Abstract
This document contains specific information that is intended for users of this HPE product.
Notices

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.


Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

Microsoft®, and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Warranty

Hewlett Packard Enterprise will replace defective delivery media replacement for a period of one year (12 months) following the date of purchase. Startup technical software support – Available for no additional charge by calling Support up to 90 days from the date of purchase. Phone support assisting customers with installation, set-up and questions pertaining to the canned scripts and respective usages are supported. Worldwide numbers for Support are available at: http://www8.hp.com/us/en/hpe/contact/ww-contact-us.html

Complete warranty can be found at: http://h20566.www2.hpe.com/portal/site/hpsc/public/

Revision history

Changes in this edition:

In the "Using iLO 3" chapter:

- Updated the URL links.
- Added details for power reading at iLO initialization in the Power Meter Readings description

<table>
<thead>
<tr>
<th>Document Manufacturing part number</th>
<th>Edition number</th>
<th>Publication Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>5200-2497</td>
<td>Eighth</td>
<td>July 2017</td>
</tr>
<tr>
<td>5200-2459</td>
<td>Seventh</td>
<td>January 2017</td>
</tr>
</tbody>
</table>
# Contents

## Introduction

<table>
<thead>
<tr>
<th>Feature</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity iLO 3 features</td>
<td>10</td>
</tr>
<tr>
<td>Always-on capability</td>
<td>10</td>
</tr>
<tr>
<td>Multiple access methods</td>
<td>10</td>
</tr>
<tr>
<td>Mirrored console</td>
<td>11</td>
</tr>
<tr>
<td>Remote power and reset</td>
<td>11</td>
</tr>
<tr>
<td>Virtual front panel</td>
<td>11</td>
</tr>
<tr>
<td>Security</td>
<td>11</td>
</tr>
<tr>
<td>User password access control</td>
<td>11</td>
</tr>
<tr>
<td>Multiple users</td>
<td>12</td>
</tr>
<tr>
<td>System management homepage</td>
<td>12</td>
</tr>
<tr>
<td>Firmware upgrades</td>
<td>12</td>
</tr>
<tr>
<td>Internal subsystem information</td>
<td>12</td>
</tr>
<tr>
<td>DHCP and DNS support</td>
<td>12</td>
</tr>
<tr>
<td>Group actions</td>
<td>13</td>
</tr>
<tr>
<td>Group actions using HPE SIM</td>
<td>13</td>
</tr>
<tr>
<td>SNMP</td>
<td>13</td>
</tr>
<tr>
<td>Event logging</td>
<td>13</td>
</tr>
<tr>
<td>Directory-based secure authentication and authorization using LDAP</td>
<td>13</td>
</tr>
<tr>
<td>Schema-free LDAP</td>
<td>13</td>
</tr>
<tr>
<td>Integrated Remote Console</td>
<td>14</td>
</tr>
<tr>
<td>Virtual Media</td>
<td>14</td>
</tr>
<tr>
<td>Power Management</td>
<td>14</td>
</tr>
<tr>
<td>HPE Insight Control power management</td>
<td>15</td>
</tr>
</tbody>
</table>

## iLO 3 Advanced Pack licensing

<table>
<thead>
<tr>
<th>Component</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Components and cables required for iLO 3 operation</td>
<td>16</td>
</tr>
<tr>
<td>Integrity iLO 3 supported browsers and client operating systems</td>
<td>16</td>
</tr>
<tr>
<td>Security</td>
<td>17</td>
</tr>
</tbody>
</table>

## Ports, buttons, LEDs, and components

<table>
<thead>
<tr>
<th>Component</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>iLO 3 Physical Presence button</td>
<td>18</td>
</tr>
<tr>
<td>Creating or modifying user passwords in Security Override mode</td>
<td>20</td>
</tr>
<tr>
<td>Using TPM Physical Presence mode for special commands</td>
<td>20</td>
</tr>
<tr>
<td>Canceling iLO Login Timeout via local Physical Presence button</td>
<td>21</td>
</tr>
<tr>
<td>HPE Integrity server blade components</td>
<td>21</td>
</tr>
<tr>
<td>HPE BladeSystem Enclosures</td>
<td>22</td>
</tr>
<tr>
<td>c7000 Enclosure</td>
<td>22</td>
</tr>
<tr>
<td>c3000 Enclosure</td>
<td>22</td>
</tr>
<tr>
<td>Onboard Administrator</td>
<td>22</td>
</tr>
<tr>
<td>Integrity rx2800 i2/i4/i6 servers</td>
<td>22</td>
</tr>
</tbody>
</table>

## Getting connected to iLO 3

<table>
<thead>
<tr>
<th>Component</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rackmount server connection</td>
<td>24</td>
</tr>
<tr>
<td>Preparing to set up iLO 3</td>
<td>24</td>
</tr>
<tr>
<td>Determining the physical iLO 3 access method</td>
<td>24</td>
</tr>
<tr>
<td>Determining the iLO 3 MP LAN configuration method</td>
<td>25</td>
</tr>
<tr>
<td>Configuring the iLO 3 MP LAN using DHCP and DNS</td>
<td>26</td>
</tr>
</tbody>
</table>
### Contents

- **Using iLO 3**
  - Text user interface .......................................................... 45
  - MP command interfaces .................................................. 45
    - **MP Main Menu commands** ........................................ 46
    - **Command Menu** ..................................................... 52
    - **Command-line interface scripting** ............................. 53
      - **Expect script example** ........................................... 54
    - **Command menu commands and standard command line scripting syntax** ................................. 55
      - `BLADE`: Display enclosure, bay, and Onboard Administrator information ................................ 56
      - `CA`: Configure serial port parameters .......................... 57
      - `DATE`: Display date .................................................. 58
      - `DC` (Default Configuration): Reset all parameters to default configurations .......................... 58
      - `DF`: Display FRUID information ................................. 59
      - `DI`: Disconnect remote or LAN console ..................... 60
      - `DNS`: DNS settings .................................................. 60
      - `FW`: Upgrade the MP firmware ................................. 60

- **Server blade connection** ............................................... 28
- **Connecting the server blade to iLO 3 using the Onboard Administrator** ........................... 28
  - **DHCP and auxiliary blades** ........................................ 28
  - **Auto login** ............................................................. 29
- **Connecting to a server blade iLO 3 using the console serial port** .................................... 31
- **Connecting to iLO 3 using the Onboard Administrator** .................................................. 31

- **Additional setup** .......................................................... 31
  - **Modifying default account configuration settings** ............... 32
  - **Changing the default password** .................................... 32
  - **Setting up user accounts** ........................................... 32
  - **Setting up security** .................................................. 32
    - **Setting security access** ........................................... 32
  - **Setting iLO MP LAN from UEFI** .................................... 32

- **Logging in to iLO 3** ...................................................... 34
  - **Logging in to iLO 3 using the web GUI** .......................... 34
  - **Logging in to iLO 3 using the command-line interface** ............ 34
  - **Logging in to iLO 3 through the OA** ............................... 35

- **Accessing the host (operating system) console** .................................................. 36
  - **Accessing a text host console through iLO 3 virtual serial console** ........................... 36
  - **Accessing online help** .............................................. 37
  - **Accessing a text host console using the TUI** ...................... 37
  - **Help system** .......................................................... 37

- **Configuring DHCP, DNS, LDAP, and schema-free LDAP** ........................................... 39
  - **Configuring DHCP** .................................................. 39
  - **Configuring DNS** ................................................... 40
  - **Configuring LDAP extended schema** ............................. 41
    - **Login process using directory services with extended LDAP** ............................... 42
  - **Configuring schema-free LDAP** ................................... 42
    - **Setting up directory security groups** .......................... 43
  - **Login process using directory services without schema extensions** ..................... 44
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>HE: Print Help Menu and MP hardware and firmware revision</td>
<td>61</td>
</tr>
<tr>
<td>ID: System information settings</td>
<td>62</td>
</tr>
<tr>
<td>IT: Modify MP inactivity timers</td>
<td>62</td>
</tr>
<tr>
<td>LC: LAN configuration usage</td>
<td>62</td>
</tr>
<tr>
<td>LDAP: LDAP directory settings</td>
<td>64</td>
</tr>
<tr>
<td>LM: License manager</td>
<td>66</td>
</tr>
<tr>
<td>LOC: Locator UID LED configuration</td>
<td>66</td>
</tr>
<tr>
<td>LS: LAN status</td>
<td>66</td>
</tr>
<tr>
<td>PC: Power control</td>
<td>67</td>
</tr>
<tr>
<td>PM: Power regulator mode</td>
<td>67</td>
</tr>
<tr>
<td>PR: Set power restore policy</td>
<td>68</td>
</tr>
<tr>
<td>PS: Power status</td>
<td>68</td>
</tr>
<tr>
<td>RS: Reset system through the RST signal</td>
<td>68</td>
</tr>
<tr>
<td>SA: Set access</td>
<td>69</td>
</tr>
<tr>
<td>SO: Security option help</td>
<td>69</td>
</tr>
<tr>
<td>SYSREV, SR: Firmware revisions</td>
<td>71</td>
</tr>
<tr>
<td>SS: System processor status</td>
<td>72</td>
</tr>
<tr>
<td>SYSET: Display system settings</td>
<td>72</td>
</tr>
<tr>
<td>TC: System reset through INIT signal</td>
<td>72</td>
</tr>
<tr>
<td>TE: Send a message to other mirroring terminals</td>
<td>73</td>
</tr>
<tr>
<td>UC: User Configuration (users, passwords, and so on)</td>
<td>73</td>
</tr>
<tr>
<td>WHO: Display a list of connected iLO 3 users</td>
<td>75</td>
</tr>
<tr>
<td>WOL: Wake-On-LAN</td>
<td>75</td>
</tr>
<tr>
<td>XD: iLO 3 diagnostics and reset</td>
<td>75</td>
</tr>
<tr>
<td>Web GUI</td>
<td>76</td>
</tr>
<tr>
<td>Accessing the iLO 3 web GUI</td>
<td>76</td>
</tr>
<tr>
<td>Status Summary</td>
<td>76</td>
</tr>
<tr>
<td>Status Summary&gt;Overview tab</td>
<td>77</td>
</tr>
<tr>
<td>Status Summary&gt;Active Users</td>
<td>77</td>
</tr>
<tr>
<td>Status Summary&gt;FW Revisions</td>
<td>79</td>
</tr>
<tr>
<td>System Health</td>
<td>79</td>
</tr>
<tr>
<td>System Event Log</td>
<td>81</td>
</tr>
<tr>
<td>Forward Progress Log</td>
<td>83</td>
</tr>
<tr>
<td>System Inventory</td>
<td>84</td>
</tr>
<tr>
<td>iLO Health</td>
<td>85</td>
</tr>
<tr>
<td>iLO Event Log</td>
<td>86</td>
</tr>
<tr>
<td>Remote Serial Console</td>
<td>86</td>
</tr>
<tr>
<td>Remote Serial Console</td>
<td>89</td>
</tr>
<tr>
<td>Integrated Remote Console</td>
<td>89</td>
</tr>
<tr>
<td>IRC requirements</td>
<td>89</td>
</tr>
<tr>
<td>Instructions for importing the iLO certificate on to the client</td>
<td>90</td>
</tr>
<tr>
<td>Configuration and usage suggestions</td>
<td>90</td>
</tr>
<tr>
<td>IRC features</td>
<td>91</td>
</tr>
<tr>
<td>IRC limitations</td>
<td>91</td>
</tr>
<tr>
<td>Using the IRC</td>
<td>91</td>
</tr>
<tr>
<td>Virtual Media</td>
<td>92</td>
</tr>
<tr>
<td>Using iLO 3 virtual media devices</td>
<td>93</td>
</tr>
<tr>
<td>Supported operating systems and USB support for virtual Media</td>
<td>99</td>
</tr>
<tr>
<td>Java Plug-in version</td>
<td>99</td>
</tr>
<tr>
<td>Client operating system and browser support for virtual media</td>
<td>100</td>
</tr>
<tr>
<td>Power Management</td>
<td>100</td>
</tr>
<tr>
<td>Power &amp; Reset</td>
<td>100</td>
</tr>
<tr>
<td>Power Meter Readings</td>
<td>102</td>
</tr>
<tr>
<td>Power Regulator &amp; Capping</td>
<td>105</td>
</tr>
<tr>
<td>Administration</td>
<td>107</td>
</tr>
</tbody>
</table>
Installing and configuring directory services ......................... 135

Directory services .................................................................................. 135
Features supported by directory integration........................................ 135
Directory services installation prerequisites...................................... 136
Installing directory services................................................................. 136
Schema documentation......................................................................... 136
Directory services support................................................................. 136
eDirectory installation prerequisites.................................................... 137
Required schema software.................................................................... 137
Schema installer..................................................................................... 137
  Schema preview............................................................................... 137
  Schema setup.................................................................................. 138
  Results............................................................................................. 139
Management snap-in installer.............................................................. 139
Directory services for Active Directory........................................... 140
  Active Directory installation prerequisites.................................... 140
  Preparing directory services for Active Directory.......................... 140
  Installing and initializing snap-ins for Active Directory................. 141
  Example: creating and configuring directory objects for use with iLO 3 in Active Directory...................................................... 142
Directory services objects....................................................................... 145
  Active Directory snap-ins............................................................... 145
  Setting login restrictions............................................................... 147
  Setting user or group role rights.................................................... 150
Directory services for eDirectory....................................................... 152
  Installing and initializing snap-ins for eDirectory.......................... 152
  Example: creating and configuring directory objects for use with iLO 3 devices in eDirectory................................................................. 152
    Creating objects.......................................................................... 153
    Creating roles.............................................................................. 153
  Directory services objects for eDirectory........................................ 155
    Adding role managed devices....................................................... 155
    Adding members........................................................................ 156
    Setting role restrictions.............................................................. 157
    Setting time restrictions............................................................. 157
    Defining client IP address or DNS name access............................ 157
  Setting Lights-Out management device rights.................................. 158
Support and other resources .......................................................... 179

Accessing Hewlett Packard Enterprise Support.................................................. 179
Accessing updates............................................................................................ 179
Customer self repair.......................................................................................... 180
Remote support................................................................................................ 180
Warranty information....................................................................................... 180
Regulatory information.................................................................................... 181
Documentation feedback.................................................................................. 181

Standard terms, abbreviations, and acronyms .............................................. 182

A......................................................................................................................... 182
B......................................................................................................................... 182
C........................................................................................................................ 183
D......................................................................................................................... 183
E......................................................................................................................... 184
F......................................................................................................................... 184
The Integrated Lights-Out Management Processor (iLO MP) for Integrity servers is an autonomous management subsystem embedded directly on the server. The iLO MP is the foundation of High Availability (HA) embedded server and fault management. The iLO MP also provides system administrators with secure remote management capabilities regardless of server status or location. The iLO is available whenever the server is connected to a power source, even if the server main power switch is in the Off position.

Remote access is the key to maximizing efficiency of administration and troubleshooting for enterprise servers. Integrity servers are designed so that administrative functions that are performed locally, can also be performed remotely. The iLO enables remote access to the operating system console, control over the server power and hardware reset functionality, and works with the server to enable remote network booting through a variety of methods.

With the release of Integrity iLO 3, Integrity servers introduce a new concept in remote management solutions which automatically scale with the size of your system. Integrity iLO 3 is an integral part of the management architecture inside new Integrity multi-bladed conjoined servers. Integrity iLO 3 management is included in all newer Integrity systems and ships with a full iLO Advanced license factory installed in every server.

This document addresses HPE Integrated Lights-Out 3 (iLO 3) for the HPE Integrity BL860c i2, BL870c i2, and BL890c i2 Server Blades; HPE Integrity BL860c i4, BL870c i4, and BL890c i4 Server Blades; HPE Integrity BL860c i6, BL870c i6, and BL890c i6 Server Blades; and HPE Integrity rx2800 i2/i4/i6 servers. To learn more about Integrity iLO, see Integrity iLO3 Quick Specs. For information on iLO for ProLiant servers and ProLiant BladeSystem server blades, see the Hewlett Packard Enterprise website at http://www.hpe.com/info/ilo.

Superdome 2

On HPE Superdome 2 servers, every cell blade contains a physical iLO 3 chip. The Superdome 2 Onboard Administrator is the primary interface for managing a Superdome Complex collecting and centralizing all data from the iLOs. Because the Superdome 2 OA is the primary interface, you do not have to directly access the iLOs. Consequently on Superdome 2, the iLO 3 GUI interface is not available, and access to the CLI is restricted. The iLO 3 functions (such as assigning virtual media), which in a BladeSystem require a user "drill down" from the OA to an iLO, are now brought up into the Superdome 2 OA. The iLO 3 functions invisibly inside the server. User commands are directed to the iLO from the Superdome 2 OA.

The iLO 3 user interfaces are not eliminated from HPE Superdome 2 iLO 3, but login capability to iLO 3 command-line interface is limited to Auto Login from the Onboard Administrator.

In addition, on HPE Superdome 2 servers, iLO 3 firmware is updated as part of the HPE Superdome 2 complex firmware update process, managed from the Onboard Administrator.

For information on the HPE BladeSystem Onboard Administrator (OA) for HPE Superdome 2 servers, see the HPE Integrity Superdome 2 Onboard Administrator User Guide on the Hewlett Packard Enterprise website at http://www.hpe.com/info/Integrity_Servers-docs.

IMPORTANT:

This guide addresses server-specific details that vary between server products. These details are frequently updated. For the latest server-specific product information, see the product-specific Quickspecs on the Hewlett Packard Enterprise website at https://www.hpe.com/info/Integrity_Servers-docs.
Features

Integrity iLO 3 features provide essential lights-out functionality on iLO 3-supported Hewlett Packard Enterprise servers as well as:

• System board management functions
• Diagnostics and troubleshooting
• Control of power, reset, and Transfer of Control (TOC)/INIT capabilities
• Monitoring of server health and status
• Display of detailed information about the various internal subsystems and field replaceable units (FRUs)
• At-a-glance virtual front panel to monitor system status and see the state of front panel LEDs
• Display and recording of system events with 4X larger console log to capture more administrative information
• Scalable management: automatically grows with your multi-bladed Integrity servers, easily managed through a consolidated iLO interface
• Direct System Firmware updating: use SUM, or iLO 3 directly, to easily update system firmware without OS assistance, even while the OS is running or the server power is off

Integrity iLO 3 advanced features provide additional functionality such as 3X faster virtual media with higher performance file transfers and updates. In addition, the advanced features increase security by integrating iLO 3 user administration with the Active Directory or eDirectory. Integrity iLO 3 advanced features are enabled automatically on every Integrity server equipped with iLO 3. The Integrity iLO 3 Advanced Pack license is built into every system. No additional licensing is needed.

Integrity iLO is completely independent of the host system and the operating system. It has its own microprocessor and runs its own firmware. The operating system cannot send packets out on the MP LAN, and packets on the MP LAN cannot go to the operating system. The MP LAN is exclusive to iLO and is driven by an embedded real-time operating system (RTOS) running on iLO.

NOTE:
The following ProLiant iLO 3 features are not available on Integrity iLO 3:

• Virtual Folder
• Shared LAN
• Graphics Console Replay

Integrity iLO 3 features

Always-on capability

Integrity iLO 3 is active and available through the connections of the iLO MP LAN and the local serial port as long as the power cord is plugged in. In the event of a complete power failure, iLO 3 data is protected by an onboard battery backup.

Multiple access methods

Access methods, with the exception of the serial console, can be enabled or disabled.

The available methods to access iLO 3 are as follows:

LAN

Using Telnet, web, or SSH to access the iLO MP LAN
NOTE:
Integrity iLO 3 ships with Telnet disabled by default.

Local serial port
Using a terminal or laptop computer for direct connection

Web
Using a graphical user interface (GUI)

Mirrored console
The system console output stream is reflected to all connected console users. Any user with write access can provide input.

Remote power and reset
Integrity iLO 3 enables you to view and control the power state of the server. It also provides options to reset the system or iLO 3.

Virtual front panel
The virtual front panel (VFP) presents a summary of the system front panel using direct console addressing.

Security
Integrity iLO 3 provides strong security for remote management in IT environments, such as the following:

- User-defined TCP/IP ports
- User accounts and access management
- Lightweight Directory Access Protocol (LDAP)-based directory services authentication and authorization
- Encrypted communication using SSL and SSH

Integrity iLO 3’s web GUI is supported with Microsoft Internet Explorer version 8, 10, and 11, Firefox version 51 or Chrome version 46. The Remote Serial Console and vMedia applets require the 32-bit Java Plug-in 1.6.0_31.

User password access control
Integrity iLO 3 is restricted by user accounts. User accounts are password protected and are assigned access rights that define a specific level of access to the server and to the iLO 3 MP commands. Integrity iLO 3 supports both LDAP directory user authentication and locally stored iLO 3 user accounts. Integrity iLO 3 users can have any of the following user rights:

Remote console access
Right to access the system console (the host operating system). This does not bypass host authentication requirements, if any.

Virtual power & reset
Right to configure power settings and reset the host platform.

Configure iLO settings
Right to configure all iLO 3 MP settings and some system settings, such as the power restore policy.
Administer user accounts
Right to create, modify, and delete local iLO 3 user accounts.

Virtual Media
Enables you to connect devices such as CD/DVD-ROM drives, network drives, and USB keys as virtual devices through the network.

Multiple users
Multiple users can interact with iLO 3. However, iLO 3 command mode and console mode are mirrored, allowing only one user at a time to have write access to the shared console. When a command is completed, write access is released, and any user can initiate another command.

**IMPORTANT:**
Although iLO 3 can support multiple simultaneous connections, to do so can impact performance. Hewlett Packard Enterprise does not recommend running more than eight simultaneous connections.

Integrity iLO 3 supports the following connections simultaneously:
- Four web (each web connection can have a remote serial console connection as well and not be counted as part of the total number of connections allowed)
- Six SSH
- One console serial port
- Two Telnet
- One vMedia

System management homepage
The HPE Insight Management Agents support a web interface for access to runtime management data through the HPE System Management Homepage. The HPE 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 HPE 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.

Firmware upgrades
Firmware upgrades enhance the functionality of iLO 3.
The iLO 3 MP firmware and system firmware is remotely upgradeable from an HTTP/HTTPS source. Integrity iLO 3 has direct system firmware updating capability. To easily update system firmware without OS assistance, even while the OS is running or the server power is off, use SUM, or iLO 3 directly.

Internal subsystem information
Integrity iLO 3 displays information about the following internal subsystems:
- FRU information
- System power state and fan status
- Processor Status

DHCP and DNS support
Integrity iLO 3 supports the Dynamic Host Configuration Protocol (DHCP) and the Domain Name System (DNS) configuration options for acquiring network information through the MP LAN port. When iLO 3
starts, it acquires the port configuration stored on a DHCP server to assign an IP address to the MP LAN port. If DNS is configured, then this information is updated on the DNS server. The simplest method to connect for the first time to iLO 3 is with the default DNS name, for example io0014c39c064f. You can find the default DNS name on the iLO Network Information Tag.

NOTE:

- On server blades, the iLO Network Information Tag is located on the right side of the monarch blade.
- On HPE Integrity rx2800 i2/i4/i6 servers, the iLO Network Information Tag is located on a pull-tab in the front panel.

Group actions

Group actions is not currently supported in Integrity iLO 3.

Group actions using HPE SIM

HPE Systems Insight Manager (SIM) is a system-level management tool that supports running commands from HPE SIM using the SSH interface. HPE SIM enables you to perform similar management activities across multiple iLO 3s (group actions) without requiring you to access each iLO 3 individually. Group actions are launched from the HPE SIM GUI and are supported at all times, regardless of the server power state.

You can download HPE SIM from the HPE website. For more information about HPE SIM, see the Hewlett Packard Enterprise website at http://www.hpe.com/servers/hpsim. For the user guide, see the Information Library.

SNMP

SNMP is not currently supported in Integrity iLO 3.

Event logging

Integrity iLO 3 provides event logging, display, and keyword search of console history and system events. The event log records the following information:

- iLO 3 MP login and logout events
- Command logging for specific commands

Directory-based secure authentication and authorization using LDAP

Directory-based authentication and authorization enables iLO 3 user accounts to be defined in a centralized database on an LDAP server. Integrity iLO 3 users are authenticated when logging in to iLO 3 and authorization is given each time an iLO 3 command runs. This provides a centralized database (LDAP server) of all user accounts and avoids the overhead of creating users in each iLO 3.

Directory authentication occurs by enabling Extended Schema or Default Schema. When Extended Schema is used, the schema in the directory server must be extended. When Default Schema is selected, schema extension is not needed.

Schema-free LDAP

Schema-free LDAP enables you to use directory authentication to log in to iLO 3 without having to perform any schema extension on the directory server or snap-in installation on the client. In addition to general directory integration benefits, iLO 3 schema-free integration provides the following:

- Minimal maintenance and administration
- Reliable security
Not extending the schema on the directory server means the directory server does not recognize the iLO 3 object or privileges, and the only thing the iLO 3 queries from the directory server is to authenticate the user name and password.

### Integrated Remote Console

The Integrated Remote Console (IRC) is a signed Direct X application, which enables a user to securely manage HPE Integrity servers with iLO. The IRC integrates the keyboard, video, and mouse functions into a virtual interface, providing an experience similar to that of the remote server graphics console. With the IRC, you can view the server system graphics display to directly interact with the server and perform maintenance activities, as well as open and run applications on the server, using the keyboard and mouse control. The console uses the hardware acceleration and advanced graphics features in .NET Framework. The console is launched by using Microsoft ClickOnce technology.

The IRC window remains open until one of the following events occurs:

- You sign out of the iLO interface by using the link in the banner
- The IRC does not detect keyboard or mouse activity for the period configured as idle connection timeout
- Another user disconnects IRC

IRC is supported with Integrity iLO 3 v1.3 management processors. For older iLO 3 systems, you can obtain IRC with a system firmware upgrade. No additional licensing is required.

**NOTE:**

To use IRC, you must have a physical VGA chip installed on the server. VGA is an optional accessory on some Integrity server models. IRC requires ActiveX control and is supported only with clients running Windows Internet Explorer.

### Virtual Media

Virtual Media (vMedia) enables connections of a CD/DVD-ROM physical device or image file from the local client system to the remote server. The virtual device or image file can be used to boot the server with an operating system that supports USB devices.

Using vMedia depends on a reliable network with good bandwidth, which is especially important when you are performing tasks such as large file transfers or operating system installs.

Virtual Media for USB Flash is supported in some Integrity iLO 3 systems. In Integrity iLO 3 v1.00, Virtual Media Flash is supported as a read-only device in the Unified Extensible Firmware Interface (UEFI) environment where it provides a convenient way to attach I/O firmware update files for updating through EFI tools. In iLO 3 v1.00, iLO vMedia Flash can be initiated through the iLO 3 user interface but not from the BladeSystem Onboard Administrator. Expanded vMedia Flash support will be available in a future iLO 3 firmware release.

**NOTE:**

If iLO 3 MP is reset, Integrity iLO 3 vMedia is disconnected. Hewlett Packard Enterprise does not recommend using iLO 3 vMedia with firmware update tools such as HPOFM, which reset the MP midway through the update process.

### Power Management

Integrity iLO Power Management features do not require an Advanced Pack license, but do require a power-aware operating system such as HP-UX 11iv3. Integrity iLO 3 systems ship equipped with an iLO 3 Advanced license which enables the following power management features:
Power & Reset

Enables you to view and control the power state of the server and also provides options to reset the system.

Power Meter Readings

Provides 24-hour graphing of power and temperature data and integration with HPE Insight Control Power Manager.

Power Regulator & Capping

Provides an easy way to manually set power efficiency modes. Works in cooperation with a host OS enabled with power management control.

A supporting operating system must be installed and booted before the Integrity iLO Power Regulator and Capping tab displays the choices for power modes: Dynamic Power Savings, Static Low Power, Static High Power, or OS Control modes.

Integrity iLO 3 Power management features can be accessed through the iLO web GUI or the Integrity MP text user interface.

HPE Insight Control power management

HPE Insight Control power management, a plug-in to HPE SIM, is an integrated power monitoring and management application that provides centralized control of server power consumption and thermal output. Integrity iLO 3 v1.00 with built-in Advanced license is integrated with Insight Control power management for power monitoring. Insight Control-initiated power regulation will be supported in a future iLO 3 firmware release.

For other operating systems, Insight Control 6.1 licenses can be applied to enable power management on Integrity servers. Information on HPE Insight power management is available on the HPE website at http://www.hpe.com/info/servermanagement.

iLO 3 Advanced Pack licensing

Advanced Pack licenses are built into every system that has Integrity iLO 3, no additional licensing is required. Multi-bladed Integrity servers, such as BL870c i2 and BL890c i2, contain multiple iLOs and each iLO contains a model-based iLO Advanced license key. This means that in multi-bladed servers, if individual blades are reordered or replaced, then the iLO Advanced keys do not have to be transferred or reapplied as all blades in that model contain identical model-based Integrity iLO keycodes.

NOTE:

ProLiant iLO keycodes do not work on Integrity blades and vice versa.
Components and cables required for iLO 3 operation

Table 1: Required components and cables

<table>
<thead>
<tr>
<th>Supported System</th>
<th>Required Components</th>
<th>Required Cables¹</th>
</tr>
</thead>
<tbody>
<tr>
<td>BL860c i2/i4/i6, BL870c i2/i4/i6, and BL890c i2/i4/i6</td>
<td>Front console serial port</td>
<td>SUV or DB-9 cable</td>
</tr>
<tr>
<td></td>
<td>Rear OA/iLO network port</td>
<td>LAN cable</td>
</tr>
<tr>
<td>rx2800 i2/i4/i6</td>
<td>iLO 3 hardware is integrated into the system board</td>
<td>LAN, serial, and VGA cables</td>
</tr>
</tbody>
</table>

¹ Cables are not provided with the server.

Integrity iLO 3 supported browsers and client operating systems

Integrity iLO 3 has an independent microprocessor. This architecture ensures that the majority of iLO 3 functionality is available regardless of the host operating system. Integrity iLO 3 web GUI functions are supported by Mozilla FireFox, Microsoft Internet Explorer or Google Chrome.

Table 2: Supported Browsers by Operating System

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Firefox 51</th>
<th>IE 10</th>
<th>IE 11</th>
<th>Chrome 46</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-UX 11.31</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 7/ Windows 8</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>WS2008 R2/ WS2012</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

You can view an updated list of supported browsers and operating systems for all Integrity iLO products on the Hewlett Packard Enterprise website at [www.hpe.com/info/Integrity_Servers-docs](http://www.hpe.com/info/Integrity_Servers-docs). The browser and OS information is located in the Quickspecs document located on this website.

Related links:
- Java for HP-UX
- Java for OpenVMS
- Mozilla Firefox for HP-UX
NOTE:
1.5.0.00 needs patch

- Mozilla Firefox for Windows and Linux
  - [http://www.mozilla.com/firefox](http://www.mozilla.com/firefox)
- Browser Support for Java 1.6.0_31

Security

You must have strong security surrounding the iLO 3 device. HPE security requirements for iLO 3 include the following:

**Authentication**

Integrity iLO 3 incorporates authentication techniques with the use of Secure Socket Layer (SSL) encryption. It is password-based for web and password- and key-based for secure shell (SSH).

**Authorization**

Using local accounts, iLO 3 enables you to define up to 19 separate users and to vary the server access rights of each user. The directory services capabilities of iLO 3 enables you to maintain network user accounts and security policies in a central, scalable database that supports thousands of users, devices, and management roles.

**Integrity**

Integrity iLO 3 incorporates a trusted Java applet for vMedia.

**Privacy**

Integrity iLO 3 uses SSL for web connections, RSL-RC4 encryption for serial console, AES128 for IRC, and AES256, AES128 or 3DES encryption algorithms for SSH connections. You can enable or disable Telnet, web, and SSH connectivity.

**NOTE:**
Integrity iLO 3 ships with Telnet disabled by default.

**Login**

Integrity iLO 3 enforces a progressive login delay after failed login attempts have occurred (default three) to protect the iLO from brute force dictionary attacks.

**IMPORTANT:**
Ensure that physical access to the server is limited. You can clear passwords by pressing the iLO 3 Physical Presence button for longer than 8 seconds.

**IMPORTANT:**
For greater security, Hewlett Packard Enterprise recommends that iLO 3 management traffic be on a separate dedicated management network that is configured to allow only limited access from selected secure systems by designated system administrators. This acts as the first line of defense against security attacks. A separate network enables you to physically and logically control which systems are allowed to connect to the network and the iLO 3 LAN port.
The iLO 3 functions are available through the server MP LAN port and the local port. On HPE Integrity server blades, the iLO management LAN port is routed internally to the HPE BladeSystem Onboard Administrator (OA) management LAN.

For locations and descriptions of iLO 3 LEDs, ports, and buttons on your server, see your user service guide or system specifications.

For more information on the Onboard Administrator for HPE server blades, see the c3000 or c7000 Enclosure documentation and The BladeSystem Onboard Administrator documentation.

### iLO 3 Physical Presence button

The iLO 3 Physical Presence button enables you to reset iLO 3 and reset the user-specific values to factory default values. A momentary (4-8 seconds) press causes a soft reset of iLO 3 when the button is released.

#### NOTE:

There is no hard reset for iLO.

#### IMPORTANT:

Physical Presence buttons on all conjoined blades are functional. However, only the buttons on monarch blades will enable TPM physical presence and iLO 3 security override modes, and events. Pressing this button on auxiliary blades will only cause a soft reset. A momentary press (less than 4 seconds) on the monarch blade resets the entire group of iLOs for the nPartition.

The iLO 3 Physical Presence button has multiple functions, depending on the length of time it is pressed. It enables you to reset iLO, enter TPM physical presence mode, and enter security override mode.

#### NOTE:

When you use the Physical Presence button to perform an iLO 3 security override, it does not require powering off, removing a blade, or rebooting your OS.

- A momentary press of the button (less than 4 seconds) resets iLO and clears any security override or TPM physical presence mode that were initiated by this button.

