
- Logging out of either window causes both window sessions to terminate. The next activity in the other window can redirect the user to the login page as if a session timeout or premature timeout occurred.
- Clicking Log Out from the second session (User2) results in a

  ```
  Logging out:  unknown page to display before redirecting the user to the login page.
  ```

- If User2 logs out then logs back in as User3, User1 assumes User3's session.
- If User1 is at login, and User2 is logged in, User1 can alter the URL to redirect to the index page. It appears as if User1 has accessed iLO 2 without logging in.

These behaviors continue as long as the duplicate windows are open. All activities are attributed to the same user, using the last session cookie set.

Displaying the current session cookie

After logging in, you can force the browser to display the current session cookie by entering `javascript:alert(document.cookie)` in the URL navigation bar. The first field visible is the session ID. If the session ID is the same among the different browser windows, then these windows are sharing the same iLO 2 session.

You can force the browser to refresh and reveal your true identity by pressing the **F5** key, selecting **View>Refresh**, or using the refresh button.

Preventing cookie-related user issues

To prevent cookie-based behavioral issues:

- Start a new browser for each login by double-clicking the browser icon or shortcut.
- Click the **Log Out** link to close the iLO 2 session before closing the browser window.

Inability to access ActiveX downloads

If your network does not allow ActiveX controls you can capture the DVC.DLL from a single system and then distribute the file to client machines on the network.

1. Log into iLO 2.
2. Enter `https://ilo_name/dvc.cab` in the browser address bar.
3. The file download dialog box appears. Click **Open** and save the DVC.DLL file to your local drive.
4. Copy the DVC.DLL file to the client system that does not allow ActiveX downloads.
5. From this client system, open a command prompt window. Navigate to the directory containing the DVC.DLL file and enter `regsvr32 dvc.dll`.

Inability to get SNMP information from HP SIM

The agents running on the managed server supply SNMP information to HP SIM. For agents to pass information through iLO 2, iLO 2 device drivers must be installed. For installation instructions, see "Installing iLO 2 device drivers" (page 21).

If you have installed the drivers and agents for iLO 2, verify that iLO 2 and the management PC are on the same subnet. You can verify this quickly by pinging iLO 2 from the management PC. Consult your network administrator for proper routes to access the network interface of iLO 2.

Incorrect time or date of the entries in the event log

You can update the time and date on iLO 2 by running the RBSU. This utility automatically sets the time and date on the processor using the server time and date. The time and date are also updated by Insight Management agents on supported network operating systems.

Inability to upgrade iLO 2 firmware

If you attempt to upgrade the iLO 2 firmware and it does not respond, does not accept the firmware upgrade, or is terminated before a successful upgrade, you can use one of the following options to restore your iLO 2 firmware. Consult the iLO 2 scripting and command-line resource guide for details on using the scripting capabilities of iLO 2.

- **Online firmware update** – Download this component and run it from the Administrator or root context of a supported operating system. This software runs on the host operating system and updates the iLO 2 firmware without requiring you to log-in to iLO 2.
- **Offline firmware update for SmartStart maintenance** – Download the component to use with the SmartStart firmware maintenance CD under ROM Update Utility on the Maintenance tab. These components can also be used with the HP Drive key boot utility.

- **Firmware Maintenance CD-ROM** – Download the component to create a bootable CD-ROM that contains many firmware updates for ProLiant servers and options.
- **Scripting with CPQLOCFG** – Download CPQLOCFG component to get the network-based scripting utility, CPQLOCFG. CPQLOCFG enables you to use RIBCL scripts that perform firmware updates, iLO 2 configuration, and iLO 2 operations in bulk, securely over the network. HP recommends that Linux users review the HP Lights-Out XML PERL scripting samples for Linux.
- **Scripting with HPONCFG** – Download the HPONCFG component to get the host-based scripting utility, HPONCFG. This utility enables you to use RIBCL scripts that perform firmware updates, and LOM processor configuration and operations in bulk, from Administrator or root account access on supported host operating systems.
- **HP Directories Support for Management Processors** – Download the component to get the directory support components. One of the components, the HPLOMIG, can be used to discover iLO, iLO 2, RILOE, and RILOE II processors and update the firmware. You do not have to use directory integration to take advantage of this functionality.

Diagnostic steps

Before attempting a flash recovery of the firmware, use the following diagnostic steps to verify that flash recovery is needed:

1. Attempt to connect to iLO 2 through the Web browser. If you are unable to connect, then there is a communication issue.
2. Attempt to ping iLO 2. If you are successful, then the network is working.

iLO 2 network flash recovery

The iLO 2 network flash recovery payload enables you to recover from a failed firmware upgrade. The flash recovery payload uses FTP, which can only be used when the flash recovery payload is active, to transfer the firmware image to iLO 2. The flash recovery payload must only be used if:

- Previous firmware upgrade attempts have failed
- You are unable to connect to the Web browser

If the iLO 2 firmware image is damaged, missing, or otherwise corrupted, then the iLO 2 flash recovery process is used to re-flash iLO 2. The flash recovery process is for the sole purpose of getting the system re-flashed. No other processes can run until the recovery process is complete.

Recovering from a bad iLO 2 flash image using network flash recovery

Perform the following steps to recover from a bad iLO 2 flash using network flash recovery:

1. Open an FTP session to the IP address or DNS name of iLO 2.
2. Log in to iLO 2 using the fixed username `flash` and the password `recovery`.

The username and password are case-sensitive.

3. At the FTP prompt, enter the `put` command, and the filename of the firmware image.

The following is an example of the entries used for the flash recovery process:

```
ftp 192.168.177.142
login: flash
password: recovery
put \iLO2_200.bin
```

If the file is found:

- The `put` command transfers the file to iLO 2
- The image validates
- The flash process begins

If the file is not found:

- Some versions of the `put` command do not display an error message

NOTE: If the directory path includes spaces, enclose the path and filename in quotes.

After the firmware image transfers, the recovery payload calculates the check sum, validates the digital signature, and reports if the image is valid. The flash reprogram begins if the image is valid, and the flash progress is reported to the client.

NOTE: This process takes a few seconds while the recovery payload decrypts the stored hash and computes a hash for the image to compare against. If the image is valid, the FTP server begins programming the image into the flash portion, and provides status updates.

When completed, the flash recovery payload module disconnects and reboots the iLO 2 processor. If the flash recovery process is unsuccessful, start the process again, and watch the progress for any errors. You might have to use a different firmware image for the process.

Recovering from a bad iLO 2 flash image using the HP Smart Update Firmware DVD

Use the following procedure to recover iLO 2 from a bad flash upgrade using the firmware DVD 9.00, and iLO 2 1.81:

1. Set the iLO 2 Security Override Switch on the system board to `On`. The location of the switch is printed on a label located on the inside of the hood cover.
2. Power the server on and boot using the Smart Update Firmware DVD version 9.00. The ISO image is available for download from the following website at http://www.hp.com/go/foundation
3. At the boot menu, select Interactive Firmware Update version 9.00.
4. After the **Select Language** screen displays, enter the following key strokes to exit the HP Smart Update Manager:

   NOTE: A command prompt displays on top of the HP Smart Update Manager window (the command prompt takes approximately 30 seconds to appear).

   `CTRL+ALT+d+b+x` (press and hold the `CTRL` and `ALT` keys while typing `d b x`).
5. At the command prompt, navigate to the Smart Update Firmware DVD directory containing the supplemental iLO 2 firmware update by using the following command:

   ```
   cd /mnt/cdrom/hp/swpackages
   ```
6. To unload the HPILO module, enter the command:

   ```
   rmmod hpilo
   ```
7. To execute the iLO 2 firmware update in direct mode, enter the command:

   ```
   sh CP012108.scexe --direct
   ```

   (this parameter requires two dash (-) characters)
8. After the iLO 2 firmware upgrade completes, power the server off and set the iLO 2 Security Override Switch on the system board to `Off`.

