HP Integrity and HP 9000 Integrated Lights-Out Management Processor Operations Guide

Manufacturing Part Number: 5971-4274
Second Edition
April 2005

Printed in U.S.A.

Legal Notices

The information contained herein is subject to change without notice.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Acrobat® is a trademark of Adobe Systems Incorporated.

Java™ is a US trademark of Sun Microsystems, Inc.

Linux® is a US registered trademark of Linus Torvalds.

Microsoft® and Windows® are US registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Contents

Contents

Contents

Contents

Figures

Figures

Preface

This preface contains the following sections:

- Intended Audience
- What's New?
- Notational Conventions
- Reader Comments and Feedback
- Related Information
- Printing History

Intended Audience

This document is intended to provide technical product and support information for authorized service providers, customer system administrators, and HP support personnel.

What's New?

- The layout of this document was changed to improve usability.

Notational Conventions

The following notational conventions are used in this publication.

WARNING	**A warning lists requirements that you must meet to avoid personal injury.**

CAUTION	A caution provides information required to avoid losing data or avoid losing system functionality.

NOTE	A note highlights useful information such as restrictions, recommendations, or important details about HP product features.

- `Commands and options` are represented using `this font`.
- **`Text that you type exactly as shown`** is represented using **`this font`**.
- *`Text to be replaced with text that you supply`* is represented using *`this font`*.

  Example:
  "Enter the `ls -l` *`filename`* command" means you must replace *`filename`* with your own text.
- **Keyboard keys and graphical interface items (such as buttons, tabs, and menu items)** are represented using **this font**.

  Examples:
  The **Control** key, the **OK** button, the **General** tab, the **Options** menu.
- **Menu —> Submenu** represents a menu selection you can perform.

Example:
"Select the **Partition —> Create Partition** action" means you must select the **Create Partition** menu item from the **Partition** menu.

- `Example screen output` is represented using `this font`.

Reader Comments and Feedback

HP welcomes your feedback on this publication. Please address your comments to **edit@presskit.rsn.hp.com** and note that you will not receive an immediate reply. All comments are appreciated.

Related Information

You can find other information on HP server hardware management, Microsoft® Windows®, and diagnostic support tools in the following publications.

Web Site for HP Technical Documentation: http://docs.hp.com

The main Web site for HP technical documentation is **http://docs.hp.com**, which has complete information available for free.

Server Hardware Information: http://docs.hp.com/hpux/hw/

The **http://docs.hp.com/hpux/hw/** Web site is the systems hardware portion of the docs.hp.com and provides HP nPartition server hardware management details, including site preparation, installation, and more.

Windows Operating System Information

You can find information about administration of the Microsoft® Windows® operating system at the following Web sites, among others:

- **http://docs.hp.com/windows_nt/**
- **http://www.microsoft.com/technet/**

Diagnostics and Event Monitoring: Hardware Support Tools

Complete information about HP's hardware support tools, including online and offline diagnostics and event monitoring tools, is at the **http://docs.hp.com/hpux/diag/** Web site. This site has manuals, tutorials, FAQs, and other reference material.

Web Site for HP Technical Support: http://us-support2.external.hp.com

HP's IT resource center Web site at **http://us-support2.external.hp.com/** provides comprehensive support information for IT professionals on a wide variety of topics, including software, hardware, and networking.

Books about HP-UX Published by Prentice Hall

The **http://www.hp.com/hpbooks/** Web site lists the HP books that Prentice Hall currently publishes, such as HP-UX books including:

- *HP-UX 11i System Administration Handbook*
  http://www.hp.com/hpbooks/prentice/ptr_0130600814.html
- *HP-UX Virtual Partitions*
  http://www.hp.com/hpbooks/prentice/ptr_0130352128.html

HP Books are available worldwide through bookstores, online booksellers, and office and computer stores.

Printing History

The Printing History below identifies the edition dates of this manual. Updates are made to this publication on an unscheduled, *as needed*, basis. The updates will consist of a complete replacement manual and pertinent on-line or CD-ROM documentation.

First Edition	November 2004
Second Edition	April 2005

1 Overview

Integrated Lights-Out (iLO) offers remote server management through an independent management processor (MP). It provides a way for you to connect to a server and perform administration or monitoring tasks for the server hardware. iLO is available whenever the system is connected to a power source, even if the server main power switch is in the off position.

iLO controls power, reset, and Transfer of Control (TOC) capabilities; provides console access; displays and records system events; and can display detailed information about the various internal subsystems. iLO also provides a virtual front panel that you can use to monitor system status and see the state of front panel LEDs. All iLO functions are available through the server LAN and the local RS-232 and remote RS-232 ports. Access to local and remote ports, telnet, and secure shell (SSH) is through the iLO text interface, while Web access is through a graphical user interface (GUI).

iLO was introduced into most 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 such as those listed in Table 1-1.

The following sections provide a list of supported systems and required components, and an overview of MP features:

- “Supported Systems and Required Components”
- “Feature Overview”
- “New Feature Details”

Supported Systems and Required Components

The following table lists the systems on which iLO is supported and the components that are required to operate iLO:

Table 1-1 Supported Systems and Required Components

Supported Systems	Required Components
rx1600; rx1620; rx2620	• iLO Manageability Card (AB9803A); optional • Minimum MP firmware version: E.03.13
rx2600; rp3410; rp3440	• iLO Manageability Card; factory installed • Minimum MP firmware version: E.03.13
rx4640; rp4440	• I/O baseboard (A6961-60001); factory installed • Minimum MP firmware version: E.03.13
rx5670	• MP/SCSI Core I/O Card (A6695-60001); factory installed • Minimum MP firmware version: E.03.13

Feature Overview

iLO offers the following features:

- Always-on capability: iLO is active as long as the power cord is plugged in
- Multiple access methods: Local, remote, telnet, and SSH use the iLO text interface. Web access uses a GUI.
  - Local Serial Port: Use a terminal or laptop computer for direct connection.
  - Remote/Modem Serial Port: Use a dedicated modem RS-232 port and external modem.
  - LAN: Use telnet, Web, or SSH to access iLO LAN.
- Remote power cycle; power on or power off; reset
- Mirrored console: The system console output stream is reflected to all connected console users, and any user can provide input.
- Independent, non mirrored sessions (from local and modem ports)
  - Direct session with OS using the MP command `SE`
  - Connection to another iLO using the MP command `CSP`
- Display of information about various internal subsystems
  - Field replaceable unit (FRU) information
  - System power state, temperature information, and fan status
  - Status of processors
- Logging, display, and keyword search of:
  - System console history
  - System events
- User access control
- DHCP and DNS support
- IPMI over LAN
- Licensing
- iLO Advanced Pack features, such as SSH access, group actions capability, and LDAP

NOTE For details on new and advanced features, see “New Feature Details” on page 16.

New Feature Details

This section provides additional information about MP features.

- User access control

  Access to the MP 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 MP commands. MP supports Lightweight Directory Access Protocol (LDAP) directory user authentication and locally stored MP user accounts.

  An MP user can have any of the following access rights:

  — Login Access: Right to log in to MP and execute “Status” or “Read-only” commands (such as view event logs, check system status, or check power status) but not execute any commands that would alter the state of MP or the system.

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

  — Power Control Access: Right to power on, power off, or reset the server, and the right to configure the power restore policy.

  — Local User Administration Access: Right to configure locally stored user accounts.

  — MP Configuration Access: Right to configure all MP settings (as well as some system settings, such as the power restore policy).

  Multiple users can interact with the MP. MP supports up to 14 simultaneous connections: 2 RS-232, 4 telnet, 4 Web, and 4 SSH.

NOTE HP does not recommend running more than eight simultaneous connections.

  From the MP Main Menu, users can choose any of the following options: enter the MP Command Menu, enter the console, view event logs, view console history, display the virtual front panel, enter a console session, or connect to another MP when connected locally. Multiple users can choose different options from the MP Main Menu at the same time. However, MP 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.

- DHCP and DNS support

  MP supports the Dynamic Host Configuration Protocol (DHCP) and the Domain Name System (DNS) configuration options for acquiring network information for the MP LAN port. When MP is first started, it acquires the port configuration stored on a DHCP server, and the MP LAN port is assigned an IP address. If DNS is configured, the information is updated on the DNS server.

- IPMI over LAN

  The Intelligent Platform Management Interface (IPMI) option provides direct access from the MP LAN port to the server Baseboard Management Controller (BMC), monitoring and controlling functions, such as temperature, voltage, fans, and power supplies. IPMI defines a common interface for platform management hardware. With IPMI over LAN enabled, BMC functions are available to other management software applications. MP supports up to four simultaneous IPMI over LAN connections.