#### NOTE:

The reset will fail if an iLO firmware upgrade is in process.

#### NOTE:

When you reset iLO, you lose LAN connections immediately.

- A 4-8 second press of the button places the system in physical presence mode for 15 minutes.

#### NOTE:

The physical presence mode will be cleared if, during the 15 minute period, you press the Physical Presence button for 4 seconds or less.
NOTE:
The 15-minute timer will restart if, during the active physical presence mode period, you press the Physical Presence button for 4-8 seconds.

• An 8-12 second press of this button places iLO into security override mode for 15 minutes. Security override mode enables you to enter iLO without being challenged for a password, enabling you to set up users.

NOTE:
The security override mode will be cleared if, during the 15 minute period, you press the Physical Presence button for 4 seconds or less.

NOTE:
The 15-minute timer will restart if, during the active security override mode period, you press the Physical Presence button for 8-12 seconds.

NOTE:
iLO 3 does not log out any connected users when the 15-minute security override mode period ends.

• Pressing the Physical Presence button for more than 12 seconds has no effect on the system.
• The UID LED blinks once after holding the Physical Presence button for 4 seconds, and once again after holding the button for 8 seconds. This helps you gauge how long the button press has been held.

NOTE:
If the UID LED is blinking when the Physical Presence button is pressed, a firmware update is in progress. During a firmware update, no ILO actions take place if the Physical Presence button is pressed.

• Blade systems without an OA account (or rack systems) are configured to permit creating or modifying user passwords while in the Security Override mode. Please refer Procedure 1: Creating or modifying user passwords in Security Override mode.

NOTE:
Security override mode is not needed for blade systems accessed via an Onboard Administrator (OA) account. You can auto-login through the OA to iLO. Then you can use the iLO TUI's UC command (MP>CM>UC) or iLO GUI's Administration>User Administration>Local Accounts page to either create a user or modify the password of an existing user.

• Some special commands on the TPM require physical presence due to their sensitive nature. Please refer Procedure 2: Using TPM Physical Presence mode for special commands.
• The Login Timeout in Minutes feature, shown in the iLO GUI screen below and in the text user interface (see so command), disables logins after too many login failure attempts occur in a short timeframe. The login delay protects the iLO from brute force dictionary attacks. The iLO system administrator can configure the number of login failures allowed (default is 3). This option is in the TUI's so command or the GUI's Access Settings page (see below). Once the fault threshold has been reached, the login process is delayed and an event is placed in the iLO Event Log (IEL). If the attack persists, a critical event will also be placed in the System Event Log (SEL).
Creating or modifying user passwords in Security Override mode

Procedure

1. Unplug the manageability LAN cable.

   **NOTE:**
   (For security reasons, this is the safest approach. Later, you will connect to iLO via the serial port.)

2. On the monarch blade, press the Physical Presence button for 8-12 seconds to place the system into Security override mode.

   **TIP:**
   The UID LED will blink at 4 seconds, and again at 8 seconds. You can release the button after the second blink.

3. Login to iLO via the serial port with no user name or password.

4. In iLO, perform the following steps:
   a. Create a new user, or modify the password of an existing user.
   b. Re-enable security via the TUI or via the GUI.

5. Plug in the manageability LAN cable.
At the end of this procedure, you do not need to press the Physical Presence button on the monarch blade. This avoids the soft reset to iLO.

Using TPM Physical Presence mode for special commands

Prerequisites

On the monarch blade, press the Physical Presence button for 4-8 seconds to put the system in Physical Presence mode.

The UID LED will blink at 4 seconds, and again at 8 seconds. You can release the button after the first blink.

Procedure

1. From a workstation on the network, or via the local serial connection, login to iLO, and bring up the console (MP>CO).
2. Perform the special TPM commands.
3. To exit, wait the remainder of the 15 minutes for the TPM physical presence mode to expire.

NOTE:
Alternatively, you can exit immediately by pushing the Physical Presence button for less than 4 seconds; however, this action will reset iLO.

Canceling iLO Login Timeout via local Physical Presence button

The system administrator with physical access to the server can bypass authentication and cancel any progressive Login Delay in progress by pressing the Physical Presence button on the monarch blade 8-12 seconds to enter Security Override mode, or by pressing the Physical Presence button less than 4 seconds to reset iLO.

The UID LED will blink at 4 seconds, and again at 8 seconds. The first blink signals Physical Presence mode (release the button after the first blink), and the second signals Security Override mode (release the button after the second blink.

When iLO is in Security Override mode, all authentication is suspended for 15 minutes, or until someone exits Security Override mode by performing any of the following actions:

- Pressing the Physical Presence button less than 4 seconds
- Manually exiting through the iLO TUI's SO command
- Manually exiting through the iLO GUI's Access Settings web page. The system administrator should examine both the IEL and SEL to determine the cause of the login failures. (Login Delay must be cancelled before you can login to iLO to view the IEL and SEL.)

HPE Integrity server blade components

For port locations and console connection procedures, see your server blade documentation. Also, for HPE server blades, see the c3000 or c7000 Enclosure documentation and The BladeSystem Onboard Administrator documentation.
HPE BladeSystem Enclosures

c7000 Enclosure

The HPE BladeSystem c7000 Enclosure is an evolution of the entire rack-mounted infrastructure. It consolidates and repackages all the supporting infrastructure elements — compute, storage, network, and power into a single infrastructure-in-a-box that accelerates the integration and optimization of the data center.

It is optimized for enterprise data center applications. It fits into standard size HPE and third-party racks; accommodates BladeSystem c-Class server blades, storage blades, and interconnect modules; and provides all the power, cooling, and I/O infrastructure needed to support them.

For information on port locations and console connection procedures, see the HPE BladeSystem c7000 Enclosure setup and installation guide on the Hewlett Packard Enterprise website at http://www.hpe.com/info/bladesystem/docs.

c3000 Enclosure

The HPE BladeSystem c3000 Enclosure is similar to the c7000. The Intelligent Management through the Onboard Administrator gives you complete control of your bladed infrastructure. For information on port locations and console connection procedures, see the HPE BladeSystem c3000 Enclosure setup and installation guide on the Hewlett Packard Enterprise website at http://www.hpe.com/info/bladesystem/docs.

Onboard Administrator

The BladeSystem Onboard Administrator (OA) for the HPE BladeSystem c7000 Enclosure is the enclosure MP, subsystem, and firmware base used to support the HPE Integrity server blades and all the managed devices contained within the enclosure. Together with the enclosure HPE Insight Display, the Onboard Administrator has been designed for both local and remote administration of HPE BladeSystem c-Class.

This module and firmware provides:

• Wizards for simple, fast setup and configuration
• Highly available and secure access to the HPE Bladesystem infrastructure
• Security roles for server, network, and storage administrators
• Automated power and cooling of the HPE Bladesystem infrastructure
• Agent-less device health and status
• Thermal Logic power and cooling information and control
• email or Insight Display communications of problems within the enclosure

Each c7000 Enclosure is shipped with a first Onboard Administrator module/firmware. If needed, you can order a second redundant Onboard Administrator module for each enclosure. When two Onboard Administrator modules are present in a c7000 Enclosure, they work in an active - standby mode, assuring full redundancy of the c7000 Enclosure integrated management.

Before setting up the HPE BladeSystem OA, Hewlett Packard Enterprise recommends that you read the HPE BladeSystem Onboard Administrator User Guide on the Hewlett Packard Enterprise website at c-Class Onboard Administrator.

Reading the guides ensures that you understand the HPE BladeSystem OA and that you properly complete the initial setup to facilitate its proper functioning.

Integrity rx2800 i2/i4/i6 servers

For complete information on the HPE Integrity rx2800 i2/i4/i6 server, such as server components, ports, LEDs, and specifications, see the HPE Integrity rx2800 i2 Server User Service Guide, HPE Integrity
Getting connected to iLO 3

This chapter provides information on getting connected to iLO 3.

The ways you connect to iLO 3 will depend on whether you have a rackmount server or a server blade.

**IMPORTANT:**

For greater security, Hewlett Packard Enterprise recommends that iLO 3 management traffic be on a separate dedicated management network that is configured to allow only limited access from selected secure systems by designated system administrators. This acts as the first line of defense against security attacks. A separate network enables you to physically and logically control which systems are allowed to connect to the network and the iLO 3 LAN port.

Rackmount server connection

For a rackmount server, you can connect directly through the serial console or you can connect using the MP LAN.

To set up the console:

**Procedure**

1. Determine the physical access method to connect cables. There are two physical connections to iLO 3:
   a. Console serial port (RS-232)
   b. MP LAN port
2. Assign an IP address to the iLO 3 MP LAN using one of the following methods:
   a. DHCP and DDNS. Though there are several methods to configuring the LAN, Hewlett Packard Enterprise recommends DHCP with DNS. DHCP with DNS comes preconfigured with default factory settings, including a default user account and password. Use the DNS name on the iLO Network Information Tag located on the front panel.
   b. Console serial port (RS-232). Use this method to assign a static IP address instead of using DHCP.

Preparing to set up iLO 3

Perform the following tasks before you configure the iLO 3 MP LAN:

- Determine the physical access method to select and connect cables.
- Determine the iLO 3 MP LAN configuration method and assign an IP address if necessary.

Determining the physical iLO 3 access method

Before you can access iLO 3, you must determine the correct physical connection method.

There are several ways you can physically connect to iLO 3. Table 3 lists the appropriate connection method, required connection components, and connectors to the host console.

Use Table 3 to determine your physical connection method.
### Table 3: Physical connection matrix

<table>
<thead>
<tr>
<th>Connection Method</th>
<th>Required Connection Components</th>
</tr>
</thead>
</table>
| Console serial port (RS-232) | • Host console  
• Console serial port (RS-232) DB-9F to DB-9F cable (modem eliminator cable)  
• Emulation terminal device (for example, a PC, laptop, or ASCII terminal) |
|                            | These connection methods directly attach to the iLO 3 MP through the console serial port. This is an RS-232 connection from a workstation to the server's iLO 3 MP console serial port. Serial cable concentrators are used to provide switched access from one workstation to multiple servers. Typically, the console serial port method is used by an administrator in the data center. |
| LAN port                   | 10/100 LAN cable                                                                                 |
|                            | Remote access to the iLO 3 is a more convenient method. This remote access is through the MP LAN port. Depending on your LAN administration, this can be restricted to the datacenter, or extended outside the data center to your company's intranet. |
|                            | The iLO 3 has a separate LAN port from the system LAN port. It requires a separate LAN drop, IP address, and networking information from that of the operating system LAN port. |

#### Determining the iLO 3 MP LAN configuration method

To access iLO 3 through the MP LAN, iLO 3 must acquire an IP address. The way iLO 3 acquires an IP address is dependent upon whether DHCP is enabled or disabled on the server, and if DHCP and DNS services are available to the server (see Table 4).

Once you have determined the iLO 3 access method, you must determine how you will configure the MP LAN in order to acquire an IP address using the following methods:

- DHCP/DNS through the management LAN (dynamically assigns an IP address): use the DNS name on the iLO Network Information Tag located on the front panel.
- Setting up a static IP address using a laptop with DHCP services and the management LAN.
- Local RS-232 serial port and a serial console (assigns a static IP address).

Table 4 provides all the possible IP address acquisition scenarios. Use this table to help you select the appropriate LAN configuration method to obtain an IP address.

### Table 4: LAN configuration methods

<table>
<thead>
<tr>
<th>DHCP</th>
<th>DNS</th>
<th>RS-232 Serial Port (iLO 3 MP LC command)</th>
<th>LAN Configuration Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>DHCP</td>
</tr>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>DHCP or RS-232 serial port</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>RS-232 serial port</td>
</tr>
</tbody>
</table>

*Table Continued*
## Configuring the iLO 3 MP LAN using DHCP and DNS

DHCP automatically configures all DHCP-enabled servers with IP addresses, subnet masks, and gateway addresses. All HPE Integrity entry class servers with iLO 3 are shipped from the factory with DHCP enabled.

Hewlett Packard Enterprise recommends using the DHCP and DNS method to simplify access to iLO 3. When you use DHCP and DNS, you can connect to iLO 3 by entering the DNS name in your browser rather than an IP address only if the following applies:

- DHCP must be enabled (DHCP is enabled by default).
- You are using a DHCP server that provides the domain name.
- The primary DNS server accepts dynamic DNS (DDNS) updates.
- The primary DNS server IP address was configured through the DHCP server.

**IMPORTANT:**
You must know the DNS domain name, which is served out by the DHCP server, unless its domain is local or the same domain.

To configure iLO 3 using DHCP and DNS:

**Procedure**

1. Obtain the factory-set DNS name from the iLO Network Information Tag located on the front panel. The DNS name is 14 characters long. It consists of the letters **ilo** followed by the 12 characters of the MAC address. For example:
   
   `ilo0014c39c064f`

2. This address is assigned to the iLO 3 MP system board. The system board has a unique MAC address that identifies the hardware on the network.

3. Connect the MP LAN cable from the server to an active network port.

4. Apply AC power to the server.

5. Open a browser, Telnet, or SSH client and enter the fully-qualified DNS name (the full path name ending in the DNS name). The iLO 3 Log In window appears.

6. Log in using the default user name and password.

**CAUTION:**
When DHCP is enabled, the system is vulnerable to security risks because anyone can access iLO 3 until you change the default user name and password.

Hewlett Packard Enterprise strongly recommends you to assign user groups and rights before proceeding.
Configuring the iLO 3 MP LAN using the console serial port

The terminal emulation device runs software that interfaces with the server. The software emulates console output as it would appear on an ASCII terminal screen and displays it on a console device screen.

To configure the iLO 3 MP LAN using the console serial port (RS-232):

1. **IMPORTANT:**
   Do not configure duplicate IP addresses on different servers within the same network. The duplicate server IP addresses conflict and the servers cannot connect to the network.

The **LC** command enables you to configure a static IP address, host name, subnet mask, and gateway address.

2. **IMPORTANT:**
   Ensure you have a console connection through the console serial port (RS-232) or a network connection through the LAN to access the iLO 3 MP CLI and use the **LC** command.

Procedure

1. Ensure the emulation software is correctly configured:
   a. Verify that the communication settings are configured as follows:
      - 8/none (parity)
      - 9600 baud
      - None (receive)
      - None (transmit)
   b. Verify that the terminal type is configured appropriately. The following are supported terminal types:
      - hpterm
      - vt100
      - vt100+
      - vt-utf8

   **IMPORTANT:**
   Do not mix hpterm and vt100 terminal types at the same time. If there are two users collaborating and viewing console output with different emulation modes set, their clients will see garbled results if the output from the system is terminal specific.

2. Consult the help section of the emulation software application for instructions on how to configure the software options.
3. To determine the required connection components and the ports used to connect the server to the console device, use **Table 3**.
4. Connect the cables.
5. Start the emulation software on the console device.
6. Log in to iLO 3. See **Logging in to iLO 3 using the command-line interface** on page 34.
7. At the MP Main Menu, enter **CM** and press **Enter** to select command mode.
8. At the command mode prompt, enter **LS** and press **Enter**. The screen displays the current LAN configuration values. Write down the default values or log the information to a file.
9. To disable DHCP, enter the **LC** command.
   a. From the **LC** command menu, enter **D** and press **Enter**.
   b. Follow the instructions on the screen to change the DHCP status from enabled to disabled.
10. Use the \texttt{LC} command to enter information for the IP address, host, subnet mask, gateway parameters, and so on.
11. Enter \texttt{XD -R -NC} to reset iLO 3.
12. After iLO 3 resets, log in to iLO 3 again and enter \texttt{CM} at the \texttt{MP>} prompt.
13. To confirm that DHCP is disabled and display a list of updated LAN configuration settings, enter the \texttt{LS} command.

\textbf{NOTE:}

HPE ProLiant servers allow you to assign a static IP address at boot time to iLO 3 using a VGA monitor, keyboard, and mouse and HPE ProLiant BIOS commands. This feature is not available on HPE Integrity servers.

\section*{Server blade connection}

You do not have to physically connect to the iLO 3 via the SUV cable on a server blade. The iLO 3 on server blades typically use the iLO/OA management connection on the blade enclosure, and are assigned LAN IP addresses by the OA.

\subsection*{Connecting the server blade to iLO 3 using the Onboard Administrator}

If the OA/iLO network port on the enclosure is connected to the local network that has a DHCP server, your iLO 3 MP IP address is automatically generated by the DHCP server. The server blade is factory set with DHCP enabled.

To connect to iLO 3 using the OA, click the \texttt{iLO} link on the OA iLO GUI page:

\textbf{Procedure}

1. To connect to iLO 3 using the OA, navigate to the Device Bay Information page for the corresponding blade server from the navigation menu on OA GUI.
2. Click on the \texttt{iLO} link on Device Bay Information page and click the \texttt{Web Administration} link to launch iLO GUI in a separate browser window.

For HPE Integrity server blades, you can use the OA to manually set the IP addresses for all iLO 3s. You can also find the iLO 3 MP address so you can log in to iLO 3 directly.

For more information on using the Onboard administrator, see the following guides on the Hewlett Packard Enterprise website at \texttt{HPE BladeSystem c-Class Onboard Administrator}:

- For CLI, see the \texttt{HPE BladeSystem Onboard Administrator Command Line Interface User Guide}.
- For web GUI, see the \texttt{HPE BladeSystem Onboard Administrator User Guide}.

\textbf{NOTE:}

No user name/password authentication is required when iLO is accessed from the OA.

\section*{DHCP and auxiliary blades}

All blades have DHCP enabled by default. If you do not want an auxiliary blade to acquire one of the site DHCP addresses, assign it an address through the OA, using Enclosure Bay IP Addressing (EBIPA).

To enable the OA to connect to the blade for its internal blade management, assign a local IP address and matching gateway. For example, in a BL890c i2 server (four blades), use EBIPA to assign IP Addresses and Gateways of 192.168.2.x, where x is the Bay ID of each Auxiliary Blade. This is just an example; other similar IP addresses (192.168.x.x) also work. EBIPA requires each assigned IP address to be unique.
IMPORTANT:
Invalid IP addresses will disable the ability for the OA to do Single Sign On (SSO) to the AUX blade(s). Alternatively, assigning a valid IP address and Gateway such as 192.168.2.x (local only to the enclosure) will enable the OA for minor blade management without requiring network DHCP addresses.

For more information on assigning IP addresses on auxiliary blades, see the *HPE BladeSystem Onboard Administrator User Guide* on the Hewlett Packard Enterprise website at [HPE BladeSystem c-Class Onboard Administrator](https://www.hpe.com).  

**Auto login**

Auto login provides direct access to iLO 3 from the OA for users who already logged in to the OA. A user who has authenticated the connection to the OA can follow a link to a server blade in the enclosure without an additional login step. Auto login features and usage are as follows:

- A user who has authenticated a connection to the OA is able to establish a connection with iLO 3 without providing the user login and password to iLO 3.
- The OA provides the following auto login connection methods to iLO 3 links to users to launch these connections to iLO 3:
  
  **iLO CLI SSH connection**
  
  If you logged in to the OA CLI through SSH, enter `connect server <bay number>` to establish an SSH connection with iLO 3.

  **iLO web GUI connection**
  
  If you logged in to the OA web GUI, click the link to launch the iLO web GUI.

  - Auto login is implemented using IPMI over Ethernet between the OA and iLO 3 to create and delete user commands.
  - Supports a maximum of four simultaneous OA user accounts. The OA keeps track of these users locally. The information maintained for each user is the user name, password, and privilege levels.
  - User accounts for the auto login feature are created in the MP database when an auto login session is established. These accounts are deleted when the auto login session is terminated.
  - If a maximum number of user accounts has already been reached, and the OA creates another account on iLO 3. The OA sends a request to iLO 3 to delete one of the previously created accounts, before attempting to create a new one.
  - If iLO 3 is rebooted or power-cycled, it verifies any previously created OA user accounts in the iLO 3 user database when it boots up. If there are any previously-created OA user accounts, it deletes those accounts.
  - View and manage user accounts created in iLO 3 by the OA like any other local user account on iLO 3. To view and manage user accounts, use the TUI WHO, UC commands; or use the User Administration page in the web GUI.
  - View and disconnect user connections established through the auto login feature just like other connections to iLO 3. To view and disconnect user connections, use the TUI WHO, DI commands, or use the User Administration pages in the web GUI.
  - The OA supports three types of users: administrators, operators, and users. These user types map to the following iLO 3 capabilities:

  **Administrators**
  
  Can perform any function including iLO 3 MP configuration. This level equates to an iLO 3 user with all privilege levels such as, Administer User Accounts, Remote Console Access, Virtual Power and Reset, Virtual Media, and Configure iLO MP settings. It enables access to all aspects of the OA including configuration, firmware updates, user management, and resetting default settings.
Operators

Provided access to the serial console and vMedia. This level equates to an iLO 3 user with Remote Console Access, Virtual Power and Reset, Virtual Media, and Configure iLO settings. It allows access to all but configuration changes and user management. This account is used for individuals who might be required to periodically change configuration settings.

Users

Provided read-only login access to iLO 3. This account is used for individuals who need to see the configuration of the OA but do not need the ability to change settings. This level equates to an iLO 3 user with no privileges set.

NOTE:

For information on how to set user roles and privilege levels in the OA, see the HPE BladeSystem Onboard Administrator User Guide on the Hewlett Packard Enterprise website at HPE BladeSystem c-Class Onboard Administrator.

Initiating an auto login session

1. The OA finds the first available auto login user by finding the first user entry with a time-created value of 0. (OAtmp1...OAtmp5).
2. If there are no available users, the oldest user is deleted.

NOTE:
This might terminate a currently active session.

The OA sends a request to iLO 3 to delete that user.
3. The OA sends a command to create an OA user.
4. The OA launches an SSH or web GUI connection to iLO 3 and logs in with the created user’s credentials.

Terminating an auto login session

When the auto login CLI or web GUI session is terminated, the temporary Auto Login iLO 3 account is deleted.

User account cleanup during IPF blade initialization

The OA and iLO 3 perform the following during an IPF blade initialization:

• When a server blade is inserted, or iLO 3 or the OA is reboot or reset, both the OA and iLO perform cleanup of the accounts that might have been created for auto login before the reset.
• When iLO 3 initializes, the OA marks all four user slots as unused.
• Integrity iLO 3 scans its local user accounts. If there are any OA-created user accounts, they are deleted from the iLO 3 user database.

Auto login troubleshooting

There might be times when auto login fails. The following information provides possible reasons for the failure:

User creation

When the OA sends a request to iLO 3 to create a new user, iLO 3 attempts to create a user in the local iLO 3 user database. Creation of an OA user might fail for a number of reasons:

• The local user database is disabled in iLO 3 and LDAP authentication is being used.
• The iLO 3 user database has reached the maximum number of users (19 users).

User login
After an OA user has been created in the iLO 3 database, the OA user login can still fail for a number of reasons:

- Maximum number of connections for the requested connection type (SSH, Telnet, web GUI) to iLO 3 has been reached.
- Requested connection type (SSH, Telnet, or web) to iLO 3 is currently disabled.

**User deletion**

When the OA sends a request to iLO 3 to delete a user, iLO 3 attempts to delete that user from the local iLO 3 user database.

Deletion of an OA user might fail when a user with the specified login does not exist (user might have been deleted through other iLO 3 user interface).

### Connecting to a server blade iLO 3 using the console serial port

When a physical connection directly to a server blade iLO 3 is necessary, you can connect through the console serial port.

For a server blade, you can connect directly through the SUV cable to the serial console or you can connect using the MP LAN internal connection in the blade enclosure. You do not cable up a separate MP LAN cable to each server blade.

To log in to iLO 3, see [Logging in to iLO 3 on page 34](#).

### Connecting to iLO 3 using the Onboard Administrator

For instructions on physically connecting a server blade to iLO 3 through the OA, see the HPE BladeSystem c7000 Enclosure setup and installation guide on the Hewlett Packard Enterprise website at [http://www.hpe.com/info/bladesystem/docs](http://www.hpe.com/info/bladesystem/docs).

Unless SSH is disabled and the local user database is disabled (enabled is default), you can connect from the OA using `connect server n`.

On HPE Integrity server blades, you also have access to the console port.

It is not necessary to physically connect to iLO 3 through the console serial port to perform management tasks. Use the OA/iLO LAN port to communicate with any iLO 3 in the enclosure and the OA. You can use the LCD panel and the OA to configure and determine the iLO MP LAN address.

To log in to iLO 3, see [Logging in to iLO 3 on page 34](#).

### Additional setup

This section provides additional information to set up iLO 3.

Integrity iLO 3 comes preconfigured with an Administrator account and a randomly generated password.

**All Rights (Administrator) level user:**

**login** = Administrator

**password** = Randomly generated password found on the iLO Network Information Tag

---

**NOTE:**

- On server blades, the iLO Network Information Tag is located on the right side of the monarch blade.
- On HPE Integrity rx2800 i2/i4/i6 servers, the iLO 3 Network Information Tag is located on a pull-tab on the front panel.

---
Modifying default account configuration settings

Log in as the Administrator.

Changing the default password

Procedure
1. Access the MP Main Menu.
2. At the hpiLO-> prompt, enter CM.
3. At the CM:hpiLO-> prompt, enter UC and follow the prompts.

Setting up user accounts

Procedure
1. Access the MP Main Menu.
2. At the hpiLO-> prompt, enter CM.
3. At the CM:hpiLO-> prompt, enter UC and follow the prompts to modify user accounts.

Setting up security

For greater security, Hewlett Packard Enterprise recommends that only administrators be granted access to modify user account information.

Setting security access

Determine the security access required and what user accounts and privileges are needed. Integrity iLO 3 provides options to control user access. To prevent unauthorized access to iLO 3, select one of the following options:

- Create local accounts. You can store up to 19 user names and passwords to manage iLO 3 access. This is ideal for small environments such as labs and small-to-medium sized businesses.
- Use corporate directory services to manage iLO 3 user access. This is ideal for environments with a large number of frequently changing users. If you plan to use directory services, Hewlett Packard Enterprise recommends leaving at least one local account enabled as an alternate method of access.

For more information on how to create local accounts and use directory services, see Installing and configuring directory services on page 135.

Setting iLO MP LAN from UEFI

Integrity iLO 3 supports the UEFI utility to view the iLO LAN parameters.

To view the iLO LAN parameters from UEFI:

Procedure
1. Boot to the UEFI Front Page. See Accessing UEFI or the OS from iLO 3 on page 46.

   **NOTE:**
   You will only be able to boot to UEFI if the operating system has not yet been booted.

2. To launch the iLO Setup Tool, press F8 or press I.
3. For a list of options, enter help. The screen displays the options.
4. Enter L. The current iLO LAN configuration appears.
Current iLO LAN configuration:
  IP Address : 15.255.99.57
  Gateway    : 15.25.96.1
  Subnet     : 255.255.248.0

NOTE:
You are viewing the iLO LAN parameters that have already been configured. To modify the LAN parameters, connect to iLO or the OA for server blades.

5. To exit, enter Q.

If the iLO LAN configuration has not been initialized, this setup tool enables you to set a static IP configuration.

IMPORTANT:
For all Integrity BL8x0c versions, the recommendation is NOT to use this tool to set the iLO IP addresses because it uses a static IP and will cause iLO to not respond to EBIPA, which is the preferred method for setting iLO addresses in a blades environment. This tool is primarily used for the Integrity rx2800 i2/i4/i6 servers—which lack OA/EBIPA tools. Future updates may not allow users to use the iLO Setup Tool to set the iLO LAN configuration on Integrity BL8x0c versions.
Logging in to iLO 3

This chapter provides instructions on how to log in to iLO 3.

Logging in to iLO 3 using the web GUI

**Procedure**

1. Obtain the iLO Network Information Tag. The default iLO 3 user name and password is on this tag.

   **NOTE:**
   - On server blades, the iLO Network Information Tag is located on the right side of the monarch blade.
   - On HPE Integrity rx2800 i2/i4/i6 servers, the iLO 3 Network Information Tag is located on a pull-tab on the front panel.

2. Open a web browser, and then enter the DNS name or the IP address for the iLO 3.
3. Log in using the default iLO 3 user name and password.

Logging in to iLO 3 using the command-line interface

**Procedure**

1. Obtain the iLO Network Information Tag. The default iLO 3 user name and password is on this tag.

   **NOTE:**
   - On server blades, the iLO Network Information Tag is located on the right side of the monarch blade.
   - On HPE Integrity rx2800 i2/i4/i6 servers, the iLO 3 Network Information Tag is located on a pull-tab on the front panel.

2. Access iLO 3 through the LAN, using Telnet, SSH, or a console emulation method. The iLO 3 MP login prompt appears.
3. Log in using the default the iLO 3 user name and password.

   The following is the MP Main Menu:

<table>
<thead>
<tr>
<th>CO:</th>
<th>Console</th>
</tr>
</thead>
<tbody>
<tr>
<td>VFP:</td>
<td>Virtual Front Panel</td>
</tr>
<tr>
<td>CM:</td>
<td>Command Menu</td>
</tr>
<tr>
<td>CL:</td>
<td>Console Logs</td>
</tr>
<tr>
<td>SL:</td>
<td>Show Event Logs</td>
</tr>
<tr>
<td>HE:</td>
<td>Main Help Menu</td>
</tr>
<tr>
<td>X:</td>
<td>Exit Connection</td>
</tr>
</tbody>
</table>

For information on the iLO 3 MP menus and commands, see [Text user interface](#) on page 45.

**TIP:**

When logging in to iLO 3, using the local or remote console serial ports, the login prompt might not appear if another user is logged in through these ports. In this event, use **Ctrl-B** to access the MP Main Menu and the **hpiLO-** prompt.
IMPORTANT:
On HPE Integrity server blades, user interfaces such as MP TUI and console on the auxiliary blades cannot be used for system control. They are enabled for HPE Support. You must enter all system-level commands only on the monarch blade.

Logging in to iLO 3 through the OA

On systems that use the OA, you can log in to the web GUI or the TUI through the OA.

To log in to the OA web GUI, click the iLO link from the OA.

To log in to the OA TUI:

Procedure

1. To see a list of what is in each bay, use `show server info` from the OA TUI.
2. To log in to that bay, use `connect server n`.

You do not need a username/account; but you do need an empty SSH connect slot. SSH needs to be enabled and there cannot be too many other SSH connections already in use.
Accessing the host (operating system) console

This chapter describes several ways to access the host console of an HPE Integrity server blade.

Accessing a text host console through iLO 3 virtual serial console

To interact with iLO 3 through the web:

Prerequisites

Web browser access is an embedded feature of iLO 3.

Before starting this procedure, you must have the following information:

- DNS name for the iLO MP LAN
- Host name

Procedure

1. Open a web browser and enter the DNS name or the IP address for the iLO 3 MP.
2. Log in using your user account name and password at the login page. (Figure 2).

3. Click **Sign In**. The Status Summary page (Figure 3) appears after login.

**NOTE:**

The iLO web GUI session times out after the configured idle connection timeout period if there is no activity; but it will not time out if the Remote Serial Console or the Integrated Remote Console is launched, or if Virtual Media is connected.
Figure 3: Status Summary page

4. Select the web interface functions by clicking the tabs at the top of the page. Each function lists options in the Navigation Control on the left side of the page.

Accessing online help

The iLO 3 web interface has a robust help system. To launch iLO 3 help and display help about that page, click the help ? at the top right corner of each page.

Accessing a text host console using the TUI

Procedure

1. Log in using your user account name and password at the login page.
2. To switch the console terminal from the MP Main Menu to mirrored/redirected console mode, enter the CO command at the hpiLO-> login prompt. All mirrored data appears.
3. To return to the iLO 3 MP command interface, enter Ctrl-B or Esc (.

Help system

Integrity iLO 3 has a robust help system. To access the Help menu from the TUI, enter HE at the hpiLO-> prompt. The following is the MP Help Main Menu:

```plaintext
==== MP Help: Main Menu ===============================================
Integrated Lights-Out for HPE Integrity - Management Processor (MP)

MP Help System
Enter a command at the help prompt:

   OVerview : Launch the help overview
   List     : Show the list of MP Main Menu commands
   <COMMAND>: Enter the command name for help on individual command
   TOpics   : Show all MP Help topics and commands
   HElp     : Display this screen
   Q        : Quit help

====

hpiLO->:HE
```
To display the Main Menu Command List, enter **LI** at the **HE:hpiLO->** prompt.

To return to the MP Main Menu, enter **Q**.

To access help from the web GUI, click **Help**. You can also click the ? at the top right corner of each page to display help about that page.
Configuring DHCP

DHCP enables you to automatically assign reusable IP addresses to DHCP clients. This section provides information on how to configure DHCP options.

This iLO 3 MP host name will appear at the iLO 3 MP command mode prompt. Its primary purpose is to identify the iLO MP LAN interface in a DNS database.

**NOTE:**
The HP-UX system name displayed by the `uname -a` command is different than the iLO 3 MP host name.

If the IP address, gateway IP address, and subnet mask are obtained through DHCP, you cannot change them without first disabling DHCP. If you change the host name and the IP address was obtained through DHCP and registered with dynamic DNS (DDNS), a “delete old name” request for the old host name and an “add name request” for the new host name are sent to the DDNS server.

If you change the DHCP status between enabled and disabled, the IP address, subnet mask, and gateway IP address are set to default values (0.0.0.0). Also, the DNS parameters are voided. When you change the DHCP status from enabled to disabled, the DNS parameters for using DHCP are set to disabled, and the `Register with DDNS` parameter is set to No. When you change the DHCP status from disabled to enabled, the DNS parameters for using DHCP are set to enabled, and the `Register with DDNS` parameter is set to Yes.

**NOTE:**
DNS is the comprehensive RFC standard; DDNS provides only a part of the DNS standard functionality.

Use the `LC` command to perform the following actions to configure DHCP:

**NOTE:**
The `LC` command sets the next boot LAN settings. It does not display the current settings. To display the current settings, you must use the `LS` command. When you change settings using the `LC` command, the settings do not take effect until the next boot of the iLO.