The iLO 2 firmware does not respond to SSL requests

The iLO 2 firmware does not respond to SSL requests when a Java warning appears. If a user is logging in to an iLO 2 browser connection and does not complete the login process by responding to the Java certificate warning, iLO 2 does not respond to future browser requests. The user must continue the login process to free the iLO 2 Web server.

Testing SSL

The following test checks for the correct security dialog prompt. A non-working server will proceed to a `Page cannot be displayed` message. If this test fails, your domain controller is not accepting SSL connections, and probably has not been issued a certificate.

1. Open a browser and navigate to `<https://<domain controller>:636`.

   You can substitute *<domain>* in place of *<domain controller>* which goes to the DNS and checks which domain controller is handling requests for the domain. Test multiple domain controllers to verify all of them have been issued a certificate.

2. If SSL is operating correctly on the domain controller (a certificate is issued), you are prompted with a security message asking if you want to proceed with accessing the site, or view the server's certificate. Clicking **Yes** does not display a web page. This is normal. This process is automatic, but might require rebooting. To avoid rebooting:
   a. Open the MMC and add the certificates snap-in. When prompted, select **Computer Account** for the type of certificates you want to view. Click **OK** to return to the certificates snap in.
   b. Select **Personal>Certificates** folder. Right-click the folder and select **Request New Certificate.**
   c. Verify Type is domain controller and click **Next** until a certificate is used.

You can also use Microsoft LDP tool to verify SSL connections. For more information on the LDP tool, go to the Microsoft website at http://www.microsoft.com/support.

An old certificate can cause issues with SSL and on the domain controller when it points to a previously trusted CA with the same name, which is rare but might happen if a certificate service is added and removed and then added again on the domain controller. To remove old certificates and issue a new one follow the instructions above in step 2.

Resetting iLO 2

In rare instances, it might be necessary to reset iLO 2; for example, if iLO 2 is not responding to the browser. To reset iLO 2, you must power down the server and disconnect the power supplies completely.

The iLO 2 firmware might reset itself in certain instances. For example, an internal iLO 2 watchdog timer resets if the firmware detects an iLO 2 issue. If a firmware upgrade is completed or a network setting is changed, iLO 2 also resets.

The HP Insight Management Agents 5.40 and later have the ability to reset iLO 2. To reset iLO 2, choose one of the following options:

- Select the **Reset** iLO 2 option on the HP Management Agent web page under the iLO 2 section.
- Click **Apply** on the Network Settings page to manually force the iLO 2 management processor to reset. You do not need to change any parameters before clicking Apply.
- Click **Reset** on the Diagnostic page of the iLO 2 browser interface.

Server name still present after ERASE utility is executed

The Server Name field is communicated to iLO 2 through the Insight Manager Agents.

To remove the Server Name field after a redeployment of a server, do one of the following:

- Load the Insight Manager Agents to update the Server Name field with the new server name.
- Use the Reset to Factory Defaults feature of the iLO 2 RBSU utility to clear the Server Name field.

  This procedure clears all iLO 2 configuration information, not just the Server Name information.
- Change the server name on the Administration>Access>Options page on the iLO 2 browser interface.

Troubleshooting a remote host

Troubleshooting a remote host server might require restarting the remote system. You can restart the remote host server by using the options listed in the Virtual Devices tab.

8 Technical support

Support information

HP iLO Advanced Pack and HP iLO Advanced Pack for Blade System included with Insight Control suites and iLO Power Management Pack include one year of 24 x 7 HP Software Technical Support and Update Service. This service provides access to HP technical resources for help in resolving software implementation or operations issues. The service also provides access to software updates and reference manuals either in electronic form or on physical media as they are made available from HP.

HP offers product support and product updates to HP iLO Advanced and HP iLO Advanced Pack for Blade System customers in two ways:

- When purchased as individual licenses, you receive startup technical software support at no additional charge by calling HP Support up to 90 days from the date of purchase. Phone support is offered, assisting you with installation, setup, and questions pertaining to the canned scripts and the respective usages. HP worldwide numbers for Support are available on the HP website (http://www.hp.com/country/us/en/support.html). You can purchase updates separately at your discretion.
- When HP iLO Advanced Pack and HP iLO Advanced Pack for Blade System are obtained with the purchase of an Insight Control suite and iLO Power Management Pack, licenses include one year of 24 x 7 HP Software Technical Support and Update Service.

  With the bundled Technical Support and Update Service, HP iLO Advanced Pack and HP iLO Advanced Pack for Blade System customers benefit from expedited issue resolution, and proactive notification and delivery of iLO Advanced and iLO Select software updates. For more information, see the HP website at http://www.hp.com/go/ilo, select your product, and review the Quickspecs.

  To activate your HP Software Technical Support and Update Service for iLO Advanced and iLO Select, you must register your software purchase through the HP website at http://www.hp.com/go/ilo. **Failure to register your service jeopardizes service fulfillment**.

  Your Service Agreement Identifier (SAID) is delivered to you after registration. After you receive your SAID, you can go to the Software Update Manager (SUM) web page to view your contract and choose electronic delivery (in addition to standard media-based updates). For more information about this service, see the HP website at http://www.hp.com/services/insight.

HP also offers a number of additional software support services. Many are provided at no additional charge.

- Startup technical software support – Phone support is available to help you with basic installation, setup, and usage questions. This support is provided by the knowledgeable HP Insight Control Management and Systems Insight Manager specialists' team and is available at no additional charge up to 90 days from the date of purchase of your server. For support in the US, call
- 1 800 334 5144. When prompted, ask for Insight Manager, P2P, or SMP.

  HP worldwide support numbers are available at the HP website at http://www.hp.com/go/assistance.
- Join the discussion on the HP website at http://forums.itrc.hp.com. The HP Support Forum is a community-based, user-supported tool designed so that HP customers can discuss HP products. To discuss Insight Control and Insight Essentials software, click **Management Software and System Tools**.

- Software and Drivers download pages are on the HP website at http://www.hp.com/support. These pages provide the latest software and drivers for your ProLiant products.
- Management Security is on the HP website at http://www.hp.com/servers/manage. HP is proactive in its approach to the quality and security of all its management software. Be sure to check this website often for the latest downloadable security updates.
- Obtain the latest SmartStart firmware on the HP website at http://www.hp.com/servers/smartstart. You can download the SmartStart, Management, and Firmware CDs by following a simple registration process from the SmartStart website. To receive physical kits with each release, you can order single release kits from the SmartStart website. To receive proactive notification when SmartStart releases are available, subscribe to Subscriber's Choice the HP website at http://www.hp.com/go/subscriberschoice.

HP contact information

For the name of the nearest HP authorized reseller:

- See the Contact HP worldwide (in English) webpage at http://www.hp.com/go/assistance.

For HP technical support:

- To obtain HP contact information for any country, see the Contact HP worldwide web site at http://www.hp.com/go/assistance.

  To contact HP by phone:

  - Call 1 800 334 5144. 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, see the HP website at http://www.hp.com/hps.

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
- Product identification number
- Applicable error messages
- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level

Acronyms and abbreviations

ACPI	Advanced Configuration and Power Interface
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ASM	Advanced Server Management
ASR	Automatic Server Recovery
BMC	baseboard management controller
CA	certificate authority
CLI	Command Line Interface
CLP	command line protocol
CR	Certificate Request
CRL	certificate revocation list
DAV	Distributed Authoring and Versioning
DDNS	Dynamic Domain Name System
DHCP	Dynamic Host Configuration Protocol
DLL	dynamic link library
DMTF	Distributed Management Task Force
DNS	domain name system
DVO	Digital Video Out
EAAS	Environment Abnormality Auto-Shutdown
EBIPA	Enclosure Bay IP Addressing
EMS	Emergency Management Services
EULA	end user license agreement
FEH	fatal exception handler
GNOME	GNU Network Object Model Environment
GUI	graphical user interface
HB	heartbeat
HEM	High Efficiency Mode
HID	human interface device
HP SIM	HP Systems Insight Manager
HPLOMIG	HP Lights-Out Migration
HPONCFG	HP Lights-Out Online Configuration utility
HPQLOMGC	HP Lights-Out Migration Command Line
ICMP	Internet Control Message Protocol
iLO	Integrated Lights-Out
iLO 2	Integrated Lights-Out 2
IML	Integrated Management Log
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
IRC	Integrated Remote Console
IRQ	interrupt request
JVM	Java Virtual Machine
KCS	Keyboard Controller Style