- Licensing

MP includes advanced features, described in the following section, which are only available with a license. The features are available with either an evaluation license or a permanent license.

iLO Advanced Pack License Features

MP includes the following advanced features, which can only be used with a license:

- Directory-based authentication and authorization (LDAP)
- Secure shell (SSH) access
- Group actions through HP Systems Insight Manager (HPSIM)

LDAP Support

The directory-based authentication and authorization option enables MP user accounts to be defined in a centralized database on an LDAP server. MP users are authenticated when logging in to an MP and authorization is given each time an MP command is executed.

SSH Support

SSH is an industry- standard client- server connectivity protocol that provides a secure remote connection. MP supports:

- SSH2 implementation
- Authentication algorithms RSA and DSA
- Encryption algorithms 3DES-CBC and AES128-CBC
- Integrity algorithms HMAC-SHA1 and MD5

Group Actions with HPSIM

HP Systems Insight Manager (HPSIM) is a system- level management tool that supports executing MP commands using the SSH interface. HPSIM enables the user to perform similar management activities across multiple MPs (group actions) without requiring the user to access each MP individually. Group actions can be taken regardless of the server power state. You can find information about HPSIM at: http://www.docs.hp.com/go/hpsim.

Obtaining and Activating iLO Advanced Pack Licensing (AB500A)

You must have an MP and the minimum required MP firmware version E.03.13 (see Table 1-1, “Supported Systems and Required Components,” on page 14 for more details) to utilize iLO Advanced Pack license features. When you order an iLO Manageability card, either separately or when you purchase a new system, you can also order the iLO Advanced Pack license. You can order just the iLO Advanced Pack license if you already have an MP.

Follow either the factory-install or manual install instructions located on the *Integrated Lights-Out Advanced Pack for HP Integrity and HP9000 Servers; Certificate of License to Use; License Installation Card* to activate your license.

2 Configuring the Management Processor

The following sections in this chapter describe how to configure the MP:

- “Configuring the MP LAN Port IP Address”
- “Accessing the Management Processor”
- “Configuring the Management Processor LAN Information”
- “Configuring DHCP and DNS”
- “Configuring LDAP”

Configuring the MP LAN Port IP Address

By connecting the MP LAN port to an active network, you have two options for configuring an IP address. The first option is to use a DHCP server, which automatically assigns an IP address, and the other is to use the ping command from another host on the same subnet to set a static IP address for the MP. After the IP address has been set, you can establish a telnet session to configure additional parameters.

If you are using a DHCP server, and it provides the Domain Name, and if the primary DNS server accepts dynamic DNS (DDNS) updates or has been configured through the DHCP server, then you can use a default host name to connect to the MP through telnet. The default host name is 14 characters long, consisting of the letters “mp” followed by the 12 characters of the Media Access Protocol (MAC). See “Configure an IP Address” on page 21 to determine the MAC address. If no DNS access is available, the telnet session can use the assigned IP address.

If you are using DHCP, proceed to “Accessing the Management Processor” on page 22. For more information on configuring DHCP, see “Configuring DHCP and DNS” on page 27. For a non-DHCP implementation, perform the following steps to configure a static IP address.

Configuring a Static IP Address (Non-DHCP)

To configure a static IP address for the MP LAN port, follow these steps:

1. Set up local terminal access.
2. Configure the IP address.

Set Up Local Terminal Access

After powering on the terminal, ensure the communications settings are as follows:

- 8/none (parity)
- 9600 baud
- None (receive)
- None (transmit)

If the terminal is a PC using Reflection 1, check or change these communications settings by performing the following steps:

Step 1. From the Reflection 1 Main screen, pull down the Connection menu and choose **Connection Setup**.

Step 2. Choose **Serial Port**.

Step 3. Choose **Com1**.

Step 4. Check the settings and change, if required.

Go to More Settings to set Xon/Xoff. Click **OK** to close the More Settings window.

Step 5. Click **OK** to close the Connection Setup window.

Step 6. Pull down the Setup menu and choose **Terminal** (under the Emulation tab).

Step 7. Choose a supported terminal type.

The preferred type is VT100.

Step 8. Click **Apply**.

This option is not highlighted if the terminal type you want is already selected.

Step 9. Click **OK**.

Configure an IP Address

To configure the MP LAN static IP address, perform the following steps:

Step 1. Determine the Media Access Control (MAC) address of the MP LAN interface by viewing the label located at the rear of the server.

Step 2. Connect a LAN cable on your local subnet to the core I/O LAN port.

Step 3. Add an Address Resolution Protocol (ARP) table entry to another host located on your local subnet. This ARP table entry maps the MAC address of the core I/O LAN interface to the IP address chosen for that interface.

NOTE Adding an entry to the ARP table is typically done using the ARP command with the appropriate option. For example, **`arp -s`** is used with Windows. Consult your operating system documentation for more information.

Step 4. Use the **`ping`** command from the host that has the new ARP table entry. The destination address is the IP address that is mapped to the MAC address of the MP. The MP LAN port should now be configured with the appropriate IP address.

Step 5. Use the **`telnet`** command to connect to the MP from a host on the local subnet.

Accessing the Management Processor

You can connect to the management processor using the following methods:

- The local serial port using a local terminal
- The remote Customer Service Modem (CSM) port using external modem (dial-up) access, if remote modem access is configured
- The MP LAN port using the Web interface, telnet, or SSH, if login access through the MP LAN is enabled

Local Terminal Access to the Management Processor

You establish communication with the MP by connecting a terminal to the local CSM I/O serial port.

You can establish a terminal session using a standalone terminal or using terminal emulation software, such as HyperTerm, Putty, or Reflection 1 running on a PC.

During installation, communicating with the MP enables such tasks as:

- Verifying that the components are present and installed correctly
- Configuring the LAN port

Interacting with the Management Processor

To interact with the MP command line interface, perform the following steps:

NOTE On initial system installation, the MP has two default user accounts:

- All Rights (Administrator) level user; login = Admin, password = Admin (both are case sensitive).
- Console Rights (Operator) level user; login = Oper, password = Oper (both are case sensitive).

For security reasons, HP recommends that you use the `UC` command during the initial logon session to modify default passwords (enter **`CM`** at the `MP>` prompt, and enter **`UC`** at the `MP:CM>` prompt).

IMPORTANT Deleting default users such as Admin prevents you from using the HP Systems Insight Manager group actions feature.

Step 1. Log in using your MP user account name and password.

NOTE If you are logged in, the MP Main Menu displays. To follow this procedure, make sure you are at the MP Main Menu. Use **Ctrl-B** to return to the MP Main Menu.

Step 2. Use the MP menus and commands as needed. Main Menu commands are shown in "MP Main Menu". You can access commands not displayed in the MP Main Menu in command mode by first using the CM command at the MP prompt. You can display a list of available commands using the MP help function. Invoke the help function from either the MP Main Menu or the Command Menu prompts by entering **HE** followed by **LI**. You can return to the MP Main Menu by pressing **Ctrl-B**.

Step 3. Log out using the X command (enter **X** at the MP> prompt) after returning to the MP Main Menu.

MP Main Menu

Following are the MP Main Menu commands:

```
MP MAIN MENU:
       CO: Console
      VFP: Virtual Front Panel
       CM: Command Menu
       CL: Console Logs
       SL: Show Event Logs
      CSP: Connect to Service Processor
       SE: Create OS Session
       HE: Main Menu Help
        X: Exit Connection
```

NOTE The previous example shows the Main Menu screen accessed through the local serial or remote modem ports. The list of commands displayed might be different and depends on your method of access to the MP.

Configuring the Management Processor LAN Information

LAN information includes the management processor network name, IP address information, and configuring DHCP and DNS service information.

To configure the management processor LAN IP address:

Step 1. At the MP Main Menu prompt (`MP>`), enter **`CM`** to choose command mode.

Step 2. At the command mode prompt (`MP:CM>`), enter **`LC`** (for LAN configuration).

The screen displays the default values and asks if you want to modify them. It is good practice to write down the information, because you might need it for future troubleshooting. See "The LC Command Screen" on page 25.

NOTE The default value in the "IP address" field is set at the factory. You must configure the actual MP LAN IP address.

Step 3. The screen displays the current `LC` data. When prompted to enter a parameter name, `A to modify All`, or `Q to Quit`, enter **`A`** to choose all parameters.

Step 4. The screen displays the current DHCP status. If DHCP is used to acquire IP address information, enter **`E`** to enable, **`D`** to disable, or **`Q`** unless you are using the local serial port.

To disable DHCP from the local serial port:

a. Use the **`LC`** command to disable DHCP.

b. Commit the DHCP change.

c. Use the **`LC`** command again to set network parameters.