- Set all default LAN settings.
  ```
  [hostname] CM:hpiLO-> LC -all DEFAULT -nc
  ```
- Display next LAN settings.
  ```
  [hostname] CM:hpiLO-> LC -nc
  ```
- Modify the MP DHCP status.
  ```
  [hostname] CM:hpiLO-> LC -dhcp disabled
  ```
- Modify the MP IP address.
  ```
  [hostname] CM:hpiLO-> LC -ip 192.0.2.1
  ```
• Modify the MP host name.
  [hostname] CM:hpiLO-> LC -h hostname
• Modify the MP subnet mask.
  [hostname] CM:hpiLO-> LC -s 255.255.255.0
• Modify the MP gateway address.
  [hostname] CM:hpiLO-> LC -g 192.0.2.1
• Set the link state to auto negotiate.
  [hostname] CM:hpiLO-> LC -link auto
• Set the link state to 10 BaseT.
  [hostname] CM:hpiLO-> LC -link x
  (Other option is -link c (100BaseT))
• Set the remote console serial port address.
  [hostname] CM:hpiLO-> LC -rsc n
• Set the SSH console port address.
  [hostname] CM:hpiLO-> LC -ssh 22

Configuring DNS

To use the DNS command to display and modify the DNS configuration:

Procedure

1. From the MP Main Menu, enter command mode.
2. At the CM:hpiLO-> prompt, enter DNS. The screen appears current DNS data.
3. To select all parameters, enter A when prompted. The screen displays the current DHCP for DNS server status.
4. When prompted, enter Enabled or Disabled. The screen displays the current DHCP for DNS domain name status.
5. When prompted, enter Enabled or Disabled. The screen displays the current register with DDNS server value.
6. When prompted, enter Yes or No. The screen displays the current DNS domain name.
7. When prompted, enter a new value. The screen displays the primary DNS server IP address.
8. When prompted, enter a new value. The screen displays the optional secondary DNS server IP address.
9. When prompted, enter a new value. The screen displays the optional tertiary DNS server IP address.
10. When prompted, enter a new value.

The DNS configuration is updated as follows:

New DNS Configuration (* modified values):

  * S - DHCP for DNS Servers      : Disabled
  * D - DHCP for DNS Domain Name  : Disabled
    R - Register with DDNS Server : Yes
  * N - DNS Domain Name           : mpdns.company.com
  * 1 - Primary DNS Server IP     : 192.0.2.1
    2 - Secondary DNS Server IP   :

Enter parameter(s) to revise, Y to confirm, or [Q] to Quit: Y

-> DNS Configuration has been updated
Configuring LDAP extended schema

The following procedure describes how to configure iLO 3 to use a directory server to authenticate a user login using the iLO 3 MP TUI.

**NOTE:**
The LDAP connection times out after 30 minutes of inactivity in Active Directory. For Novell directory, there is no inactivity timeout.

To configure using the web interface, see Group Accounts on page 115.

To configure LDAP extended schema:

**Procedure**

1. From the MP Main Menu, enter command mode.
2. At the CM:hpiLO-> prompt, enter LDAP.
3. To select Directory Settings, enter D. The current LDAP directory settings appear.
4. To select all parameters enter A. The current LDAP directory authentication status appears. The local iLO 3 user accounts database status also appears. If enabled, the local iLO 3 user database is used if there is an authentication failure using the LDAP Directory.
5. Enter D for disabled, or E for enabled. You must enter E if LDAP directory authentication is disabled. The current LDAP server IP address appears.
6. Enter the IP address of the LDAP server. The current LDAP server port address appears.
7. Enter a new port number. The screen displays the current object distinguished name. This specifies the full distinguished name of the iLO 3 device object in the directory service. For example, CN=RILOE2OBJECT, CN=Users, DC=HP, DC=com. Distinguished names are limited to 255 characters maximum plus one for the NULL terminator character.
8. Enter a new name. The Current User Search Context 1 appears.

**NOTE:**
The context settings 1, 2, and 3 point to areas in the directory service where users are located, so that users do not have to enter the complete tree structure when logging in. For example, CN=Users, DC=HP, DC=com. Directory user contexts are limited to 127 characters maximum plus one for the NULL terminator character for each directory user context.

10. Enter a new search setting. The screen displays the Current User Search Context 3.
11. When prompted, enter a new search setting.

The updated LDAP configuration is as follows:

**New Directory Configuration (marked values):**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>* L - LDAP Directory Authentication</td>
<td>Enabled</td>
</tr>
<tr>
<td>M - Local MP User database</td>
<td>Enabled</td>
</tr>
<tr>
<td>* I - Directory Server IP Address</td>
<td>192.0.2.1</td>
</tr>
<tr>
<td>P - Directory Server LDAP Port</td>
<td>636</td>
</tr>
<tr>
<td>D - Distinguished Name (DN)</td>
<td>cn=mp,o=demo</td>
</tr>
<tr>
<td>1 - User Search Context 1</td>
<td>o=mp</td>
</tr>
<tr>
<td>2 - User Search Context 2</td>
<td>o=demo</td>
</tr>
<tr>
<td>3 - User Search Context 3</td>
<td>o=test</td>
</tr>
</tbody>
</table>

Enter Parameter(s) to revise, Y to confirm, or [Q] to Quit: y
Login process using directory services with extended LDAP

You can choose to enable directory services to authenticate users and authorize user privileges for groups of iLO 3s. The iLO 3 directory services feature uses the industry-standard LDAP. HPE layers LDAP on top of SSL to transmit the directory services information securely to the directory servers.

Hewlett Packard Enterprise provides tools to extend directory schema and install snap-ins for Microsoft Active Directory and Novell e-directory. Please refer to Chapter 8, “Installing and configuring directory services” for more information on installation and configuration of directory services.

When LDAP is enabled with extended schema in iLO 3, after users enter their login and password, the browser sends the cookie to iLO 3. The iLO 3 processor accesses the directory service to determine which roles are available for that user login. The iLO 3 first uses the credentials to access the iLO 3 device object in the directory. The directory service returns only the roles for which the user has rights. If the user credentials allow read access to the iLO 3 device object and the role object, iLO 3 determines the role object distinguished name and the associated user privileges. The iLO 3 then calculates the current user privileges based on those roles and grants them to that user.

Configuring schema-free LDAP

**IMPORTANT:**

Due to command syntax changes in schema-free LDAP, some customer-developed scripts may not run. You must change any scripts you developed to enable them to run with the new schema-free LDAP syntax.

Integrity iLO 3 schema-free directory integration enables you to use the standard directory schema instead of adding HPE schema to the directory database. You accomplish this by authenticating users from the directory database and authorizing iLO 3 privileges based on matching groups stored on each iLO 3.

In addition to general directory integration benefits, iLO 3 schema-free integration provides the following advantages:

- Easy implementation without schema extensions.
  - iLO 3 schema-free integration is configured from any iLO 3 user interface (browser, command line, or script).
- Minimal administration and maintenance.
  - After initial setup, only groups and permissions require maintenance support on iLO 3; typically group and permission changes occur infrequently.
  - The schema-free approach does not require updating directory databases with new iLO 3 devices objects.
- Reliable security.

Integrity iLO 3 schema-free integration does not affect standard directory attributes, avoiding conflicting use of attributes that can result over time.

**NOTE:**

If you have already extended your directory with HPE schema, there is no need to switch to the schema-free approach. Schema extension provides the lowest maintenance approach for directory integration. When this process has taken place, there is no advantage for the schema-free approach until a schema change is required.

To configure schema-free LDAP:
1. Follow the procedure for **Configuring LDAP extended schema** on page 41, but omit Step 8. It is not necessary to enter a new port number.
2. Set up directory security groups.

**Setting up directory security groups**

The following procedure describes how to set up directory security groups in schema-free LDAP using the iLO 3 MP TUI. To use the web interface, see **Group Accounts** on page 115.

**NOTE:**
Due to command syntax changes in schema-free LDAP, some customer-developed scripts may not run. You must change any scripts you developed to enable them to run with the new schema-free LDAP syntax.

**NOTE:**
You must select the default schema from the **LDAP** command for the schema-free LDAP settings to work.

To set up directory security groups:

**Procedure**

1. At the **CM:hpiLO->** prompt, enter **LDAP**. The screen displays the current LDAP options.

   ```
   [hqgstlb3] CM:hpiLO-> ldap
   LDAP
   Current LDAP options:
   D - Directory settings
   G - Security Group Administration
   ```

2. Enter G. The current group configuration appears.

   ```
   Enter menu item or [Q] to Quit: G
   Current Group Configuration:
   Group Names        Group Distinguished Names        Access Rights
   --------------------------------------------------------------------------
   1 - Administrator                                       C, P, M, U
   2 - User                                                C, P
   3 - Custom1                                             None
   4 - Custom2                                             None
   5 - Custom3                                             None
   6 - Custom4                                             None
   ```

   Only the first 30 characters of the Group Distinguished Names are displayed.

   ```
   Enter number to view or modify, or [Q] to Quit:
   ```

3. Enter the number for the group you want to view or modify. The current LDAP group settings appear.

4. Set up a group distinguished name.

5. Select rights for the group.

6. Enter **Y** to confirm.
Login process using directory services without schema extensions

You can control access to iLO 3 using directories without schema extensions. Integrity iLO 3 acquires the user name to determine group membership from the directory. The iLO 3 then cross-references the group names with its locally stored names to determine user privilege level. Integrity iLO 3 must be configured with the appropriate group names and their associated privileges. To configure iLO 3, use one of the following methods:

- Web GUI (Administration > Directory Settings > Group Administration page)
- iLO 3 MP TUI (LDAP command)
Using iLO 3

There are several options for using iLO 3. This chapter provides information and instructions on each available option.

Text user interface

This section provides information on the text user interface (TUI) commands you can run in iLO 3.

NOTE:
HPE Integrity server blades do not have fans or power supplies. Therefore, the response to certain commands are different than a rackmount server.

MP command interfaces

Table 5: MP command interfaces

<table>
<thead>
<tr>
<th>MP Command Interface</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MP Main Menu</td>
<td>The MP Main Menu appears when you first access the iLO 3 MP. The MP Main Menu supports the basic MP commands for server control and the iLO 3 MP configuration.</td>
</tr>
<tr>
<td>Command Menu</td>
<td>The Command menu provides a set of commands that help monitor and manage the server. It switches the console terminal from the MP Main Menu to command interface mode. To access the Command menu, enter <code>CM</code> at the MP Main Menu and enter <code>HE LI</code> at the <code>[hostname] CM:hpiLO-&gt;</code> prompt.</td>
</tr>
</tbody>
</table>

MP main menu

After logging in to the iLO 3 MP, the MP Main Menu appears. The MP Main Menu runs as a private session. Other iLO 3 users do not see the actions you perform in the private session.

Integrity iLO 3 can support multiple sessions to perform independent tasks:

- Multiple windows logged into iLO 3 to monitor VFP or study event logs in one window while administering the server from another window.
- Resetting a server from one window and monitoring the boot from another window while interacting with the console from a third window.

Table 6 lists the MP Main Menu commands.

Table 6: MP Main Menu commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO</td>
<td>Selects console mode</td>
</tr>
<tr>
<td>VFP</td>
<td>Displays the virtual front panel</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM</td>
<td>Enters command interface mode</td>
</tr>
<tr>
<td>CL</td>
<td>Views the console log</td>
</tr>
<tr>
<td>SL</td>
<td>Shows event logs</td>
</tr>
<tr>
<td>HE</td>
<td>Displays help for the menu or command</td>
</tr>
<tr>
<td>X</td>
<td>Exits</td>
</tr>
</tbody>
</table>

**TIP:**
An effective method for using iLO 3 is to log in more than once with different views for each session. For instance, one window logged in viewing the console, and another viewing the virtual front panel.

**MP Main Menu commands**

The following sections describe the MP Main Menu commands.

**CO (Console): Leave the MP Main Menu and enter console mode**

CO switches the console terminal from the MP Main Menu to mirrored/redirected console mode. All console output is mirrored to all users in console mode. Only one of the mirrored users at a time has write access to the console. To get console write access, press `<Ctrl-Ec>`.

To return to the MP Main Menu, press either `<Ctrl-B>` or `<Esc>` and `. Verify that all mirrored consoles are of the same terminal type for proper operation.

To run an ASCII screen-oriented application (SAM) or a file transfer program (ftp), the console is not the recommended connection. Hewlett Packard Enterprise recommends using the LAN and connecting directly with Telnet or the web to the system over the system LAN.

**Accessing UEFI or the OS from iLO 3**

The UEFI is an Itanium-based architecture feature that provides an interface between the server blade OS and the server blade firmware. UEFI provides a standard environment for booting an OS and running preboot applications.

To access UEFI or the OS from iLO 3:

**Procedure**

1. From the MP Main Menu, enter CO to access the Console Menu. Depending on how the server blade was configured from the factory, and if the OS is installed at the time of purchase, you should be in one of two places:
   a. EFI Boot Manager menu
   b. OS login prompt
2. If the server blade has a factory-installed OS, you can interrupt the boot process to configure your specific EFI parameters.

**VFP (Virtual Front Panel): Simulate the display panel**

VFP simulates the display panel on the front of the server. It gives real-time feedback on the results of system events and user actions. VFP works by decoding system events. It provides a live display of major states of the system, the latest system activity, and the state of front panel LEDs.
IMPORTANT:

Integrity iLO 3 has no LED that equates to the Blade Health LED located on the front panel of each individual BL8x0c i2/i4/i6 server blade. The Blade Health LED represents the health of the individual server blade. The virtual LEDs in the iLO GUI and TUI reflect system and partition health. The closest equivalency to the Blade Health LED is a field called Bay [x] Health on the System Health page of the iLO GUI.

The VFP is a representation of the system and partition state and the system status in the boot process (running non-OS code, and more).

The following virtual LEDs are located in the VFP:

- Health
- System
- Locator
- Power

VFP shows forward progress during boot by indicating how many events have been received since the boot started and whether there have been any errors (events with alert level 3 or greater) since the last boot. To clear the yellow attention indicator on the front of the system, use the SL command and access the System Event Log (SEL).

Each user viewing VFP is in private session mode.

See also: LOC (locator LED), and SL (show logs).

CM (Command Mode): Enter command mode

CM switches the console terminal from the MP Main Menu to mirrored command interface mode. The Command menu provides you with a set of standard command-line interface commands that help monitor and manage the server.

To display the list of MP command mode commands:

Procedure

1. From the MP Main Menu, enter CM.
2. Enter HE LI at the CM: hpiLO-> prompt.

To return to the MP Main Menu, press Ctrl-B.

CL Display console Menu history

Command access level: Remote Console access for viewing the log. Configure MP Settings access for clearing the log.

The CL command displays up to 256KB of logged console data (or about 250 pages of output) sent from the system to the console path and stored for later analysis.

Console data is stored in a buffer in nonvolatile memory. By default, data is displayed from the beginning of the buffer to the end of the buffer. You can control the starting point from which the data displays and navigate through the data.

An image of the console history appears when you enter the CL command. Console output continues to be logged while this buffer is read, and nothing is lost in the meantime.

The CL command does not support command line usage or scripting.

See Also: SL, VT
SL (Show Logs): Display the status logs

SL displays the contents of the status logs, System Event Log (SEL), Forward Progress Log (FPL), and iLO Log. You can also run the status in live mode presenting each event as it is received.

**NOTE:**

After entering the SL command, any subcommand you enter (such as SE log selection, SL menu options) does not require entering <CR>. The only exception to this is when a log entry number is requested. You must enter <CR> after entering a log number.

Events communicate system information from the source of the event to other parts of the system, then to the system administrator. Events are produced by intelligent hardware modules, the operating system, and system firmware. Events funnel into iLO 3 from different sources throughout the server. The iLO 3 stores new events in nonvolatile memory.

The SL command also displays the contents of the iLO 3 Event Log. The following events are recorded:

- iLO 3 MP login and logout attempts
- Command logging for specific commands
- All entries in the existing history log with more detail

Each time a user logs in or out of iLO 3, an event is logged. In the event of a login failure, an event is logged if the number of continuous login failure attempts equals the password fault value.

The following example shows the event log viewer menu:

```
Event Log Viewer Menu:

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Entries</th>
<th>% Full</th>
<th>Latest Timestamped Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>E - System Event</td>
<td>51</td>
<td>2 %</td>
<td>27 Mar 2010 02:22:38</td>
</tr>
<tr>
<td>F - Forward Progress</td>
<td>1556</td>
<td>7 %</td>
<td>27 Mar 2010 02:33:26</td>
</tr>
<tr>
<td>I - iLO Event</td>
<td>12</td>
<td>2 %</td>
<td>27 Mar 2010 02:33:26</td>
</tr>
<tr>
<td>C - Clear SEL and FPL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L - Live Events</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Enter menu item or [Ctrl-B] to Quit:

The following example shows the display in the SL menu E system event submenu:

```
#     Location   |Alert | Encoded Field  |  Data Field    | Keyword/Timestamp
--
10    SFW  3,1,0,0    2  5488006341E10011 0000000000000000 BOOT_START
27 Mar 2010
20:07:51
9     SFW  4,0,0,0    2  548C006301E1000F 0000000000000000 BOOT_START
27 Mar 2010
20:07:51

SL:hpiLO (+,-,<CR<?,D,F,L,J,H,K,T,A,?,Q or Ctrl-B to Quit)->t
SL:hpiLO (+,-,<CR<?,D,F,L,J,H,K,T,A,?,Q or Ctrl-B to Quit)->j

Jump to entry number: 10

Log Entry 10: 27 Mar 2010 20:07:51
Alert Level 2: Informational
Keyword: BOOT_START
CPU starting boot
```
Logged by: System Firmware located in bay 3, socket 1, cpu 0, thread 0
Data: Major change in system state - Boot Start
5488006341E10011 0000000000000000

In this example: the “Alert” has a “*” because all alerts >= 3 have a “*”.

<table>
<thead>
<tr>
<th>#</th>
<th>Location</th>
<th>Alert</th>
<th>Encoded Field</th>
<th>Data Field</th>
<th>Keyword/Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>69</td>
<td>ILO 3</td>
<td>*3</td>
<td>608022E620E10086 0000000000000000</td>
<td>ILO_SPECIAL_MODE</td>
<td>01 Jan 2001 12:32:51</td>
</tr>
</tbody>
</table>

- “#” is the entry number. Use this with the “j” menu comment to a particular log (if you don’t want to scroll to it).
- Location: 3,1,0,0 means blade 3, socket 1, cpu 0, thread 0.
- To find out more about these events, use T to switch to text mode.

Command logging is run for the following commands: CA, DC, DI, DNS, FW, ID, IT, LC, LDAP, LM, PC, PM, PR, RS, SA, SO, TC, UC, WOL

Events are listed as follows:

**Table 7: Events**

<table>
<thead>
<tr>
<th>Log Name</th>
<th>Acronym</th>
<th>Log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E - System Event</td>
<td>SEL</td>
<td>System Error Log</td>
<td>Records high-attention events and errors</td>
</tr>
<tr>
<td>F - Forward Progress</td>
<td>FPL</td>
<td>Forward Progress Log</td>
<td>Records all events. The Integrity iLO stores a detailed FPL of system operation during boot, crash, and any other abnormal conditions that can be used to extensively troubleshoot the server. This log goes far beyond the capabilities of standard IPMI for fault management. The FPL is available using the text interface only.</td>
</tr>
<tr>
<td>I - iLO Event</td>
<td>IEL</td>
<td>iLO Event Log</td>
<td>Records the following: • Events corresponding to iLO 3 MP login and logout actions • Command logging for specific iLO 3 MP commands</td>
</tr>
<tr>
<td>C - Clear SEL and FPL</td>
<td>- - -</td>
<td>SEL Log</td>
<td>Clears all entries in the System Event and Forward Progress logs</td>
</tr>
<tr>
<td>L - Live Events</td>
<td>LIVE</td>
<td>Live Event Viewer</td>
<td>Presents each event as it is received</td>
</tr>
</tbody>
</table>
NOTE:
Integrity iLO 3 captures and stores the server System Event Log for access through a browser or text interface even when the server is not operational. This capability can be helpful when troubleshooting remote host server problems.

Reading the SEL is the only way to turn off the attention LED (flashing yellow light).

**Table 8** lists the events and actions used to navigate within the logs.

**Table 8: Events**

<table>
<thead>
<tr>
<th>Event</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>Displays the next block (forward in time)</td>
</tr>
<tr>
<td>-</td>
<td>Displays the previous block (backward in time)</td>
</tr>
<tr>
<td>Enter (&lt;CR&gt;)</td>
<td>Continues to the next or previous block</td>
</tr>
<tr>
<td>D</td>
<td>Dumps the entire log for capture or analysis</td>
</tr>
<tr>
<td>F</td>
<td>Displays the first entry</td>
</tr>
<tr>
<td>L</td>
<td>Displays the last entry</td>
</tr>
<tr>
<td>J</td>
<td>Jumps to entry number</td>
</tr>
<tr>
<td>H</td>
<td>Displays the mode configuration (hex)</td>
</tr>
<tr>
<td>K</td>
<td>Displays the mode configuration (keyword)</td>
</tr>
<tr>
<td>T</td>
<td>Displays the view mode configuration (text)</td>
</tr>
<tr>
<td>A</td>
<td>Displays the alert level filter options</td>
</tr>
<tr>
<td>U</td>
<td>Displays the alert level unfiltered</td>
</tr>
<tr>
<td>Q</td>
<td>Quits and returns to the Event Log Viewer Menu</td>
</tr>
<tr>
<td>?</td>
<td>Displays the Help Menu</td>
</tr>
<tr>
<td>Ctrl-B</td>
<td>Exits and returns to the MP Main Menu</td>
</tr>
</tbody>
</table>

Integrity iLO 3 Event Log navigation provides additional filtering options as shown in **Table 9**.
Table 9: iLO 3 Event Log filter options

<table>
<thead>
<tr>
<th>Filtering Option</th>
<th>Filter Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>N: User Login</td>
<td>Filter by user Login ID</td>
</tr>
<tr>
<td>P: Port Name</td>
<td>Filter by port name (Serial, Telnet, SSH, WEB)</td>
</tr>
<tr>
<td>I: IP Address</td>
<td>Filter by user IP Address (dotted decimal format)</td>
</tr>
<tr>
<td>M: Date</td>
<td>Filter by date stamp of the records entries (MM/DD/YYYY)</td>
</tr>
</tbody>
</table>

If you select more than one filtering option, it acts as an additional filter. For example, if you select the filtering option N followed by P, the logs displayed are the logs that satisfy the filtering criteria for options N and P.

---

**NOTE:**
The iLO 3 Event Logs cannot be cleared.

A finite number of records are stored. The older records are replaced as the log fills up.

Table 10: Alert levels

<table>
<thead>
<tr>
<th>Severity</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Minor forward progress</td>
</tr>
<tr>
<td>1</td>
<td>Major forward progress</td>
</tr>
<tr>
<td>2</td>
<td>Informational</td>
</tr>
<tr>
<td>3</td>
<td>Warning</td>
</tr>
<tr>
<td>5</td>
<td>Critical</td>
</tr>
<tr>
<td>7</td>
<td>Fatal</td>
</tr>
</tbody>
</table>

See also: DC and VFP

**HE (Help): Display help for the menu or command in the MP Main Menu**

The HE command displays the MP hardware and firmware version identity, and the date and time of firmware generation. When issued from the MP Main Menu, HE displays general information about iLO 3, and those commands available in the MP Main Menu. When issued in command mode, HE displays a list of Command menu commands available. It also displays detailed help information in response to a topic or command at the help prompt.

**X (Exit): Exit iLO 3**

X exits you from the MP Main Menu. If the terminal is the local serial port, the login prompt appears. For all other types of terminals, you are disconnected from iLO 3.
Command Menu

The Command menu provides you with a set of standard command-line interface commands that help monitor and manage the server.

Table 11: Command menu commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BLADE</strong></td>
<td>Display enclosure, bay, and Onboard Administrator information</td>
</tr>
<tr>
<td><strong>CA</strong></td>
<td>Configure serial port parameters</td>
</tr>
<tr>
<td><strong>DATE</strong></td>
<td>Display the current date</td>
</tr>
<tr>
<td><strong>DC</strong></td>
<td>Reset all parameters to default configuration</td>
</tr>
<tr>
<td><strong>DF</strong></td>
<td>Display field replaceable unit information (FRUID)</td>
</tr>
<tr>
<td><strong>DI</strong></td>
<td>Disconnect users</td>
</tr>
<tr>
<td><strong>DNS</strong></td>
<td>Configure DNS parameters</td>
</tr>
<tr>
<td><strong>FW</strong></td>
<td>Update firmware</td>
</tr>
<tr>
<td><strong>HE</strong></td>
<td>Print the help menu; or display help for the menu or command</td>
</tr>
<tr>
<td><strong>ID</strong></td>
<td>Display or modify system information</td>
</tr>
<tr>
<td><strong>IT</strong></td>
<td>Modify the iLO 3 inactivity timers</td>
</tr>
<tr>
<td><strong>LC</strong></td>
<td>Configure LAN, SSH, and web ports</td>
</tr>
<tr>
<td><strong>LDAP</strong></td>
<td>Configure LDAP parameters</td>
</tr>
<tr>
<td><strong>LM</strong></td>
<td>View current license status</td>
</tr>
<tr>
<td><strong>LOC</strong></td>
<td>Locator LED configuration</td>
</tr>
<tr>
<td><strong>LS</strong></td>
<td>Current LAN settings</td>
</tr>
<tr>
<td><strong>PC</strong></td>
<td>Remote power control</td>
</tr>
<tr>
<td><strong>PM</strong></td>
<td>Power regulator mode</td>
</tr>
<tr>
<td><strong>PR</strong></td>
<td>Set the power restore policy</td>
</tr>
<tr>
<td><strong>PS</strong></td>
<td>Power management module status</td>
</tr>
</tbody>
</table>

*NOTE:* This command is available only on a server blade.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS</td>
<td>Reset the system through the RST signal</td>
</tr>
<tr>
<td>SA</td>
<td>Configure remote, LAN, Telnet, and web access options</td>
</tr>
<tr>
<td>SO</td>
<td>Configure security options</td>
</tr>
<tr>
<td>SYSREV, SR</td>
<td>Display all firmware revisions</td>
</tr>
<tr>
<td>SS</td>
<td>Display system processor status</td>
</tr>
<tr>
<td>SYSSET</td>
<td>System settings</td>
</tr>
<tr>
<td>TC</td>
<td>Transfer of control (TOC) - System reset through the INIT signal</td>
</tr>
<tr>
<td>TE</td>
<td>Tell - send a message to other users</td>
</tr>
<tr>
<td>UC</td>
<td>User configuration</td>
</tr>
<tr>
<td>WHO</td>
<td>Display a list of connected users</td>
</tr>
<tr>
<td>WOL</td>
<td>Turn the Wake-On-LAN feature On or Off for system LANs</td>
</tr>
<tr>
<td>XD</td>
<td>Diagnoses or resets iLO 3</td>
</tr>
</tbody>
</table>

The following is a quick reference list that provides MP Command mode activities:

- To access the Command menu, enter **CM** at the MP Main Menu.
- To see all the available commands, enter **HE** at the **CM:hpiLO->** prompt, and then enter **LI**.
- To modify the inactivity timeout, enter the **IT** command. The inactivity timer aborts a command if you do not complete it within a certain time period and redirects you back to the command prompt.
- To abort most commands, enter **Q** at the point when the iLO 3 MP is asking for input.
- To return to the MP Main Menu from any of these commands, press **Ctrl-B**.

### Command-line interface scripting

A command-line interface is provided for all commands to assist you in scripting. This section provides syntax examples used in the iLO 3 MP command-line or scripted interface.

Typically, tools like Expect (see Expect script example on page 54) and [http://expect.nist.gov/](http://expect.nist.gov/) are used to string together several commands to accomplish a task. These scripting tools enable you to write a script for one iLO 3, and use it to apply the same commands to additional iLO 3s. Scripting tools have capabilities that enable you to do the following:

- Write scripts that make decisions based on the output of commands
- Use variables in the script to customize it for each target automatically
- Compensate for delays in output

Scripting tools and the command-line interfaces enable you to carry out commands to multiple iLO 3s such as setting the IP address on 10 iLO 3s pulled from a list of 10 IP addresses read from a file local to your script. To automatically administer any part of the system during any stage of its operation, you can use the scripting tool to log in to iLO 3, access the console, and send and receive commands in UEFI or the operating system.
NOTE:

This guide is not meant as a substitute for instruction on various scripting tools that are available for automating command-line interfaces. The iLO 3 MP TUI (when used with command-line arguments) was created with these types of scripting tools in mind to facilitate powerful automation capabilities.

Expect script example

The following provides a simple Expect script example with no timeouts and no error checking using Telnet instead of SSH.

```
#!/usr/local/bin/expect -f

# (Portions of) this Expect script (were) was generated by autoexpect on
#     Tue Nov 21 08:45:11 2006
# Expect and autoexpect were both written by Don Libes, NIST.
#
# Note that autoexpect does not guarantee a working script. It
# necessarily has to guess about certain things. Two reasons a script
# might fail are:
#
# 1) timing - A surprising number of programs (rn, ksh, zsh, telnet,
# etc.) and devices discard or ignore keystrokes that arrive "too
# quickly" after prompts. If you find your new script hanging up at
# one spot, try adding a short sleep just before the previous send.
# Setting "force_conservative" to 1 makes Expect do this
# automatically - pausing briefly before sending each character. This
# pacifies every program I know of. The -c flag makes the script do
# this in the first place. The -C flag allows you to define a
# character to toggle this mode off and on.
#
# 2) differing output - Some programs produce different output each time
# they run. The "date" command is an obvious example. Another is
# ftp, if it produces throughput statistics at the end of a file
# transfer. If this causes a problem, delete these patterns or replace
# them with wildcards. An alternative is to use the -p flag (for
# "prompt") which makes Expect only look for the last line of output
# (i.e., the prompt). The -P flag allows you to define a character to
# toggle this mode off and on.
#
# Read the man page for more info.
#
# -Don
#
# (End of auto-expect generated content)
```

```
# USER
set mp_user "Admin"

# PASSWORD- get password from terminal instead of storing it in the script
```
Command menu commands and standard command line scripting syntax

The following list of commands is provided to familiarize you with the Command menu commands. Command-line interface scripting syntax for each command is provided to help you accomplish a scripting task. The following rules apply to scripting syntax:

- The -nc (no confirmation) is optional. This special keyword designates that no user confirmation is required to run the command. If you enter -nc at the end of the command line, the command is issued without asking you for user input. Without the -nc option, you are asked to confirm the changes. The only exception to this rule is when a password must be entered. In that case, you are prompted for a
password separately. However, commands that require a password can have that password entered on the command line (FW, UC).

If –nc is specified on a command with no other parameters or with only a specific multilevel selector, the command displays all or just the specific multilevel parameters. The absence of a specific multilevel parameter on a command that has multilevels causes all the multilevel parameters to display.

- Most commands accept -all default. This causes all parameters for that command to be set to the default values.
- In some multilevel commands, you can use default to set that level to its default values.
- Further use of default on many individual parameters causes that parameter to be set to its default value.
- –? (MP command-specific help) is optional. If you enter –? by itself with the command, a usage display appears. In the event of an incorrect command line usage, in addition to the error message, the usage display appears.
- Arguments in brackets [ ] are optional.
- Without any arguments, commands enter Menu Mode where individual selections can be made or undone before command is confirmed.

**BLADE**: Display enclosure, bay, and Onboard Administrator information

---

**NOTE:**
This command is available only on a server blade.

---

Command access level: Login access

The BLADE command facilitates the cabling and initial installation of HPE Integrity server blades. It also provides a quick view of the enclosure status.

**Onboard administrator configuration**

**OA IP address**

IP address of the OA.

---

**IMPORTANT:**

Integrity iLO 3 must have a reachable IP address as the default gateway address. Since the OA is reachable, HPE recommends using the OA IP address as the gateway address for Integrity iLO 3. If you use the Enclosure IP mode, this solution works during a failover. In the Enclosure IP mode, a static IP address is assigned to the active OA, and during a failover, the same IP address follows the active OA. If the OA IP address is assigned using DHCP, the solution does not work. In such instances, HPE recommends manually changing the iLO 3 gateway address.

---

**OA MAC address**

MAC address of the OA.

**Server blade configuration**

**Rack name**

Logically groups together enclosures in a rack. The rack name is shared with the other enclosures in the rack.

**Rack UID**

Rack unique identifier.
Bay number
The bay number is used to locate and identify a blade.

Enclosure information

Enclosure name
Logically groups together the server blades installed in the same enclosure. The enclosure name is shared with the other server blades in the enclosure.

Health Indicates one of three states of health of this enclosure.

OK
Normal operation, any issues have been acknowledged.

Degraded
Typically loss of redundancy or partial failure of a component.

Critical
Failure with loss or imminent loss of system function.

Command line usage and scripting:

```
[ -nc ]
blade -?
```

Example of the command with output

```
[gstlhpg1] CM:hpiLO-> blade

Onboard Administrator Information:
IP Address             : 192.0.2.1
MAC Address            : 0x00xxxxxexxbb

Server Blade Information:
Rack name               : RACK
Rack UID                : 000z00xx0000
Bay Number              : 3

Enclosure Information:
Enclosure name          : encl
Health                  : OK

-> Command successful.
```

CA: Configure serial port parameters

Command access level: MP configuration access

The CA command sets the parameters for the local serial console. Input and output data rates are the same. The value returned by the stty command on HP-UX is not the local serial port console speed.

Set up the local serial port parameters as follows:

Baud rates
Input and output data rates are the same. Possible values are as follows: 300, 1200, 2400, 4800, 9600, 19200, 38400, 115200 bit/sec.
Flow control
Xon/Xoff

Mode of operation
Aux UART, iLO MP

The iLO 3 mirrors the system console to the iLO 3 MP local and LAN ports. One console output stream is reflected to all connected console users. If several different terminal types are used simultaneously, some users can see unexpected results.

Command line usage and scripting:

```
CA [ -local ] [ -bit <n> ] [ -flow >software|hardware> ]
CA -?
```

Server blade usage

```
CA [ -local ] [ -bit <n> ] [ -flow >software|hardware> ]
   [ -mode ,aux|ilo> ] [ -nc ]
CA -?
```

See also: SA

**DATE:** Display date

Command access level: Login access

The `DATE` command displays the date of the iLO 3 MP real-time clock.

Command line usage and scripting:

```
DA | DATE [ -nc ]
DA | DATE -?
```

**DC (Default Configuration): Reset all parameters to default configurations**

⚠️ **CAUTION:**

All user information (logins, passwords, and so on) is erased when you use any of the following reset methods.

Command access level: Configure MP settings access

The `DC` command restores all MP configurations to the default values. This command also clears SSH key pairs.

To restore specific configurations to the default values, use the following commands:

```
LAN IP Configuration                          : LC -all DEFAULT
Set Access Configuration                      : SA -all DEFAULT
Inactivity Timer Configuration                : IT -all DEFAULT
Security Options                              : SO -option DEFAULT
User Configuration                            : UC -all DEFAULT
LDAP Directory Configuration                  : LDAP -all DEFAULT
DNS Configurations                            : DNS -all DEFAULT
Power Restore Configuration                   : PR -all DEFAULT
Wake-On-LAN Configuration                     : WOL -all DEFAULT
Local Serial Port Configuration               : CA -all DEFAULT

< MP will be reset if you confirm this request
```

Use any of the following methods to reset passwords in iLO 3:
• In the UC command, change individual users or reset all users to default values.
• Reset passwords by pressing the iLO 3 Physical Presence button on the back panel of your server for longer than 8 seconds. After iLO 3 reboots, the local console terminal displays a message for 5 seconds. Responding to this message in time enables a local user to reset the passwords.

Command line usage and scripting:

```
DC  [-all default [-nc ] ]
DC  -?
```

See Also: CA, IT, LC, SA, SO, UC, LDAP, DNS, WOL

**DF: Display FRUID information**

Command access level: Login access

The DF command displays a formatted list of the Field Replaceable Unit (FRU) information for the modules in the system.

Information provided includes serial number, part number, model designation, name and version number, and manufacturer.

Server blades that occupy multiple bays use a DF command menu organized by bays as follows:
CM:hpiLO-> df.

DF

To dump all available FRU information without any paging, use the command line interface: DF -ALL -NC

Display FRU Information Menu:
1 - Specific FRU Bay 1
2 - Specific FRU Bay 2
A - All available FRUs
V - Display Mode: Text

Enter menu item or [Q] to Quit: 1

1

FRU IDs (Bay 1):

```
----------------
00-System Board      01-SAS Backplane     20-Processor 0
21-Processor 1       24-Processor 0 RAM   25-Processor 1 RAM
40-Virtual Mezz 1    41-Virtual Mezz 2    82-DIMM CPU0 -  3A
83-DIMM CPU0 -  4A   CC-SBL
```

Select FRU ID:

Server blades that occupy a single bay use the traditional DF command menu:

Display FRU Information Menu:
S - Specific FRU
A - All available FRUs
V - Display Mode: Text

Enter menu item or [Q] to Quit:

Command line usage and scripting:

To select the display format, use the -view keyword. The default display mode is TEXT. For this command, the -nc keyword (if entered), implies that no paging takes place. In other words, when the command is started, no intervention by the user is necessary.
To select FRUs in a specific bay on multi-bay server blades, use the optional –bay keyword. If the –bay keyword is omitted, FRUs in all bays appear.