KDE	K Desktop Environment (for Linux)
KVM	keyboard, video, and mouse
LAN	local-area network
LDAP	Lightweight Directory Access Protocol
LED	light-emitting diode
LOM	Lights-Out Management
LSB	least significant bit
MAC	Media Access Control
MLA	Master License Agreement
MMC	Microsoft Management Console
MP	Multilink Point-to-Point Protocol
MTU	maximum transmission unit
NIC	network interface controller
NMI	non-maskable interrupt
NVRAM	non-volatile memory
PERL	Practical Extraction and Report Language
PKCS	Public-Key Cryptography Standards
POST	Power-On Self Test
PSP	ProLiant Support Pack
RAS	remote access service
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
RILOE II	Remote Insight Lights-Out Edition II
ROM	read-only memory
RSA	Rivest, Shamir, and Adelman public encryption key
RSM	Remote Server Management
SAID	Service Agreement Identifier
SBIPC	Static Bay IP Configuration
SLES	SUSE Linux Enterprise Server
SMASH	System Management Architecture for Server Hardware
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
SSO	single sign-on
SUM	software update manager
SUV	serial, USB, video
TCP	Transmission Control Protocol
TPM	trusted platform module
UART	universal asynchronous receiver-transmitter
UID	unit identification
USB	universal serial bus
VM	Virtual Machine

VPN	virtual private networking
VRM	voltage regulator module
WINS	Windows Internet Naming Service
WS	web services
XML	extensible markup language

Index

A

access options
  Configuring iLO 2 access, 33
  iLO 2 Remote Console and Remote Serial Console access, 41
  Remote Console overview and licensing options, 81
access, VT320 serial console, 100
accessing Onboard Administrator, 124
accessing software, browser, 21
ACPI (Advanced Configuration and Power Interface), 112
acquire, remote console, 92
Active Directory integration
  Active Directory installation prerequisites, 140
  Active Directory Lights-Out management, 148
  Directory services for Active Directory, 140
  Directory services preparation for Active Directory, 141
  Installing certificate services, 132
  Introduction to certificate services, 132
  Introduction to directory-enabled remote management, 156
  Management snap-in installer, 140
  Restricting roles, 158
  Setup, 138
  User login using directory services, 156
  Using existing groups, 157
  Verifying certificate services, 133
ActiveX
  ActiveX controls are enabled and I see a prompt but the domain/name login format does not work, 192
  Inability to access ActiveX downloads, 201
adding HP SIM trusted servers, 56
adding new users, 29
Address Resolution Protocol (ARP), 64
administration
  HP Systems Insight Manager integration, 178
  SSL certificate administration, 45
  User administration, 28
Advanced Configuration and Power Interface, ACPI, 112
Advanced Server Management (ASM)
  Linux device driver support, 22
  Microsoft device driver support, 22
alert and trap issues
  Inability to get SNMP information from HP SIM, 201
  Troubleshooting alert and trap issues, 190
alert messages
  Configuring Insight Manager integration, 67
  ProLiant BL p-Class alert forwarding, 124
alert testing, 65
alerts
  Inability to receive HP SIM alarms (SNMP traps) from iLO 2, 191
  SNMP generated trap definitions, 66
alerts, level of data, 67
American Standard Code for Information Interchange (ASCII)
  hpqRoleIPRestrictions, 174
  Text-based remote console overview, 95
Apache server configuration, 194
ARP (Address Resolution Protocol), 64
ASCII (American Standard Code for Information Interchange)
  hpqRoleIPRestrictions, 174
  Text-based remote console overview, 95
ASM (Advanced Server Management)
  Linux device driver support, 22
  Microsoft device driver support, 22
ASR (Automatic Server Recovery)
  Diagnostics, 79
  Using Console Capture, 90
authentication, two-factor, 46
authentication, two-factor setup, 47
authentication, WS-Management, 13
authorized reseller
  HP contact information, 207
  Technical support, 206
automatic certificate request
  Configuring Automatic Certificate Request, 133
  Directory services preparation for Active Directory, 141
  Introduction to certificate services, 132
Automatic Server Recovery (ASR)
  Diagnostics, 79
  Using Console Capture, 90
autosense, 61

B

BL c-Class alerts, 66
BL c-Class tab, 124
BL p-Class advanced configuration, 69
BL p-Class blade server
  ProLiant BL p-Class Advanced management, 119
BL p-Class enclosure configuration, 68
BL p-Class iLO 2 configuration screen, 71
BL p-Class standard configuration, 69
BL p-Class, iLO 2 IP address, 70
BL p-Class, power notification, 124
BL p-Class, server POST tracking, 123
blade configuration
  Blade configuration and information, 121
  HP BladeSystem setup, 70
blade information
  Blade configuration and information, 121
  ProLiant BladeSystem HP Onboard Administrator, 124
blade LED, 123
boot options, 20
brown-out recovery, 119
browser interface, 14
browser-based setup
  Schema-free browser-based setup, 133
  setting up iLO 2 with the browser-based option, 21
browsers, supported, 15
bulk import tools, 161

C

CA (certificate authority)
- Installing certificate services, 132
- Setting up a user for two-factor authentication, 48
- Two-factor authentication, 46
- Two-factor authentication login, 49
- Using two-factor authentication with directory authentication, 50
- Verifying certificate services, 133

CD-ROM, virtual, 109
certificate authority (CA)
- Installing certificate services, 132
- Setting up a user for two-factor authentication, 48
- Two-factor authentication, 46
- Two-factor authentication login, 49

Certificate Request (CR)
- Configuring Automatic Certificate Request, 133
- Directory services preparation for Active Directory, 141
- Introduction to certificate services, 132
- SSL certificate administration, 45
- Two-factor authentication login, 49

certificates
- Inability to log in to iLO 2 after installing the iLO 2 certificate, 189
- SSL certificate administration, 45

certificates, installing
- Active Directory preparation, 132
- Inability to log in to iLO 2 after installing the iLO 2 certificate, 189
- Installing certificate services, 132
- Setting up a user for two-factor authentication, 48
- Setting up two-factor authentication for the first time, 47
- SSL certificate administration, 45
- Two-factor authentication, 46
- Two-factor authentication login, 49
- Using two-factor authentication with directory authentication, 50
- Verifying certificate services, 133

CLI (Command Line Interface)
- Access options, 38
- Integrated Remote Console option, 85
- Multi-user access to the Integrated Remote Console, 89
- Two-factor authentication, 46

CLP (Command Line Protocol)
- Encryption, 53
- Encryption settings, 54
- HP SIM single sign-on (SSO), 55
- preparing to set up iLO 2, 17
- Remote Console overview and licensing options, 81
- Remote Serial Console troubleshooting, 193
- Setting up user accounts, 20
- Using Console Capture, 90

Command Line Interface (CLI)
- Access options, 38
- Integrated Remote Console option, 85
- Multi-user access to the Integrated Remote Console, 89
- Two-factor authentication, 46

Command Line Protocol (CLP)
- Encryption, 53
- Encryption settings, 54
- HP SIM single sign-on (SSO), 55
- preparing to set up iLO 2, 17
- Remote Console overview and licensing options, 81
- Remote Serial Console troubleshooting, 193
- Setting up user accounts, 20
- Using Console Capture, 90

commands, WS-Management, 13
compatibility, directory migration, 162
compatibility, WS-Management, 13
computer lock, remote console, 58
configuration options
- Remote console hot keys, 83
- Setting up iLO 2 using iLO 2 RBSU, 20
- setting up iLO 2 with the browser-based option, 21
- Setting up user accounts, 20

configuration parameters
- Configuring static IP bay settings, 69
- Directory services preparation for Active Directory, 141

configuration procedures, 24
configuration, LOM processor
- Introduction to directory-enabled remote management, 156
- Schema-free HPLOMIG-based setup, 134
- Using bulk import tools, 161

connecting to iLO 2 with encryption, 54
connection overview, 18
Console Capture, using, 90
console replay, troubleshooting, 195
console, remote, 93
console, remote serial, 100
contacting HP
- Before you contact HP, 207
- HP contact information, 207

cookie behavior
- Cookie order behavior, 200
- Cookie sharing between browser instances and iLO 2, 199

cookie, displaying, 201
cookie, shared, 200
cookie, user-related issues, 201
core attributes
- Core attribute definitions, 173
- Core attributes, 172

core classes
- Core class definitions, 172
- Core classes, 172

CR (Certificate Request)
- Configuring Automatic Certificate Request, 133
- Directory services preparation for Active Directory, 141
- Introduction to certificate services, 132
- SSL certificate administration, 45
- Two-factor authentication login, 49