CAUTION Modifying the DHCP, IP address, gateway IP address, or subnet mask parameters will drop all present LAN and Web connections.

NOTE Changing DHCP status to Enabled or Disabled resets IP address, gateway IP address, and subnet mask parameters to factory default values.

NOTE If the IP address, gateway IP address, and subnet mask are obtained through DHCP, you cannot change them without first disabling DHCP.

Step 5. The screen displays the current IP address. When prompted to enter a new value or `Q`, enter the new IP address.

Step 6. The screen displays the current host name. When prompted to enter a new value or `Q`, enter the new MP network name.

This is the host name for the MP LAN displayed at the command prompt. It is also used to identify the MP LAN interface in a DNS database. The name can be up to 64 characters in length, and must start with a letter, end with a letter or number, and contain only letters, numbers, or dashes.

NOTE The host name is not case sensitive.

Step 7. The screen displays the current subnet mask name. When prompted to enter a new value or Q, enter the new subnet mask name.

Step 8. The screen displays the current gateway address. When prompted to enter a new value or Q, enter the new gateway address.

Step 9. The screen displays the current link state information. When prompted to enter a new value or Q, press **enter**. The message `-> Current Link State has been retained` displays.

Step 10. The screen displays the current Web console port number. When prompted to enter a new value or Q, press **enter**. The message `-> Current Web Console Port Number has been retained` displays.

Step 11. The screen displays the current SSH console port number. When prompted to enter a new value or Q, press **enter**. The message `-> Current SSH Console Port Number has been retained` displays.

NOTE SSH settings will not display if you do not have Integrated Lights-Out Advanced Pack licensing.

Step 12. The screen displays a new LC listing, including the values entered in the preceding steps. Verify that the desired values have been accepted. When prompted to enter a parameter for revision, Y to confirm, or Q to Quit, enter **Y** to confirm all parameters.

```
> LAN Configuration has been updated

-> Reset MP (XD command option 'R') for configuration to take effect.

MP Host Name: mpserver
```

Step 13. Enter **XD -reset** to reset the MP.

Step 14. After the MP resets, log in to the MP again. Then enter the MP command mode (enter **CM** at the MP: prompt).

Step 15. At the MP:CM> prompt, enter **LS** to confirm the new LAN settings.

Step 16. Enter **SA** to enable or disable Web console and telnet access after the MP has been reset.

The LC Command Screen

The following screen shows LC command output:

```
MP:CM> LC -nc
Current LAN Configuration:
     MAC Address             : 0x0060b0f54c51
     DHCP Status             : Enabled
     IP Address              : 127.1.1.1
     MP Host Name            : maestro
     Subnet Mask             : 255.255.248.0
     Gateway Address         : 127.1.1.1
```

```
     Link State              : Auto Negotiate
     Web Console Port Number : 2023
     SSH Access Port Number  : 22
     IPMI/LAN Port Number    : 626
LAN status: UP and RUNNING
-> Command successful.
MP:CM>
```

NOTE The SSH console port number does not display if you do not have Integrated Lights-Out Advanced Pack licensing.

Configuring DHCP and DNS

This section presents DHCP and DNS configuration information.

DHCP

The LC command enables a user to display and modify the LAN configuration.

The MP host name that can be set through this command is the one that is displayed at the MP command mode prompt. Its primary purpose is to identify the MP LAN interface in a DNS database.

NOTE The HPUX system name visible through a `uname -a` command is different than the 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), then a “delete old name” request for the old host name, and an “add name request” for the new host name is sent to the DDNS server.

If you change the DHCP status between Enabled and Disabled, then the IP address, subnet mask and gateway IP address are set to default values (127.0.0.1:0xffffff00). 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 portion of the DNS standard functionality.

Perform the following actions with the LC command to configure DHCP:

- Set all default LAN settings:

  ```
  MP:CM> LC -all DEFAULT -nc
  ```

- Display current LAN settings:

  ```
  MP:CM> LC -nc
  ```

- Modify MP DHCP status:

  ```
  MP:CM> LC -dhcp disabled (or LC -d d )
  ```

- Modify MP IP address:

  ```
  MP:CM> LC -i 15.1.1.1 (or LC -ip 15.1.1.1 )
  ```

- Modify MP host name:

  ```
  MP:CM> LC -h hostname (or LC -host hostname)
  ```

- Modify MP subnet mask:

  ```
  MP:CM> LC -s 255.255.255.0 (LC -subnet 255.255.255.0)
  ```

- Modify MP gateway address:

  ```
  MP:CM> LC -g 15.8.144.1 (or LC -gateway 15.8.144.1)
  ```

- Set link state to auto negotiate:

  ```
  MP:CM> LC -link auto (or LC -l a)
  ```

- Set link state to 10 BaseT:

  ```
  MP:CM> LC -link t
  ```

- Set Web console port address:

  ```
  MP:CM> LC -web 2023 (or LC -w 2023)
  ```

- Set SSH console port address:

  ```
  MP:CM> LC -ssh 22 (or LC -ss 22)
  ```

DNS

Use the DNS command to display and modify the DNS configuration as follows:

Step 1. At the MP Main Menu prompt (`MP>`), enter **`CM`** to choose command mode.

Step 2. At the command mode prompt (`MP:CM>`), enter **`DNS`** (for the DNS configuration).

Step 3. The screen displays `current DNS` data. When prompted to enter a parameter name, `A to modify All`, or `Q to Quit`, enter **`A`** to choose all parameters.

Step 4. The screen displays the current DHCP for DNS servers status. When prompted, enter **`Enabled`**, **`Disabled`**, or **`Q`**.

Step 5. The screen displays the current DHCP for DNS domain name status. When prompted, enter **`Enabled`**, **`Disabled`**, or **`Q`**.

Step 6. The screen displays the current register with DDNS server value. When prompted, enter, **`Yes`**, **`No`**, or **`Q`**.

Step 7. The screen displays the current DNS domain name. When prompted, enter a new value or **`Q`**.

Step 8. The screen displays the primary DNS server IP address. When prompted, enter a new value or **`Q`**.

Step 9. The screen displays the optional secondary DNS server IP address. When prompted, enter a new value or **`Q`**.

Step 10. The screen displays the optional tertiary DNS server IP address. When prompted, enter a new value or **`Q`**.

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     : 127.1.1.1
     2 - Secondary DNS Server IP   :
     3 - Tertiary DNS Server IP    :
Enter parameter(s) to revise, Y to confirm, or [Q] to Quit: Y
-> DNS Configuration has been updated
[mpserver] MP:CM>
```

Configuring LDAP

The following procedure shows how to configure the Management Processor to use a directory server to authenticate a user login. For a description of directory services and steps to configure the LDAP server, see Chapter 6, “MP Directory Services Installation and Configuration,” on page 63.

NOTE You can only use the LDAP feature if you have Integrated Lights-Out Advanced Pack licensing.

Step 1. At the MP Main Menu prompt (`MP>`), enter **`CM`** to choose command mode.

Step 2. At the command mode prompt (`MP:CM>`), enter **`LDAP`** (for the LDAP configuration).

Step 3. The screen displays the current `LDAP` data. When prompted to enter a parameter name, `A to modify All`, or `Q to Quit`, enter **`A`** to choose all parameters.

Step 4. The screen displays the current LDAP Directory Authentication status is displayed. When prompted, enter **`Enabled`**, **`Disabled`**, or **`Q`**.

Step 5. The screen displays the current Local MP User database status. If enabled, the local MP User database is used if there is an authentication failure using the LDAP Directory. When prompted, enter **`Enabled`**, **`Disabled`**, or **`Q`**.

NOTE This parameter must be enabled if LDAP Directory Authentication is disabled.

Step 6. The screen displays the current LDAP server IP address. When prompted, enter a new address or **`Q`**.

Step 7. The screen displays the current LDAP server port address. When prompted, enter a new port number or **`Q`**.

Step 8. The screen displays the current Object Distinguished Name. This specifies the full distinguished name of the MP device object in the directory service. For example, CN=RILOE2OBJECT, CN=Users, DC=HP, DC=com. Distinguished names are limited to 256 characters. When prompted, enter a new name or **`Q`**.

Step 9. The screen displays the current User Search Context 1. When prompted, enter a new search setting or **`Q`**.

NOTE The Context Settings 1, 2, and 3 point to areas in the directory service where users are located so the user does 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 128 characters each.

Step 10. The screen displays the current User Search Context 2. When prompted, enter a new search setting or **`Q`**.

Step 11. The screen displays the current User Search Context 3. When prompted, enter a new search setting or **`Q`**.

Following is the updated LDAP configuration:

```
New Directory Configuration (* modified values):
  * L - LDAP Directory Authentication: Enabled
    M - Local MP User database      : Enabled
  * I - Directory Server IP Address   : 127.1.1.1
    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
```

3 Connecting to the Management Processor

You can connect to the management processor directly through the local or remote RS-232C ports or through the LAN using telnet, SSH, or the Web GUI.

When connected by the serial ports or the LAN using telnet or SSH, you use the MP command line interface. You use the MP graphical user interface when connected through the Web.

The following sections in this chapter offer detailed instructions on how to connect to and interact with the MP:

- “Interacting with the MP Command Line Interface”
- “MP Welcome Screen”
- “Interacting with MP Through the Web”

Interacting with the MP Command Line Interface

To interact with the MP command line interface, perform the following steps:

Step 1. If you are connecting to MP through telnet or SSH, open a connection to MP using the IP address of the MP LAN port. You are automatically connected using the local or remote RS-232C ports.

Step 2. Log in using your MP user account name and password.

NOTE When logging in using the local or remote RS-232C ports, the login prompt might not display if another user is logged in through these ports. Use **Ctrl-B** to access the MP Main Menu and the MP prompt (`MP>`).

Step 3. Use the MP menus and commands as needed. You can display a list of available commands for the MP Main Menu by using the MP help function (in the MP Main Menu, enter **`HE`** followed by **`LI`** at the `MP HELP:` prompt). Log out using the `X` command (in the MP Main Menu, enter **`X`** at the `MP>` prompt) when done.

To display a list of available Command Menu commands, invoke help from within the Command Menu. Access the Command Menu by first using the `CM` command at the `MP>` prompt.

MP Welcome Screen

Following are the MP Welcome screen commands:

```
MP:CM> fw
*********************************************************************
*****                                                           *****
*****                    Firmware Update Utility                *****
*****                                                           *****
*****            (C) Copyright 2001 Hewlett-Packard Company     *****
*****                    All Rights Reserved                    *****
*****                                                           *****
*****            THIS PROGRAM IS NOT LICENSED TO CUSTOMERS      *****
*****                                                           *****
***** This program is intended for use by trained HP support    *****
***** personnel only. HP shall not be liable for any damages    *****
***** resulting from unauthorized use of this program. This     *****
***** program is the property of HP.                            *****
*****                                                           *****
*****                       Version 4.00                        *****
*****                                                           *****
*********************************************************************
                                      Flash     Current
Number    Cabinet   Name  Partition   Handle   Firmware Version  Comments
------ --------- -------- ---------- -------- ------------------ --------
1              0     MP 0          0        0           5.010    Master
2              0     MP 1          1        1           5.010    Slave
3              0   PDHC 0          0      256           3.006      -
4              0    SFW 0          0      320           0.018      -
5              0   PDHC 1          1      257           3.006      -
6              0    SFW 1          1      321           0.018      -
7              0   PDHC 2         -1      258           3.006      -
8              0    SFW 2         -1      322           0.018      -
9              0   PDHC 3         -1      259           3.006      -
10             0    SFW 3         -1      323           0.018      -

Enter the Entities to be upgraded (Ex: 3,4,10) :2
Enter your user name: anonymous
Enter your user password: ********
Enter the ip address where the firmware can be found: 192.1.1.1
Enter the path where the firmware can be found: /dist/version1
Enter the filename of the firmware image for the MP: mp_A.5.11.0.bin
Are you sure that you want to continue(Y/N): y
```

You can access commands not displayed in the MP Main Menu in command mode by first using the `CM` command at the `MP>` prompt.

MP commands are described in Chapter 5, “Command Menu Interface Reference.”

Management Processor Help System

The MP has a robust help system. To invoke MP help, enter **`HE`** after the `MP>` prompt. Following is the MP help menu:

```
HE

==== MP Help: Main Menu ============================================

Hardware Revision a1 Firmware Revision E.02.20 May 30 2003,15:18:47

Integrated Lights-Out for HP Integrity and HP 9000 - Management Processor (MP)