```
DF [ -specific[ <fruid> ] | -all ] [ -bay <bay number> ]
   [ -view <text|hex> ] [ -nc ]
DF   -?
```

Rack servers and single-bay server blades do not support the –bay keyword:

```
DF [ -specific[ <fruid> ] | -all ] [ -view <text|hex> ] [ -nc ]
DF   -?
```

**DI: Disconnect remote or LAN console**

Command access level: MP configuration access

The DI command causes web, or SSH connections to close. It does not disable the ports. To disable the ports, see the SA command for LAN/web/SSH access. Use the TE and WHO commands to identify the connected users before running this command.

The number following the Connected status indicates how many user are connected through that access method.

```
T - Telnet : Disconnected
W - Web SSL : Connected (1)
H - SSH : Disconnected
```

Command line usage and scripting:

```
DI [ -web ] [ -ssh ] [ -nc ]
DI   -?
```

See also: SA, TE, WHO

**DNS: DNS settings**

Command access level: MP configuration access

The DNS command configures the DNS server settings. You can only use this command with DHCP enabled. It enables you to configure DNS Domain Name and up to two DNS servers manually or automatically using DHCP. You can also perform a DDNS update through the primary DNS server as long as it is authoritative for the zone.

If no DNS server IP addresses are specified, or the DNS domain is undefined, DNS is not used.

If an IP address was obtained through DHCP, an add name request is sent to the DDNS server if it is enabled and registered.

Command line usage and scripting:

```
DNS [ [ -server <e|d> ] [ -domain <text> ] [ -name <e|d> ]
   [ -register <y|n> ] [ -1ip <ipaddr> ] [ -2ip <ipaddr> ]
   [ -all default ] [ -nc ]
DNS   -?
```

See also: LC

**FW: Upgrade the MP firmware**

The FW command upgrades iLO MP or specific system programmable firmware. If you are only upgrading the iLO MP firmware, the iLO MP automatically resets upon successful completion and drops all iLO MP LAN connections. To use this feature, you must have the Configure iLO Settings user right.
This upgrade does not affect server operation if it is for iLO MP only.
If this upgrade is system programmable firmware, the upgrade continues when the system power is off.

**NOTE:**
It can take up to ten minutes before the server begins to boot.


**IMPORTANT:**
When performing a firmware upgrade that contains system programmable hardware, you must properly shut down any operating system that is running before starting the firmware upgrade process.

Select the download for Integrity firmware and follow the directions provided in the release notes.

**CAUTION:**
If the firmware upgrade process is interrupted at any time, the core I/O will need to be repaired or replaced.

At the end of the upgrade process, the iLO MP is reset. Reconnect and log in.
If a firmware request is pending when you enter the `FW` command, a `SYSREV` table appears. You will be prompted to either cancel the firmware upgrade request or exit. Follow the prompts on the screen.

**TIP:**
Before performing certain iLO 3 functions, verify that you have the supported firmware version required to carry out the task.

**Command line usage and scripting:**

```
FW [ -url <http|https>://host/filepath> [-force <e\d>] [ -nc ] ]
    [ -cancel [ -nc ] ]
FW -?
```

**HE: Print Help Menu and MP hardware and firmware revision**

Command access level: Login access

The `HE` command displays the MP hardware and firmware version and date and time of firmware generation. The MP hardware version is the MP FPGA version that can be read through firmware.

Additional help is available at the help prompt. Given a topic or command, more detailed help is available.

- When issued in command mode, `HE` displays the list of the MP Command Mode commands available according to the level of the MP Command Mode of the requestor (Operator or Administrator) and the MP mode (Normal or Manufacturing).
- `HE` also displays the MP Help: Command Menu List of detailed help information in response to a topic or command at the help prompt.

**Command line usage and scripting:**

```
HE [ -topic | command ] [ -nc ]
HE -?
```
**ID: System information settings**

Command access level: MP configuration access

The ID command displays and modifies the following:

- Host System Configuration
- Asset Tag information

**Command line usage and scripting:**

```plaintext
ID [ { -host } [ -tag <text> } ] [ -nc ]
ID -?
```

**IT: Modify MP inactivity timers**

Command access level: MP configuration access

The IT command prevents sessions on the system from being inadvertently left open. When you initiate an iLO 3 MP command, other users are prohibited from running any commands until the first command has been completed or until it times out. Command interface inactivity timeout specifies that timeout value. This prevents a user from inadvertently keeping iLO 3 locked in a command, preventing other users from running iLO 3 MP commands.

The inactivity timeout effects how long a user can stay inactive within a command in the text user interface before they are placed back at the command prompt. There is no session timeout on the Integrity iLO 3 text interfaces.

**NOTE:**

The iLO 3 MP command interface inactivity timeout cannot be deactivated.

Use the flow control timeout to prevent any user who is using a terminal that does not obey flow control from locking the system out from other users.

The following are IT command parameters:

- **iLO 3 inactivity timeout**
  1 to 30 minutes (default is 3 minutes).

- **Flow control timeout**
  0 to 60 minutes. If the flow control timeout is set to zero, no timeout is applied. A mirroring flow control condition ceases when no flow control condition exists on any port. This timeout prevents mirrored flow control from blocking other ports when inactive.

**Command line usage and scripting:**

```plaintext
IT [ -command <n> ] [ -flow <n> ] [ -nc ]
IT -?
```

See also: SA

**LC: LAN configuration usage**

Command access level: MP configuration access

The LC command displays and modifies the LAN configuration parameters.

The LC command sets next boot LAN settings. It does not display the current settings. Use the LS command for that purpose. The LC no longer does an automatic reset but advises that a reset is needed to make the changes you performed.
IMPORTANT:
If you are connected through a network and you make any changes to DHCP status, IP address, subnet mask, or gateway IP address, iLO 3 alerts you to manually reset iLO 3 when you confirm the change (see below).

Figure 4: Reset dialogue from TUI (SSH/Telnet/RSC)

If you are connected through a serial console and you make any changes to DHCP status, IP address, subnet mask, or gateway IP address, iLO 3 alerts you to manually reset iLO 3 (see below).

Figure 5: Reset window from web GUI

Configurable parameters include the following:
- iLO 3 MP IP address
- DHCP status (default is enabled)
- When DHCP is enabled, the IP address, gateway IP address and subnet mask are obtained through DHCP. These parameters cannot be changed manually without first disabling DHCP.
- If you change the DHCP status to enabled or disabled, the IP address, subnet mask, and gateway address are set to the default values (0.0.0.0), and the DNS parameters are voided.
- When you change the DHCP status from enabled to disabled, the DNS parameters for DHCP are set to disabled, and the Register with DDNS parameter is set to No.
- When you change the DHCP status from disabled to enabled, the DNS parameters for DHCP are set to enabled, and the Register with DDNS parameter is set to Yes.

- **iLO 3 MP host name**
  - The iLO 3 MP host name set in this command is displayed at the iLO 3 MP command mode prompt. Its primary purpose is to identify the iLO MP LAN interface in a DNS database.
  - If you change the iLO 3 MP host name and the IP address was obtained through DHCP and DDNS is registered, a delete old name request for the old host name and an add name request for the new host name are sent to the DDNS server.
  - Typically you enter the DNS name for the LAN IP. You can program this field to any useful name or phrase. For clarity, enter MPNAME-on-SYSTEM as the MP Host name, so both names show up in the prompt. The limit is 31 characters, and no spaces are allowed.

- **Subnet mask**
- **Gateway IP address**
- **Local console serial port**
- **Link state**

---

**IMPORTANT:**

On Integrity rx2800 i2/i4/i6 servers, the link state 1000BaseT option (or Duplex Option) is not currently supported.

An Integrity rx2800 i2/i4/i6 server can run at 1000BaseT, but only if the switch it connects to supports auto-negotiate to 1000BaseT, and the rx2800 i2/i4/i6 server is similarly set to auto-negotiate. If you want to set a specific LAN speed (10BaseT or 100BaseT), those are the only options that iLO 3 currently supports.

- **SSH access port number**

**Command line usage and scripting:**

```
LC [ -ip <ipaddr> ] [ -subnet <subnet> ] [ -gateway <ipaddr> ]
[ -link <auto|x(10BT)|c(100BT)> ] [ -option <full|half> ]
[ -host <text> ] [ -rsc <n> ] [ -ssh <n> ] [ -dhcp <e|d> ] [ -nc ]
```

See also: DC, ID, SA, SO

**LDAP:** LDAP directory settings

Command access level: MP configuration access

The **LDAP** command displays and modifies the following LDAP directory settings:

- **Directory Authentication**: Activates or deactivates directory support on iLO 3.
  - Enable with Extended Schema: Selects directory authentication and authorization using directory objects created with the HPE schema. Select this option if the directory server is extended with the HPE schema and you plan to use it.
  - Enable with Default Schema: Selects directory authentication and authorization using user accounts in the directory which has not been extended with the HPE schema. User accounts and group memberships are used to authenticate and authorize users. Data in the Group Administration page must be configured after you select this option. In the Group Administration
page, configure one or more directory groups by entering the distinguished name of the group and privileges to be granted to users who are members of that group.

- **Disable**: Deactivates directory support on iLO 3.
- **Local User Accounts**: Includes or excludes access to local iLO 3 user accounts. If local user accounts are enabled, you can log in to iLO 3 using locally stored user credentials. If they are disabled, access is limited to valid directory credentials only.

**NOTE:**
Locally stored user accounts can be active while directory support is enabled. This enables both local- and directory-based user access. If both directory authentication and local user accounts are enabled, login is attempted using the directory first, then using local accounts.

- **Directory Server IP Address**: IP address or host name of the directory server.
- **Directory Server LDAP Port**: Port number for the secure LDAP service on the server. The default value for this port is 636.
- **Distinguished Name**: Specifies where this iLO 3 instance is listed in the directory tree. For example:
  
  \[ cn=MP Server, ou=Management Devices, o=hp \]

- **User Search Contexts (1,2,3)**: User name contexts that are applied to the login name entered to access iLO 3.

User name contexts are used to locate an object in the tree structure of the directory server and applied to the login name entered to access iLO 3. All objects listed in the directory can be identified using the unique distinguished name. However, distinguished names can be long, users might not know the distinguished names, or they might have accounts in different directory contexts. Search contexts enables users to specify common directory contexts, so that they do not have to enter the full distinguished name at login. The iLO 3 attempts to authenticate a user in the directory first by the login name entered, and then by applying user search contexts to that login name until login succeeds. For example:

Instead of logging in as \( cn=user, ou=engineering, o=hp \), search context of \( ou=engineering, o=hp \) enables a user to log in as \( user \).

When extended schema is selected and Active Directory is used as a directory server. Microsoft Active Directory has an alternate user credential format. A user can log in as: \( user@domain.hp.com \), in which case a search context of \@domain.hp.com enables the user to login as \( user \).

**Command line usage and scripting:**

```
LDAP [ -directory [ -ldap <d|x>s> ] [ -mp <e|d> ]
[ -ip <hostname/ipaddr> ] [ -port <n> ]
[ -dn <text> ] [ -1context <text> ]
[ -2context <text> ] [ -3context <text> ]
| -groups [ -change <groupNo.> ] [ -dn <text> ]
[ rights <e|d> ]
<console|mp|power|user|virtual|all|none> ]
[ -list <groupNo.> ]]
| -nc ]
LDAP -?
```

See also: LOGIN, UC

**LDAP: LDAP group administration**

The LDAP command enters one or more directory groups by specifying the distinguished name of the group and privileges to be granted to users who are members of that group.

You must configure group administration information when the directory is enabled with the default schema.
The group administration section of the LDAP command enables users to enter one or more directory groups by specifying the distinguished name of the group and privileges to be granted to users who are members of that group.

When a user attempts to log in to iLO 3, iLO 3 reads that user’s directory name in the directory to determine which groups the user is a member of. The iLO 3 compares this information with a list of configured groups. The rights of all the matched groups are combined and assigned to that user.

**LDAP: Schema-free LDAP**

The Schema-Free LDAP command enables you to use directory authentication for logging in to iLO 3 without having to do any schema extension on the directory server or snap-in installation on the client. For information on schema-free LDAP, see Configuring schema-free LDAP on page 42.

**LM: License manager**

Command access level: MP configuration access

The **LM** command enables you to view your current license status.

**NOTE:**

An Advanced Pack License key is built into all Integrity servers equipped with Integrity iLO 3. No additional licensing is necessary.

**Command line usage and scripting:**

```
LM [ -key <license key> ] [ -nc ]
LM -?
```

**LOC: Locator UID LED configuration**

Command access level: Login access

The **LOC** command displays the current status of the Locator LED.

The Locator LED flashes blue if a firmware upgrade is in progress or if the Physical Presence button is pushed.

In HPE Integrity server blades, this command also enables you to turn the enclosure Locator LED on or off. The LED physically identifies the blade in a data center environment. It emits a blue light when turned on.

**Command line usage and scripting:**

```
LOC [ -on | -off ] [ -nc ]
LOC -?
```

**Server blade usage**

```
LOC [ -server <on | off> ] [ -enclosure <on | -off>] [ -nc ]
LOC -?
```

**LS: LAN status**

Command access level: Login access

The **LS** command.

**Command line usage and scripting:**
**PC: Power control**

Command access level: Power control access

The **PC** command is used to obtain an instantaneous power reading and control system power. It provides the following options for remote control of system power:

**ON**

Turns the system power on. This command has no affect if the power is already on.

**OFF**

Turns the system power off. This command is equivalent to turning the system power off at the front panel switch. There is no signal sent to the operating system to shut the software down before power is turned off. To turn the system off gracefully, ensure that the operating system is shut down before running this command.

**CYCLE**

Turns the system power off, then on. The delay between off and on is 6 seconds.

**Graceful Shutdown**

A signal is sent to the operating system to shut down prior to turning off the system power.

**Command line usage and scripting:**

```
PC [ -on | -off | -graceful | -cycle ] [ -nc ]
PC -?
```

**Example:**

```
[gstlhpg1] CM:hpiLO-> pc -on -nc
PC -on -nc
System will be powered on.
   -> System is being powered on.
-> Command successful.
[gstlhpg1] CM:hpiLO->
```

See also: **PR, PS**

**PM: Power regulator mode**

Command access level: Power control access

The **PM** command provides the following options for remote control of the system power regulator:

**Dynamic**

Enables the system to dynamically change the processor power level when needed based on current operating conditions. The system remains in this mode unless the system is reset or an operating system-hosted application requests a processor state change. In these cases, power management mode changes to operating system Control Mode.
Low
Sets the processor to the lowest supported processor state and forces it to stay in that lowest state
until the system is reset. If the processor is reset, the power mode changes to operating system
Control Mode.

High
Sets the processor to the highest supported processor state and forces it to stay in that highest state
unless the system is reset or an operating system-hosted application requests a state change. If the
processor is reset, the power mode changes to operating system Control Mode.

OS
Sets the control of the power regulator to the operating system.

Command line usage and scripting
Example

[gst10074] CM:hpiLO-> pm
PM [ -dynamic | -low | -high | -os ] [ -nc ]
PM -?

See also: PC, PR

PR: Set power restore policy
Command access level: MP configuration access
The PR command configures the power restore policy. The power restore policy determines how the
system behaves when AC power returns after an AC power loss.

• If PR is set to On or Previous, the system powers on after AC is applied.
• If PR is set to Off, the system stays powered off after AC is applied. To power on the system, push
  the system power button or run the PC command.
• If PR is set to Previous, the power is restored to the state that was in effect when the AC power was
  removed or lost.

Command line usage and scripting:

PR [ -policy <on|off|previous> ] [ -nc ]
PR -?

See also: PC

PS: Power status
Command access level: Login access
The PS command displays the system power status.

Command line usage and scripting:

PS [ -nc ]
PS -?

See also PC, SS.

RS: Reset system through the RST signal
Command access level: Power control access
IMPORTANT:
During normal system operation, shut down the operating system before issuing the RS command.

The RS command resets the system (except iLO 3) through the RST signal.

Running this command irrecoverably halts all system processing and I/O activity and restarts the system.
The effect of this command is similar to cycling the system power. The operating system is not notified, no
dump is taken as the system shuts down, and so on.

Command line usage and scripting:

RS [ -nc ]
RS -?

See also: TC

SA: Set access

Command access level: MP configuration access

The SA command configures the access mode for the LAN and the Command mode. You can set iLO 3 to enable web or SSH access. SSH and web SSL is enabled by default.

If LAN users are connected when a disable from this command runs, they are disconnected. Any future incoming connection request to the corresponding port is rejected. A message appears prior to being rejected.

NOTE:
Currently, when an access method is first set to disabled, the message is sent. However, after an iLO reboot, the port is not opened.

Command line usage and scripting:

SA [ -telnet <e|d> ] [ -web <e|d> ] [ -ssh <e|d> ]
[ -nc ]
SA -?

See also: DI, LC

SO: Security option help

Command access level: MP configuration access

The SO command enables you to modify the security options of iLO 3.

For user configuration, see the UC command. For SSH enable/disable, see the SA command.

The security options menu is as follows:

O – Security Options
  • Login timeouts
  • Allowed password faults
  • Exit security override mode
  • Idle connection timeout
  • Enforce AES/3DES

L – SSL Certificate Options
  This option enables users to do the following –
• View the details of the SSL certificate being used by iLO. The SSL Certificate is used to connect to iLO web GUI.

• Generate a new SSL certificate for iLO web GUI access with user defined parameters.

  By default, iLO uses a self-signed certificate generated automatically the first time the iLO 3 is booted or if the NVRAM in which it is stored gets corrupted. You might want to regenerate this certificate with your own parameters or regenerate it when it is close to expiring. The initial certificate has a 10-year expiration date from the build date of the MP binary image. A regenerated certificate is only valid for 2 years from the system date.

• Generate a Certificate Signing Request (CSR) with user defined parameters and view the generated CSR.

  Generated CSR can be used to obtain a SSL Certificate signed by a trusted Certificate Authority (CA). The signed certificate can be imported into iLO for a more secure SSL connection.

  **NOTE:**
  
The importing of the signed certificate is possible through Web User Interface and the option to import is not available in CLI interface.

H – SSH Key Pairs

This option would only be used if the SSH keys need to be changed by choice or the keys which are stored in NVRAM get corrupted. The first time the iLO 3 is booted, these keys are generated automatically. These key pairs are used for SSH connections to the iLO.

B – Login Security Banner Options

This option is used to configure the security banner displayed on the iLO login page.

The following are SSH command parameters:

• Login timeout: 0 to 5 minutes. This is the maximum time allowed to enter login name and password after the connection is established. The connection is interrupted when the timeout value is reached. The local console restarts the login; for all other terminal types, the connection is closed. A timeout value of 0 means there is no timeout set for the login.

  The login timeout and the timeout value is effective on all ports including the local port. However, the local port cannot be disconnected like other ports on login timeout. For example, if a local port user sits at the `hpilo-> Login:` prompt, no action occurs even when a timeout occurs. However, if a local port user enters a login name, sits at the `hpilo-> Password:` prompt, and a timeout occurs, then this login is cancelled and the `hpilo-> Login:` prompt reappears.

• Number of password faults allowed: 1 to 10. This parameter defines the number of times a user can attempt to log in to a console before being rejected and having its connection closed.

• Idle connection timeout: 15, 30, 60 or 120 or Infinite. This parameter defines how long a user can be inactive, in minutes, before the iLO web interface or Integrated Remote Console session ends automatically. The default value is 15 minutes. Inactive users are not logged out when this option is set to Infinite. While the Remote Serial Console or the Virtual Media applet is connected, the idle connection timeout is not applicable.

• Enforce AES/3DES: Enabling this option enforces iLO to enter into enhanced security mode where it uses only secure encryption algorithms like AES256, AES128, 3DES for SSH and web GUI connections. iLO will reset automatically when this configuration is modified.

  **NOTE:** From iLO 3 firmware version 01.71.06 or later, TLS 1.0, TLS 1.1 protocols and SHA, 3DES based ciphers are no longer supported in enhanced security mode (Enforce AES/3DES option is enabled) for web GUI connections.

• SSL certificate: Enables the generation of SSL certificates.
If you specify the certificate using the command line, then you must specify every parameter.

- Certificate Signing Request (CSR): Allows user to generate a CSR. When the command is used without "-generate" argument, the CSR parameters are updated. When "-generate" option is used, the CSR is generated with the configured parameters. The "-dump" option enables users to view the generated CSR.
- SSH keys generation: Enables SSH keys authorization.
- Login security banner state: When this is enabled, the configured security banner message will be displayed in the iLO login page.
- Login security banner message: Enables users to configure the security banner message. If the security banner message is very long, then it has to be split into smaller chunks and configured using multiple command line operations. The "-message" option can be used to configure the first part of the message and "-append" option can be used to append the other parts to the configured message.

Command line usage and scripting:

```
SO [ { -options [ -login <n> ] [ -number <n> ]
   [ -security_overide disable ]
   [ -idle_conn_timeout <n> ]
   [ -enforce_aes3des <e|d> ] } ]
| { -banner [ -state <e|d> ] } ]
| { -banner [ -message <text> ] } ]
| { -banner [ -append <text> ] } ]
| [ -ssl [ -name <text> ] [-org <text>]
   [ -unit <text> ]
   [ -country <text> ]
   [ -region <text> ]
   [ -locality <text> ]
   [ -email <text> ] ]
| { -csr [ -name <text> ] [-org <text> ]
   [ -unit <text> ]
   [ -country <text> ]
   [ -region <text> ]
   [ -locality <text> ]
   [ -email <text> ]
   [ -generate ] ]
| { -csr [ -dump ] ]
| { -ssh } ] [ -nc ]
```

Some of the security features like the option to enforce AES/3DES ciphers, import of trusted SSL Certificate into iLO and configurable idle session timeout are available in iLO3 versions 01.68.08 or later.

SYSREV, SR: Firmware revisions

Command access level: Login access

The SYSREV, SR command displays the current firmware and hardware revisions in the system.

Command line usage and scripting:

```
SYSREV [ -nc ]
SYSREV -?
```
NOTE:
You can only directly obtain system firmware revision information when the system power is off.

**SS: System processor status**

Command access level: Login access

The **SS** command displays the status of the system processors in the system and which processor is the monarch.

For both server blades and rackmount servers, use the **SS** command from the MP CLI interface for an instantaneous power reading.

The iLO 3 learns the system configuration through the events it receives from the system. There is usually a delay between any processor configuration change and what is displayed by this command. For the most up-to-date processor configuration information, use the UEFI prompt.

Command line usage and scripting:

```
SS [-nc ]
SS -?
```

See also: **PS**

**SYSSET: Display system settings**

Command access level: Login access

The **SYSSET** command displays the following system information: Manufacturer, Product Name, Product Number (primary and secondary), Serial Number (primary and secondary), UUID (primary and secondary), and Product ID.

If primary and secondary parameters do not match, **SYSSET** provides an option to copy one set of parameters to the other

Command line usage and scripting

```
SYSSET [ [-prodname <text>] [-prodnum <text>] ]
[ [-serial <text>] [-uuid <text>] ]
[ [-login <text>] [-password <text>] ]
[ [-copy] ]
[ [-magic] [-nc ] ]
```

SYSSET -?

**TC: System reset through INIT signal**

Command access level: MP configuration access

**IMPORTANT:**

This command is intended to be used only when an operating system is hung.

The action of the **TC** command depends on the current state of the system. If the system is at UEFI, the **TC** command behaves just like the **RS** command. If the system is at an operating system, usually HP-UX, a system crash dump is taken.

The **TC** command disconnects sessions with the system if some sessions are active. If a session was active prior to this command, the console client returns to the Main Menu with respect to the security rules.
Before issuing this command, the MP queries the power monitor to discover the status of the power on
the system. If the power monitor does not respond or the power is OFF, the command is not issued.

Command line usage and scripting:

```
TC [ -nc ]
TC -?
```

See also: RS

**TE: Send a message to other mirroring terminals**

Command access level: MP configuration access

The **TE** command treats all displayable characters following the command as a comment. Characters
typed are broadcast to the connected console clients when you press **Enter**. The string size is limited to
80 characters. Any extra characters are not broadcast to other console clients.

**NOTE:**

The broadcast message is sent only to Command menu clients, and does not include users connected to MP Main Menu functions.

Command line usage and scripting:

```
TE <text> [ -nc ]
TE -?
```

**UC: User Configuration (users, passwords, and so on)**

Command access level: User administration access

The **UC** command adds, modifies, re-enables, or deletes any of the following user parameters:

- User Login ID
- User Password
- User Name
- Workgroup
- Access Rights
- Operating Mode
- User State: Enabled/Disabled

The default user is **Administrator**. The **Administrator** user has all rights (C, P, M, U, and V). You can change the configuration of the Administrator with the **UC** command.

All users have the right to log in to iLO 3 and to run Status (read-only) commands (view event logs, check
system status, power status, and so on), but not to run any commands that alter the state of iLO 3 or the
system.

The following commands are available to all users: **DATE, DF, HE, LOC, LS, PS, SL, SS, SYSREV, TE, VFP, WHO, XD** (LAN status only)

There are two menu items:

- **ping**, can be used by all users
- **reboot**, limited to certain users

An iLO 3 user can also have any or all of the following access rights:

**Console access**

Right to access the system console (the host operating system). This does not bypass host
authentication requirements, if any.
Command: **CO**

**Power control access**

Right to power on, power off, or reset the server, and to configure the power restore policy.

Commands: **PC, PR, RS, TC**

**Local user administration access**

Right to configure locally stored user accounts.

Commands: **UC**

**MP configuration access**

Right to configure all iLO 3 MP settings (and some system settings, such as the power restore policy).

Commands: **CA, CL, DC, DI, FW, ID, IT, LC, LDAP, LOC, PG, SA, SO, XD**

**Virtual Media access**

Right to use the vMedia applet.

**Command line usage and scripting:**

```
UC [ -new <login> -user <text> [ -workgroup <text> ] ]
[ -rights <e|d> <console|mp|power|user|virtual|all|none> ]
[ -mode <single|multiple> ] [ -enable <e|d> ]
[ -password <value> ]
[ -change <login> [-login <newlogin>][ -user <text> ]
[ -rights <e|d> <console|mp|power|user|virtual|all|none> ]
[ -workgroup <text> ] [ -mode <single|multiple> ]
[ -enable <e|d> \ [ -password [ <value> ]
[ -delete <login> ] | [ -list <login> ] ] [ -nc ]
```

**Example:**

```
[gstlhpg1] CM:hpiLO-> uc -delete Oper -nc

UC -delete Oper -nc

Current User Parameters:
User Login ID         : Oper
User Password         : ************
User Name             : Default Operator
User Workgroup        :
User Access Rights    : Console access, Virtual Media
User Operating Mode   : Multiple
User Enabled/Disabled : Enabled

-> Current User will be deleted

User may be disconnected in this process

-> User Configuration has been updated.