D

data protection methods, 53
defining hot keys, 83
device drivers, installing
- Installing iLO 2 device drivers, 21

Novell NetWare device driver support, 22
DHCP (Dynamic Host Configuration Protocol)
BL p-Class and BL c-Class features, 129
DHCP/DNS Settings, 64
iLO 2 Log, 77
Network, 60
Network Settings, 60
preparing to set up iLO 2, 17
DHCP/DNS settings, 64
diagnosing issues, 182
diagnostic port
iLO 2 diagnostic port configuration parameters, 72
Inability to connect to the iLO 2 Diagnostic Port, 188
diagnostic tools
Diagnostic steps, 202
Diagnostics, 79
Event log entries, 183
iLO 2 diagnostic port configuration parameters, 72
iLO 2 POST LED indicators, 182
iLO 2 Security Override switch, 191
Testing SSL, 204
Using a remote Windows Kernel Debugger, 103
directory authentication, two-factor authentication
Schema-free scripted setup, 133
Using two-factor authentication with directory authentication, 50
directory configuration
Configuring directories when HP Extended schema is selected, 168
Configuring directories when schema-free integration is selected, 169
Setting up management processors for directories, 170
directory error, 187
directory integration, benefits
Benefits of directory integration, 130
Features supported by HP schema directory integration, 136
directory integration, overview
Features supported by HP schema directory integration, 136
Introduction to directory-enabled remote management, 156
Overview of directory integration, 130
directory login restrictions, 158
directory services for eDirectory
Directory services for eDirectory, 149
Directory Services objects for eDirectory, 152
eDirectory installation prerequisites, 149
directory services objects
Directory services objects, 145
HP Devices, 146
Members, 146, 153
Role managed devices, 152
Directory Services schema, 171
directory services settings
Directory services for Active Directory, 140
Directory services for eDirectory, 149
Directory services preparation for Active Directory, 141
Directory services support, 137
Directory-enabled remote management, 156
Features supported by HP schema directory integration, 136
Introduction to directory-enabled remote management, 156
Management snap-in installer, 140
Results, 139
Schema documentation, 137
Schema installer, 138
Schema required software, 137
Setting up HP schema directory integration, 136
Setup, 138
User login using directory services, 156
Using two-factor authentication with directory authentication, 50
directory services, errors, 133
directory services, integration
Benefits of directory integration, 130
Setting up HP schema directory integration, 136
directory services, migration, 162
directory services, support, 137
directory services, troubleshooting, 191
directory services, verifying, 53
directory settings, 51
directory settings, configuring, 51
directory user restrictions
Creating multiple restrictions and roles, 160
User restrictions, 159
directory user roles, 158
Directory-Enabled remote management
Integrating iLO 2 with HP SIM, 178
Introduction to directory-enabled remote management, 156
disk image files
Creating iLO 2 disk image files, 111
Virtual Floppy media applet is unresponsive, 199
diskette, changing, 109
display settings, 95
DLL (dynamic link library)
HP Lights-Out directory package, 163
Inability to access ActiveX downloads, 201
DNS (domain name system)
DNS-based restrictions, 160
Enforced client IP address or DNS name access, 148, 154
hpqRoleIPRestrictions, 174
Introduction to directory-enabled remote management, 156
DNS name, 61
DNS server, 61
DNS settings, 64
domain name system (DNS)
DNS-based restrictions, 160
Enforced client IP address or DNS name access, 148, 154
hpqRoleIPRestrictions, 174
Introduction to directory-enabled remote management, 156
domain/name login, 191

drive key, support, 106
DVD-ROM, virtual, 109
Dynamic Host Configuration Protocol (DHCP)
  BL p-Class and BL c-Class features, 129
  DHCP/DNS Settings, 64
  iLO 2 Log, 77
  Network, 60
  Network Settings, 60
  preparing to set up iLO 2, 17
dynamic link library (DLL)
  HP Lights-Out directory package, 163
  Inability to access ActiveX downloads, 201

E

EBIPA (Enclosure Bay IP Addressing), 125
EBIPA, settings, 125
eDirectory
  Directory services for eDirectory, 149
  Directory Services objects for eDirectory, 152
  eDirectory installation prerequisites, 149
  eDirectory Lights-Out Management, 155
  eDirectory Role Restrictions, 154
  Enforced client IP address or DNS name access, 154
  Introduction to directory-enabled remote management, 156
  Members, 153
  Restricting roles, 158
  Setting up HP schema directory integration, 136
  Setup, 138
  Snap-in installation and initialization for eDirectory, 150
  Time restrictions, 154
  Using existing groups, 157
Emergency Management Services (EMS)
  Integrating iLO 2 with HP SIM, 178
  Remote Serial Console, 100
  Terminal Services Passthrough option, 35
  Virtual serial port and remote serial console, 99
  Virtual serial port raw mode, 102
  Windows? EMS Console, 102
EMS (Emergency Management Services)
  Integrating iLO 2 with HP SIM, 178
  Remote Serial Console, 100
  Terminal Services Passthrough option, 35
  Virtual serial port and remote serial console, 99
  Virtual serial port raw mode, 102
  Windows? EMS Console, 102
EMS Console, 102
enable SSH, 44
enable, Terminal Services passthrough, 36
enabling, 130
enclosure fan, control, 128
enclosure information, 122
enclosure information, status, 122
enclosure, temperature, 128
encryption, 53
encryption settings, 54
encryption, connecting to iLO 2 with, 54
end user license agreement (EULA)
  Activating iLO 2 licensed features with a browser, 21
error messages, 191
EULA (end user license agreement)
  Activating iLO 2 licensed features with a browser, 21
event capture, remote console, 80
event log entries
  Event log entries, 183
  IML, 78
event log, date entries, 201
event logs
  iLO 2 Log, 77
  IML, 78
events, WS-Management, 13

F

fan management
  Fans, 76
  iLO 2 Virtual Fan, 128
feature, comparison, 12
file transfer, virtual folder, 111
Firefox support, 15
firewall, allowing traffic, 189
firmware, downgrading, 26
firmware, updating
  Inability to upgrade iLO 2 firmware, 201
  Updating the firmware using the maintenance CD, 25
  Upgrading firmware on management processors, 165
  Upgrading iLO 2 firmware, 24
  Upgrading iLO 2 with a browser, 25
folder, virtual, 111

G

G1 BL-series blade enclosure, 68
GNOME, troubleshooting, 197
graceful shutdown, 118
graphical remote console, 80
graphical user interface (GUI), 14
Group Administration, 32
groups, 157
GUI (graphical user interface), 14

H

hardware troubleshooting, 186
health, system, 75
high performance mouse, 88
host server troubleshooting, 205
hot keys, international keyboards, 85
hot keys, remote, 83
hot keys, supported, 84
HP BladeSystem information, 124
HP BladeSystem setup, 70
HP Extended schema options
  Advantages and disadvantages of schema-free directories and HP schema directory, 131
  Configuring directories when HP Extended schema is selected, 168
  HP Lights-Out directory package, 163
  Results, 139
  Setting up HP schema directory integration, 136
HP Insight Control software, 12