                        MP Help System

Enter a command at the help prompt:
```

```
          OVerview  : Launch the help overview
          LIst      : Show the list of MP 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
Enter one of the commands described above:
```

You can display a list of available commands by entering **LI** at the `MP Help:` prompt. You can return to the MP Main Menu by typing **Q**.

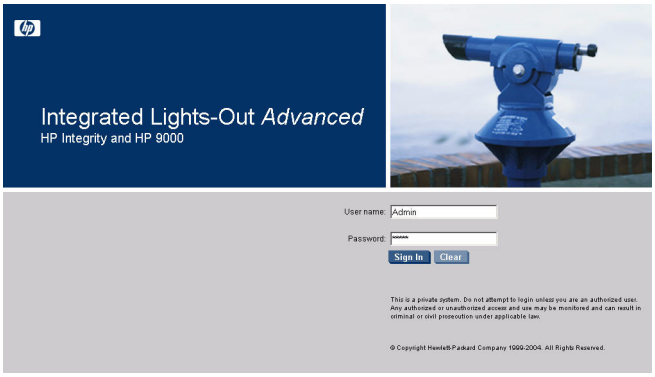
Interacting with MP Through the Web

To interact with the MP graphical user interface, perform the following steps:

Step 1. Open a connection using the MP LAN port IP address.

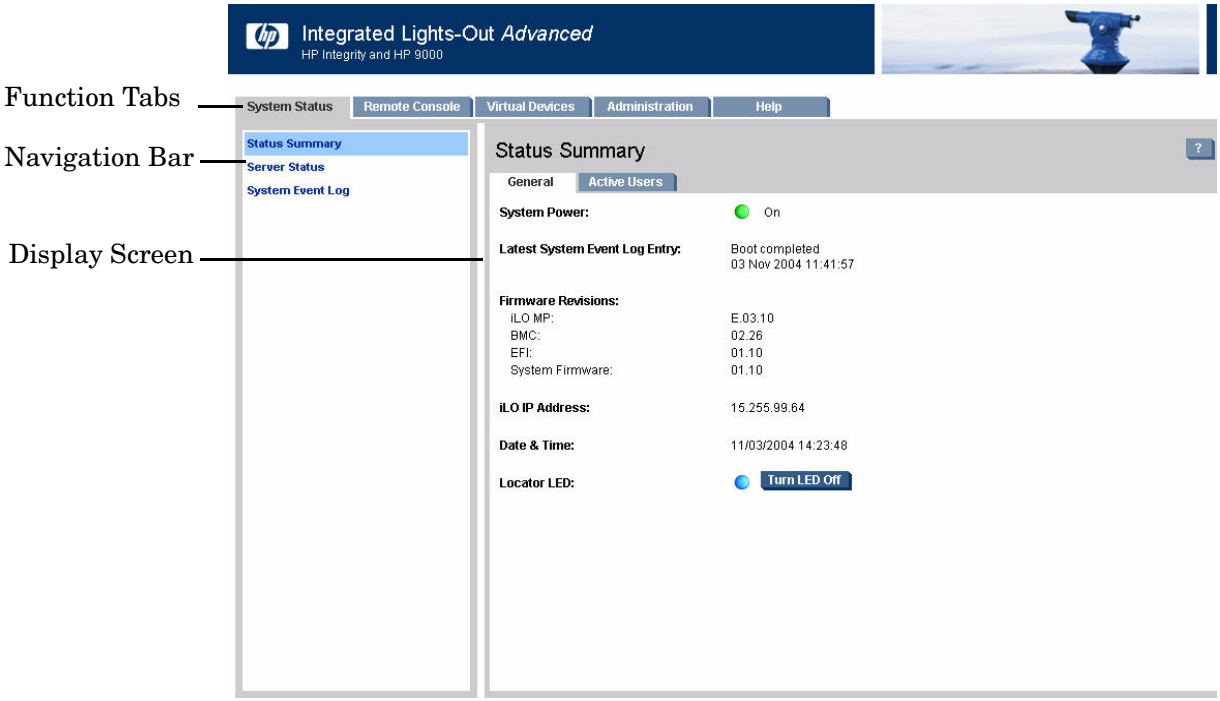
Step 2. Log in using your MP user account name and password at the login page (Figure). Click **Sign In**.

Figure 3-1 Web Login Page



The System Status Summary page displays after login (Figure). Choose Web interface functions by clicking the Function tabs at the top of the page. Each function lists options in the Navigation Bar on the left side of the page. Click an option link to display data in the Display Screen. Click Refresh to update the display.

Figure 3-2 Status Summary Page



The MP Web interface has a robust help system. To invoke MP help, click the Help tab to display help information in the Display Screen. Click the **?** at the top right corner of each page to display help about that page.

For a description of the Web interface, see Chapter 4, “Web Interface Summary.”

4 Web Interface Summary

The following sections in this chapter describe the features and functions of the MP Web interface:

- “System Status”
- “Remote Console”
- “Virtual Devices”
- “Administration”

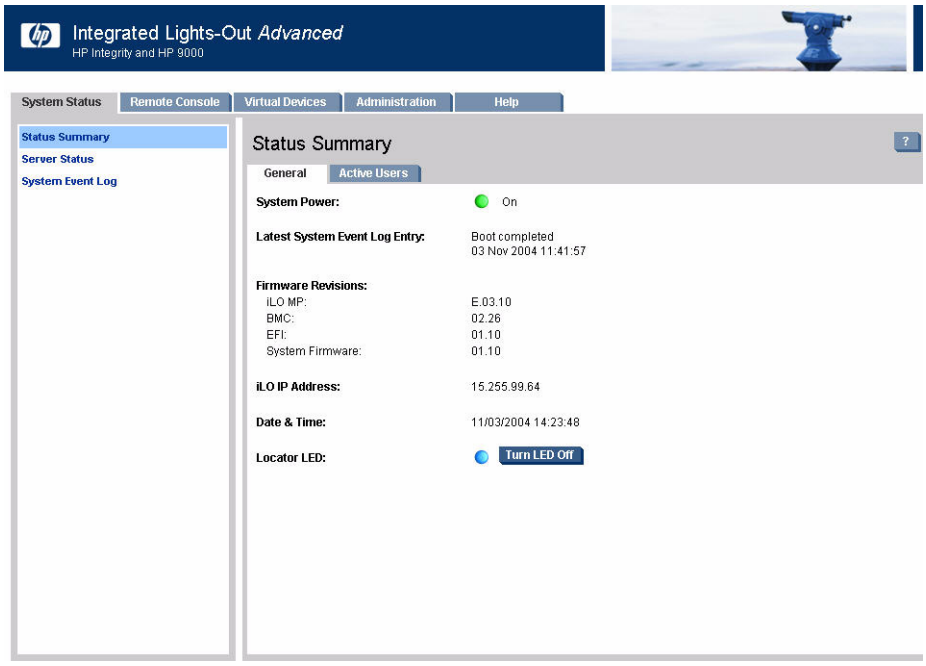
Web Interface Description

The following describes the functions and options of the Web interface.

System Status

The System Status Summary page (Figure 4-1) includes the following options to display server information:

Figure 4-1 System Status Summary Page



System Status > Status Summary > General

This page displays a brief status summary of the system:

- System Power status
- Latest System Event Log Entry
- Firmware Revisions
- iLO IP Address
- Date & Time
- Locator LED status

System Status > Status Summary > Active Users

This page displays information about the users currently logged in to MP.

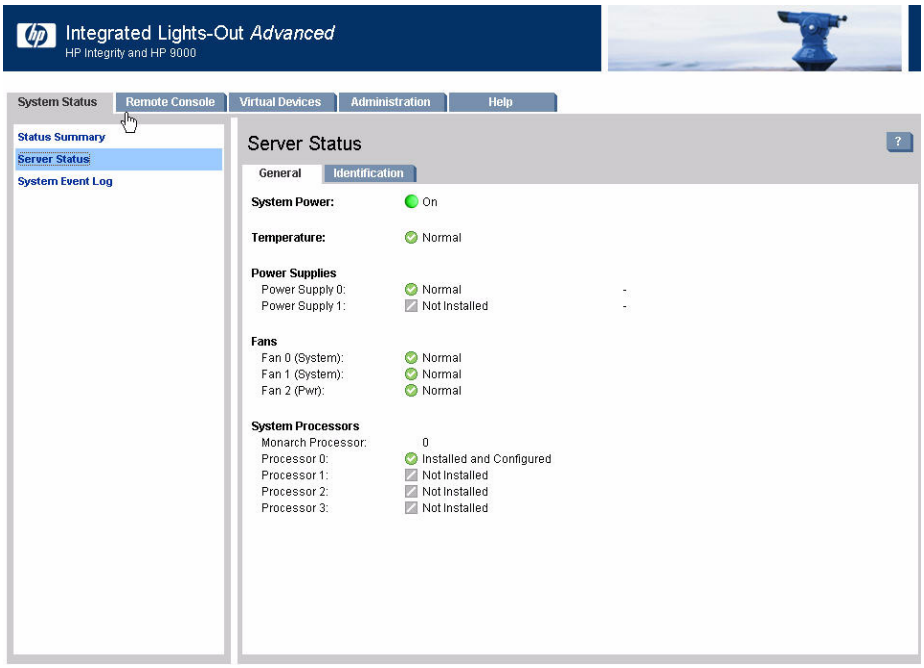
The Disconnect button enables a user with sufficient privileges to disconnect users of a certain access type.

System Status > Server Status > General

This page (Figure 4-2) displays a brief status summary of the server:

- System Power status
- Temperature
- Power Supplies
- Fans
- System processors

Figure 4-2 System Status > Server Status Page



System Status > Server Status > Identification

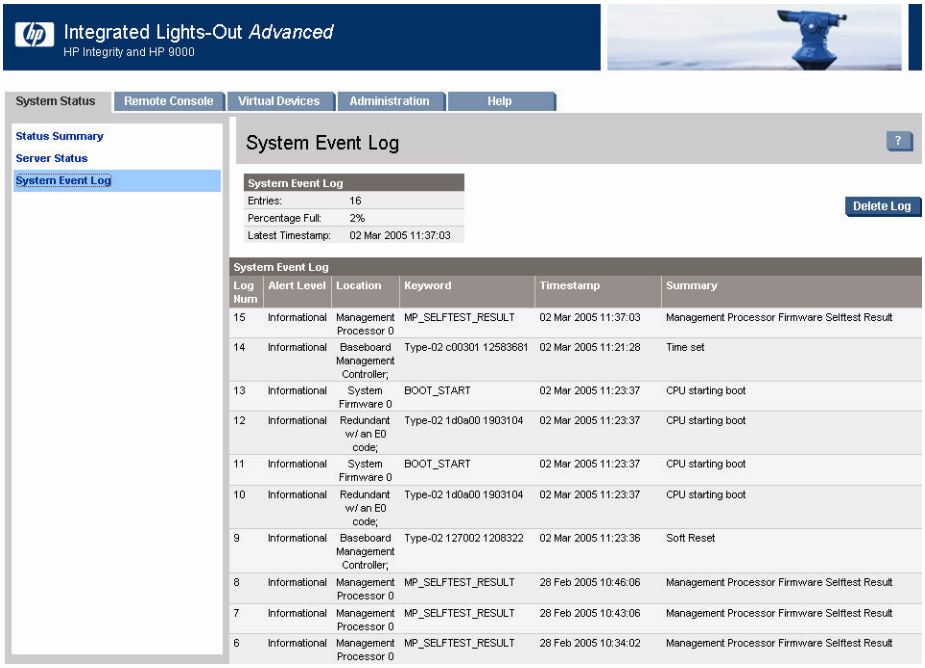
This page enables you to configure system information, such as host name (default is “uninitialized”), and enter relevant details, such as location, rack ID, and position. You can also store the name, telephone number, email, and pager number of a contact person.

System Status > System Event Log

This page (Figure 4-3) enables a user to view the contents of the event logs that have been stored in nonvolatile memory. A user with login rights can view the system event log. Only a user with MP Configuration Access can clear the logs.

The system event log contains priority events and errors. Reading the system event log turns off the attention LED (or blinking yellow light on the system LED).

Figure 4-3 System Status > System Event Log Page



Remote Console

Remote Console > Remote Serial Console

Remote Serial Console enables a user with console access to securely view and manage a server. You can click **View Console** to connect to the system console. Using this feature you can view and interact with the boot sequence of your server, perform maintenance activities in text mode, and manage non-graphical mode operating systems.

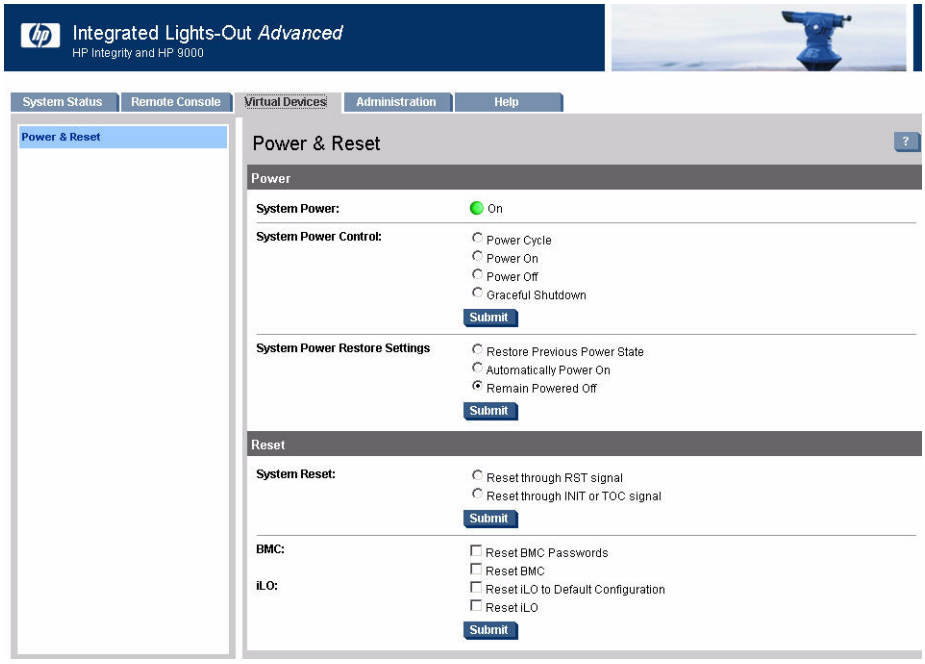
Console output is mirrored to all users in console mode. Only one of the mirrored users at a time has write access to the console. To get console write access, type **Ctrl-Ecf**. Type **Ctrl-B** or **Esc-(** to return to the Main MP Menu on the Text User Interface.

Virtual Devices

Virtual Devices > Power & Reset