-> Command successful.
```

See also: **CA, SO**
**WHO:** Display a list of connected iLO 3 users

Command access level: Login access

The **WHO** command displays the login name of the connected console client users, the ports on which they are connected, and the mode used for the connection.

- Login name
- Login type (LDAP or local authentication)
- User access rights
- Connection port (local, remote, Telnet, web, SSH)
- IP address (for Telnet, web, SSH)
- Current MP mode that user is in (MA-MP Main Menu, CM-Command menu, LIVE-live event viewer, VFP-VFP mode)

For LAN, web, and serial console clients, the command displays the IP address. When DNS is integrated, the host name appears as well.

The local port requires a user to log in. A user must be logged in to the system, or no local port appears.

**Command line usage and scripting:**

```
WHO [ -nc ]
WHO -?
```

See also: DI, TE, UC

---

**WOL:** Wake-On-LAN

This command enables you to turn the Wake-On-LAN feature On or Off for system LANs.

Wake-On-LAN (WOL) is not supported with Integrity servers running Windows or OpenVMS environments. WOL is supported with Integrity BL860c i2, BL870c i2, and BL890c i2 Server Blades running HP-UX 11i v3. The supported remote power-on solution for Windows and OpenVMS is iLO. For details, see the User Service Guide for your server.

**Command line usage and scripting:**

```
WOL [ -on | -off [ -nc ] ]
WOL -?
```

See also: DC

---

**XD:** iLO 3 diagnostics and reset

Command access level: Configure MP settings access for resetting the MP, Login access for all other XD options

The **XD** command enables you to perform a LAN access test to check the connectivity status of the MP. To perform the LAN connectivity test, use the **ping** command.

You can use the **XD** command plus its **R** command option to reset the MP. You can safely perform an MP reset without affecting the operation of the server. You can also reset the MP by pressing the iLO 3 Physical Presence button.

**Command line usage and scripting:**

```
XD [ -lan <ipaddr> | -reset ] [ -nc ]
XD -?
```
Web GUI

When using the iLO 3 web GUI, keep the following information in mind:

- To successfully log in to the iLO 3 web GUI, you must enable cookies on the web browser.
- The appearance of the web GUI pages might differ depending on your server.
- Different browser applications must be used to perform multiple logins to the same iLO from a single client.

Accessing the iLO 3 web GUI

Procedure

1. Open a web browser and enter the DNS name or the IP address for the iLO 3.
2. The Integrated Lights-Out 3 log in page appears.

![Image of the iLO 3 web GUI log in](image)

3. Log in using the default iLO 3 user name and password (Administrator/password found on the iLO Network Information Tag).

**NOTE:**

- On server blades, the iLO Network Information Tag is located on the right side of the monarch blade.
- On HPE Integrity rx2800 i2/i4/i6 servers, the iLO Network Information Tag is located on a pull-tab on the front panel.

Status Summary

The Status Summary menu provides access to server information and enables you to perform server management tasks.
Status Summary>Overview tab

The Status Summary Overview tab displays a brief status summary of the system.

![Figure 7: Overview tab](image)

Table 12: Overview description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Displays system information. When the UUID and serial number are virtualized, they also appear as UUID (logical) and serial number (logical) respectively. Displays the current System platform firmware version and the most recent entry in the System Event Log (SEL) as well.</td>
</tr>
<tr>
<td>Momentary Press</td>
<td>Causes a graceful power off when the system power is on as well as causes a power on when the system power is off.</td>
</tr>
<tr>
<td>Press &amp; Hold</td>
<td>Forces the power off and is only available when system power is on. When system power is off, this button is not visible.</td>
</tr>
<tr>
<td>Turn Locator UID On or Off</td>
<td>Enables you to turn the server Locator UID LED on or off.</td>
</tr>
<tr>
<td>Launch SMH</td>
<td>Provides a link to the System Management Homepage. When there are no OS agents running, the button is disabled.</td>
</tr>
<tr>
<td>iLO</td>
<td>Displays the iLO Health Status, IP Address, Date &amp; Time, and License Type installed on iLO, the current iLO Management Processor firmware version and the most recent entry in the iLO Event Log (IEL).</td>
</tr>
</tbody>
</table>

Relevant iLO MP TUI commands: DATE, ID, LM, LOC, LS, PC, SL, SYSREV

Status Summary>Active Users

The Active Users tab displays information about the users currently logged in to the iLO 3.
**Table 13: Active Users description**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Type</strong></td>
<td>There are several access methods: Serial, Telnet, SSH, or web. Virtual Media users are not listed in web GUI sessions. A check in the checkbox indicates which access methods are turned off when you click <strong>Disconnect</strong>. Serial users are not provided with a checkbox so they cannot be disconnected.</td>
</tr>
<tr>
<td><strong>Login Name</strong></td>
<td>Displays the user currently logged in.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>Displays the IP address of the active user.</td>
</tr>
<tr>
<td><strong>Authorized</strong></td>
<td>Displays the type of authentication:</td>
</tr>
<tr>
<td></td>
<td>• LDAP directory user authentication (LDAP)</td>
</tr>
<tr>
<td></td>
<td>• Locally stored iLO 3 user accounts (local)</td>
</tr>
<tr>
<td></td>
<td>• SecurityOverride</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rights</td>
<td>Displays the rights a user has. The following user access rights are available:</td>
</tr>
<tr>
<td></td>
<td>• Console: Remote Console Access</td>
</tr>
<tr>
<td></td>
<td>• Power: Virtual Power &amp; Reset</td>
</tr>
<tr>
<td></td>
<td>• iLO: Configure iLO Settings</td>
</tr>
<tr>
<td></td>
<td>• User: Administer User Accounts</td>
</tr>
<tr>
<td></td>
<td>• vMedia: Virtual Media</td>
</tr>
<tr>
<td></td>
<td>You can configure a user to have some, none, or all access rights. Every user has default rights unless the user has been disabled. You can enable or disable users on the Administration &gt; User Administration &gt; Local Accounts page.</td>
</tr>
<tr>
<td>Mode</td>
<td>Displays the current iLO 3 mode the user is in.</td>
</tr>
<tr>
<td>Disconnect</td>
<td>Enables a user with the Configure iLO Settings right to disconnect users of a certain access type.</td>
</tr>
</tbody>
</table>

Relevant iLO MP TUI commands: **DI, WHO**

**Status Summary>FW Revisions**

The FW Revisions tab displays current revisions of the system firmware and hardware and if any updates are pending.

![Figure 9: FW Revisions](image)

**System Health**

The System Health page displays system health information, as determined by iLO, obtained from iLO sensors, OS events, and system firmware events.
Table 14: System Health description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Summary</td>
<td><strong>Blade Health LED</strong>&lt;br&gt;Only displays for blade servers in the current system. For further details, consult the System Event Log and Component Health.</td>
</tr>
<tr>
<td></td>
<td><strong>System Event Log Health</strong>&lt;br&gt;Displays the SEL health state for both blade and rackmount servers. For further details, see the System Event Log.</td>
</tr>
<tr>
<td>Component Health</td>
<td>Displays the overall Component Health state, which is a summary of the Processor, Memory, I/O, Power, and Temperature Health states as they apply to the system. The display differs for server blade versus rackmount servers.</td>
</tr>
<tr>
<td></td>
<td><strong>Server Blade</strong>&lt;br&gt;Processor, Memory, I/O, Power, Temperature. Clicking a tab displays component health information for that Blade. If only one Blade is in the system, then the Component Health tab does not appear.</td>
</tr>
<tr>
<td></td>
<td><strong>Rackmount</strong>&lt;br&gt;Processor, Memory, Fan, Power, Temperature.</td>
</tr>
<tr>
<td>Processor Health</td>
<td>Displays the status of the processors and lists their speed, L3 cache, and part number.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Memory Health</td>
<td>Displays the status of the memory modules (DIMMs).</td>
</tr>
<tr>
<td>I/O Health</td>
<td>Displays the status of the installed I/O modules, including mezzanine cards. The I/O health only displays for server blades.</td>
</tr>
<tr>
<td>Fan Health</td>
<td>Displays the fan status. The fan health only displays for rackmount servers.</td>
</tr>
<tr>
<td>Power Health</td>
<td>Lists the power state, power usage in watts, power cap in watts, and power allocations in watts. The display is different for rackmount versus server blades.</td>
</tr>
<tr>
<td></td>
<td><strong>Blade</strong></td>
</tr>
<tr>
<td></td>
<td>Power State, Power Usage, Power Cap, Power Allocation</td>
</tr>
<tr>
<td></td>
<td><strong>Rack</strong></td>
</tr>
<tr>
<td></td>
<td>Power State, Power Usage, Power Cap, Power Supply 1, Power Supply 2</td>
</tr>
<tr>
<td>Temperature Health</td>
<td>Displays the ambient temperature in Celsius and the temperature status.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong></td>
</tr>
<tr>
<td></td>
<td>For BL c-Class servers, you can obtain information on power supplies and fans through the OA.</td>
</tr>
</tbody>
</table>

You can expand information for individual items by clicking the + button or collapse it by clicking the - button to the left of the category. You can expand all the categories or collapse them all at once by clicking the ++ or -- buttons at the top of the list.

**System Event Log**

The System Event Log page enables you to view the contents of the System Event Log stored in nonvolatile memory. Only a user with the Configure iLO Settings right can clear the log.

**NOTE:**

Integrity iLO captures and stores the server System Event Log for access through a browser or text interface even when the server is not operational. This capability can be helpful when troubleshooting remote host server problems.
Table 15: System Event Log description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Event Log Summary</td>
<td>Lists log status and error summary.</td>
</tr>
<tr>
<td>Clear Logs</td>
<td>Clears all entries in the System Event and Forward Progress logs.</td>
</tr>
</tbody>
</table>

Relevant iLO MP TUI command: SL

**NOTE:**
You can view only the most pertinent fields for each event on the web. For a more complete decoding of the events, use the TUI CLI by logging in to iLO 3 through Telnet or SSH.

**Events**

Events can be a result of a failure or an error (such as fan failure, Machine-Check Abort, and so on). They can indicate a major change in system state (such as, firmware boot start or, system power on or off), or they can be forward progress markers (such as CPU self-test complete).

Events are produced by intelligent hardware modules, the operating system, and system firmware. Events funnel into the BMC from different sources throughout the server. The iLO 3 polls the BMC for new events and stores them in nonvolatile memory. Events communicate system information from the source of the event to other parts of the system, and ultimately to the system administrator.

The log viewer contains an event decoder to help you interpret events.

The following event severity (or alert) levels are defined:
0: Minor forward progress
1: Major forward progress
2: Informational
3: Warning
5: Critical
7: Fatal

**Forward Progress Log**

The log viewer enables you to view the contents of the Forward Progress Log stored in nonvolatile memory. To clear the log, you must have the Configure iLO Settings user right.

The Integrity iLO stores a detailed Forward Progress Log of system operation during boot, crash, and any other abnormal conditions that can be used to extensively troubleshoot the server. This log goes far beyond the capabilities of standard IPMI for fault management.

---

**Table 16: Forward Progress Log descriptions**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forward Progress Log</td>
<td>Lists log status and event summary.</td>
</tr>
<tr>
<td>Log Summary</td>
<td></td>
</tr>
<tr>
<td>Forward Progress Log</td>
<td>Lists all events.</td>
</tr>
<tr>
<td>Clear Logs</td>
<td>Clears all entries in the System Event and Forward Progress logs.</td>
</tr>
</tbody>
</table>
System Inventory

The System Inventory page enables you to view data on all FRUs in the system. It also enables any user to view the asset tag for the system. To change the asset tag for the system, you must have the Configure iLO Settings user right.

![System Inventory](image)

Figure 13: System Inventory

You can expand information for individual FRUs by clicking +, or collapse by clicking - to the left of the FRU name. You can expand or collapse all the FRUs at once by clicking ++ or -- at the top of the list. If there are multiple bays in the partition, FRUs for each bay appear separately in tabs. You can access each bay by clicking its corresponding tab.

Table 17: System Inventory descriptions

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset Tag</td>
<td>Displays the asset tag for the system. Asset tags can consist of any alphanumeric string 1 to 31 characters long.</td>
</tr>
<tr>
<td>Submit</td>
<td>To change the current value, enter a new value in the text field and click Submit. If you do not have sufficient rights, the Submit button is disabled and the text field is read only.</td>
</tr>
<tr>
<td>Clear</td>
<td>To reset a modified value to the current one before submitting, click Clear.</td>
</tr>
</tbody>
</table>
iLO Health

The iLO Health page enables you to reset the iLO or reset iLO to the default configuration and view the iLO Self Test Results. To issue either of the two reset iLO options, you must have the Configure iLO settings user right. You can safely perform an iLO reset without affecting server operation.

Table 18: iLO Health descriptions

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset the iLO to Default Configuration</td>
<td>Resets sets all iLO parameters to the default values.</td>
</tr>
<tr>
<td>Reset iLO</td>
<td>All iLO parameters retain their current values. Note: iLO reset is disabled during a firmware upgrade.</td>
</tr>
<tr>
<td>Submit</td>
<td>Submits your request to the system</td>
</tr>
</tbody>
</table>

iLO Self Test Results

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NVRAM</td>
<td>The status of non-volatile RAM.</td>
</tr>
<tr>
<td>EEPROM</td>
<td>The status of the EEPROM.</td>
</tr>
</tbody>
</table>

Relevant iLO MP TUI commands: DC, XD –R
The log viewer enables you to view the contents of the iLO Event Log stored in nonvolatile memory.

Figure 15: iLO Event Log

Table 19: iLO 3 Event Log descriptions

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iLO 3 Event Log Summary</td>
<td>Displays alert level information.</td>
</tr>
<tr>
<td>iLO 3 Event Log</td>
<td>Displays all the events corresponding to iLO 3 MP login/logout actions and</td>
</tr>
</tbody>
</table>
<pre><code>                       | running of iLO 3 MP commands.                                              |
</code></pre>

Relevant iLO MP TUI command: SL

Remote Serial Console

The Remote Serial Console enables you to securely view and manage a remote server. You can view and interact with the boot-up sequence of an HPE server, perform maintenance activities in text mode, and manage non-graphical mode operating systems.

To use this feature, you must have the Remote Console Access user right. To assign privileges to this right, use the Administration>User Administration page.
Remote Serial Console requires prior installation of Java Plug-in to be installed on the client system.

**NOTE:**
Pop-up blocking applications prevent Remote Serial Console from running. Before starting the Remote Serial Console, disable any pop-up blocking applications.

The iLO 3 mirrors the system console to the iLO 3 MP local, remote, and LAN ports. One console output stream is reflected to all the connected console users. If several different terminal types are used simultaneously by the users, some users may see unexpected results. Only one mirrored user at a time has write access to the console. Write access is retained until another user requests console write access. To obtain console write access, press **Ctrl-Ecf**.

To ensure proper operation of the remote serial console, verify the following conditions:

- Your emulator can run the supported terminal type.
- The iLO 3 terminal setting in the applet is a supported setting.
- The operating system environment settings and your client terminal type are set properly.
- All mirrored consoles are of the same terminal type for proper operation.

The setting in the Java applet (for example, HPterm, VT100, and so on) must match the console type of the OS you are connecting to. A similar issue occurs when using `CO` (or `CL`) from the TUI menu. You must make sure your terminal emulator matches what is in the console log so that terminal-specific output does not garble the display.

**IMPORTANT:**
Do not mix hpterm and vt100 terminal types at the same time. If two collaborating users view console output with different emulation modes set, clients see garbled results when the output from the system is terminal specific.
To launch the applet and connect to the system serial console (Figure 17: Remote Serial Console window on page 88), click Launch. After connecting to the console, you might have to log in to the operating system to perform administration functions.

NOTE:
If Launch is disabled, you do not have the Remote Console Access user right. To add the user right, see User Administration.

Figure 17: Remote Serial Console window

Using this feature, you can do the following:

• View and interact with the boot sequence of your server.
• Perform maintenance activities in text mode.
• Manage nongraphical mode operating systems.

The console window remains open until you sign out of the iLO 3 interface using the provided link in the banner, leave the iLO 3 site, or refresh the entire page.

The remote serial console provides the console, and the GUI provides the iLO 3 MP Main Menu functionality.

Output from the console is stored in nonvolatile memory in the console log, regardless of whether or not any users are connected to a console.
Remote Serial Console

Integrity iLO 3 contains a remote serial console that enables it to actually be the console hardware device for the operating system. This console is a serial interface between the host system and iLO 3. Integrity iLO 3 converts the serial data stream to be available remotely through the remote serial console (a VT320 Java applet). The remote serial console must be correctly enabled and configured in the host. The remote serial console function is a bidirectional data flow of the data stream appearing on the server serial port. Using the remote console paradigm, a remote user can operate as if a physical serial connection is present on the server serial port. With the remote serial console, an administrator can access a console application such as Windows EMS remotely over the network. Integrity iLO 3 contains the functional equivalent of the standard serial port (16550 UART) register set, and the iLO 3 firmware provides a Java applet that connects to the server serial port. If the serial redirection feature is enabled on the host server, iLO 3 intercepts the data coming from the serial port, encrypts it, and sends it to the web browser applet.

For Linux users, the iLO remote serial console provides an important function for remote access to the Linux server. By configuring a Linux login process attached to the server serial port, you can use the iLO remote serial console to remotely log in to the Linux operating system over the network.

Integrated Remote Console

The Integrated Remote Console (IRC) is a signed Direct X application which enables a user to securely manage HPE Integrity Servers with Integrated Lights-Out. The IRC integrates keyboard, video, and mouse into a virtual interface providing an experience similar to that of the remote server graphics console. With the IRC, you can view the server graphics display to directly interact with the server and perform maintenance activities as well as open and run applications on the server using the keyboard and mouse control. The console makes use of the hardware acceleration and advanced graphics features in .NET Framework. The console is launched using Microsoft ClickOnce technology.

The IRC window remains open until one of the following events occurs:
- You sign out of the iLO interface using the provided link in the banner
- The IRC does not detect keyboard or mouse activity for the period configured as idle connection timeout
- Another user disconnects IRC

IRC requirements
- The host operating system needs to supports IRC.
- The client operating system needs to be Microsoft Windows.
- Microsoft .NET Framework 3.5 or above needs to be installed. (available through Windows Update)
- Firefox needs an Add-on to allow it to launch ClickOnce applications. Visit the Firefox Add-on site to find the latest version of the Microsoft .NET Framework Assistant.
- iLO Advanced Pack license needs to be installed.
- The user needs iLO Remote Console Access and Virtual Power & Reset rights. These rights can be enabled from the iLO User Administration pages.
The URL used to log into iLO needs to use the iLO certificate's Common Name (for example, https://<iLO Common Name>).

If iLO is using an imported and trusted SSL Certificate, then client should be able to establish the certificate chain of trust to launch IRC.

If iLO is using a self-signed certificate generated during initial boot or generated by the user with custom parameters, then the iLO certificate needs to be imported on to the client. (see detailed instructions below).

**NOTE:**

In enhanced security mode (when "Enforce AES/3DES" option is enabled), TLS 1.0, TLS 1.1 and SHA1 are disabled by default. If the .Net framework or the .Net ClickOnce application used in the client does not support TLS 1.2, IRC application download will fail. It is recommended to upgrade the Microsoft .Net framework. As an alternative, iLO Text User Interface command "SO" provides an option "Enable TLS1" to enable TLS 1.0, TLS 1.1 and SHA1 in enhanced security mode (Enforce AES/3DES option is enabled).

---

**Instructions for importing the iLO certificate on to the client**

If the IRC application download did not succeed, it is likely that the iLO certificate needs to be imported on to the client. This allows for a secure console session.

**Procedure**

1. **First**, login to the iLO web interface using Internet Explorer.
   a. If IE7 or IE8
      Click the **Certificate Error** located after the URL in the pink box.
      If IE 6.0
      Click the **yellow padlock** in the bottom right hand corner.
   b. Click **View certificates**.
   c. Click **Install Certificate**…
   d. Click **Next**.
   e. Select **Place all certificates in the following store**.
   f. Click **Browse**.
   g. Select **Trusted Root Certification Authorities**.
   h. Click **OK**.
   i. Click **Next**.
   j. Click **Finish**.
   k. Click **Yes**.

2. **Second**, use the Common Name in the iLO certificate to log in to iLO using either Internet Explorer or Firefox.
   a. The "Common Name" is displayed on the login screen and also on the Access Certificate page. The Common Name can be set to the iLO IP address, hostname, or fully-qualified hostname. If the desired access method to iLO is not the current value in the iLO certificate’s Common Name, go to the Access Settings page and generate a new certificate with the desired Common Name. You will need to reset the iLO and import the new certificate following the steps outlined above.

**Configuration and usage suggestions**

- For better responsiveness, select plain wallpaper on the host server system.
- Do not use an animated mouse pointer or enable "mouse trails" on the host server.
• For best remote console performance, set the client screen resolution higher than the host server.
• For security reasons, if you log into a host server through the IRC, you must log out before closing the IRC.

**IRC features**

• IRC maximum supported resolution is 1024 X 768 pixels.
• IRC data is encrypted with the AES encryption algorithm.
• IRC uses encryption and compression providing a secure, reduced bandwidth connection.

**IRC limitations**

• IRC supports only a single user connection.
• IRC does not yet provide identical virtualization of a Windows keyboard. Known issues are:
  ◦ No support for system level commands such as (ctrl) + (esc), (print screen).
  ◦ No support for simultaneous mouse click and keystroke combinations.
• IRC application closes after the configured idle connection timeout if there is no keyboard or mouse activity.
• IRC attempts to pick the best client display settings for that resolution, however some monitors may have trouble with the highest screen refresh rates supported by the clients video adapter. Use Control Panel/ Display/ Settings/ Advanced/ Monitor and select a lower screen refresh rate.

**Using the IRC**

**Procedure**

1. Click the Launch button on the Integrated Remote Console page.

![Figure 18: Integrated Remote Console](image)

The following message appears when the IRC fails to launch:
2. To view the Error Summary, click Details.... If the following error message appears in the IRC log Error Summary section, then the certificate has not been imported:

The underlying connection was closed: Could not establish trust relationship for the SSL/TLS secure channel. + The remote certificate is invalid according to the validation procedure.

3. If iLO is using an imported certificate, as long as the client can establish the certificate chain of trust and the requirements mentioned in IRC page are met, the application download should succeed.

4. If iLO is using a self-signed certificate generated during initial boot or generated by user with custom parameters, connecting to the IRC requires several additional steps. To complete connection, see Instructions for importing the iLO certificate on to the client on page 90.

5. In enhanced security mode (when "Enforce AES/3DES" option is enabled), TLS 1.0, TLS 1.1 and SHA1 are disabled by default. If the .Net framework or the .Net ClickOnce application used in the client does not support TLS 1.2, IRC application download will fail. It is recommended to upgrade the Microsoft .Net framework.

As an alternative, iLO Text User Interface command "SO" provides an option "Enable TLS1" to enable TLS 1.0, TLS 1.1 and SHA1 in enhanced security mode (Enforce AES/3DES option is enabled).

Once you successfully access the IRC, you will have full functionality to use the IRC.

### Virtual Media

Virtual Media (vMedia) enables connections of a CD/DVD-ROM physical device or image file from the local client system to the remote server. The virtual device or image file can be used to boot the server with an operating system that supports USB devices. Virtual Media depends on a reliable network with good bandwidth. This is especially important when you perform tasks such as large file transfers or operating system installations.

The vMedia device can be a physical CD/DVD-ROM drive on the management workstation, or it can be an image file stored on a local disk drive or network drive.

Booting from the iLO 3 CD/DVD-ROM enables administrators to upgrade the host system ROM, upgrade device drivers, deploy an operating system from the network drives, and perform disaster recovery of failed operating systems, among other tasks.

The iLO 3 device uses a client-server model to perform the vMedia functions. The iLO 3 device streams the vMedia data across a live network connection between the remote management console and the host server. The vMedia Java applet provides data to the iLO 3 as it requests it.

---

**NOTE:**

The iLO 3 vMedia is automatically disconnected if the iLO 3 MP is reset. Hewlett Packard Enterprise does not recommend using iLO 3 vMedia with firmware update tools such as HPOFM, which reset the MP midway through the update process.
Using iLO 3 virtual media devices

Connect client-based vMedia to a host HPE Integrity server blade through a graphical interface using a signed Java applet. Refusing to accept the applet certificate prevents browser-based vMedia from functioning (a red X appears). It also prevents the remote console applet from functioning because it is also signed using the same certificate.

**NOTE:**
You can use the vMedia applet only on x86 clients.

To access the iLO 3 vMedia devices using the graphical interface:

**Procedure**

1. Select **Virtual Media**. The Virtual Media page appears (**Figure 19: Virtual Media** on page 93).

   ![Figure 19: Virtual Media](image)

2. To load the vMedia applet, click **Launch**. The vMedia applet loads in support of the vMedia device.
3. At this point, you can connect to a virtual CD/DVD-ROM or USB key device or create an iLO 3 disk image file.
   a. Check the **USB Key for EFI Only** box.
   b. Click **Launch**.
   c. Select **Local Media Drive** in the correct virtual media section.
   d. Select the drive letter of the desired USB key drive on your client PC from the menu. To ensure the source diskette or image file is not modified during use, select the **Force read-only access** option.
   e. Click **Connect**. The connected drive icon and LED change state to reflect the current status of the virtual Drive.
NOTE:
When you disconnect the iLO 3 vMedia, you might receive a warning message from the host operating system regarding unsafe removal of a device. To avoid this warning, use the operating system stop-device function before disconnecting it from the vMedia.

Virtual CD/DVD-ROM


Booting from the iLO 3 virtual CD/DVD-ROM enables you to deploy an operating system from network drives with DVDs or CDs that contain data in the El Torito Bootable CD format, as well as perform other tasks.

If the host server operating system supports USB mass storage devices, the iLO 3 virtual CD/DVD-ROM is also available after the host server operating system loads. Use the iLO 3 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 a problem with the NIC driver.

The virtual CD/DVD-ROM can be the physical CD/DVD-ROM drive on the client system (which you are running on the web browser), or an image file stored on the client or network drive. For maximum performance, HPE recommends using local image files stored either on the hard drive of your client system or on a network drive accessible through a high-speed network link.

The iLO 3 vMedia CD/DVD-ROM appears to your operating system just like any other CD/DVD-ROM. When using the iLO 3 for the first time, the host operating system might prompt you to complete a **New Hardware Found** wizard.

NOTE:
This feature requires that the Java Plug-in 1.4.2 or later is installed.

This feature requires the Virtual Media right. If a user does not have the vMedia right, it can be granted from the User Administration page under the Administration tab by a user with Admin privileges.

To use a physical CD/DVD-ROM drive in your client system:

**Procedure**

1. Select **Virtual Media**. The Virtual Media content page appears.
2. To load the applet and connect to USB CD/DVD-ROM devices and disk image files available on the client as virtual devices on the server, click **Launch**. The vMedia applet appears ([Figure 20: Virtual Media dialog box (before connection)](#)) on page 95).

NOTE:
Only one user and one device can be connected at a time.

**IMPORTANT:**

Only CD and DVD-ROM image files are supported.

If you use a USB key image file, you must select the Floppy/USB Key option. The USB key image file is not interchangeable with the CD or DVD-ROM and vice versa.
Figure 20: Virtual Media dialog box (before connection)

3. Select **Local Media Drive**.

4. Select the drive letter of the desired physical CD/DVD-ROM drive on your client system from the list.

5. Click **Connect**. The connected drive icon and LED changes states to reflect the current status of the virtual CD/DVD-ROM.

Figure 21: Virtual Media dialog box (after connection)

After you are connected, virtual devices are available to the host server until you close the vMedia applet or sign out from a web session.

6. When you are finished using the virtual CD/DVD-ROM, disconnect the device from the host server or close the applet.

---

**NOTE:**

The vMedia applet must remain open when using a vMedia device.
Virtual Media CD/DVD-ROM operating system

You can view the list of supported browser and operating systems in the Quickspec document on the Hewlett Packard Enterprise website.

The vMedia CD/DVD-ROM supports the following operating systems:

- UEFI console currently supports only El Torito bootable CD format media.
- Windows Server 2003 or 2008:

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

- Linux (Red Hat and SUSE)

  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 HPE Integrity server blades) 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
  ```

- HP-UX 11i

  To recognize the hardware path and special files, run the `ioscan -kfnC disk` command.

  To mount the virtual CD/DVD-ROM/image file on a directory, run the `# mount <special files path> /<dir-name>` command.

- OpenVMS 8.3-1H1 and 8.4

  **NOTE:**
  
  Post operating system boot data format is dependent on the operating system.

Creating the iLO 3 disk image files

The iLO 3 vMedia feature enables you to create CD and DVD image files within the same applet. The image files created are ISO-9660 file system images and El Torito bootable CD images. The performance of the iLO 3 vMedia is faster when image files are used. The utility to create the iLO 3 CD/DVD-ROM disk image files is integrated into the vMedia applet.

Store image files on your client computer or on a network drive that you can access from the client using a fast network segment. A disk image file produces better performance than using a physical CD in your client computer.

To create image files from physical diskettes, CDs, or DVDs, use the Disk>Image option. The Disk>Image button changes to Image>Disk when clicked. The Image>Disk option is not valid for a virtual CD/DVD-ROM image.

  **NOTE:**
  
  The iLO 3 Create Media Image utility does not currently support USB devices in Linux or NetWare.

To create an iLO 3 disk image file:

**Procedure**

1. In the Virtual CD-ROM section of the vMedia applet, select **Local Image File**.
2. Select **Local Media Drive**.
3. To open the Create Media Image dialog box and locate the image file, enter the path or file name of the image in the text box or click **Browse**.

4. Click **Create Disk Image**. The vMedia applet begins the process of creating the image file. This process creates a file that emulates a CD/DVD-ROM on the local system. The process is complete when the progress bar reaches 100%. To cancel the creation of an image file, click **Cancel**.

To insert the next CD during an operating system installation or any application installation with multiple image files:

- To select the next image file or to replace the CD/DVD-ROM with the next CD/DVD-ROM, click **Browse**
- To continue the installation, click **OK** on the host server.

**IMPORTANT:**

Do not click **Disconnect** to select the next CD/DVD-ROM image file.

The connected drive icon and LED change states to reflect the current status of the virtual CD/DVD-ROM. After you are connected, virtual devices are available to the host server until you close the vMedia applet. When you are finished using the virtual CD/DVD-ROM, you can disconnect the device from the host server or close the applet. The vMedia applet must remain open when you use a vMedia device.
The iLO 3 vMedia CD/DVD-ROM appears like any other CD/DVD-ROM to your operating system. When you use iLO 3 for the first time, the host operating system might prompt you to complete a New Hardware Found wizard.

**Virtual USB key**

The iLO 3 vMedia devices connect to the host server using USB technology. Using USB also enables new capabilities for the iLO 3 vMedia devices when connected to USB-supported operating systems. Integrity iLO 3 v1.00 supports Virtual USB flash as a read-only device for use only with EFI, not with a client operating system.

The USB key can be the physical USB key 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, HPE 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 the USB key drive in your client PC:

**Procedure**

1. Click **Launch**.
2. Select **Local Media Drive** in the correct virtual media section.
3. Check the USB box on the right-hand side of the window.
4. Select the drive letter of the desired USB key drive on your client PC from the menu. To ensure the source diskette or image file is not modified during use, select the **Force read-only access** option.
5. Click **Connect**. The connected drive icon and LED change state to reflect the current status of the virtual Drive.

![Virtual USB key](image)

**Figure 24: Virtual USB key**

To use an image file:

1. Click **Launch**.
2. Within the virtual USB key section of the vMedia applet, select **Local Image File**.
3. In the text-box, enter the path or file name of the image, or to locate the image file by using the Choose Disk Image File dialog, click **Browse**. To ensure the source diskette or image file is not modified during use, select **Force read-only access**.
IMPORTANT:
You must select the USB key image file with this option.
If you use CD or DVD-ROM image files, you must select the CD/DVD-ROM option. The CD or DVD-ROM option is not interchangeable with the USB key image file and vice versa.

4. Click Connect. The connected drive icon and LED change state to reflect the current status of the virtual USB key drive. When connected, the virtual devices are available to the host server until you close the vMedia applet.

5. When you are finished using the virtual USB key, disconnect the device from the host server or close the applet.

Performance
• A disk image file results in better performance than a physical drive.
• Store the image files on the client or on a network drive accessed using a fast network segment.
• The drive-connected icon and LED change state to reflect the connection status of the virtual drive.
• The connected drive appears with data on the host while the nonconnected device appears as an empty drive.
• To ensure that the source diskette or image file is not modified during use, you can use the force read-only access.
• The vMedia applet connects to iLO 3 using port number 17988.

Server blade Onboard Administrator DVD
The following requirements apply for all server blades:
• The USB key is only available through the applet in the iLO 3 web GUI.
• You can connect vMedia using either the BladeSystem Onboard Administrator DVD or the applet in iLO web GUI. You cannot use both connection methods at the same time.
• If you need to install operating systems using both CD and USB key, you must connect both from the applet in the iLO 3 web GUI.

Virtual Media applet timeout
The vMedia applet does not timeout when it is connected to a host server. The vMedia applet must remain open when using a vMedia device. The vMedia applet closes when you sign out of the iLO interface using the provided link in the banner, leave the iLO site, or refresh the entire page.

Supported operating systems and USB support for virtual Media
To use vMedia devices, your operating system must support USB mass storage devices.
Different operating systems provide different levels of USB support. Integrity iLO 3 uses the built-in USB drivers of the operating server. The level of USB support in the operating system affects the level of support for iLO 3 vMedia. In general, any operating system issues that affect a USB CD/DVD-ROM drive also affect iLO 3 vMedia.
The HPE server ROM provides support during server boot for vMedia with the El Torito bootable CD format.
You can view the list of supported operating systems on the Hewlett Packard Enterprise website at https://www.hpe.com/h20195/v2/getpdf.aspx/c04154454.pdf.

Java Plug-in version
The vMedia feature requires prior installation of Java Plug-in 1.4.2_10, 1.5 or 1.6.0. With iLO 3 firmware version 02.00.0x or later, the virtual media applet should work with Java 1.7 and Java 1.8.
Client operating system and browser support for virtual media

You can view the list of supported client operating systems and browser support on the Hewlett Packard Enterprise website at http://www.hpe.com/info/Integrity_Servers-docs. The browser and OS information is located in the Quickspec document located on this website.

Power Management

The iLO 3 power management feature enables you to view and control the power state of the server, monitor power usage, and monitor the processor. You must have the Virtual Power & Reset user right to choose options on the power pages except where stated that the Configure iLO Settings user right is required.

The Power Management menu has the following options:

- Power & Reset
- Power Meter Readings
- Power Regulator & Capping

The pages are automatically refreshed every 10 seconds.

Power & Reset

The Power & Reset page enables you to view and control the power state and power options of the server. To choose options on this page, except where stated that the Configure iLO Settings right is required, you must have the Virtual Power & Reset right.

Figure 25: Power & Reset

For information on how to set the power management options in the OA, see the HPE BladeSystem Onboard Administrator User Guide on the Hewlett Packard Enterprise website.
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Power</td>
<td>The current power state of the system.</td>
</tr>
<tr>
<td>System Power Control</td>
<td>Power control access enables you to issue the following options for remote control of the system power:</td>
</tr>
<tr>
<td>Graceful Power Off</td>
<td>The iLO 3 sends a signal to the operating system to shutdown before turning off system power. Supported by IPF operating systems.</td>
</tr>
<tr>
<td>Force Power Off</td>
<td>Turns system power off. This action is equivalent to forcing the system power off with the front panel power switch. No signal is sent to the operating system to bring the software down before power is turned off. To power off the system properly, shut down the operating system before issuing this command.</td>
</tr>
<tr>
<td>Force System Reset with Crash Dump (TOC/INIT)</td>
<td>Causes the system to be reset through the INIT or TOC signal. All system processing and I/O activity is irrecoverably halted. The processors are signaled to dump state on the way down.</td>
</tr>
<tr>
<td>Force System Reset</td>
<td>Causes the system to reset through the RST signal. All system processing and I/O activity is irrecoverably halted. The effect of this command is very similar to cycling the system power. The operating system is not notified, no crash dump is taken on the way down, and so on.</td>
</tr>
<tr>
<td>Force Power Cycle</td>
<td>Turns system power off, waits 30 seconds, then turns the system power back on.</td>
</tr>
<tr>
<td>System Power Restore Settings</td>
<td>The power restore policy determines how the system behaves when AC power returns after an AC power loss. To issue these options, you must have the Configure iLO Settings user right.</td>
</tr>
<tr>
<td>Restore Previous Power State</td>
<td>The power is restored to the state that was in effect when AC power was removed or lost.</td>
</tr>
<tr>
<td>Automatically Power On</td>
<td>The system is powered on after AC power is applied.</td>
</tr>
<tr>
<td>Remain Powered Off</td>
<td>The system remains powered off after AC power is applied. To power on the system, you must push the system power switch or choose the Power On option under System Power Control.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Power On Delay     | **NOTE:**
|                    | The power on delay feature is only available on rackmount servers. For server blades, the OA handles the power on delay feature. |
|                    | The power on delay specifies how many seconds the system will delay power on after AC power is applied. The power on delay is applicable when the power restore policy is set to Restore Previous Power State or Automatically Power On. The default power on delay is 0 seconds. |
| Wake-On-LAN        | Enables or disables Wake-On-LAN for the system LANs.                        |
|                    | **NOTE:**
|                    | Wake-On-LAN (WOL) is not supported with Integrity servers running Windows or OpenVMS environments. WOL is supported with Integrity BL860c i2/i4/i6, BL870c i2/i4/i6, and BL890c i2/i4/i6 Server Blades running HP-UX 11i v3. The supported remote power-on solution for Windows and OpenVMS is iLO. For details, see the User Service Guide for your server. |

Relevant iLO MP TUI commands: **PC, PR, PS, WOL**

**Power Meter Readings**

The Power Meter Readings page enables you to view the Power Meter Readings over time.