HP Lights-Out Migration Command Line (HPQLOMGC)
HP Lights-Out directory package, 163
Using bulk import tools, 161
HP Onboard Administrator, 124
HP Onboard Administrator, iLO option, 128
HP Onboard Administrator, Web Administration, 128
HP schema directory integration
Features supported by HP schema directory integration, 136
Introduction to directory-enabled remote management, 156
Setting up HP schema directory integration, 136
HP SIM trusted servers, adding, 56
HP SIM, SNMP information, 201
HP Systems Insight Manager
HP SIM links, 179
HP SIM port matching, 181
HP SIM status, 179
HP SIM systems lists, 180
HP technical support, 207
HPLOMIG (HP Lights-Out Migration)
Introduction to HPLOMIG utility, 162
Schema-free HPLOMIG-based setup, 134
Using bulk import tools, 161
HPQLOMGC (HP Lights-Out Migration Command Line)
HP Lights-Out directory package, 163
Using bulk import tools, 161
hpqLOMRightConfigureSettings, 177
hpqLOMRightLogin, 175
hpqLOMRightRemoteConsole, 176
hpqLOMRightServerReset, 176
hpqLOMRightVirtualMedia, 176
hpqLOMv100, 175
hpqPolicy, 173
hpqPolicyDN, 173
hpqRole, 172
hpqRoleIPRestrictionDefault, 173
hpqRoleIPRestrictions, 174
hpqRoleMembership, 173
hpqRoleTimeRestriction, 174
hpqTarget, 172
hpqTargetMembership, 173

I

iLO 2 access, 33
iLO 2 advanced features
Activating iLO 2 licensed features with a browser, 21
Reviewing Advanced Pack license information in HP SIM, 181
iLO 2 and iLO, 12
iLO 2 configuration, BL p-Class
iLO 2 configuration screen, 71
iLO 2 firmware upgrade, 24
iLO 2 IRC, 85
iLO 2 server reset, 188
iLO 2 setup, 17
iLO 2 Telnet access, 188
iLO 2 user administration, 28
image files, disk, 111
IML (Integrated Management Log)
Blade configuration and information, 121
Fans, 76
IML, 78
Linux device driver support, 22
Power, 77
System status and status summary information, 74
Temperatures, 76
initial access, 20
install, Terminal Services passthrough , 36
installation overview
Active Directory installation prerequisites, 140
HP SIM functional overview, 178
Setting up directory services, 136
installing software
eDirectory installation prerequisites, 149
Linux device driver support, 22
Microsoft device driver support, 22
Novell NetWare device driver support, 22
Integrated Management Log (IML)
Blade configuration and information, 121
Fans, 76
IML, 78
Linux device driver support, 22
Power, 77
System status and status summary information, 74
Temperatures, 76
integrated remote console, 85
Integrated Remote Console (IRC)
Configuring Remote Serial Console, 100
Integrated Remote Console option, 85
IRC Fullscreen, 85
No console replay while server is powered down, 195
power management, 112
Re-enabling the dedicated iLO 2 management port, 63
Server power data, 115
Troubleshooting alert and trap issues, 190
Using Console Capture, 90
Using multiple roles, 157
Virtual folder, 111
integration, HP Insight Control Software, 12
Intelligent Platform Management Interface (IPMI), 13
interface, browser
iLO 2 browser interface overview, 14
User interface is not displaying correctly, 198
international keyboard, 85
Internet Explorer support, 15
IP address assignment, 70
IP addresses, setting up
Configuring the IP address, 19
Enabling iLO 2 IP address assignment, 70
IP address and subnet mask restrictions, 159
IP address range restrictions, 159
Network Settings, 60
IPMI (Intelligent Platform Management Interface), 13
IRC (Integrated Remote Console)
Configuring Remote Serial Console, 100
Integrated Remote Console option, 85
IRC Fullscreen, 85

No console replay while server is powered down, 195
power management, 112
Re-enabling the dedicated iLO 2 management port, 63
Server power data, 115
Troubleshooting alert and trap issues, 190
Using Console Capture, 90
Using multiple roles, 157
Virtual folder, 111
IRC, sharing, 89
IRC, troubleshooting
Inactive IRC, 196
Internet Explorer 7 and a flickering remote console screen, 194
IRC Failed to connect to server error message, 196
IRC toolbar icons do not update, 196
Repeating keys on the Remote Console, 197
Troubleshooting Integrated Remote Console issues, 194

J

Java support
JVM support, 186
Supported browsers and client operating systems, 15

K

KCS (Keyboard Controller Style)
Server management through IPMI version 2.0 compliant applications, 13
SSL certificate administration, 45
kernel debugger, using, 103
Keyboard Controller Style (KCS)
Server management through IPMI version 2.0 compliant applications, 13
SSL certificate administration, 45
keyboard, video, mouse (KVM)
iLO 2 Remote Console, 80
Integrated Remote Console option, 85
Text-based remote console overview, 95
Virtual media, 104
KVM, (keyboard, video, mouse)
iLO 2 Remote Console, 80
Integrated Remote Console option, 85
Text-based remote console overview, 95
Virtual media, 104

L

LDAP (Lightweight Directory Access Protocol)
Active Directory installation prerequisites, 140
Active Directory preparation, 132
Advantages and disadvantages of schema-free directories and HP schema directory, 131
Benefits of directory integration, 130
Configuring directory settings, 51
Directory settings, 51
eDirectory installation prerequisites, 149
HP Lights-Out directory package, 163
HP Management Core LDAP OID classes and attributes, 171
Lights-Out Management specific LDAP OID classes and attributes, 175
Schema-free setup options, 134
Security, 41
Setup, 138
User address restrictions, 159
User login using directory services, 156
LDAP OID core classes and attributes, 171
LDAP OID HP specific classes and attributes, 175
LED behavior, 195
LED, p-Class server, 123
LED, POST, 182
license information, viewing, 181
license key, installing, 21
license options
Licensing, 26
Remote Console overview and licensing options, 81
licensing options, remote console, 81
Lights-Out Management attributes, LDAP
Lights-Out Management attribute definitions, 175
Lights-Out Management attributes, 175
Lights-Out Management classes, LDAP
Lights-Out Management class definitions, 175
Lights-Out Management classes, 175
Lights-Out Management, directory services, 148
Lightweight Directory Access Protocol (LDAP)
Active Directory installation prerequisites, 140
Active Directory preparation, 132
Advantages and disadvantages of schema-free directories and HP schema directory, 131
Benefits of directory integration, 130
Configuring directory settings, 51
Directory settings, 51
eDirectory installation prerequisites, 149
HP Lights-Out directory package, 163
HP Management Core LDAP OID classes and attributes, 171
Lights-Out Management specific LDAP OID classes and attributes, 175
Schema-free setup options, 134
Security, 41
Setup, 138
User address restrictions, 159
User login using directory services, 156
Linux remote serial console configuration, 101
Linux server support, 15
Linux support
Linux device driver support, 22
Mounting USB Virtual Media/USBKey in Linux, 108
Remote Console applet has a red X when running Linux client browser, 192
Supported server operating system software, 15
Using a Linux session, 99
logging in, 20
login access, 188
login issues, 187
login, failure, 187
login, privileges, 44
login, security, 44
login, two-factor authentication, 49
LOM access, HP Onboard Administrator

iLO option, 128
Web Administration, 128

M

MAC (media access control)
Encryption, 53
NIC, 77
management port, re-enabling, 63
management processor name troubleshooting, 187
management processors,
Finding management processors, 163
Selecting a directory access method, 166
management processors, naming, 167
media, virtual, 104
medium access control (MAC)
Encryption, 53
NIC, 77
memory
Memory, 77
Out of Memory error starting Integrated Remote Console, 195
Microsoft Management Console (MMC)
Benefits of directory integration, 130
Configuring Automatic Certificate Request, 133
Directory services preparation for Active Directory, 141
Testing SSL, 204
User administration, 28
Microsoft software
Directory services, 130
Directory services for Active Directory, 140
Microsoft support
Supported browsers and client operating systems, 15
Supported server operating system software, 15
migration utilities, 162
migration utilities, overview, 162
MMC (Microsoft Management Console)
Benefits of directory integration, 130
Configuring Automatic Certificate Request, 133
Directory services preparation for Active Directory, 141
Testing SSL, 204
User administration, 28
mounting virtual media
Mounting USB Virtual Floppy/USBKey in NetWare 6.5, 107
Mounting USB Virtual Media/USBKey in Linux, 108
mouse, 88
mouse settings, 88
mouse settings, high performance, 88
Mozilla support, 15