The Virtual Devices Page (Figure 4-4) enables you to view and control the power state of the server. It also provides you with options to reset the system, the BMC, or the MP.

Figure 4-4 Virtual Devices Page



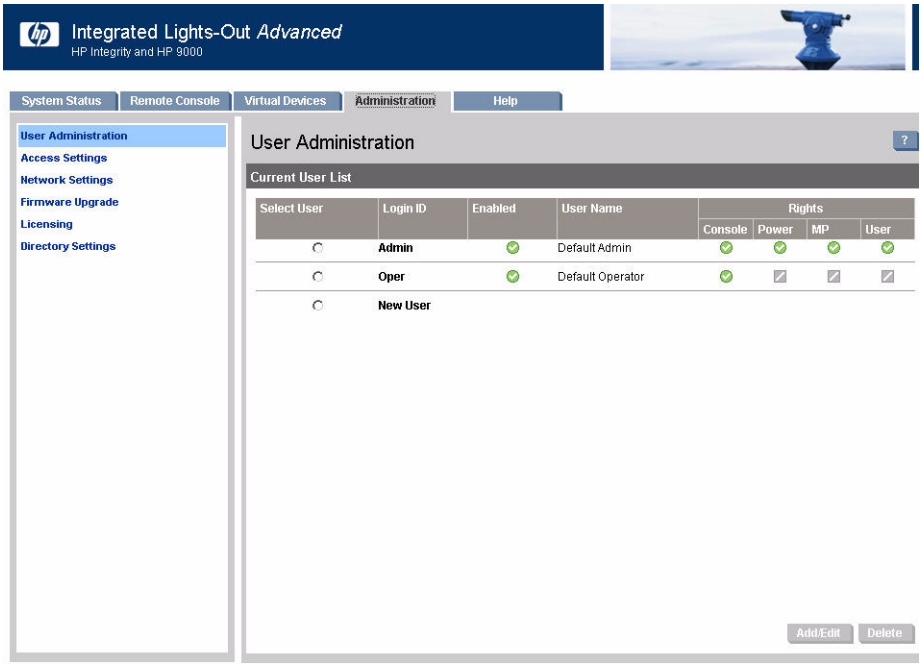
- System Power: The current power state of the system.
- System Power Control: A user with Power Control Access can issue options for remote control of the system power.
- System Reset: A user with Power Control Access can issue any of the following signals to reset the system: RST, INIT, or Transfer of Control (TOC).
- BMC: A user with MP Configuration Access can issue a BMC reset or reset the Operator or Admin passwords.
- iLO: A user with MP Configuration Access can issue this option to set all MP parameters back to their default values.

Administration

Administration >User Administration

The User Administration page (Figure 4-5) displays the current list of users, their privilege rights, and whether they are enabled or disabled. There are two default users: Admin and Oper. The Admin user has all five rights (L, C, P, M, and U), and the Oper user has the Login and Console Access rights by default. The Add/Edit and Delete buttons enable users with User Administration Access to modify the user configuration of the MP: add new users, and modify or delete existing users.

Figure 4-5 User Administration Page

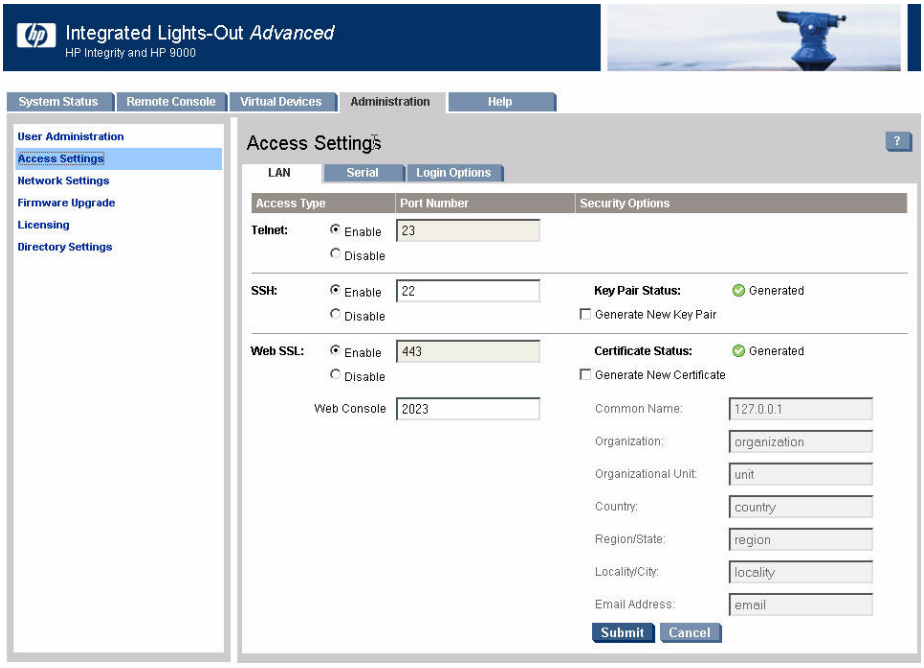


Administration > Access Settings > LAN

A user with MP Configuration Access can use the following options on the Administration > Access Settings Web page (Figure 4-6) to modify the LAN settings:

- Telnet: These options are used to enable or disable telnet access to MP.
- SSH: SSH is one of the advanced features that can be used only in the presence of a license.
- SSL: The Web SSL access to MP can be enabled or disabled using the enable or disable option. In order to make an SSL connection, you need to generate a certificate. The certificate status indicates if a certificate has been generated previously. To generate a new certificate, fill in the fields shown and check **Generate New Certificate**.

Figure 4-6 Administration > Access Settings Page



Administration > Access Settings > Serial

This option enables a user with MP Configuration Access to set the serial port parameters.

Administration > Access Settings > Login Options

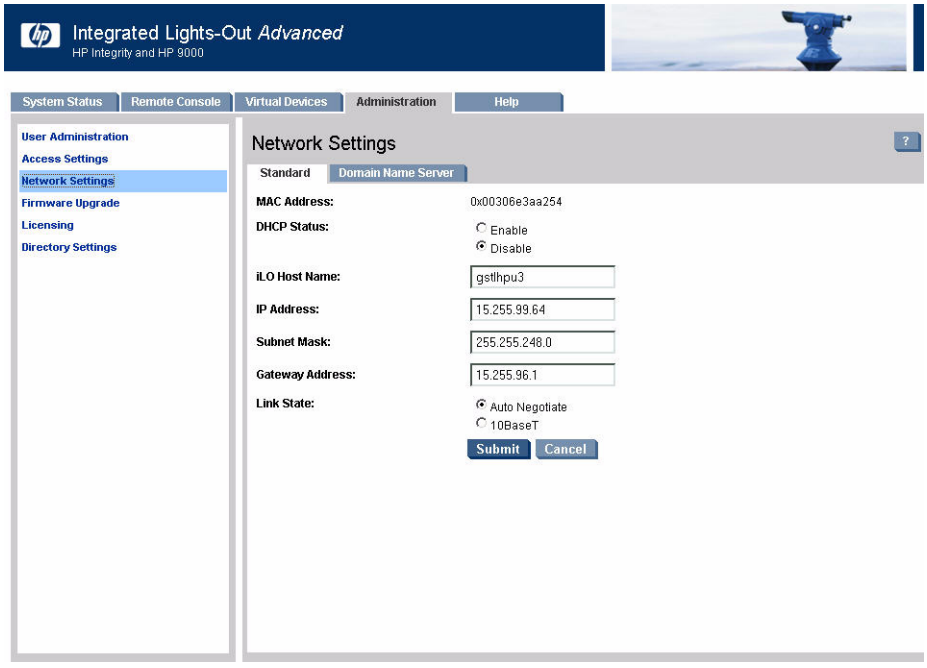
A user with MP Configuration Access can modify the security options of MP from this page.

- Login Timeout in Minutes: The timeout value in minutes is effective on all ports, including local ports.
- Password Faults Allowed: This sets a limit on the number of password faults allowed when logging into MP. The default number of password faults allowed is three.

Administration > Network Settings

The Network Settings page (Figure 4-7) enables you to configure the network settings. Only users with MP Configuration Access can configure the network settings.

Figure 4-7 Administration > Network Settings Page



Administration > Network Settings > Standard A user with MP Configuration access rights can modify the LAN configuration.

The configurable parameters are:

- MAC Address: The 12 digit (hexadecimal) MAC address.
- DHCP Status: Enable/Disable.
- ILO Host Name: The host name set here is displayed at the MP command interface prompt.
- IP Address: The MP IP address. If DHCP is being used, the IP address is automatically supplied.
- Subnet Mask: The subnet mask for the MP IP network. If DHCP is being used, the subnet mask is automatically supplied.
- Gateway Address: The IP address of the network gateway. If DHCP is being used, the gateway IP address is automatically supplied.
- Link State: Auto Negotiate or 10BaseT option.

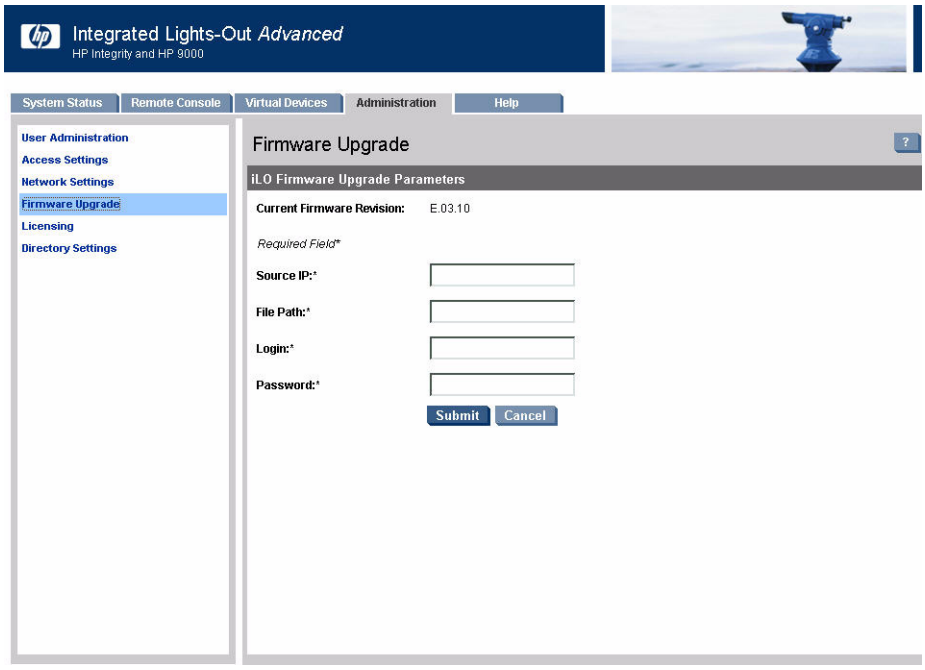
Administration > Network Settings > DNS The DNS page enables a user with MP Configuration Access to configure the DNS server settings. It is only meaningful when used with DHCP enabled. Using this page, a user can configure the domain name and up to three DNS servers either manually or automatically through DHCP. It further enables a DDNS update through the primary DNS server as long as it is authoritative for the zone.

- Use DHCP supplied domain name: Use the DHCP server-supplied domain name.