Power meter readings shares information with Insight Power Manager.

The Power Meter Readings page has two graphs: a 24-Hour History Graph and a 20-Minute History Graph.
**Figure 26: Power Meter Readings**

**IMPORTANT:**

Power consumption data readings are dependent on the configuration, architecture, components, and levels of activity of the server at any given time.
### Table 21: Power Meter Readings description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>History Graphs</td>
<td>The graphs display recent server power usage. The graph data is reset whenever the iLO MP is reset. Samples are taken in 5 minute and 10 second time increments.</td>
</tr>
<tr>
<td></td>
<td><strong>24-Hour History Graph</strong></td>
</tr>
<tr>
<td></td>
<td>24-hour display with samples taken every 5 minutes.</td>
</tr>
<tr>
<td></td>
<td><strong>20-Minute History Graph</strong></td>
</tr>
<tr>
<td></td>
<td>20-minute display with samples taken every 10 seconds.</td>
</tr>
<tr>
<td></td>
<td>Each sample includes the power usage, power regulator mode, temperature, and time stamp of when the sample was taken. You can display this information by positioning the mouse over a sample on each graph. The peak, average, and cap samples display by default. You can display or hide peak, average, and cap samples on the graphs by toggling the appropriate checkbox.</td>
</tr>
<tr>
<td></td>
<td><strong>Peak</strong></td>
</tr>
<tr>
<td></td>
<td>Samples are red and appear in the background.</td>
</tr>
<tr>
<td></td>
<td><strong>Average</strong></td>
</tr>
<tr>
<td></td>
<td>Samples are blue.</td>
</tr>
<tr>
<td></td>
<td><strong>Minimum</strong></td>
</tr>
<tr>
<td></td>
<td>Samples are gray and appear in the foreground.</td>
</tr>
<tr>
<td></td>
<td><strong>Cap</strong></td>
</tr>
<tr>
<td></td>
<td>Samples are black.</td>
</tr>
<tr>
<td>Power Units</td>
<td>You can display the samples in either watts or Btu/hr by selecting the appropriate units in the <em>Show values in</em> menu.</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current State</td>
<td>Displays the current power readings.</td>
</tr>
<tr>
<td></td>
<td>• Present Power Reading</td>
</tr>
<tr>
<td></td>
<td>• Present Power Cap</td>
</tr>
<tr>
<td></td>
<td>• Power Regulator Mode</td>
</tr>
<tr>
<td></td>
<td>Displays the power reading at iLO initialization.</td>
</tr>
<tr>
<td></td>
<td>• Power Input Voltage</td>
</tr>
<tr>
<td>Power History</td>
<td>Displays power history collected in 5 minute, 20 minute, and 24 hour</td>
</tr>
<tr>
<td></td>
<td>increments.</td>
</tr>
<tr>
<td></td>
<td><strong>Peak</strong></td>
</tr>
<tr>
<td></td>
<td>Displays the highest power usage of the samples collected.</td>
</tr>
<tr>
<td></td>
<td><strong>Average</strong></td>
</tr>
<tr>
<td></td>
<td>Displays the average power usage of all the samples collected.</td>
</tr>
<tr>
<td></td>
<td><strong>Minimum</strong></td>
</tr>
<tr>
<td></td>
<td>Displays the lowest power usage of the samples collected.</td>
</tr>
</tbody>
</table>

**Power Regulator & Capping**

The Power Regulator & Capping page enables you to view and control the power regulator and power capping settings for the server. To change this setting, you must have the Configure iLO Settings user right.

The Power Regulator feature is available on systems where support is provided by the operating system, processors, PDH (processor dependant hardware), SFW (System Firmware), and iLO firmware. For more information on power regulation support, see your server model Quickspecs document.
Figure 27: Power Regulator & Capping
### Table 22: Power Regulator & Capping description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Power Regulator Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Dynamic Power Savings Mode</strong></td>
<td>This mode enables the system to dynamically change processor p-states when needed based on current operating conditions. The implementation of this mode is operating system specific. For details, see your operating system documentation.</td>
</tr>
<tr>
<td><strong>Static Low Power Mode</strong></td>
<td>This mode sets the processor to the lowest supported power consumption state and forces it to stay in this lowest state.</td>
</tr>
<tr>
<td><strong>Static High Performance Mode</strong></td>
<td>This mode sets the processor to the highest supported performance processor state and forces it to stay in this highest state.</td>
</tr>
<tr>
<td><strong>OS Control Mode</strong></td>
<td>This mode configures the server to enable the operating system to control the processor p-states. Use this setting to put the Operating System (including OS-hosted applications) in charge of power management.</td>
</tr>
<tr>
<td><strong>Power Capping Settings</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Power Cap Value</strong></td>
<td>The power cap value in watts or Btu/hr and percentage.</td>
</tr>
<tr>
<td><strong>Maximum Power Rating</strong></td>
<td>Maximum power cap allowed.</td>
</tr>
<tr>
<td><strong>Peak Observed Power</strong></td>
<td>A power cap at or above this value should have no impact on server performance.</td>
</tr>
<tr>
<td><strong>Minimum Observed Power</strong></td>
<td>Idle power consumption and lowest possible power cap. A power cap near minimum power might have significant impact on server performance.</td>
</tr>
<tr>
<td><strong>Show values in Btu/hr or Show values in watts</strong></td>
<td>Select how you want the values to display.</td>
</tr>
</tbody>
</table>

**NOTE:**

Power caps set to less than 50% of the difference between peak observed power and minimum observed power might become unreachable due to changes in the server. Power caps set to less than 20% are not recommended, and might cause the server to reboot or the server OS to stop responding.

Relevant iLO MP TUI command: **PM**

### Administration

The Administration menu enables you to access the following pages:
Firmware Upgrade

The Firmware Upgrade page enables you to upgrade the iLO 3 and system programmable firmware. To use this feature, you must have the Configure iLO Settings user right.

Figure 28: Firmware Upgrade

NOTE:

Bundles containing firmware (iLO firmware, System firmware, and/or System programmable hardware) that may be installed using this Firmware Upgrade page are available for download. It is important to check the compatibility of the firmware revisions in the bundle with the current revisions on the system prior to updating. Use of the HP SUM firmware upgrade tool will automatically perform compatibility checking.

To find appropriate bundles for this system:
Procedure

2. Search for this server product, for download drivers and software.
3. Choose your operating system, if you want to get a bundle that can be installed from the operating system; or, choose **OS independent (BIOS, Firmware, Diagnostics, etc.)**, if you want to get a bundle to install using this SUM, Firmware Upgrade page, a CD, or using UEFI with the system down.
4. Locate **Firmware - System** or **Firmware - Management** in the list of offerings. To perform the upgrade, follow the instructions under the description for the bundle.

Perform the upgrade through the MP LAN by http(s). Enter the information required for the upgrade through the \texttt{FW} command interface.


**IMPORTANT:**
When performing a firmware upgrade that contains system programmable hardware, you must properly shut down any operating system that is running before starting the firmware upgrade process.

**CAUTION:**
If the firmware upgrade process is interrupted at any time, you must repair or replace the core I/O.

At the end of the upgrade process, the MP is reset. Reconnect and log in.

If a firmware request is pending when you enter the \texttt{FW} command, a \texttt{SYSREV} table appears. You will be prompted to either cancel the firmware upgrade request or exit. Follow the prompts on the screen.

The \texttt{FW} command upgrades iLO MP or specific system programmable firmware.

- If only upgrading the iLO MP firmware, the iLO MP automatically resets upon successful completion dropping all iLO MP LAN connections. This upgrade will not affect server operation if it is for iLO MP only.
- If this upgrade is system programmable firmware, the upgrade can be completed without resetting iLO, however, the server needs to be reset for the pending system programmable firmware revisions to become active. Resetting the server to activate pending firmware can take up to 10 minutes before the server begins to boot.

After the upgrade, reconnect and log in.

**TIP:**
Before performing certain iLO 3 functions, verify that you have the supported firmware version required to carry out the task.

**Licensing**

The Licensing page displays the factory-installed iLO 3 Advanced Pack License Key.

The iLO 3 firmware comes with a full-featured permanent default Advanced Pack Licensing Key built in. No additional licensing is necessary. The **New Permanent Licensing Key** field is reserved for future use. This field is unused in Integrity iLO 3 v1.00.
IMPORTANT:
The HPE ProLiant iLO 3 Advanced Pack Licensing Key will not work on an HPE Integrity server blade and vice versa.

Figure 29: Licensing

The following Advanced Pack features are available in this firmware release:

- Virtual Media
- Directory Services Integration for iLO 3 user management using LDAP-based directory services
- Schema-free LDAP based directory services (LDAP-lite)
- Power Meter Readings
- Integration with Insight Power Management

These features can change without notice. Not all features are supported by all operating systems. Not all features are supported by all platforms. Some features require configuration and additional support.

Table 23: Licensing description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensing Key Status</td>
<td>Displays the status of the license.</td>
</tr>
<tr>
<td>Install Date</td>
<td>Displays the date the license was installed.</td>
</tr>
<tr>
<td>Licensing Key</td>
<td>Displays the license key.</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Permanent Licensing Key</td>
<td>Optional field reserved for future use. This field is unused in Integrity iLO 3 v1.00.</td>
</tr>
<tr>
<td>Submit</td>
<td>Submits the key for activation.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancels the action.</td>
</tr>
</tbody>
</table>

**User Administration>Local Accounts**

The Local Accounts page displays the current list of local users, their privilege rights and whether those rights are enabled or disabled. This page enables you to modify the user configuration of iLO 3. To use this feature, you must have the Administer User Accounts user right.
Figure 30: Local Accounts

The default user is Administrator. The Administrator user has all access rights.
Table 24: Local Accounts description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select User</td>
<td>To edit or delete a user account, select an existing user from the list of user names and click <strong>Edit</strong> or <strong>Delete</strong> to either edit or delete that user account.</td>
</tr>
<tr>
<td>New</td>
<td>To create a new user account, click <strong>New</strong>. This opens a page that enables you to enter account information for the new user. By default, a new user is granted the Remote Console Access and Virtual Media rights. The operating mode is set to multiple logins, and the user is enabled.</td>
</tr>
<tr>
<td>Edit</td>
<td>Click this button after selecting the user account to modify or to add a new account. For an existing account, you can modify any of the parameters shown, provided the user has sufficient privileges.</td>
</tr>
</tbody>
</table>

Table Continued
Clicking **Edit** or **New** brings up a page that enables a user to enter the following user account information:

**Login ID**
- This field is required. This is the name that must be used when logging in to the iLO MP. The Login ID must be unique. The maximum length is 24 characters.

**Password**
- This field is required. The password must be provided when logging in to iLO 3. The password must be a minimum of 5 characters and can contain a maximum of 24 characters.

**Password Confirmation**
- This field is required. The password must be provided a second time for verification.

**User Name**
- This field is required. This name appears in the user list and on the home page. It is not necessarily the same as the Login ID. The User Name must be unique. The maximum allowed length is 24 characters.

**Workgroup**
- This field is optional, and can be initialized to an intuitive name.

**Access Rights**
- iLO MP user privileges control user access to the iLO MP functions that a user can perform. You can configure iLO 3 users to have any (or all) of the following privileges: Remote Console Access, Virtual Power & Reset, Configure iLO Settings, Administer User Accounts, and Virtual Media.

  For more information on access rights, see the User Rights page located under the Help tab.

**Operating Mode**
- Multiple logins allow a user to log in more than once. If the mode is Single, the state is changed to disabled after the first login.

**User Enabled/Disabled**
- Enabled allows a user to log in to the iLO MP. If disabled is selected, the user will not be able to log in to the iLO MP.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Click this button after selecting the user account to delete. If you do not have the User Administration Access right, this button is disabled.</td>
</tr>
</tbody>
</table>
NOTE:
You must configure the HPE System Insight Manager group actions feature for iLO 3 to use an existing iLO user name.

To configure, manually edit the `MpTools.xml` file and replace the `<execute-as-user>` attribute with an existing user name on the iLOs. This new user name must have all access rights. To find the `MpTools.xml` file, look in the tools directory on the Central Management Server.

Additionally, iLO 3 supports user accounts created for login from the BladeSystem Onboard Administrator. These user accounts appear as OAtmp#, where # is a number from 1-5. Removing the BladeSystem Onboard Administrator user accounts is not recommended.

Relevant iLO MP TUI command: `UC`

**Group Accounts**

The Group Accounts page enables you to enter one or more directory groups by specifying the distinguished name of the group and privileges that can be granted to users who are members of that group. To use this feature, you must have the Configure iLO Settings user right.

Group administration information must be configured when the directory is enabled with the default schema.

When a user attempts to log in to iLO 3, iLO 3 reads that user’s directory name in the directory to determine the groups that include the user as a member. The iLO 3 compares this information with a list of groups configured by the user. The rights of all the matched groups are combined and assigned to that user.
Figure 31: Group Accounts
Table 25: Group Accounts description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>Click this radio button and click <strong>Edit</strong> to open a page that enables you to change settings for the Administrator group.</td>
</tr>
<tr>
<td>User</td>
<td>Click this radio button and click <strong>Edit</strong> to open a page that enables you to change settings for the User group.</td>
</tr>
<tr>
<td>Custom (1,2,3,4)</td>
<td>Click one of these radio buttons and click <strong>Edit</strong> to open a page that enables you to change settings for the chosen Custom group.</td>
</tr>
<tr>
<td>Clear</td>
<td>Cancels the action.</td>
</tr>
</tbody>
</table>

Relevant iLO MP TUI command: **LDAP**

**Access Settings**

The Access Settings page enables you to access the following tabs:
- LAN
- Serial
- Login Options
- Login Security Banner
- Encryption

**LAN**

The LAN tab enables you to modify LAN settings. To use this feature, you must have the Configure iLO Settings user right.

![LAN Access Settings](image)

**Figure 32: LAN**
Table 26: LAN description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet</td>
<td>You can enable or disable Telnet access to iLO 3 using the enable or disable option. This does not affect the IP configuration or the ability of iLO 3 to perform upgrades over the LAN. The Telnet port number is 23. You cannot change it.</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>Integrity iLO 3 ships with Telnet disabled by default.</td>
</tr>
</tbody>
</table>
| SSH                | You can enable or disable SSH access to the iLO 3 using the enable or disable option. The default SSH port number is 22. You can configure this port number to a value in the range 2000-2400. If the port number is modified, it takes effect the next time iLO 3 is rebooted. To secure an SSH connection, select **Enable** and ensure that an SSH key pair has been generated. SSH is an industry-standard client-server connectivity protocol that provides a secure remote connection. The iLO 3 firmware supports:  
  • SSH2 implementation  
  • Authentication algorithms RSA and DSA  
  • Encryption algorithms 3DES-CBC, AES128-CBC, AES256-CBC, and AES256-CTR  
  • Integrity algorithms HMAC-SHA256, HMAC-SHA1, and MD5.  
  • When 'Enforce AES/3DES' is enabled, the weaker ciphers will be disabled. |
| Key Pair Status    | Indicates if a key pair has been generated previously. To generate a new SSH key pair, check **Generate New Key Pair** and click **Submit**.             |
| Web SSL            | You can enable or disable the web SSL access to iLO 3 using the enable or disable option. The port value is 443. You cannot change it. To make an SSL connection, a valid SSL Certificate is required. For SSL Certificate status and related configuration, please visit SSL Certificate Settings page under **Administration > Settings** |
| Certificate Status | The iLO MP auto generates an SSL certificate when it is first powered on at initial installation. It is expected that you will generate a new certificate with valid information when you log in. The certificate status indicates if a certificate has been generated previously. To generate a new certificate, select **Generate New Certificate**, fill in the fields, and click **Submit**. |
| Remote Serial Console | The Remote Serial Console default port value is 2023. You can configure it to a value in the range 2000-2400. If the port number is modified, it takes effect the next time iLO 3 is rebooted. |
| Integrated Remote Console | The Integrated Remote Console default port value is 17990. You cannot change it.                                                                 |
Virtual Media | The Virtual Media default port value is 17988. You cannot change it.
Submit | Submits the information.
Clear | Cancels the action.

Relevant iLO MP TUI commands: LC, SA, SO

Serial

The Serial tab enables you to set the serial port parameters. To change the external serial port mode, the iLO baud rate, and the iLO flow control settings, you must have the Configure iLO Settings user right.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode of Operation</td>
<td>Enables you to set the local serial mode of operation to either the iLO MP, Auxiliary UART mode or Persistent Auxiliary UART mode. Switching to AUX UART mode when MP LAN access is disabled requires a push-button reset of the iLO 3 Physical Presence button to return to iLO 3 mode. Persistent Auxiliary UART mode is same as Auxiliary UART mode, but the serial port will not revert iLO3 MP mode after AC power loss. If baud rate settings are not consistent between the serial port and the attached serial device, communication issues occur.</td>
</tr>
<tr>
<td>iLO Bit Rate in Bits per Second</td>
<td>Enables you to set the iLO 3 baud rate. Input and output data rates are the same. The iLO 3 default baud rate is 9600 bps, 8 bits, 1 stop, no parity.</td>
</tr>
<tr>
<td>Flow Control</td>
<td>Enables you to set the iLO 3 flow control. Flow control can be through hardware or software. Hardware uses RTS/CTS. Software uses Xon or Xoff.</td>
</tr>
</tbody>
</table>

Table 27: Serial description

Table Continued
### Login Options

The Login Option tab enables you to modify the security options of iLO 3. To use this feature, you must have the Configure iLO Settings user right.

![Login Options](image-url)

**Figure 34: Login Options**

<table>
<thead>
<tr>
<th>Table 28: Login Options description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Item</strong></td>
</tr>
<tr>
<td>Login Timeout in Minutes</td>
</tr>
<tr>
<td>Password Faults Allowed</td>
</tr>
<tr>
<td>Security Override Mode</td>
</tr>
</tbody>
</table>

*Table Continued*
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle Connection Timeout (minutes)</td>
<td>This setting specifies how long a user can be inactive, in minutes, before the iLO web interface and Integrated Remote Console session end automatically. The following settings are valid: 15, 30, 60, or 120 minutes, or Infinite. The default value is 15 minutes. Inactive users are not logged out when this option is set to Infinite. Failure to log out of iLO by either browsing to a different site or closing the browser also results in an idle connection. The iLO firmware supports a finite number of iLO connections. Misuse of the Infinite timeout option might make iLO inaccessible to other users. Idle connections are recycled after they time out. This setting applies to local and directory users. Directory server timeouts might preempt the iLO setting. While the Remote Serial Console or the Virtual Media applet is connected, the idle connection timeout is not applicable. Changes to the setting might not take effect immediately in current user sessions, but will be enforced immediately in all new sessions.</td>
</tr>
</tbody>
</table>

Submit | Submits the information. |

Clear | Cancels the action. |

Relevant iLO MP TUI command: `SO`

**Login Security Banner**

The Login Security Banner tab enables you to configure the security banner displayed on the iLO login page. To use this feature, you must have the Configure iLO Settings user right.

![Login Security Banner](image)

**Figure 35: Login Security Banner**
### Table 29: Login Security Banner description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Security Banner</td>
<td>To enable or disable the security banner displayed on the iLO login page. Login Security Banner is disabled by default.</td>
</tr>
<tr>
<td>Security Message</td>
<td>To customize the security message, enter a custom message in the Security Message text box. The byte counter above the text box indicates the remaining number of bytes allowed for the message. The maximum is 1,500 bytes.</td>
</tr>
<tr>
<td>Submit</td>
<td>Submits the information</td>
</tr>
<tr>
<td>Use Default Message</td>
<td>To restore the security message to the default text that iLO uses.</td>
</tr>
</tbody>
</table>

**Figure 36: iLO login page with default Security Banner**

**Encryption**

The Encryption tab enables you to enable or disable enhanced network security mode.
Table 30: Encryption description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Cipher</td>
<td>Shows the cipher that has been negotiated and is being used by the current web GUI session.</td>
</tr>
<tr>
<td>Enforce AES/3DES encryption</td>
<td>When this option is enabled, iLO will try to negotiate the strongest encryption algorithms and will not use any weak encryption algorithms for Web GUI and SSH connections. By default, it is disabled. iLO prefers AES256, AES128 and 3DES algorithms for encryption in the same order as specified.</td>
</tr>
<tr>
<td>Submit</td>
<td>Submits the information.</td>
</tr>
<tr>
<td>Cancel</td>
<td>Cancels the action.</td>
</tr>
</tbody>
</table>

Relevant iLO MP TUI command: so

Certificate Settings

The Certificate Settings page enables you to access the following tabs:

- SSL Certificate
- Import Certificate
- Generate Certificate

SSL Certificate

The SSL Certificate tab displays the details of the SSL certificate that is currently being used by iLO for web GUI connections.
The iLO MP auto generates an SSL Certificate when it is first powered on at initial installation. It is expected that you will generate or import a new certificate with valid information when you log in. The certificate status indicates if the certificate has been generated or imported previously.

To import a certificate with user defined parameters, signed by trusted Certificate Authority (CA), visit Import Certificate tab. To generate a new iLO self-signed certificate with user defined parameters, visit Generate Certificate tab.

**Import Certificate**

The Import Certificate tab enables you to generate a Certificate Signing Request (CSR) and to import a certificate signed by a trusted Certificate Authority (CA) into iLO for a secure SSL connection for web GUI interface of iLO3.
Table 31: Import Certificate description

<table>
<thead>
<tr>
<th>Column Head</th>
<th>Column Head</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generation of CSR</td>
<td>The CSR status indicates if a Certificate Signing Request (CSR) has been generated.</td>
</tr>
<tr>
<td></td>
<td>To generate a new CSR, fill in the fields shown and select Generate CSR. This operation might take anywhere from 1 to 10 minutes. Please wait for the operation to complete and the page will refresh automatically.</td>
</tr>
<tr>
<td></td>
<td>The generated CSR will be in base-64 encoded PKCS #10 format. Select Display CSR to view or copy CSR.</td>
</tr>
<tr>
<td></td>
<td>The CSR can be sent to a Certificate Authority (CA). The CA will process the request and provide a signed certificate that can be imported into iLO.</td>
</tr>
<tr>
<td>Import a Certificate</td>
<td>The iLO security features can be enhanced by importing a trusted certificate.</td>
</tr>
<tr>
<td></td>
<td>Use the procedure mentioned above to generate a CSR and get a signed Certificate from a trusted Certificate Authority.</td>
</tr>
<tr>
<td></td>
<td>To import this certificate into iLO, click on Import Certificate button. Paste the certificate contents into the Window that pops up and click on Import button.</td>
</tr>
<tr>
<td></td>
<td>You must restart iLO after importing a certificate. When iLO comes back, it will start using the imported certificate for all SSL connections.</td>
</tr>
</tbody>
</table>

**NOTE:**
- Certificate contents to be imported has to be in Base64-encoded (.pem) format. iLO supports certificates that are up to 3KB in size.
- A certificate works only with the keys generated with its corresponding Certificate Signing Request (CSR). If another CSR is generated before the certificate that corresponds to the previous CSR is imported, the certificate Import might fail. In that case, a new certificate that corresponds to the new CSR must be obtained and imported into iLO.
Generate Certificate

The Generate Certificate tab enables you to generate a new SSL Certificate with the parameters defined by you.

Figure 41: Generate SSL Certificate

To generate a new certificate, fill in the fields shown and select Generate Certificate. You must restart the iLO MP after you generate a new certificate.

This certificate will be valid for 2 years. The system alerts you when the certificate is about to expire or it has already expired. You will need to generate a new certificate before you can continue.

Directory Settings>Current LDAP Parameters

The Current LDAP Parameters page enables you to edit the directory parameters. To use this feature, you must have the Configure iLO Settings user right.
Figure 42: Current LDAP Parameters
Table 32: Current LDAP Parameters description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Directory Authentication | Choosing enable or disable, activates or deactivates directory support on iLO 3:  
  Enable with Extended Schema  
  Selects directory authentication and authorization using directory objects created with HPE schema. Select this option if the directory server has been extended with the HPE schema.  
  Enable with Default Schema  
  Selects directory authentication and authorization using user accounts in the directory which has not been extended with the HPE schema. User accounts and group memberships are used to authenticate and authorize users. In the Administration>User Administration>Group Accounts page, configure one or more directory groups by entering the Group Distinguished Name of the group and the rights granted to users who are members of that group. You must configure data in the Group Administration page after you select this.  
  Disable  
  Deactivates directory support on this iLO 3. |
| Local User Accounts    | Includes or excludes access to local iLO 3 user accounts. Locally-stored user accounts can be active while LDAP directory support is enabled. If local user accounts are enabled, you may log in to the iLO 3 using locally-stored user credentials. If they are disabled, access is limited to valid directory credentials only. |
| Directory Server IP Address | Displays the IP address or hostname of the directory server. |
| Directory Server LDAP Port | Displays the port number for the secure LDAP service on the server. The default value for this port is 636. It can be configured to a value in the range 2000-2400. |
| iLO Distinguished Name | Displays the Distinguished Name of iLO 3, specifies where this iLO 3 instance is listed in the directory tree.  
  Example: cn=MP Server,ou=Management Devices,o=hp |
User Search Contexts

User search contexts locate an object in the tree structure of the directory server and are applied to the login name entered to access the iLO MP.

All objects listed in the directory can be identified using the unique distinguished name. However, distinguished names can be long, or users might not know the distinguished usernames, or they may have accounts in different directory contexts. Search contexts enable the user to specify common directory contexts, so that users do not have to enter the full distinguished name at login.

The iLO 3 attempts to authenticate a user in the directory first by the login name entered, and then by applying user search contexts to that login name until successful. For example:

Example 1: Instead of logging in as `cn=user,ou=engineering,o=hp`, a search context of `ou=engineering,o=hp` allows the user to login as `user`.

Example 2: (This format can be used only when extended schema is selected and Active Directory is used as a directory server). Microsoft Active Directory has an alternate user credential format. A user may login as: `user@domain.hp.com`, in which case a search context of `@domain.hp.com` allows the user to login as `user`.

Network Settings

The Network Settings page enables you to access the following tabs:

- Standard
- Domain Name Server

**IMPORTANT:**

If you are connected through a network and you make any changes to DHCP status, IP address, subnet mask, or gateway IP address, iLO 3 automatically resets after you confirm the change. The automatic reset occurs only after a warning appears before you save the changes. If you enter `-nc`, no warning appears and iLO 3 reboots.

If you are connected through a serial console and you make any changes to DHCP status, IP address, subnet mask, or gateway IP address, iLO 3 alerts you to manually reset iLO 3. A warning about dropped network connections is sent prior to committing the change. The warning does not appear if you enter `-nc`.

If a firmware upgrade is in progress, the commitment phase to the `LC` command fails and indicates that an upgrade or reset is in progress, and changes to the `LC` parameters are not made.

Network Settings>Standard

The Standard tab enables you to configure the network settings and LAN configuration. To configure the network settings, you must have the Configure iLO Settings user right.
NOTE:
If valid changes are made to the DHCP Status, IP Address, Subnet Mask, or Gateway Address, and the changes are submitted, a reset of iLO 3 is required for the changes to take effect.

![Network Settings](image)

**Figure 43: Standard network settings**

**Table 33: Standard network settings description**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Displays the 12-digit (hexadecimal) MAC address.</td>
</tr>
<tr>
<td>DHCP Status</td>
<td>To enable iLO 3 to obtain an IP address, Subnet Mask, and Gateway Address from a DHCP server, select <strong>Enable</strong>. Changes to those three network settings are not allowed while the DHCP Status is enabled. To manually assign those three network settings to iLO 3, select <strong>Disable</strong>. If the DHCP status is changed and submitted, a reset of iLO 3 is required for the changes to take effect.</td>
</tr>
<tr>
<td>iLO 3 MP Host Name</td>
<td>Displays the host name set at the iLO 3 TUI prompt. Typically, the DNS name for the LAN IP is entered. This field can be programmed to any useful name or phrase.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the iLO 3 MP IP address. If DHCP is being used, the IP address is automatically supplied. If not, enter a static IP address here. If the IP address is changed to a valid address and submitted, a reset of iLO 3 is required for the changes to take effect.</td>
</tr>
<tr>
<td><strong>Item</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Displays the subnet mask for the iLO 3 IP network. If DHCP is being used, the subnet mask is automatically supplied. If not, enter the subnet mask for the network. If the subnet mask is changed to a valid mask and submitted, a reset of iLO 3 is required for the changes to take effect.</td>
</tr>
<tr>
<td>Gateway Address</td>
<td>Displays the IP address of the network gateway. If DHCP is being used, the gateway IP address is automatically supplied. If not, enter the network gateway address. If the gateway address is changed to a valid address and submitted, a reset of iLO 3 is required for the changes to take effect.</td>
</tr>
<tr>
<td>Link State</td>
<td>Select Auto Negotiate, 10BaseT, or 100BaseT.</td>
</tr>
</tbody>
</table>

**IMPORTANT:**

On Integrity rx2800 i2/i4/i6 systems, the link state 1000BaseT option (or Duplex Option) is not currently supported.

Integrity rx2800 i2/i4/i6 systems can run at 1000BaseT, but only if the switch it connects to supports auto negotiate to 1000BaseT and the rx2800 i2/i4/i6 is similarly set to auto negotiate. If you want to set a specific LAN speed (10BaseT or 100BaseT) those are the only options that iLO 3 currently supports.

**Submit**

Submits the information.

**Clear**

Cancels the action.

Relevant iLO MP TUI command: `LC`

**Domain Name Server**

The Domain Name Server (DNS) tab enables you to configure the DNS server settings, domain name, and up to two DNS servers manually or automatically through DHCP. It further enables a DDNS update through the primary DNS server as long as it is authoritative for the zone. It is only meaningful when used with DHCP enabled. To use this feature, you must have the Configure iLO Settings user right.

You can only configure the DNS server if DHCP is enabled.
Figure 44: Domain Name Server

Table 34: DNS description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use DHCP supplied domain name</td>
<td>To use the DHCP server-supplied domain name, select Yes. Or enter a domain name in the Domain Name field.</td>
</tr>
<tr>
<td>Domain name</td>
<td>Enter the name of the domain where the system resides. This can be entered if DHCP is not being used (No was selected in the previous option), but DNS is wanted. This represents the DNS suffix of the subsystem. For example, hp.com in ilo.hp.com.</td>
</tr>
<tr>
<td>Use DHCP supplied DNS servers</td>
<td>To use the DHCP server-supplied DNS server list, select Yes. Or, enter one in the Primary / Secondary DNS server IP fields.</td>
</tr>
<tr>
<td>Primary / Secondary DNS Server IP</td>
<td>The IP addresses of the DNS servers. If supplied by the DHCP server, these boxes are filled automatically. Otherwise, enter the IP addresses manually.</td>
</tr>
<tr>
<td>Register with Dynamic DNS Server</td>
<td>To register the iLO MP Host Name with a DDNS server, select Yes.</td>
</tr>
<tr>
<td>Submit</td>
<td>Submits the DNS information.</td>
</tr>
<tr>
<td>Clear</td>
<td>Cancels the action.</td>
</tr>
</tbody>
</table>

Relevant iLO MP TUI command: DNS
Onboard Administrator

The BladeSystem Onboard Administrator page provides a view of the enclosure status. The Onboard Administrator page only displays for server blades.

Table 35: Onboard Administrator description

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OA IP Address</td>
<td>Displays the IP address of the OA.</td>
</tr>
<tr>
<td><strong>IMPORTANT:</strong></td>
<td></td>
</tr>
<tr>
<td>Integrity iLO 3 must have a reachable IP address as the default gateway address. Since the OA is reachable, Hewlett Packard Enterprise recommends using the OA IP address as the gateway address for Integrity iLO 3. If you use the Enclosure IP mode, this solution works during a failover. In the Enclosure IP mode, a static IP address is assigned to the active OA, and during a failover, the same IP address follows the active OA. If the OA IP address is assigned using DHCP, the solution does not work. In such instances, Hewlett Packard Enterprise recommends manually changing the iLO 3 gateway address.</td>
<td></td>
</tr>
<tr>
<td>OA MAC Address</td>
<td>Displays the MAC address of the OA.</td>
</tr>
<tr>
<td>Active OA Sign In Page</td>
<td>Click this button to launch the OA Sign In page.</td>
</tr>
</tbody>
</table>

Table Continued
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rack Name</td>
<td>Used to logically group together enclosures in a rack. The rack name is shared with the other enclosures in the rack.</td>
</tr>
<tr>
<td>Rack UID</td>
<td>The rack universal unique identifier.</td>
</tr>
<tr>
<td>Bay Number</td>
<td>The bay number is used to locate and identify the monarch blade.</td>
</tr>
<tr>
<td>Bays Consumed (full height)</td>
<td>Lists bay numbers in the enclosure populated by blades that are part of this server or partition.</td>
</tr>
<tr>
<td>Enclosure Name</td>
<td>Used to logically group together the server blades installed in the same enclosure. The enclosure name is shared with the other servers in the enclosure.</td>
</tr>
<tr>
<td>Enclosure Health</td>
<td>Displays the health of the enclosure.</td>
</tr>
<tr>
<td></td>
<td><strong>OK</strong></td>
</tr>
<tr>
<td></td>
<td>Normal operation, any issues have been acknowledged.</td>
</tr>
<tr>
<td></td>
<td><strong>Degraded</strong></td>
</tr>
<tr>
<td></td>
<td>Typically loss of redundancy or partial failure of a component.</td>
</tr>
<tr>
<td></td>
<td><strong>Critical</strong></td>
</tr>
<tr>
<td></td>
<td>Failure with loss or imminent loss of system function.</td>
</tr>
<tr>
<td>Locator UID LED</td>
<td>Enables you to turn the enclosure Locator UID LED on or off.</td>
</tr>
</tbody>
</table>

Relevant iLO MP TUI commands: `BLADE, LOC`

Before setting up the HPE BladeSystem OA, Hewlett Packard Enterprise recommends that you read the *HPE BladeSystem Onboard Administrator User Guide* on the Hewlett Packard Enterprise website at [HPE BladeSystem c-Class Onboard Administrator](https://www.hpe.com). Reading this guide ensures that you obtain an overall understanding of the HPE BladeSystem OA and that you properly complete the initial setup to facilitate proper functioning of the OA.