N

NetWare server support
Novell NetWare device driver support, 22
Supported browsers and client operating systems, 15
Supported server operating system software, 15
network component information, 123
network connection troubleshooting, 188
network connections, 18
network interface card (NIC)
iLO 2 Shared Network Port, 61
Inability to connect to the iLO 2 processor through the NIC, 189
NIC, 77
preparing to set up iLO 2, 17
network settings
Network, 60
Network Settings, 60
new features, 11
NIC (network interface card)
iLO 2 Shared Network Port, 61
Inability to connect to the iLO 2 processor through the NIC, 189
NIC, 77
preparing to set up iLO 2, 17
Novell NetWare, 22

O

operating system, virtual folder, 112
operating systems supported
Active Directory preparation, 132
Virtual Media CD/DVD-ROM operating system notes, 110
operating systems, supported client, 15
operational overview
iLO 2 overview, 11
Introduction to certificate services, 132
Operational overview, 11
optimizing performance
Microsoft? Windows? Server 2003 settings, 95
Recommended client settings, 94
Recommended server settings, 95
Red Hat Linux and SUSE Linux server settings, 95
overview of configuration procedure, 24
overview, blade features, 129
overview, directory integration
Advantages and disadvantages of schema-free directories and HP schema directory, 131
Schema-free directory integration, 131
overview, guide, 11
overview, IPMI, 13
overview, product, 11
overview, virtual file, 111

P

p-state, 116
passwords, 42
phone numbers, 207
port matching, 181
port settings, 62
ports, Systems Insight Manager, 181
POST error messages, 182
POST LED indicators, 182
power management
brown-out recovery, 119
Dynamic power capping for server blades, 127
HP Insight Control Software deployment, 12
Power, 77
Power enclosure information, 122

power management, 112
power monitoring, 77
power regulator, 112
power regulator settings
Dynamic power capping for server blades, 127
power management, 112
Server power settings, 113
power supply, status
Power, 77
power management, 112
power, monitoring, 115
powering down
Graceful shutdown, 118
power management, 112
powering up/down, 112
Practical Extraction and Report Language (Perl)
Inability to upgrade iLO 2 firmware, 201
Integrating iLO 2 with HP SIM, 178
preparing to set up iLO 2, 17
SSL certificate administration, 45
Upgrading iLO 2 firmware, 24
preinstallation, guidelines
Active Directory installation prerequisites, 140
Active Directory preparation, 132
Schema required software, 137
preinstallation, overview, 17
preparation procedures, 141
privilege levels
Adding a new user, 29
Group administration, 32
HP SIM single sign-on (SSO), 55
Viewing or modifying existing user settings, 31
processor information, 77
processor states, 116
ProLiant Support Pack (PSP)
Installing iLO 2 device drivers, 21
Microsoft device driver support, 22
Novell NetWare device driver support, 22
proxy settings, 190
PSP (ProLiant Support Pack)
Installing iLO 2 device drivers, 21
Microsoft device driver support, 22
Novell NetWare device driver support, 22
PuTTY utility
Initial PuTTY input slow, 197
PuTTY client unresponsive with Shared Network Port, 197

Q

quick setup, 17

R

rack resources
Enclosure information, 122
Network component information, 123
Power enclosure information, 122
Rack View, 120
rack settings, 119
Rack View, 120
RAID configuration, 71
Rapid Deployment Pack (RDP), 12
RBSU (ROM-Based Setup Utility)
Access options, 38
Adding a new user, 29
Configuring Remote Serial Console, 100
DHCP/DNS Settings, 64
Group administration, 32
Network Settings, 60
preparing to set up iLO 2, 17
Securing RBSU, 42
Setting up iLO 2 using iLO 2 RBSU, 20
RBSU Erase Option, 204
RDP (Remote Desktop Protocol)
Remote Console and Terminal Services clients, 37
Terminal Services client requirements, 35
Terminal Services Passthrough option, 35
Windows RDP passthrough service, 36
rear panel connectors, 119
recovering from a brown-out, 119
recovering from a failed firmware update, 26
Red Hat support
iLO 2 Remote Console, 80
iLO 2 Remote Console and Remote Serial Console access, 41
Recommended server settings, 95
Remote Console, 93
Remote Console and Terminal Services clients, 37
Remote Console overview and licensing options, 81
Supported browsers and client operating systems, 15
Supported server operating system software, 15
Troubleshooting Remote Console issues, 192
remote console fullscreen, 85
remote console playback troubleshooting, 197
remote console, acquire, 92
remote console, computer lock, 58
remote console, enhanced features, 94
Remote Console, Integrated, 85
remote console, mouse settings
High Performance Mouse settings, 88
Optimizing mouse performance for Remote Console or Integrated Remote Console, 88
remote console, optimizing, 88
remote console, recommended settings
Recommended client settings, 94
Recommended server settings, 95
remote console, repeating keys troubleshooting, 197
Remote Console, Shared, 89
remote console, sharing, 89
remote console, text-based
Customizing iLO 2 Text Console, 97
Text-based console during POST, 95
Text-based remote console overview, 95
Using a Linux session, 99
Using iLO Text Console, 97
remote console, troubleshooting
Inability to access virtual media or graphical remote console, 188

Inability to navigate the single cursor of the Remote Console to corners of the Remote Console window, 192
Remote Console applet has a red X when running Linux client browser, 192
Remote Console no longer opens on the existing browser session, 193
Remote console text window not updating properly, 193
Remote Console turns gray or black, 193
Troubleshooting Remote Console issues, 192
Remote Desktop Protocol (RDP)
Remote Console and Terminal Services clients, 37
Terminal Services client requirements, 35
Terminal Services Passthrough option, 35
Windows RDP passthrough service, 36
remote hosts
IML, 78
ProLiant BL p-Class Advanced management, 119
Supported hot keys, 84
Troubleshooting a remote host, 205
Remote Insight Board Command Language (RIBCL)
Encryption, 53
Encryption settings, 54
High Performance Mouse settings, 88
Inability to upgrade iLO 2 firmware, 201
Integrated Remote Console option, 85
Multi-user access to the Integrated Remote Console, 89
preparing to set up iLO 2, 17
Schema-free scripted setup, 133
Securing RBSU, 42
Setting up directory services, 136
SSL certificate administration, 45
Upgrading iLO 2 firmware, 24
Using bulk import tools, 161
remote management overview, 156
remote management structure, 157
remote management, directory-enabled, 156
remote serial console
iLO 2 Remote Console and Remote Serial Console access, 41
Remote Serial Console, 100
remote serial console, configuring, 100
remote serial console, troubleshooting, 193
Remote Server Management (RSM)
Linux configuration example, 101
Linux device driver support, 22
Recovering from a failed iLO 2 firmware update, 26
remote text console issues
Passing data through an SSH terminal, 199
Troubleshooting remote text console issues, 199
Viewing the Linux installer in the text console, 199
required information, 207
required software, 137
requirements, Terminal Services
Terminal Services client requirements, 35
Terminal Services Passthrough option display, 37
resetting to defaults, 204
restore factory presets, 204
restoring, 204
RIBCL (Remote Insight Board Command Language)
Encryption, 53
Encryption settings, 54
High Performance Mouse settings, 88
Inability to upgrade iLO 2 firmware, 201
Integrated Remote Console option, 85
Multi-user access to the Integrated Remote Console, 89
preparing to set up iLO 2, 17
Schema-free scripted setup, 133
Securing RBSU, 42
Setting up directory services, 136
SSL certificate administration, 45
Upgrading iLO 2 firmware, 24
Using bulk import tools, 161
ROM-Based Setup Utility (RBSU)
Access options, 38
Adding a new user, 29
Configuring Remote Serial Console, 100
DHCP/DNS Settings, 64
Group administration, 32
iLO 2 RBSU unavailable after iLO 2 and server reset, 188
Network Settings, 60
preparing to set up iLO 2, 17
Securing RBSU, 42
Setting up iLO 2 using iLO 2 RBSU, 20
RSM (Remote Server Management)
Linux configuration example, 101
Linux device driver support, 22
Recovering from a failed iLO 2 firmware update, 26