- Domain name: This represents the DNS suffix of the subsystem, for example, “hp.com” in “ilo.hp.com”.
- Use DHCP supplied DNS servers: Use the DHCP server-supplied DNS server list.
- Register with Dynamic DNS: Register its name with a DDNS server.

Administration > Firmware Upgrade

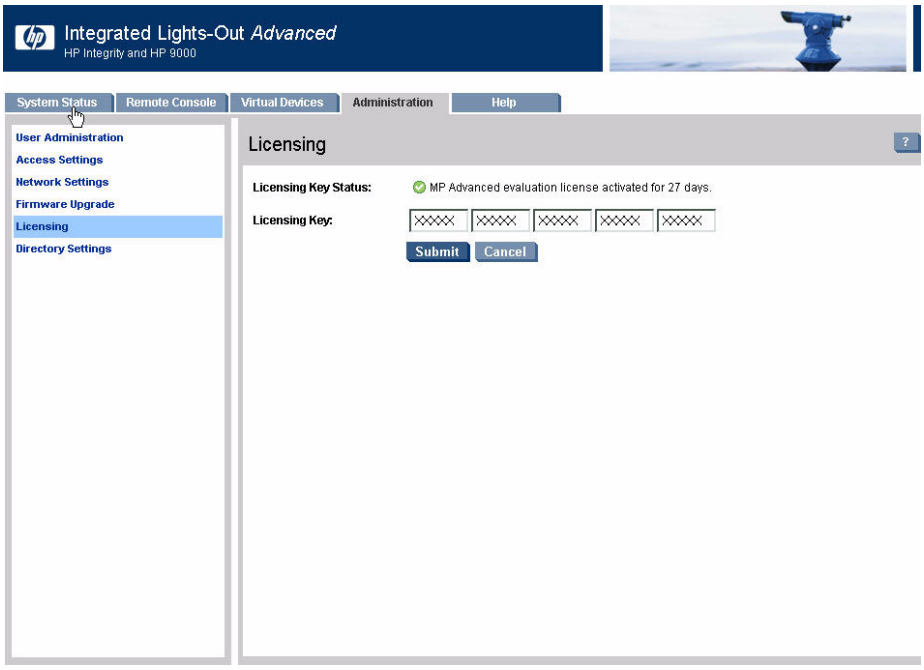
The Firmware Update page (Figure 4-8) enables a user with MP Configuration Access to remotely upgrade the firmware from an FTP source.

Figure 4-8 Administration > Firmware Upgrade Page



Administration > Licensing The Licensing page (Figure 4-9) enables you to enter a license key to enable the Integrated Lights-Out Advanced Pack features. MP offers some advanced features, which can be used only in the presence of a license.

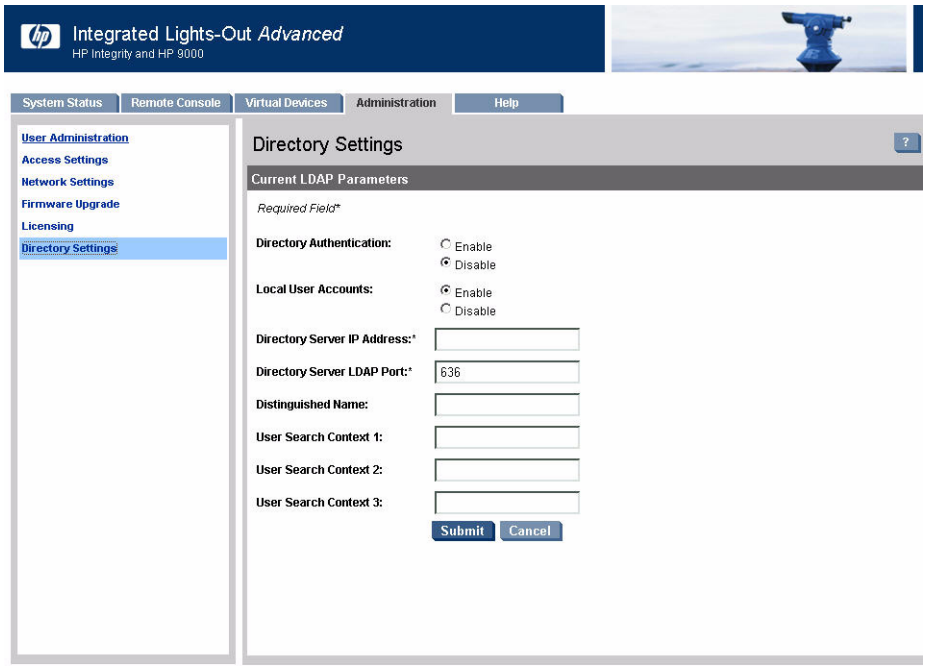
Figure 4-9 User Administration > Licensing Page



- Directory-based authentication and authorization
- SSH access
- Group actions through HP Systems Insight Manager

Administration > Directory Settings The Directory Settings page (Figure 4-10) enables users with the MP Configuration Access to edit the following directory parameters.

Figure 4-10 Administration > Directory Settings Page



- Directory Authentication: Choosing Enable/Disable, activates or deactivates directory support on this MP.
- Local User Accounts: Includes or excludes access to local MP user accounts.
- Directory Server IP Address: IP address of the directory server.
- Directory Server LDAP Port: Port number for the secure LDAP service on the server.
- Distinguished Name: Distinguished Name of the MP, specifying where this MP instance is listed in the directory tree.
- User Search Contexts (1,2,3): User name contexts that are applied to the login name entered to access MP.

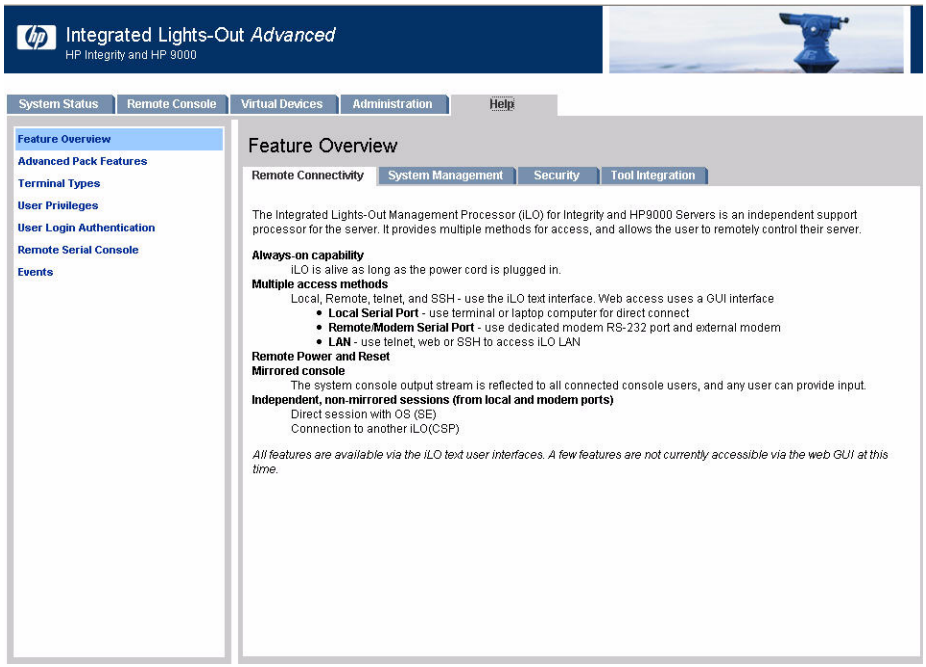
Help

The iLO Help page (Figure 4-11) is divided into four subtabs that represent different iLO functions: Remote Connectivity, System Management, Security, and Tool Integration. You can choose the following help topics for each of the four iLO functions:

- Feature Overview
- Advanced Pack Features
- Terminal Types
- User Privileges
- User Login Authentication
- Remote Serial console

- Events

Figure 4-11 Help Page



5 Command Menu Interface Reference

There are two menus from which commands can be executed: the MP Main Menu and the Command Menu. You access the Command Menu by first using the `CM` command at the `MP>` prompt.

The following sections provide a reference for commands available through the command line interface:

- “MP Main Menu Commands”
- “Command Menu Commands”

MP Main Menu Commands

Commands are listed in the Table 5-1 and described in the following paragraphs.

Table 5-1 MP Main Menu Commands and Descriptions

Command	Description
CL	View console log
CM	Enter command mode
CO	Select console mode
CSP	Connect to another service processor
HE	Display help for menu or command
SE	Enter OS session
SL	Show event logs
VFP	Display virtual front panel
X	Exit

MP Main Menu Command Summary

CL: Console log—view the history of the console output

This command displays up to 60 KB of console data (about 60 pages of display in text mode) sent from the SPU 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 end of the buffer. You can control the starting point from which the data displays and navigate through the data.

What is displayed is an image of the console history at the time the CL command is entered. Console output continues to be logged while this buffer is read, and nothing is lost.

CM: Command Mode—enter command mode

This command switches the console terminal from the MP Main Menu to mirrored command interface mode. Both access to command mode and command execution are controlled independently by user access rights. If a command is in progress, a message is displayed warning the new user of system status.

CO: Console—leave command mode and enter console mode

This command switches the console terminal from the MP Main Menu to mirrored/redirected console mode. All mirrored data is displayed. Type either **Ctrl-B**, or **Esc** and then **+** to return to the MP command interface.

CSP: Connect to remote management processor over the LAN