**Help**

The iLO 3 has a robust help system.

To access iLO 3 help, click the ? at the top right corner of each page.

Select any of the topics listed in the left navigation bar to access that particular help screen.
You can install and configure iLO 3 directory services to leverage the benefits of a single point of administration for iLO 3 user accounts.

This chapter provides information on how to install and configure iLO 3 directory services.

Directory services

The following are benefits of directory integration:

Scalability
Leverage the directory to support thousands of users on thousands of iLO 3s.

Security
Robust user password policies are inherited from the directory. User password complexity, rotation frequency, and expiration are policy examples.

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. When you change a single role, the change applies to all users and the iLO 3 devices associated with that role.

Single point of administration
You can use native administrative tools, like Microsoft Management Console (MMC) and ConsoleOne, to administer the iLO 3 users.

Immediacy
A single change in the directory rolls out immediately to associated iLO 3s, eliminating the need to script this process.

Reuse of user name 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 iLO 3.

Flexibility
You can create a single role for a single user on a single iLO 3; you can create a single role for multiple users on multiple iLO 3s; or you can use a combination of roles to best fit your enterprise.

Compatibility
The iLO 3 directory integration applies to the iLO 3 products and supports the popular directories Active Directory and eDirectory.

Standards
The iLO 3 directory support builds on the LDAP 2.0 standard for secure directory access.

Features supported by directory integration

The iLO 3 directory services functionality enables you to do the following:

• 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 3 and iLO 3 users.

To install directory services for the iLO 3, a schema administrator must extend the directory schema.
The local user database is retained. You can choose not to use directories, to use a combination of directories and local accounts, or to use directories exclusively for authentication.

**Directory services installation prerequisites**

Before installing directory services, you must configure LDAP.

**Installing directory services**

To successfully enable directory-enabled management on any iLO 3:

**Procedure**

1. **Plan.**
   - Review the following sections:
     - Directory services on page 135
     - Directory services schema (LDAP) on page 170
     - Directory-enabled remote management on page 164

2. **Install.**
   - a. Download the HPE Lights-Out Directory Package containing the schema installer, the management snap-in installer, and the migrations utilities from the HPE website ([http://www.hpe.com/info/ilo](http://www.hpe.com/info/ilo)).
   - b. Run the schema installer once to extend the schema. See Schema installer on page 137.
   - c. Run the management snap-in installer and install the appropriate snap-in for your directory service on one or more management workstations. See Management snap-in installer on page 139.

3. **Update.**
   - a. With the directory-enabled firmware, flash the ROM on iLO 3.
   - b. From the Directory Settings in the iLO 3 user interface, set directory server settings and the distinguished name of the iLO 3 objects.

4. **Manage.**
   - a. Create a management device object and a role object using the snap-in. See Directory services objects on 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 about managing directory service, see Directory-enabled remote management on page 164. Examples are available in: Directory services for Active Directory on page 140 and Directory services for eDirectory on page 152.

**Schema documentation**

To assist with the planning and approval process, HPE documents the changes made to the schema during the schema setup process. To review the changes made to your existing schema, see Directory services schema (LDAP) on page 170.

**Directory services support**

Integrity iLO 3 supports the following directory services:

- Microsoft Active Directory
- Windows Server 2008 Active Directory and above
- Novell eDirectory 8.6.2
- Novell eDirectory 8.7
- HP-UX Directory Server
The iLO 3 software is designed to run within the Microsoft Active Directory Users and Computers, and Novell ConsoleOne management tools. This enables you to manage user accounts on Microsoft Active Directory or Novell eDirectory. There is no distinction made between eDirectory running on NetWare, Linux, or Windows operating systems. To spawn an eDirectory schema extension, you must have Java 1.4.2 or later for SSL authentication.

**eDirectory installation prerequisites**

Directory services for iLO 3 uses LDAP over SSL to communicate with the directory servers. Integrity iLO 3 software is designed to install in eDirectory Version 8.6.1 (and later) tree. Hewlett Packard Enterprise does not recommend installing this product if you have eDirectory servers with a version earlier than eDirectory 8.6.1. Before installing snap-ins and schema extensions for eDirectory, read and have available the following technical information documents (available at Novell Support at: [http://support.novell.com](http://support.novell.com)).

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

To install directory services for iLO 3, an administrator must extend the eDirectory schema.

**Required schema software**

The iLO 3 requires specific software to extend the schema and provide snap-ins to manage the iLO 3 network. An HP Smart Component that contains the schema installer and the management snap-in installer is available for download from the Hewlett Packard Enterprise website at [http://www.hpe.com/info/ilo](http://www.hpe.com/info/ilo).

The two components you need for Integrity iLO 3 directory integration are the Schema Extender Utility and the Snap-in Installer.

**Schema installer**

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

The schema installer includes three important screens:

- Schema Preview
- Setup
- Results

**Schema preview**

The Schema Preview screen enables you to view proposed extensions to the schema. This application reads the selected schema files, parses the XML, and displays the schema on the screen in a tree view listing all of the details of the attributes and classes that are installed.
Schema setup

To enter information before extending the schema, use the Setup screen.

The Directory Server section of the Setup screen enables you to select whether to use Active Directory or eDirectory, and to set the computer name and the port to be used for LDAP communications.
IMPORTANT:
To extend the schema on Active Directory you must be an authenticated schema administrator, the schema must not be write protected, and the directory must be the flexible single master operation (FSMO) role owner in the tree. The installer attempts to make the target directory server the FSMO schema master.

To obtain write access to the schema in Windows 2000, you must change the registry safety interlock. If you select the Active Directory option, the schema extender attempts to change the registry. The schema extender can only change the registry if the administrator who is extending the schema has the appropriate rights. 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, which 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 continues using an unencrypted (clear text) connection.

Results
The Results screen displays the results of the installation, including whether the schema can be extended and what attributes were changed.

![Figure 48: Schema Results screen](image)

Management snap-in installer
The management snap-in installer installs the snap-ins required to manage iLO 3 objects in a Microsoft Active Directory Users and Computers directory or in a Novell ConsoleOne directory.

To create an iLO 3 directory using iLO 3 snap-ins:
1. Create and manage iLO 3 objects and role objects.
2. Make the associations between iLO 3 objects and role objects.
Directory services for Active Directory


The following sections provide installation prerequisites, preparation, and a working example of directory services for Active Directory.

Active Directory installation prerequisites

The following are prerequisites for installing Active Directory:

- The Active Directory must have a digital certificate installed to enable iLO 3 to connect securely over the network.
- The Active Directory must have the schema extended to describe iLO 3 object classes and properties.

Directory services for iLO 3 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:

**IMPORTANT:**

To install directory services for iLO 3, an Active Directory schema administrator must extend the schema.

- Microsoft Knowledge Base articles:
  - 216999 “How to Install the Remote Server Administration Tools in Windows”
  - 314978 “How to Use Adminpak.msi to Install a Specific Server Administration Tool in Windows 2000”
  - 247078 “How to Enable SSL Communication over LDAP for Windows 2000 Domain Controllers”
  - 321051 “How to Enable LDAP over SSL with a Third-Party Certification Authority”
  - 299687 MS01-036 “Function Exposed by Using LDAP over SSL Could Enable Passwords to Be Changed”

Integrity iLO 3 requires a secure connection to communicate with the directory service. This secure connection requires the installation of the Microsoft CA. For more information, see the following Microsoft technical references:

- Microsoft Knowledge Base Article 321051 “How to Enable LDAP over SSL with a Third-Party Certification Authority”

Preparing directory services for Active Directory

To set up directory services for use with iLO 3:

**Procedure**

1. Install Active Directory. For more information, see the resource kit, Installing Active Directory in the Microsoft Windows 2000 Server.
2. Install the Microsoft Admin Pack (the `ADMINPAK.MSI` file, which is located in the i386 subdirectory of the Windows 2000 Server or Advanced Server CD). For more information, see 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 you have appropriate rights. You can also do this by setting `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\Schema Update Allowed` in the registry to a nonzero value (see the “Order of Processing When Extending the Schema” section of the Installation of Schema Extensions in the Windows 2000 Server Resource Kit), or by doing the following:

⚠️ **CAUTION:**

Incorrectly editing the registry can severely damage your system. Hewlett Packard Enterprise recommends creating a backup of any valued data on the computer before making changes to the registry.

**NOTE:**

This step is not necessary if you are using Windows Server 2003 or later.

a. Start the MMC.
b. In MMC, install the Active Directory schema snap-in.
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 may need to be expanded for the checkbox to be available.

4. Create a certificate or install Certificate Services. This step is necessary because iLO 3 uses SSL to communicate with Active Directory.

5. To specify that a certificate be issued to the server running Active Directory, do the following:
   a. Launch MMC on the server and add the default domain policy snap-in (Group policy and 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.


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 runs anywhere MSI is supported (Windows XP, Windows 2000, Windows 98). However, some parts of the schema extension application require the .NET Framework, which you can download from the Microsoft website at: [http://www.microsoft.com](http://www.microsoft.com)

### Installing and initializing snap-ins for Active Directory

To install the snap-ins and configure the directory service:

**Procedure**

1. To install the snap-ins, run the snap-in installation application.
2. Configure the directory service with the appropriate objects and relationships for iLO 3 management:
a. Use the management snap-ins from HP to create iLO 3 policy, admin, and user role objects. 
b. Use the management snap-ins from HP to build associations between the iLO 3 object, the policy object, and the role object.
c. Point the iLO 3 object to the admin and user role objects (admin and user roles automatically point back to the iLO 3 object).

For more information about iLO 3 objects, see Directory services objects on page 145.

At a minimum, create:

• One role object that contains one or more users and one or more iLO 3 objects.
• One iLO 3 object corresponding to each iLO 3 using the directory.

Example: creating and configuring directory objects for use with iLO 3 in Active Directory

The following example shows how to set up roles and HP devices in an enterprise directory with the domain mpiso.com, which consists of two organizational units: Roles and MPs.

NOTE:
Roles, such as hpqTargets and so on, are for extended schema LDAP only. They are not used in schema-free LDAP.

Assume that a company has an enterprise directory including the domain mpiso.com, arranged as shown in Figure 49: Directory example on page 142.

Figure 49: Directory example
Procedure

1. Create an organizational unit to contain the iLO 3 devices managed by the domain. In this example, two organizational units are created, Roles and MPs.

2. Use the Active Directory Users and Computers snap-ins provided by HP to create iLO 3 objects for several iLO 3 devices in the MP organizational unit.
   a. In the mpiso.com domain, right-click the MPs organizational unit and select **NewHPObject**.
   b. In the Create New HP Management Object dialog box, select **Device** for the type.

   ![Create new HP Management Object dialog box](image)

   **Figure 50: Create new HP Management Object dialog box**

   c. In the Name field of the dialog box, enter an appropriate name. In this example, the DNS host name of the iLO 3 device, `lpmp`, is used as the name of the iLO 3 object, and the surname is iLO 3.
   d. Enter and confirm a password in the Device LDAP Password and Confirm fields (this is optional).
   e. Click **OK**.

3. Use the HP provided Active Directory Users and Computers snap-ins to create HP role objects in the roles organizational unit.

4. Right-click the **Roles** organizational unit, select **New**, and select **Object**. The Create New HP Management Object dialog box appears.
   a. In the **Type** field, select **Role**.
   b. In the **Name** field, enter an appropriate name. In this example, the role contains users trusted for remote server administration and is named remoteAdmins.
   c. Click **OK**
   d. Repeat the process, creating a role for remote server monitors named remoteMonitors.

5. Use the Active Directory Users and Computers snap-ins provided by HP to assign the roles rights, and associate the roles with users and devices.
   a. In the **Roles** organizational unit in the mpiso.com domain, right-click the **remoteAdmins** role, and select **Properties**.
   b. Select the HP Devices tab and click **Add**.
c. From the Select Users dialog box, select the iLO 3 object created in step 2: (lpmp in folder mpiso.com/MPs).

![Select Users dialog box](image)

**Figure 51: Select Users dialog box**

d. Click OK.
e. To save the list, click **Apply**.
f. To add users to the role, click the Members tab and use the **Add** button and the Select Users dialog box. Devices and users are now associated.

**6.** To set the rights for the role, use the Lights-Out Management tab. All users and groups within a role have rights assigned to the role on all of the iLO 3 devices managed by the role. In this example, the users in the remoteAdmins role are given full access to the iLO 3 functionality. Select the appropriate rights and click **Apply**.

![Lights-Out Management tab](image)

**Figure 52: Lights-Out Management tab**
7. Click OK.
8. Using the same procedure in step 4, edit the properties of the remoteMonitors role, add the lpmp device to the Managed Devices list on the HP Devices tab, and use the Members tab to add users to the remoteMonitors role.
10. Click Apply and OK. Members of the remoteMonitors role are able to authenticate and view the server status.

User rights to any iLO 3 are calculated as the sum of all the rights assigned by all the roles in which the user is a member and the iLO 3 is a managed device. Following the preceding examples, if a user is included in both the remoteAdmins and remoteMonitors roles, he or she has all the rights of those roles, because the remoteAdmins role also has those rights.

To configure iLO 3 and associate it with an iLO 3 object, use settings similar to the following (based on the preceding example) in the iLO 3 Directory Settings text user interface:

```
RIB Object DN = cn=lpmp,ou=MPs,dc=mpiso,dc=com
Directory User Context 1 = cn=Users,dc=mpiso,dc=com
```

For example, user Mel Moore (with the unique ID MooreM, located in the Users organizational unit within the mpiso.com domain, and a member of one of the remoteAdmins or remoteMonitors roles) can be allowed to log in to the iLO 3. To log in, he can enter mpiso\moorem, or moorem@mpiso.com, or Mel Moore, in the Login Name field of the iLO 3 login, and use his Active Directory password in the Password field.

**Directory services objects**

One of the keys to directory-based management is proper virtualization of the managed devices in the directory service. This virtualization enables the administrator to build relationships between a managed device and user or groups already contained within the directory service. The iLO 3 user management requires the following basic objects in the directory service:

- iLO 3
- Role
- User

Each object represents a device, user, or relationship that is required for directory-based management.

**NOTE:**

After you install the snap-ins, restart ConsoleOne and MMC to display the new entries.

After the snap-in is installed, you can create iLO 3 objects and roles in the directory. Using the Users and Computers tool, you can:

- Create iLO 3 objects 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 in Active Directory Users and Computers after you have installed the HP snap-ins.

**Managing HP devices in a role**

To add HP devices to be managed in a role, use the HP Devices tab.

- To browse to a specific HP device and add it to the list of member devices, click Add.
- To browse to a specific HP device and remove it from the list of member devices, click Remove.
Managing users in a role

After user objects are created, use the Members tab to manage the users within the role.

• To add a user, browse to the specific user you want to add, and click Add.
• To remove a user from the list of valid members, highlight an existing user and click Remove.
Figure 54: Members tab

Setting login restrictions

The Role Restrictions tab enables you to set login restrictions for a role. These restrictions include:

- Time Restrictions
- IP Network Address Restrictions
  - IP/Mask
  - IP Range
  - DNS Name
Setting time restrictions

- To manage the hours available for login by members of the role, click the Effective Hours button. The Logon Hours screen appears (Figure 56: Logon Hours screen on page 149).
- To select the times available for login each day of the week in half-hour increments, use the Logon Hours screen. 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.
- Use the default setting to allow access at all times.
Defining client IP address or DNS name access

From the Role Restrictions tab, you can grant or deny access to an IP address, IP address range, or DNS names.

In the By Default list, select whether to grant or deny access from all addresses except for specified IP addresses, IP address ranges, and DNS names.

To restrict an IP address:

Procedure

1. From the Role Restrictions tab, select IP/MASK and click Add. The New IP/Mask Restriction dialog box appears.
2. In the **New IP/Mask Restriction** dialog box, enter the information and click **OK**.

3. To restrict access based on a DNS, select **DNS Name** and click **Add**. The **New DNS Name Restriction** dialog box appears. The DNS Name option enables 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. Enter the information and click **OK**.

5. To save the changes, click **OK**.

To remove any of the entries, highlight the entry in the display list and click **Remove**.

### Setting user or group role rights

After you create a role, you can select rights for that role. You can enable users and group objects to be members of the role, giving each the rights granted by the role.

To manage rights, use the Lights-Out Management tab.
Table 36: Lights-Out Management rights

<table>
<thead>
<tr>
<th>MP Rights</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>Controls whether users can log in to the associated devices and issue Status or Read-only commands (view event logs and console logs, check system status, power status, and so on) but not issue any commands that might alter the state of iLO 3 or the system.</td>
</tr>
<tr>
<td>Remote Console</td>
<td>Enables users to access the system console (the host operating system).</td>
</tr>
<tr>
<td>Virtual Media</td>
<td>Enables users to connect devices through the network such as CD, DVD, and network drives as virtual devices.</td>
</tr>
<tr>
<td>Server Reset and Power</td>
<td>Enables users to issue iLO 3 power operations to remotely power on, power off, or reset the host platform, as well as configure the system power restore policy.</td>
</tr>
<tr>
<td>Administer Local User Accounts</td>
<td>Enables users to administer local iLO 3 user accounts.</td>
</tr>
<tr>
<td>Administer Local Device Settings</td>
<td>Enables users to configure all iLO 3 settings, as well as reboot iLO 3.</td>
</tr>
</tbody>
</table>
Directory services for eDirectory

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

NOTE:
Schema-Free LDAP is not supported with eDirectory.

Installing and initializing snap-ins for eDirectory

For instructions on using the snap-in installation application, see Installing and initializing snap-ins for Active Directory on page 141.

NOTE:
After you install snap-ins, restart ConsoleOne and MMC to show the new entries.

Example: creating and configuring directory objects for use with iLO 3 devices in eDirectory

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

Assume that samplecorp has an enterprise directory arranged according to that in Figure 59: Roles and Devices example on page 152.

Figure 59: Roles and Devices example

Begin by creating organizational units in each region to contain iLO 3 devices and roles specific to that region. In this example, two organizational units are created, roles and HP devices, in each organizational unit (region1 and region2).
Creating objects
To create iLO 3 objects:

Procedure
1. Use the ConsoleOne snap-ins provided by Hewlett Packard Enterprise to create iLO 3 objects in the HP devices organizational unit for several iLO 3 devices.
2. From in the region1 organizational unit, right-click the HP devices organizational unit. Select New, and select Object.
   a. Select hpqTarget from the list of classes, and click OK.
   b. Enter an appropriate name and surname in the New hpqTarget dialog box. In this example, the DNS host name of the iLO 3 device, rib-email-server, is used as the name of the iLO 3 object, and the surname is RILOEII (iLO 3). Click OK. The Select Object Subtype dialog box appears.

   ![Select Object Subtype dialog box](image)

   c. Select Lights-Out Management Device from the list, and click OK.
   d. Repeat the process for several more iLO 3 devices with the 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.

Creating roles
To create roles:

Procedure
1. Use the ConsoleOne snap-ins provided by HP to create HP role objects in the roles organizational units.
a. From the region2 organizational unit, right-click the **roles** organizational unit. Select **New**, and select **Object**.
b. Select **hpqRole** from the list of classes, and click **OK**.
c. Enter an appropriate name in the New hpqRole dialog box. In this example, the role contains users trusted for remote server administration and is named remoteAdmins.
d. Click **OK**. The Select Object Subtype dialog box appears.
e. Select **Lights-Out Management Devices** from the list, and click **OK**.

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

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

   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 subtab of the HP Management tab, and click **Add**.
   
   c. Using the Select Objects dialog box, browse to the HP devices organizational unit in the region1 organizational unit. Select the three iLO 3 objects created in step 2. Click **OK** and click **Apply**.
   
   d. Add users to the role. Click the Members tab, and add users using **Add** and the Select Objects dialog box. The devices and users are now associated.
   
   e. To set the rights for the role, use the Lights-Out Management Device Rights subtab of the HP Management tab.

4. Using the same procedure as in step 3, edit the properties of the remoteMonitors role:

   a. From the region2 organizational unit, right-click the **roles** organizational unit. Select **New**, and select **Object**.
   
   b. Select **hpqRole** from the list of classes, and click **OK**.
   
   c. Enter an appropriate name in the New hpqRole dialog box. In this example, the role contains users trusted for remote server administration and is named remoteAdmins.
   
   d. Click **OK**. The Select Object Subtype dialog box appears.
   
   e. Select **Lights-Out Management Devices** from the list, and click **OK**.

   f. To close the property sheet, click **Close**.

Figure 61: Setting role rights

All users within a role will have rights assigned to the role on all he iLO 3 devices managed by the role. In this example, users in the remoteAdmins role are given full access to iLO 3 functionality. Select the boxes next to each user right, and click **Apply**.

f. To close the property sheet, click **Close**.

4. Using the same procedure as in step 3, edit the properties of the remoteMonitors role:
a. Add the three iLO 3 devices within HP devices under region1 to the Managed Devices list on the Role Managed Devices subtab of the HP Management tab.

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

c. Using the Lights-Out Management Device Rights subtab of the HP Management tab, click the Login checkbox, and click Apply and Close. Members of the remoteMonitors role are now able to authenticate and view the server status.

User rights to any iLO 3 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 iLO 3 device is a managed device. Using the preceding examples, if a user is in both the remoteAdmins and remoteMonitors roles, he or she has all rights, because the remoteAdmins role has those rights.

To configure an iLO 3 device from the previous example and associate it with an iLO 3 object, use settings similar to the following on the iLO 3 directory settings TUI.

NOTE:
In LDAP Distinguished Names, use commas, not periods, 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, and is a member of one of the remoteAdmins or remoteMonitors roles) is allowed to log in to iLO 3. To gain access, he enters csmith (case insensitive) in the Login Name field of the iLO 3 login, and uses his eDirectory password in the Password field.

**Directory services objects for eDirectory**

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

**Adding role managed devices**

Use the Role Managed Devices subtab under the HP Management tab to add HP devices to be managed within a role.
To browse to the specific HP device and add it as a managed device, click Add.

Adding members

After you create user objects, use the Members tab to manage users within a role.
To browse to the specific user you want to add, click Add.

To remove a user from the list of valid members, highlight the user name and click Delete.

Setting role restrictions

The Role Restrictions subtab enables you to set login restrictions for a role.

![Role Restrictions subtab (eDirectory)](image)

Figure 64: Role Restrictions subtab (eDirectory)

These restrictions include the following:

- Time Restrictions
- IP Network Address Restrictions
  - IP/Mask
  - IP Range
- DNS Name

Setting time restrictions

You can manage the hours available for login by members of a role, using the time grid that appears in the Role Restrictions subtab (Figure 63). You can select the times available for login for each day of the week in half-hour increments. You can change a single square by clicking it or 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.

Defining client IP address or DNS name access

You can grant or deny access to an IP address, IP address range, or DNS names.

Using the By Default list, select whether to allow or deny access from all addresses except the specified IP addresses, IP address ranges, and DNS names.
Procedure

1. To restrict an IP address, select **IP/MASK** in the Role Restrictions subtab and click **Add**. The **Add New Restriction** dialog box for the IP/_mask option appears.

2. In the **Add New Restriction** dialog box (Figure 65: Add New Restriction dialog box on page 158), enter the information, and click **OK**.

![Figure 65: Add New Restriction dialog box](image)

3. In the Role Restrictions subtab, select **DNS Name** and click **Add**. The DNS Name option enables 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`. The **New DNS Name Restriction** dialog box appears.

4. Enter the information and click **OK**.

5. To save the changes, click **Apply**.

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

**Setting Lights-Out management device rights**

After you create a role, you can select rights for the role and make users and group objects members of the role, which gives users or groups of users the rights granted by that role. To manage rights, use the Lights-Out Management Device Rights subtab of the HP Management tab.
Table 37: Management Device Rights

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>This option controls whether users can log in to the associated devices and issue status or read-only commands (view event logs and console logs, check system status, power status, and so on) but not issue any commands that might alter the state of iLO 3 or the system.</td>
</tr>
<tr>
<td>Remote Console</td>
<td>This option enables users to access the system console (the host operating system).</td>
</tr>
<tr>
<td>Virtual Media</td>
<td>This option enables users to connect devices through the network such as CD, DVD, and network drives as virtual devices.</td>
</tr>
<tr>
<td>Server Reset and Power</td>
<td>This option enables users to issue iLO 3 power operations to remotely power on, power off, or reset the host platform, as well as configure the system power restore policy.</td>
</tr>
<tr>
<td>Administer Local User Accounts</td>
<td>This option enables users to administer local iLO 3 user accounts.</td>
</tr>
<tr>
<td>Administer Local Device Settings</td>
<td>This option enables users to configure all iLO 3 settings, as well as reboot iLO 3.</td>
</tr>
</tbody>
</table>
Installing snap-Ins and extending schema for eDirectory on a Linux platform

This section describes a method that does not require a Windows client to install snap-ins and extend schema for eDirectory on a Linux platform.

Schema extension is the addition of new classes to existing classes. You can use these classes to create objects to support a specific utility. New classes are added, such as `hpqTarget`, `hpqPolicy` and `hpqRole`. HP has created objects using these classes to support iLO 3 devices (created using the `hpqTarget` class), and iLO 3 administrators and monitors (created using the `hpqRole` class). These objects support the Login Authentication utility to the iLO 3 device and enable iLO 3 users to run commands based on the assigned roles.

Installing the Java Runtime Environment

As a prerequisite for extending schema, you must have Java Runtime Environment (JRE) 1.4.2 installed. To ensure you have the correct version of JRE installed on your system:

Procedure

1. To determine the Java version, run the following command:
   
   `# java -version`

2. The Java version installed on your system is displayed.

3. If Java is not installed on your system, run the following command:
   
   `# rpm -iv j2re-1_4_2_04-linux-i586.rpm`
   
   **NOTE:**
   
   You can download this `rpm` file from the Java website.

4. Run the following command if:
   
   a. Java is installed and the version is older than 1.4.2.
   b. You want to upgrade the Java version and uninstall an older version.

   `# rpm -Uv j2re-1_4_2_04-linux-i586.rpm`

5. Add the entry `/usr/java/j2re1.4.2_04/bin` to the `.bash_profile` file.

Installing snap-Ins

Create the HP directory under the `/usr/ConsoleOne/snapins/` directory, and copy the two `.jar` snap-in files, `hpqLOMv100.jar` and `hpqMgmtCore.jar`, to the HP directory. When the `hpdsse.sh` file is issued, the HP directory is automatically created and the two `.jar` files are copied to it.

**NOTE:**


Select Software and Drivers, and the operating system for the schema extension you want to install.

Extending schema

To obtain the `hpdsse.sh` file:
Procedure

1. Download the tar file to the Linux system where eDirectory is installed.
2. Extract the tar file to obtain the hpdsse.sh file by running the following command:
   ```
   # tar -xvf Schema.tar
   ```
3. Run this file by issuing the following command:
   ```
   # ./hpdsse.sh
   ```
4. This command displays instructions. As indicated in the instructions to extend the schema, provide the server name, admin DN, and admin password as command line arguments.
5. To see the results, view the schema.log file, (created after the schema extension is complete).
6. The log file lists the created classes and attributes. In addition, it shows the result as Succeeded. If the objects already exist, the message Already Exists appears in the log file.

The Already Exists message appears only when you try to run the same .sh file after the schema extension is complete.

The SSL port (636) is used during the schema extension. You can verify this by running the `netstat -nt | grep :636` command while the hpdsse.sh file is running.

Verifying snap-in installation and schema extension

To verify the installation of snap-ins and schema extension:

Procedure

1. Run ConsoleOne and log on to the tree.
2. Verify the new classes by opening the Schema Manager from the Tools list.
3. All the classes related to the HP directory services must be present in the classes list. The classes are hpqRole, hpqTarget, hpqPolicy, and hpqLOMv100.

Using the LDAP command to configure directory settings

Use the LDAP Command Menu in the iLO 3 MP TUI to configure iLO 3 LDAP directory settings.

The following is an example of the LDAP command output:

```
[mp1] CM:hpiLO-> LDAP

Current LDAP Directory Configuration:
L - LDAP Directory Authentication        : Disabled
M - Local MP User database              : Enabled
I - Directory Server IP Address         : 192.0.2.1
P - Directory Server LDAP Port          : 636
D - Distinguished Name (DN)             : cn=mp, o=demo
1 - User Search Context 1               : o=mp
2 - User Search Context 2               : o=demo
3 - User Search Context 3               : o=test
Enter parameter(s) to change, A to modify All, or [Q] to Quit: a

For each parameter, enter:
New value, or
<CRC> to retain the current value, or
DEFAULT to set the default value, or
Q to Quit

LDAP Directory Authentication:
  E - Enabled
Current > D - Disabled (default)

Enter new value, or Q to Quit: e
```
> LDAP Directory Authentication will be updated

Local MP User Accounts:
  D - Disabled (default)
Current > E - Enabled

Enter new value, or Q to Quit: <CR>
-> Current Local MP User Accounts has been retained

Directory Server IP Address:
  Current -> 127.0.0.1 (default)

Enter new value, or Q to Quit: 192.0.2.1
-> Directory Server IP Address will be updated

Directory Server LDAP Port:
  Current -> 636 (default)

Enter new value, or Q to Quit: <CR>
-> Current Directory Server LDAP Port has been retained

Distinguished Name (DN):
  Current -> cn=mp,o=demo

Enter new value, or Q to Quit: <CR>
-> Current Distinguished Name has been retained

User Search Context 1:
  Current -> o=mp

Enter new value, or Q to Quit: <CR>
-> Current User Search Context 1 has been retained

User Search Context 2:
  Current -> o=demo

Enter new value, or Q to Quit: <CR>
-> Current User Search Context 2 has been retained

User Search Context 3:
  Current -> o=test

Enter new value, or Q to Quit: <CR>
-> Current User Search Context 3 has been retained

New Directory Configuration (* modified values):
*L - LDAP Directory Authentication: Enabled
M - Local MP User database          : Enabled
*I - Directory Server IP Address    : 192.0.2.1
P - Directory Server LDAP Port     : 636
D - Distinguished Name (DN)         : cn=mp,o=demo
1 - User Search Context 1          : o=mp
2 - User Search Context 2          : o=demo
3 - User Search Context 3          : o=test

Enter Parameter(s) to revise, Y to confirm, or [Q] to Quit: y
-> LDAP Configuration has been updated

User login using directory services

The MP 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
  The short form of the login name by itself does not identify which domain you are trying to access. To identify the domain, 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)
  Directory users that are specified with the @ searchable form can be located in one of three searchable contexts that are configured within Directory Settings.
  Example: jsmith@hp.com
• User name form
  Example: John Smith
  Directory users that are specified with the user name form can be located in one of three searchable contexts that are configured within Directory Settings.
• Local users - Login ID
  For the iLO 3 login, the maximum length of the Login Name is 25 characters for local users. For directory services users, the maximum length of the Login Name is 256 characters.

Certificate services

The following sections provide instructions for installing Certificate Services, verifying directory services, and configuring automatic certificate requests.

Installing certificate services

To install certificate services:

Procedure

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 Certificate Services and click Next.
5. At the warning that the server cannot be renamed, click OK. 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 in the Valid for field and click Next.
7. Accept the default locations of the certificate database and the database log. Click Next.
8. Browse to the c:\i386 folder when prompted for the Windows 2000 Advanced Server CD.
9. Click Finish to close the wizard.

Verifying directory services

Because iLO 3 communicates with Active Directory using SSL, you must create a certificate or install Certificate Services. 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 an automatic certificate request

To request that a certificate be issued to the server:

Procedure

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.
8. When the Automatic Certificate Request Setup wizard starts, click Next.
9. Select the Domain Controller template, and click Next.
10. Select the certificate authority listed. (the same CA defined during the Certificate Services installation). Click Next.
11. Click Finish to close the wizard.

Directory-enabled remote management

This section is for administrators who are familiar with directory services and with the iLO 3 product. To familiarize yourself with the product and services, see Directory services on page 135. Be sure you understand the examples and are comfortable with setting up the product.

In general, you can use the HP provided snap-ins to create objects. It is useful to give the iLO 3 device objects meaningful names, such as the device network address, DNS name, host server name, or serial number.

Directory-enabled remote management enables you to:

- Create iLO 3 objects:

  Each device object created represents each device that will use the directory service to authenticate and authorize users. For more information, see the following sections:

  Directory services for Active Directory on page 140

  Directory services for eDirectory on page 152

- Configure iLO 3 devices:

  Every iLO 3 device that uses the directory service to authenticate and authorize users must be configured with the appropriate directory settings. For details about the specific directory settings, see Using the LDAP command to configure directory settings on page 161. In general, each device is configured with the appropriate directory server address, iLO 3 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 multihost DNS name.

Using existing groups

Many organizations arrange users and administrators into groups. In many cases, it is convenient to use existing groups and associate these groups with one or more iLO 3 role objects. When the devices are associated with role objects, you can control access to the iLO 3 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, or create nested groups. Role objects are considered groups and can include other groups directly. To include other groups
directly, add the existing nested group directly to the role and assign the appropriate rights and restrictions. Add new users to either the existing group or to the role.

Novell® eDirectory does not allow nested groups. In eDirectory, any user who 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. Add new users to either the existing object or to the role.

When you use trustee or directory rights assignments to extend role membership, users must be able to read the iLO 3 object representing the iLO 3 device. Some environments require the trustees of a role to also be read trustees of the iLO 3 object to successfully authenticate users.