S

schema documentation
HP Management Core LDAP OID classes and attributes, 171
Lights-Out Management specific LDAP OID classes and attributes, 175
Schema documentation, 137
Schema-free HPLOMIG-based setup, 134
schema installer
Directory services preparation for Active Directory, 141
HP Lights-Out directory package, 163
Results, 139
Schema installer, 138
Schema required software, 137
Setup, 138
schema preview, 138
schema-free integration, 132
schema-free options
Advantages and disadvantages of schema-free directories and HP schema directory, 131
Schema-free browser-based setup, 133
Schema-free directory integration, 131
Schema-free setup options, 134
schema-free, setup
Active Directory preparation, 132
Configuring directories when schema-free integration is selected, 169

Schema-free browser-based setup, 133
Schema-free scripted setup, 133
Setting up management processors for directories, 170
screen capture and replay, 80
scripted setup, 133
scripts, 161
Secure Shell (SSH)
Access options, 38
Configuring Remote Serial Console, 100
Connecting to the iLO 2 using AES/3DES encryption, 54
Encryption, 53
Encryption settings, 54
HP SIM single sign-on (SSO), 55
preparing to set up iLO 2, 17
Remote Console overview and licensing options, 81
Remote Serial Console troubleshooting, 193
Security, 41
SSH key administration, 44
SSH text support from a Remote Console session, 197
Text-based remote console overview, 95
Troubleshooting SSH and Telnet issues, 197
Two-factor authentication, 46
Virtual serial port and remote serial console, 99
Virtual serial port raw mode, 102
Secure Sockets Layer (SSL)
Active Directory installation prerequisites, 140
Active Directory preparation, 132
Advantages and disadvantages of schema-free directories and HP schema directory, 131
Authentication code error message, 191
Configuring directories when HP Extended schema is selected, 168
Directory services preparation for Active Directory, 141
Directory services support, 137
Directory settings, 51
eDirectory installation prerequisites, 149
Encryption, 53
Finding management processors, 163
iLO 2 does not respond to SSL requests, 204
Inability to access the login page, 188
Inability to connect to the iLO 2 Diagnostic Port, 188
Introduction to certificate services, 132
Schema-free setup options, 134
Security, 41
Setup, 138
SSL certificate administration, 45
Testing SSL, 204
Verifying certificate services, 133
WS-Management compatibility overview, 13
security enhancements
Password guidelines, 42
Securing RBSU, 42
security features
Encryption, 53
Security, 41
SSH key administration, 44
security override, 42
security settings
General security guidelines, 41
Login security, 44
Password guidelines, 42
Privileges, 44
Securing RBSU, 42
security, computer lock, 58
security, login delay, 20
serial console, configuring remote, 100
serial console, remote, 100
serial port, virtual, 99
server POST tracking, BL p-Class, 123
server status, 74
server warnings and cautions, 180
session options, 195
setting up iLO 2, 17
setting up single sign-on, 55
settings
Configuring directory settings, 51
Directory services, 130
Microsoft? Windows? Server 2003 settings, 95
Recommended server settings, 95
Red Hat Linux and SUSE Linux server settings, 95
Schema-free setup options, 134
SSH key administration, 44
settings, BladeSystem HP Onboard Administrator, 124
settings, directory services, 51
settings, HP SIM
Setting up HP SIM SSO, 57
Setting up iLO 2 for HP SIM SSO, 55
settings, iLO 2 access, 33
settings, iLO 2 and c-Class enclosure addressing, 125
settings, iLO 2 encryption options, 53
settings, iLO 2 HP SIM, 65
settings, iLO 2 network access
Network, 60
Network Settings, 60
settings, iLO 2 security, 41
settings, iLO 2 SNMP, 65
settings, iLO 2 users, 28
settings, Remote Console, 81
settings, two-factor athentication, 46
setup, blade
HP BladeSystem setup, 70
ProLiant BladeSystem HP Onboard Administrator, 124
setup, browser-based
Schema-free browser-based setup, 133
setting up iLO 2 with the browser-based option, 21
Setting up user accounts, 20
setup, schema-free
Schema-free browser-based setup, 133
Schema-free HPLOMIG-based setup, 134
Schema-free scripted setup, 133
Schema-free setup options, 134
setup, scripted
Schema-free scripted setup, 133
Setting up user accounts, 20
shared network port, enabling
Enabling the iLO 2 Shared Network Port feature through iLO 2 RBSU, 62

Enabling the iLO 2 Shared Network Port feature through the web interface, 63
Re-enabling the dedicated iLO 2 management port, 63
shared network port, features
Enabling the iLO 2 Shared Network Port feature, 62
iLO 2 Shared Management Port features and restrictions, 62
shared network port, requirements, 61
shared network port, restrictions, 62
Shared Remote Console, 89
sign-on, HP SIM single, 57
Simple Network Management Protocol (SNMP)
Enabling SNMP alerts, 65
Event log entries, 183
iLO 2 configuration overview, 24
iLO 2 Security Override switch, 191
iLO 2 Security Override Switch administration, 42
Inability to get SNMP information from HP SIM, 201
Inability to receive HP SIM alarms (SNMP traps) from iLO 2, 191
Installing iLO 2 device drivers, 21
Integrating iLO 2 with HP SIM, 178
ProLiant BL p-Class Advanced management, 119
ProLiant BL p-Class alert forwarding, 124
Receiving SNMP alerts in HP SIM, 180
SNMP/Insight Manager settings, 65
Supported server operating system software, 15
single sign-on, setting up, 55
single sign-on, setting up HP SIM, 57
SLES procedures, 192
SMASH (System Management Architecture for Server Hardware)
Integrated Remote Console option, 85
Multi-user access to the Integrated Remote Console, 89
preparing to set up iLO 2, 17
Setting up user accounts, 20
Snap-In installer
Active Directory snap-ins, 146
HP Devices, 146
Management snap-in installer, 140
Members, 146
Snap-in installation and initialization for Active Directory, 142
Snap-in installation and initialization for eDirectory, 150
SNMP (Simple Network Management Protocol)
Enabling SNMP alerts, 65
Event log entries, 183
iLO 2 configuration overview, 24
iLO 2 Security Override switch, 191
iLO 2 Security Override Switch administration, 42
Inability to get SNMP information from HP SIM, 201
Inability to receive HP SIM alarms (SNMP?traps) from?iLO 2, 191
Installing iLO 2 device drivers, 21
Integrating iLO 2 with HP SIM, 178
ProLiant BL p-Class Advanced management, 119
ProLiant BL p-Class alert forwarding, 124
Receiving SNMP alerts in HP SIM, 180
SNMP/Insight Manager settings, 65
Supported server operating system software, 15
SNMP alert, definitions, 66
SNMP alerts
Enabling SNMP alerts, 65
ProLiant BL p-Class alert forwarding, 124
Receiving SNMP alerts in HP SIM, 180
SNMP settings
Enabling SNMP alerts, 65
SNMP/Insight Manager settings, 65
software installation, 72
software supported, 15
software troubleshooting, 186
SSH (Secure Shell)
Access options, 38
Configuring Remote Serial Console, 100
Connecting to the iLO 2 using AES/3DES encryption, 54
Encryption, 53
Encryption settings, 54
HP SIM single sign-on (SSO), 55
preparing to set up iLO 2, 17
Remote Console overview and licensing options, 81
Remote Serial Console troubleshooting, 193
Security, 41
SSH key administration, 44
SSH text support from a Remote Console session, 197
Text-based remote console overview, 95
Troubleshooting SSH and Telnet issues, 197
Two-factor authentication, 46
Virtual serial port and remote serial console, 99
Virtual serial port raw mode, 102
SSH key authorization, 44
SSH key, adding, 44
SSL certificate administration, 45
SSL connection
Active Directory preparation, 132
eDirectory installation prerequisites, 149
Introduction to certificate services, 132
Setup, 138
SSL certificate administration, 45
SSL requests, iLO 2 response, 204
SSL, (Secure Sockets Layer)
Active Directory installation prerequisites, 140
Active Directory preparation, 132
Advantages and disadvantages of schema-free directories and HP schema directory, 131
Authentication code error message, 191
Configuring directories when HP Extended schema is selected, 168
Directory services preparation for Active Directory, 141
Directory services support, 137
Directory settings, 51
eDirectory installation prerequisites, 149
Encryption, 53
Finding management processors, 163
iLO 2 does not respond to SSL requests, 204
Inability to access the login page, 188
Inability to connect to the iLO 2 Diagnostic Port, 188
Introduction to certificate services, 132