**Using multiple roles**

Most deployments do not require that the same user be in multiple roles managing the same device. However, these configurations are useful for building complex rights relationships. When building multiple-role relationships, users receive all the rights assigned by every applicable role. Roles only grant rights, not revoke them. If one role grants a user a right, 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 might have two types of users: administrators of the iLO 3 device or host server, and users of the iLO 3 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 iLO 3 administrators in that role, and the administrative role.

**Figure 67: Admin user gaining admin role right, example 1** on page 165 shows one way that an administrative user gains admin role right. The admin user’s initial login right is granted through the regular user role. After the initial login, more advanced rights are assigned to the admin user through the admin role such as server reset and remote console.

**Figure 67: Admin user gaining admin role right, example 1**

In **Figure 68: Admin user gaining admin role right, example 2** on page 166, the admin user gains the admin role right in a different way. The admin user initially logs in through the admin role and is immediately assigned admin rights (server reset, remote console, and login).
Creating roles that follow organizational structure

Often, 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 enable subordinate administrators to create and manage their own roles.

Restricting roles

Restrictions enable you to limit the scope of a role. A role only grants rights to those users who satisfy the role restrictions. Using restricted roles creates users with dynamic rights that change based on the time of day or network address of the client.

For step-by-step instructions on how to create network and time restrictions for a role, see Setting role restrictions on page 157 or Setting time restrictions on page 157.

Role time restrictions

You can place time restrictions on iLO 3 roles. Users are only granted rights that are specified for the iLO 3 devices listed in the role if they are members of the role and meet the time restrictions for that role.

The iLO 3 devices use local host time to enforce time restrictions. If the iLO 3 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 enforced if the time is set on the iLO 3 device. The time is normally set when the host is booted and is maintained by running the agents in the host operating system, which enables iLO 3 device to compensate for leap years and minimize clock drift with respect to the host. Events such as unexpected power loss or the flashing of MP firmware can cause the iLO 3 device clock not to be set. Also, the host time must be correct for the iLO 3 device to preserve time across firmware flashes.

IP address range restrictions

IP address range restrictions enable you 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. You can specify an address range 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 you to specify a range of addresses that are granted or denied access by the restriction. This format has similar capabilities to those in an IP address range but can 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 on the same logical network.
In binary math, if the bits of a client machine address are added to the bits of the subnet mask, and these bits match the restriction subnet address, 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 fails 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.

⚠️ CAUTION:
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. When implementing DNS-based address restrictions, take organizational security policies into consideration.

Role address restrictions

Role address restrictions are enforced by the MP firmware, based on the client IP network address. When the address restrictions are met for a role, the rights granted by the role apply.

Address restrictions can be difficult to manage if access is attempted across firewalls or through network proxies. Either of these mechanisms can change the apparent network address of the client, causing the address restrictions to be enforced in an unexpected manner.

Enforcing directory login restrictions

Figure 69: User and role access restrictions on page 168 shows how two sets of restrictions potentially limit a directory user’s access to iLO 3 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 iLO 3 privileges based on rights specified in one or more roles.
Enforcing user time restrictions

You 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 on the directory server, but if the directory server is located in a different time zones or a replica in a different time zone is accessed, time zone information from the managed object can be used to adjust for relative time.

While directory server evaluates user time restrictions, the determination can be complicated by time zone changes or by the authentication mechanism.

Figure 70: User time restrictions on page 168 shows the user time restrictions.
User address restrictions

You can place network address restrictions on a directory user account, and the directory server enforces these restrictions. For information about the enforcement of address restrictions on LDAP clients, such as a user logging in to an iLO 3 device, see the directory service documentation.

Network address restrictions placed on the user in the directory may not be enforced in the expected manner if the directory user logs in through a proxy server. When a user logs in to an iLO 3 device as a directory user, the iLO 3 device attempts authentication to the directory as that user, which means that address restrictions placed on the user account apply when accessing the iLO 3 device. However, because the user is proxied at the iLO 3 device, the network address of the authentication attempt is that of the iLO 3 device, not that of the client workstation.

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 you to create arbitrary, complex rights relationships with a minimum number of roles.

For example, an organization might have a security policy in which iLO 3 administrators are allowed to use the iLO 3 device from within the corporate network but are only able to reset the server outside of regular business hours.

Directory administrators may 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.

**Figure 71: Restricting general use** on page 169 shows how security policy dictates that general use is restricted to clients within the corporate subnet, and server reset capability is additionally restricted to after hours.

Alternatively, the directory administrator can create a role that grants the login right and restrict it to the corporate network, 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 unsecure because ongoing administration can create another role that grants users from addresses outside the corporate network the login right, which might unintentionally grant the iLO 3 administrators in the server reset role the ability to reset the server from anywhere, provided they satisfy the time constraints of that role.
CAUTION:
The previous configuration satisfies 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 might be to restrict the reset role, as well as the general use role.

Figure 72: Restricting the reset role

Directory services schema (LDAP)

A directory schema specifies the types of objects that a directory can have and the mandatory and optional attributes of each object type. The following sections describe both the HP management core, and the LDAP object identifier classes and attributes that are specific to iLO 3.

HP management core LDAP object identifier classes and attributes

Object identifiers (OIDs) are unique numbers that are used by LDAP to identify object class, attribute, syntaxes (data types), matching rules, protocol mechanisms, controls, extended operation and supported features.

Changes made to the schema during the schema setup process include changes to the following:

- Core classes
- Core attributes

NOTE:
Roles such as `hpqTargets`, and so on, are for extended schema LDAP only. They are not used in schema-free LDAP.
Core LDAP OID classes

Table 38: Core classes

<table>
<thead>
<tr>
<th>Class Name</th>
<th>Assigned OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>hpqTarget</td>
<td>1.3.6.1.4.1.232.1001.1.1.1.1</td>
</tr>
<tr>
<td>hpqRole</td>
<td>1.3.6.1.4.1.232.1001.1.1.1.2</td>
</tr>
<tr>
<td>hpqPolicy</td>
<td>1.3.6.1.4.1.232.1001.1.1.1.3</td>
</tr>
</tbody>
</table>

Core LDAP OID attributes

Table 39: Core attributes

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Assigned OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>hpqPolicyDN</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.1</td>
</tr>
<tr>
<td>hpqRoleMembership</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.2</td>
</tr>
<tr>
<td>hpqTargetMembership</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.3</td>
</tr>
<tr>
<td>hpqRoleIPRestrictionDefault</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.4</td>
</tr>
<tr>
<td>hpqRoleIPRestrictions</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.5</td>
</tr>
<tr>
<td>hpqRoleTimeRestriction</td>
<td>1.3.6.1.4.1.232.1001.1.1.2.6</td>
</tr>
</tbody>
</table>

Core class definitions

Table 40, Table 41, and Table 42 define the HP management core classes.

hpqTarget

Table 40: 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 |
| Remarks | None |
Table 41: hpqRole

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.1.1.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>This class defines role objects, providing the basis for HP products using directory-enabled management.</td>
</tr>
<tr>
<td>Class Type</td>
<td>Structural</td>
</tr>
<tr>
<td>SuperClasses</td>
<td>Group</td>
</tr>
<tr>
<td>Attributes</td>
<td>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</td>
</tr>
<tr>
<td>Remarks</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 42: hpqPolicy

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.1.1.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>This class defines policy objects, providing the basis for HP products using directory-enabled management.</td>
</tr>
<tr>
<td>Class Type</td>
<td>Structural</td>
</tr>
<tr>
<td>SuperClasses</td>
<td>Top</td>
</tr>
<tr>
<td>Attributes</td>
<td>hpqPolicyDN—1.3.6.1.4.1.232.1001.1.1.2.1</td>
</tr>
<tr>
<td>Remarks</td>
<td>None</td>
</tr>
</tbody>
</table>

Core attribute definitions

Table 43 through Table 48 define the HP management core class attributes.

Table 43: hpqPolicyDN

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.1.2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>This attribute provides the Distinguished Name of the policy that controls the general configuration of this target.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Distinguished Name—1.3.6.1.4.1.1466.115.121.1.12</td>
</tr>
</tbody>
</table>

Table Continued
OID | 1.3.6.1.4.1.232.1001.1.1.2.1
--- | ---
Options | Single Valued
Remarks | None

**hpqRoleMembership**

Table 44: hpqRoleMembership

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.1.2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>This attribute provides a list of hpqTarget objects to which this object belongs.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Distinguished Name—1.3.6.1.4.1.1466.115.121.1.12</td>
</tr>
<tr>
<td>Options</td>
<td>Multi Valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>None</td>
</tr>
</tbody>
</table>

**hpqTargetMembership**

Table 45: hpqTargetMembership

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.1.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>This attribute provides a list of hpqTarget objects that belong to this object.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Distinguished Name—1.3.6.1.4.1.1466.115.121.1.12</td>
</tr>
<tr>
<td>Options</td>
<td>Multi Valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>None</td>
</tr>
</tbody>
</table>

**hpqRoleIPRestrictionDefault**

Table 46: hpqRoleIPRestrictionDefault

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.1.2.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>This attribute is a Boolean expression representing access by unspecified clients, which partially specifies rights restrictions under an IP network address constraint.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Boolean—1.3.6.1.4.1.1466.115.121.1.7</td>
</tr>
<tr>
<td>Options</td>
<td>Single Valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>If this attribute is TRUE, IP restrictions are satisfied for unexceptional network clients. If this attribute is FALSE, IP restrictions are unsatisfied for unexceptional network clients.</td>
</tr>
</tbody>
</table>
## hpqRoleIPRestrictions

### Table 47: hpqRoleIPRestrictions

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.1.2.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>This attribute provides a list of IP addresses, DNS names, domain, address ranges, and subnets, which partially specify right restrictions under an IP network address constraint.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Octet String-1.3.6.1.4.1.1466.115.121.1.40</td>
</tr>
<tr>
<td>Options</td>
<td>Multi Valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>This attribute is only used on role objects. The 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 &lt;0x01&gt;, 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 can be represented as &lt;0x01 0x7F 0x00 0x00 0x01 0xFF 0x00 0x00 0x00&gt;. For IP ranges, the identifier is &lt;0x02&gt;, 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 is represented as &lt;0x02 0x0A 0x00 0x00 0x01 0x0A 0x00 0x0A 0xFF&gt;. For DNS names or domains, the identifier is &lt;0x03&gt;, followed by the ASCII encoded DNS name. DNS names can be prefixed with a * (ASCII 0x2A), to indicate they match names that end with the specified string. For example, match the DNS domain *.acme.com is represented as &lt;0x03 0x2A 0x2E 0x61 0x63 0x6D 0x65 0x2E 0x63 0x6F 0x6D 0x6E&gt;. General access is allowed.</td>
</tr>
</tbody>
</table>

## hpqRoleTimeRestriction

### Table 48: hpqRoleTimeRestriction

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.1.2.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>This attribute represents a 7-day time grid, with 30-minute resolution, which specifies rights restrictions under a time constraint.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Octet String {42}-1.3.6.1.4.1.1466.115.121.1.40</td>
</tr>
<tr>
<td>Options</td>
<td>Single Valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>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.</td>
</tr>
</tbody>
</table>
iLO 3-specific LDAP OID classes and attributes

The schema attributes and classes in Table 49 and Table 50 might depend on attributes or classes defined in the HP management core classes and attributes.

iLO 3 classes

Table 49: iLO 3 classes

<table>
<thead>
<tr>
<th>Class Name</th>
<th>Assigned OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>hpqLOMv100</td>
<td>1.3.6.1.4.1.232.1001.1.8.1.1</td>
</tr>
</tbody>
</table>

iLO 3 attributes

Table 50: iLO 3 attributes

<table>
<thead>
<tr>
<th>Class Name</th>
<th>Assigned OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>hpqLOMRightLogin</td>
<td>1.3.6.1.4.1.232.1001.1.8.2.1</td>
</tr>
<tr>
<td>hpqLOMRightRemoteConsole</td>
<td>1.3.6.1.4.1.232.1001.1.8.2.2</td>
</tr>
<tr>
<td>hpqLOMRightVirtualMedia</td>
<td>1.3.6.1.4.1.232.1001.1.8.2.3</td>
</tr>
<tr>
<td>hpqLOMRightServerReset</td>
<td>1.3.6.1.4.1.232.1001.1.8.2.4</td>
</tr>
<tr>
<td>hpqLOMRightLocalUserAdmin</td>
<td>1.3.6.1.4.1.232.1001.1.8.2.5</td>
</tr>
<tr>
<td>hpqLOMRightConfigureSettings</td>
<td>1.3.6.1.4.1.232.1001.1.8.2.6</td>
</tr>
</tbody>
</table>

iLO 3 class definitions

hpqLOMv100

Table 51: hpqLOMv100

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.8.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>This class defines the rights and settings used with HPE iLO 3 products.</td>
</tr>
<tr>
<td>Class Type</td>
<td>Auxiliary</td>
</tr>
<tr>
<td>SuperClasses</td>
<td>None</td>
</tr>
</tbody>
</table>
### iLO 3 attribute definitions

Table 52 through Table 57 define the iLO 3 core class attributes.

#### hpqLOMRightLogin

**Table 52: hpqLOMRightLogin**

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.8.2.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Login right for HPE iLO 3 products.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Boolean-1.3.6.1.4.1.1466.115.121.1.7</td>
</tr>
<tr>
<td>Options</td>
<td>Single Valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>The attribute is meaningful only on role objects. If TRUE, members of the role are granted the right.</td>
</tr>
</tbody>
</table>

#### hpqLOMRightRemoteConsole

**Table 53: hpqLOMRightRemoteConsole**

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.8.2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Remote console right for iLO 3 products. Meaningful only on role objects.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Boolean-1.3.6.1.4.1.1466.115.121.1.7</td>
</tr>
<tr>
<td>Options</td>
<td>Single valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>This attribute is only used on role objects. If this attribute is TRUE, members of the role are granted the right.</td>
</tr>
</tbody>
</table>
### hpqLOMRightRemoteConsole

**Table 54: hpqLOMRightRemoteConsole**

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.8.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Virtual Media right for HPE iLO 3 products.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Boolean-1.3.6.1.4.1.1466.115.121.1.7</td>
</tr>
<tr>
<td>Options</td>
<td>Single valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>This attribute is only used on role objects. If this attribute is TRUE, members of the role are granted the right.</td>
</tr>
</tbody>
</table>

### hpqLOMRightServerReset

**Table 55: hpqLOMRightServerReset**

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.8.2.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Remote server reset and power button right for HPE iLO 3 products.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Boolean-1.3.6.1.4.1.1466.115.121.1.7</td>
</tr>
<tr>
<td>Options</td>
<td>Single valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>This attribute is only used on role objects. If this attribute is TRUE, members of the role are granted the right.</td>
</tr>
</tbody>
</table>

### hpqLOMRightLocalUserAdmin

**Table 56: hpqLOMRightLocalUserAdmin**

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.8.2.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Local user database administration right for HPE iLO 3 products.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Boolean-1.3.6.1.4.1.1466.115.121.1.7</td>
</tr>
<tr>
<td>Options</td>
<td>Single valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>This attribute is only used on role objects. If this attribute is TRUE, members of the role are granted the right.</td>
</tr>
</tbody>
</table>
**hpqLOMRightConfigureSettings**

**Table 57: hpqLOMRightConfigureSettings**

<table>
<thead>
<tr>
<th>OID</th>
<th>1.3.6.1.4.1.232.1001.1.8.2.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Configure devices settings right for HPE iLO 3 products.</td>
</tr>
<tr>
<td>Syntax</td>
<td>Boolean-1.3.6.1.4.1.1466.115.121.1.7</td>
</tr>
<tr>
<td>Options</td>
<td>Single valued</td>
</tr>
<tr>
<td>Remarks</td>
<td>This attribute is only used on role objects. If this attribute is TRUE, members of the role are granted the right.</td>
</tr>
</tbody>
</table>
Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
  [http://www.hpe.com/assistance](http://www.hpe.com/assistance)
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates:
  Hewlett Packard Enterprise Support Center
  [www.hpe.com/support/hpesc](http://www.hpe.com/support/hpesc)
  Hewlett Packard Enterprise Support Center: Software downloads
  [www.hpe.com/support/downloads](http://www.hpe.com/support/downloads)
  Software Depot
  [www.hpe.com/support/softwaredepot](http://www.hpe.com/support/softwaredepot)
- To subscribe to eNewsletters and alerts:
  [www.hpe.com/support/e-updates](http://www.hpe.com/support/e-updates)
- To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center More Information on Access to Support Materials page:

**IMPORTANT:**

Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.
Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

http://www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

If your product includes additional remote support details, use search to locate that information.

Remote support and Proactive Care information

HPE Get Connected
www.hpe.com/services/getconnected
HPE Proactive Care services
www.hpe.com/services/proactivecare
HPE Proactive Care service: Supported products list
www.hpe.com/services/proactivecaresupportedproducts
HPE Proactive Care advanced service: Supported products list
www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central
www.hpe.com/services/proactivecarecentral
Proactive Care service activation
www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

To view the warranty for your product or to view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products reference document, go to the Enterprise Safety and Compliance website:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional warranty information

HPE ProLiant and x86 Servers and Options
www.hpe.com/support/ProLiantServers-Warranties
HPE Enterprise Servers
www.hpe.com/support/EnterpriseServers-Warranties
HPE Storage Products
www.hpe.com/support/Storage-Warranties
Regulatory information

To view the regulatory information for your product, view the Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products, available at the Hewlett Packard Enterprise Support Center:

www.hpe.com/support/Safety-Compliance-EnterpriseProducts

Additional regulatory information

Hewlett Packard Enterprise is committed to providing our customers with information about the chemical substances in our products as needed to comply with legal requirements such as REACH (Regulation EC No 1907/2006 of the European Parliament and the Council). A chemical information report for this product can be found at:

www.hpe.com/info/reach

For Hewlett Packard Enterprise product environmental and safety information and compliance data, including RoHS and REACH, see:

www.hpe.com/info/ecodata

For Hewlett Packard Enterprise environmental information, including company programs, product recycling, and energy efficiency, see:

www.hpe.com/info/environment

Documentation feedback

Hewlett Packard Enterprise is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.
3DES
Triple Data Encryption Algorithm

address
In networking, a unique code that identifies a node in the network. Names such as host1.hp.com are translated to dott-quad addresses such as 168.124.3.4 by the Domain Name Service (DNS).

address path
An address path is one in which each term has the appropriate intervening addressing association.

administrator
A person managing a system through interaction with management clients, transport clients, and other policies and procedures.

AES
Advanced Encryption Standard. This is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST).

authentication
The process that verifies the identity of a user in a communication session, or a device or other entity in a computer system, before that user, device, or other entity can access system resources. Session authentication can work in two directions: a server authenticates a client to make access control decisions, and the client can also authenticate the server. With Secure Sockets Layer (SSL), the client always authenticates the server.

authorization
The process of granting specific access privileges to a user. Authorization is based on authentication and access control.

bind
In the Lightweight Directory Access Protocol (LDAP), refers to the authentication process that LDAP requires when users access the LDAP directory. Authentication occurs when the LDAP client binds to the LDAP server.

BIOS
Basic Input/Output System. System software that controls the loading of the operating system and testing of hardware when the system is powered on. The BIOS is stored in read-only memory (ROM).

BMC
Baseboard Management Controller. A device used to manage chassis environmental, configuration, and service functions, and receive event data from other parts of the system. It receives data through sensor interfaces and interprets this data by using the sensor data record (SDR) for which it provides an interface. The BMC also provides an interface to the SEL. Typical functions of the BMC are
measuring processor temperature, power supply values, and cooling fan status. The BMC can take autonomous action to preserve system integrity.

C

CIM
See Common Information Model.

Cipher
In cryptography, a cipher (or cypher) is an algorithm for performing encryption or decryption.

Command Line Interface (CLI)
A text user interface (TUI) for interacting with a computer operating system or software by typing commands at a command prompt to perform specific tasks.

Common Information Model (CIM)
An industry standard that was developed by the DMTF. CIM describes data about applications and devices so that administrators and software management programs can control applications and devices on different platforms in the same way, ensuring interoperability across a network.

CIM provides a common definition of management information for systems, components, networks, applications, and services, and it allows for vendor extensions. CIM common definitions enable vendors to exchange management information between systems.

Using techniques of object-oriented programming, CIM provides a consistent definition and structure of data, including expressions for elements such as object classes, properties, associations, and methods.

For example, if an enterprise purchases four different servers from four different vendors and networks them together, using CIM, the administrator can view the same information about each of the devices, such as manufacturer and serial number, the device's model number, its location on the network, its storage capacity, and its relationship to the applications that run throughout the network.

c (console)
The interface between iLO 3 and the server that controls basic functionality. Also known as host console.

D

DDNS
Dynamic Domain Name System. DDNS is how iLO 3 automatically registers its name with the Domain Name System so that when iLO 3 receives its new IP address from DHCP, users can connect to the new iLO 3 using the host name, rather than the new IP address.

DHCP
Dynamic Host Configuration Protocol. A protocol that enables a DHCP server to assign Internet Protocol (IP) addresses dynamically to systems on a Transmission Control Protocol/Internet Protocol (TCP/IP) network. Without DHCP, IP addresses must be entered manually at each computer, and when computers are moved to another location on another part of the network, a new IP address must be entered.

directory server
In the Lightweight Directory Access Protocol (LDAP), a server which stores and provides information about people and resources within an organization from a logically centralized location.
distinguished name (DN)

In the Lightweight Directory Access Protocol (LDAP), a unique text string that identifies an entry's name and location within the directory. A DN can be a fully qualified domain name (FQDN) that includes the complete path from the root of the tree.

DNS

Domain Name Server. The server that typically manages host names in a domain. DNS servers translate host names, such as `www.example.com`, into Internet Protocol (IP) addresses, such as `030.120.000.168`.

Domain Name Service. The data query service that searches domains until a specified host name is found.

Domain Name System. A distributed, name resolution system that enables computers to locate other computers on a network or the Internet by domain name. The system associates standard Internet Protocol (IP) addresses, such as `00.120.000.168`, with host names, such as `www.hp.com`. Machines typically acquire this information from a DNS server.

domain

A grouping of hosts that is identified by a name. The hosts usually belong to the same Internet Protocol (IP) network address.

domain name

The unique name assigned to a system or group of systems on the Internet. The host names of all the systems in the group have the same domain name suffix. Domain names are interpreted from right to left.

E

Encryption

Encryption is the process of encoding messages or information in such a way that only authorized parties can read it.

ethernet

An industry-standard type of local area network (LAN) that enables real-time communication between systems connected directly through cables. Ethernet uses a Carrier Sense Multiple Access/Collision Detection (CSMA/CD) algorithm as its access method, which all nodes listen for, and any node can begin transmitting data. If multiple nodes attempt to transmit at the same time (a collision), the transmitting nodes wait for a random time before attempting to transmit again.

event

A change in the state of a managed object. The event-handling subsystem can provide a notification, to which a software system must respond when it occurs, but which the software did not solicit or control.

extended schema

A platform-specific schema derived from the common model. An example is the Win32 schema.

F

firmware

Software that is typically used to help with the initial booting stage of a system and with system management. Firmware is embedded in read-only memory (ROM) or programmable ROM (PROM).
FPGA
Field Programmable Gate Array. A semiconductor device containing programmable logic components and programmable interconnects.

FTP
File Transfer Protocol. A basic Internet protocol based on Transmission Control Protocol/Internet Protocol (TCP/IP) that enables the retrieving and storing of files between systems on the Internet without regard for the operating systems or architectures of the systems involved in the file transfer.

gateway
A computer or program that interconnects two networks and passes data packets between the networks. A gateway has more than one network interface.

gateway address
Where the packet needs to be sent. This can be the local network card or a gateway (router) on the local subnet.

GUI
Graphical User Interface. An interface that uses graphics, along with a keyboard and mouse, to provide easy-to-use access to an application.

host
A system, such as a backend server, with an assigned Internet Protocol (IP) address and host name. The host is accessed by other remote systems on the network.

host ID
Part of the 32-bit Internet Protocol (IP) address used to identify a host on a network. Host ID is also known as DNS Name or Host Name.

host console
The interface between iLO 3 and the server that controls basic functionality. Also known as console.

host name
The name of a particular machine within a domain. Host names always map to a specific Internet Protocol (IP) address.

HTTP
Hypertext Transfer Protocol. The Internet protocol that retrieves hypertext objects from remote hosts. HTTP messages consist of requests from client to server, and responses from server to client. HTTP is based on Transmission Control Protocol/Internet Protocol (TCP/IP).

in-band system management
A server management capability that is enabled only when the operating system is initialized and the server is functioning properly.
Integrated Lights-Out (iLO)

The iLO functionality offers remote server management through an independent management processor (MP). Integrity iLO was introduced into most HP Integrity entry class servers in late 2004. Prior to that, embedded remote server management was referred to as MP functionality. All legacy MP functionality has been carried forward and combined with new features, all under the heading of "iLO". Therefore, "iLO" and "MP" mean the same thing for entry class servers.

IP

Internet Protocol. IP specifies the format of packets and the packet addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP), which establishes a virtual connection between a destination and a source. TCP/IP establishes a connection between two hosts so that they can send messages back and forth for a period of time. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255; for example, 1.160.10.240. Within an isolated network, you can assign IP addresses at random as long as each one is unique. However, connecting a private network to the Internet requires using registered IP addresses (called Internet addresses) to avoid duplicates.

IP Address

An identifier for a computer or device on a TCP/IP network.

IPMI

Intelligent Platform Management Interface. A hardware-level interface specification designed primarily for the out-of-band management of server systems over a number of different physical interconnects. The IPMI specification describes extensive abstractions regarding sensors, enabling a management application running on the operating system or in a remote system to comprehend the environmental makeup of the system and to register with the IPMI subsystem to receive events. IPMI is compatible with management software from heterogeneous vendors. IPMI functionality includes inventory reporting, system monitoring, logging, system recovery (including local and remote system resets, and power on and power off capabilities), and alerting.

K

kernel

The core of the operating system that manages the hardware and provides fundamental services that the hardware does not provide, such as filing and resource allocation.

KVM switch

Keyboard, Video, Mouse. A hardware device that allows a user, or multiple users, to control multiple computers from a single keyboard, video monitor and mouse.

L

LDAP

Lightweight Directory Access Protocol. A directory service protocol used for the storage, retrieval, and distribution of information, including user profiles, distribution lists, and configuration data. LDAP runs over Transmission Control Protocol/Internet Protocol (TCP/IP) across multiple platforms.

M

Media Access Control (MAC)

Worldwide unique, 48-bit, hardware address number that is programmed in to each local area network interface card (NIC) at the time of manufacture. In the Ethernet standard, every network connection must support a unique MAC value.
MAP
Manageability Access Point. A network-accessible interface for managing a computer system. A MAP can be initiated by a management process, a management processor, a service processor, or a service process.

MAP address space
This is the hierarchical graph of the UFIs contained in the MAP’s AdminDomain. Each instance starting at the AdminDomain is a node in the graph. Each supported association forms a link in the graph to another instance node, and so on, until a terminating instance node is encountered.

managed object
The actual item in the system environment that is accessed by the provider. For example, a Network Interface Card (NIC).

Management Information Base (MIB)
The MIB defines the properties of the managed object within the device to be managed. Every managed device keeps a database of values for each definition written in the MIB. MIB is not the actual database itself and is implementation dependant.

Management Processor (MP)
The component that provides a LAN interface to the system console and system management. Prior to iLO 3, embedded remote server management was referred to as MP functionality. All legacy MP functionality has been carried forward and combined with new features, all under the heading of "iLO 3". Therefore, "iLO 3" and "MP" mean the same thing for entry class servers.

MFW
Manageability FirmWare.

Monarch
The monarch server blade is always in the lowest numbered enclosure bay, and all communication to the conjoined server blade is done through the monarch server blade.

MP Upgradeability
Firmware remotely upgradeable through MP LAN, offline update through EFI, and OS-initiated firmware updates for all Integrity support OS.

Network Interface Card (NIC)
An internal circuit board or card that connects a workstation or server to a networked device.

network mask
A number used by software to separate a local subnet address from the rest of an Internet Protocol (IP) address.

node
An addressable point or device on a network. A node can connect a computing system, a terminal, or various peripheral devices to the network.

Onboard Administrator
The BladeSystem Onboard Administrator (OA) is the enclosure MP, subsystem, and firmware base used to support HP Integrity server blades and all the managed devices contained within the
enclosure. The OA provides a single point from which to perform basic management tasks on server blades or switches within the enclosure. Utilizing this hard-wired information, the OA performs initial configuration steps for the enclosure, allows for run-time management and configuration of enclosure components, and informs administrators about problems within the enclosure through email or the Insight Display.

**out-of-band system management**

Server management capability that is enabled when the operating system network drivers or the server are not functioning properly.

**P**

**port**

The location (socket) where Transmission Control Protocol/Internet Protocol (TCP/IP) connections are made. Web servers traditionally use port 80, the File Transfer Protocol (FTP) uses port 21, and Telnet uses port 23. A port enables a client program to specify a particular server program in a computer on a network. When a server program is started initially, it binds to its designated port number. Any client that wants to use that server must send a request to bind to the designated port number.

**port number**

A number that specifies an individual Transmission Control Protocol/Internet Protocol (TCP/IP) application on a host machine, providing a destination for transmitted data.

**POST**

Power-On Self-Test. The series of steps that the host system CPU performs following power-on. Steps include testing memory, initializing peripherals, and running option ROMs. Following POST, the host ROM passes control to the installed operating system.

**properties**

Properties are attributes that are relevant to a target that are passed as parameters to the command. Property keywords map to properties of CIM class.

**protocol**

A set of rules that describes how systems or devices on a network exchange information.

**proxy**

A mechanism whereby one system acts on behalf of another system in responding to protocol requests.

**R**

**rackmount**

Electronic equipment and devices designed to fit industry-standard-sized computer racks and cabinets (19" wide). Rackmount devices are also standard 1.75 inch units.

**remote system**

A system other than the one on which the user is working.

**S**

**schema**

Definitions that describe what type of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the
directory may be unable to display the proper results. Schemas come in many forms, such as a text file, information in a repository, or diagrams.

security
Secure Socket Layer Secure Shell (SSH) version 2 (Password and certificate), SSL, and integration with enterprise directory services.

serial console
A terminal connected to the serial port on the service processor. A serial console is used to configure the system to perform other administrative tasks.

server blade
A single circuit board populated with components such as processors, memory, and network connections that are usually found on multiple boards.

SSH
Secure Shell. A UNIX shell program and network protocol that enables secure and encrypted log in and running of commands on a remote system over an insecure network.

SSL
Secure Sockets Layer. A protocol that enables client-to-server communication on a network to be encrypted for privacy. SSL uses a key exchange method to establish an environment in which all data exchanged is encrypted with a cipher and hashed to protect it from eavesdropping and alteration. SSL creates a secure connection between a web server and a web client. Hypertext Transfer Protocol Secure (HTTPS) uses SSL.

subnet
A working scheme that divides a single logical network into smaller physical networks to simplify routing. The subnet is the portion of an Internet Protocol (IP) address that identifies a block of host IDs.

subnet mask
A bit mask used to select bits from an Internet address for subnet addressing. The mask is 32 bits long, and selects the network portion of the Internet address and one or more bits of the local portion. Also called an address mask.

System Event Log (SEL)
A log that provides nonvolatile storage for system events that are logged autonomously by the service processor, or directly with event messages sent from the host.

T

target address
The target addressing scheme provides an easy-to-use method to accurately address CIM objects. The target address term of the CLP syntax in this architecture is extensible. The addressing scheme provides a unique target for CLP commands. The scheme is finite for parsing target names, and unique for unambiguous access to associated instance information needed to support association traversal rooted at the MAP AdminDomain instance.

target address scheme resolution service
This entity is responsible for discovering and enumerating the managed elements within the local domain, for maintaining the addressing and naming structure of the local domain, and coordinating this information with the operation invocation engine.
Telnet
A telecommunications protocol providing specifications for emulating a remote computer terminal so that one can access a distant computer and function online using an interface that appears to be part of the user's local system.

TUI
Text User Interface. A command-line interface that enables you to enter and run commands in the MP.

Unified Extensible Firmware Interface (UEFI)
EFI is an Itanium-based architecture feature that defines the interfaces between the operating system and the system firmware, and between firmware driver and the system firmware. EFI provides a standard environment for booting an OS and running preboot applications. EFI post-1.10 activities is owned by the nonprofit organization named Unified EFI Forum, Inc. The Unified EFI Forum is a nonprofit collaborative trade organization formed to promote and manage the UEFI standard. As an evolving standard, the UEFI specification is driven by contributions and support from member companies of the UEFI Forum.

Universal Serial Bus (USB)
An external bus standard that supports data transfer rates of 450 Mb/s (USB 2.0). A USB port connects devices such as mouse pointers, keyboards, and printers, to the computer system.

User account
A record of essential user information that is stored on the system. Each user who accesses a system has a user account.

User Friendly Tag (UFT)
A short, user-friendly tag for a CIM class name or instance. There are two types of UFTs; UFcT and UFiT.

User Friendly class Tag (UFcT)
A short, user-friendly synonym for a CIM class name. It has the same properties and methods as the CIM class it represents.

User Friendly instance Tag (UFiT)
A unique instance tag within the scope of the target instance’s containment class. A UFiT is created by adding an nonzero positive-integer suffix to the target instance’s UFcT.

User Friendly instance Path (UFiP)
A unique path to an instance formed by concatenating the UFiTs of each instance from the root instance to the terminating instance. The intervening ‘/’ between each UFiT represents an address association.

User name
A combination of letters, and possibly numbers, that identifies a user to the system.

UTF-8
Virtual Media

Also, vMedia. Connects a CD/DVD-ROM drive or CD disk image files on client system to the remote server so they appear local to the server during system boot or while the operating system is available. Supports HP-UX, Windows, and Linux server operating environments using Windows and Linux clients.

vKVM

Virtual keyboard, video, mouse.

VPN

Virtual private network. A network that is constructed using public wires (the Internet) to connect nodes. These systems use encryption and other security mechanisms to ensure only authorized users can access the network and that the data cannot be intercepted.