Schema-free setup options, 134
Security, 41
Setup, 138
SSL certificate administration, 45
Testing SSL, 204
Verifying certificate services, 133
WS-Management compatibility overview, 13
SSL, WS-Management, 13
static IP bay settings
Configuring static IP bay settings, 69
Static IP bay configuration, 68
static IP configuration, BL p-Class, 68
status, WS-Management, 13
subnet mask, 60
subsystem name, 61
support, 206
supported operating systems, 15
supported software
JVM support, 186
Supported browsers and client operating systems, 15
Supported server operating system software, 15
System Erase Utility, 204
system information summary, 75
System Information tab, 75
System Management Architecture for Server Hardware (SMASH)
Integrated Remote Console option, 85
Multi-user access to the Integrated Remote Console, 89
preparing to set up iLO 2, 17
Setting up user accounts, 20
System Management Homepage, 80
system status
Diagnostics, 79
iLO 2 Log, 77
IML, 78
System status and status summary information, 74
Web Administration, 128
system, health information, 75
Systems Insight Manager association, 179
Systems Insight Manager integration
Configuring Insight Manager integration, 67
Integrating iLO 2 with HP SIM, 178
Systems Insight Manager port matching, 181
Systems Insight Manager, overview, 178

T

technical support
Before you contact HP, 207
HP contact information, 207
Technical support, 206
telephone numbers
Before you contact HP, 207
HP contact information, 207
Technical support, 206
Telnet, troubleshooting, 198
Telnet, using, 198
temperature monitoring, 76
Terminal Services Client requirements
Remote Console and Terminal Services clients, 37
Terminal Services client requirements, 35
Terminal Services Passthrough option, 35
Terminal Services Passthrough option display, 37
Troubleshooting terminal services issues, 197
Windows RDP passthrough service, 36
Terminal Services passthrough option, 36
Terminal Services passthrough, enable, 36
Terminal Services passthrough, installation, 36
Terminal Services, availability
Terminal Services Passthrough option display, 37
Terminal Services warning message, 37
Terminal Services, troubleshooting
Terminal Services button is not working, 197
Terminal Services proxy stops responding, 198
Terminal Services troubleshooting, 38
Terminal Services warning message, 37
Troubleshooting terminal services issues, 197
text-based remote console
Customizing iLO 2 Text Console, 97
Text-based console during POST, 95
Text-based remote console overview, 95
Using a Linux session, 99
Using iLO Text Console, 97
timeout, Virtual Media, 104
TPM (Trusted Platform Module), 43
trap messages, 191
troubleshooting, console replay, 195
troubleshooting, directory services, 191
troubleshooting, GNOME interface, 197
troubleshooting, IRC
Inactive IRC, 196
Internet Explorer 7 and a flickering remote console screen, 194
IRC Failed to connect to server error message, 196
IRC toolbar icons do not update, 196
Repeating keys on the Remote Console, 197
Troubleshooting Integrated Remote Console issues, 194
troubleshooting, miscellaneous, 199
troubleshooting, remote console playback, 197
troubleshooting, remote serial console, 193
troubleshooting, repeating keys, 197
troubleshooting, using event log entries, 183
two-factor authentication
Two-factor authentication, 46
Two-factor authentication error, 190
two-factor authentication, directory authentication, 50
two-factor authentication, first time use, 47
two-factor authentication, login, 49
two-factor authentication, setup, 47
two-factor authentication, user certificates, 48

U

UID (unit identification)
Enclosure information, 122
iLO 2 BL c-Class tab, 124
Power enclosure information, 122
System status and status summary information, 74
WS-Management compatibility overview, 13
unit identification (UID)

Enclosure information, 122
iLO 2 BL c-Class tab, 124
Power enclosure information, 122
System status and status summary information, 74
WS-Management compatibility overview, 13
updating drivers
Linux device driver support, 22
Microsoft device driver support, 22
Novell NetWare device driver support, 22
updating the firmware, 24
USB devices, 105
USB drive key, 105
USB key, support, 106
USB support, 107
user access
How user time restrictions are enforced, 160
iLO 2 browser interface overview, 14
User accounts and access, 43
User address restrictions, 159
User administration, 28
User login using directory services, 156
user account, adding, 29
user account, deleting, 31
user account, modifying, 31
user accounts
User accounts and access, 43
Viewing or modifying existing user settings, 31
user certificates, two-factor authentication, 48
user contexts, 192
user interface mode, 14
user roles
Active Directory role restrictions, 147
Creating multiple restrictions and roles, 160
DNS-based restrictions, 160
eDirectory Role Restrictions, 154
Enforced client IP address or DNS name access, 148, 154
How user time restrictions are enforced, 160
IP address and subnet mask restrictions, 159
IP address range restrictions, 159
Restricting roles, 158
Role address restrictions, 159
Role time restrictions, 159
Time restrictions, 147, 154
User address restrictions, 159
Using multiple roles, 157
user settings, 43
using Console Capture, 90
using the GUI, 14
using the web interface, 14

V

video issues
Troubleshooting iLO Video Player issues, 199
Troubleshooting video and monitor issues, 198
Video applications not displaying in the Remote Console, 198
virtual CD/DVD-ROM, 109
virtual CD/DVD-ROM mounting, 110
virtual CD/DVD-ROM, support, 110
virtual devices, 107
virtual floppy
iLO 2 Virtual Floppy/USBKey, 105
Mounting USB Virtual Floppy/USBKey in NetWare 6.5, 107
Mounting USB Virtual Media/USBKey in Linux, 108
Troubleshooting Virtual Media issues, 198
virtual floppy, support, 106
Virtual folder operating system notes, 112
virtual indicators, 74
virtual media access
Connect Virtual Media screen, 72
Inability to access virtual media or graphical remote console, 188
Mounting USB Virtual Floppy/USBKey in NetWare 6.5, 107
Mounting USB Virtual Media/USBKey in Linux, 108
Operating system USB support, 107
Troubleshooting Virtual Media issues, 198
Virtual media, 104
Virtual Media applet has a red X and will not display, 199
virtual media image files, 111
Virtual Media, using
Mounting USB Virtual Floppy/USBKey in NetWare 6.5, 107
Mounting USB Virtual Media/USBKey in Linux, 108
Troubleshooting Virtual Media issues, 198
Using iLO 2 Virtual Media devices, 104
virtual serial port, 99
virtual serial port, raw mode, 102
VRM monitoring, 77
VT320 serial console, access, 100

W

Warning and alarm messages, 37
warning messages, Terminal Services, 37
website, HP, 207
Windows EMS Console, enabling, 102
Windows server support
Microsoft device driver support, 22
Supported browsers and client operating systems, 15
Supported server operating system software, 15
WINS name, 61
WINS server, 61
WS-Management, 13

X

XML (Extensible Markup Language)
Connecting to the iLO 2 using AES/3DES encryption, 54
Encryption, 53
High Performance Mouse settings, 88
preparing to set up iLO 2, 17
SSL certificate administration, 45
Upgrading iLO 2 firmware, 24
Using Console Capture, 90
Using iLO 2 Virtual Media devices, 104

Virtual media, 104