This command enables the local or remote port user to connect over the MP LAN to another MP on the network. The user that launches the command is given a private connection to the other MP over the LAN. To return to the original MP, type **Ctrl+]** to disconnect the CSP session.

HE: Display help for menu or command

This command displays the MP hardware and firmware version identity, and the date and time of firmware generation. If executed from the MP Main Menu, it displays general information about the MP, and those commands available in the MP Main Menu. If executed in command mode, this command displays a list of command interface commands available to the user. It also displays detailed help information in response to a topic or command at the help prompt.

SE: Log in to the system on a local or remote port

This command enables you to leave the MP Main Menu and enter a system session. Two sessions can be active simultaneously: one each for the local and remote ports.

To return to the Main Menu, exit the user session. The MP reconnects the console to the Main Menu after the driver releases the connection.

The MP regularly checks the activity of the session. If nothing has happened since the inactivity timer was started, then the connection with the system is closed (modem signals are dropped), and the port returns to the Main Menu. This inactivity timer cannot be disabled, because this is the only means for a local port to leave the session if the session is hung.

When the local or remote operator enters the SE command, a 10-second timer is started. If the system fails to initiate a session (above the corresponding 16550 UART) within that time period, the SE command relinquishes control of the port and keeps the operator in the Main Menu.

If the system and the MP local or remote ports have been configured with different port speeds, the UART connected to the remote modem is configured to operate at the speed defined by the operating system (OS).

SL: Display contents of the system status logs

This command displays the contents of the event logs that have been stored in nonvolatile memory.

- System event log (SEL)—Events (filtered by alert level) and errors
- Forward progress—All events
- Current boot log—All events between “start of boot” and “boot complete”
- Previous boot log—The events from the previous boot

Reading the system event log turns off the system LED. Accessing this log is the only way to turn off the system LED when it is flashing and alerts have not been acknowledged at the alert display level.

Events are encoded data that provide system information to the user. Some well-known names for similar data would be chassis codes or post codes. Events are produced by intelligent hardware modules, the OS, and system firmware. Use SL to view the event log.

Navigate within the logs as follows:

- + — View the next block (forward in time)
- - — View the previous block (backward in time)
- Enter (<CR>) — Continue to the next or previous block
- D — Dump the entire log for capture or analysis
- F — First entry
- L — Last entry
- J — Jump to entry number __

- H — View mode configuration (hex)
- K — View mode configuration (keyword)
- T — View mode configuration (text)
- A — Alert level filter options
- U — Alert level unfiltered
- Q — Quit and return to the Event Log Viewer Menu
- V — View mode configuration (text, keyword, hex)
- ? — Display this help menu
- Ctrl-B — Exit command, and return to the Main Menu

Table 5-2 defines alert (or severity) levels.

Table 5-2 Alert Levels

Severity	Definition
0	Minor forward progress
1	Major forward progress
2	Informational
3	Warning
5	Critical
7	Fatal

VFP: Display virtual front panel

The `VFP` command presents a summary of the system by using direct console addressing. If the terminal is not recognized by the MP, VFP mode is rejected. Each individual user gets this summary in order to avoid issues related to terminal type and screen display mode.

X: Exit MP

This command exits users from the Main Menu. If the terminal is the local serial port, then users return to the login prompt. For all other types of terminals, users are disconnected from the MP session.

Command Menu Commands

Commands are listed in Table 5-3 and described in the following paragraphs.

Table 5-3 Command Menu Commands and Descriptions

Command	Description
BP	Reset BMC passwords
CA	Configure async or serial ports
DATE	Display the current date
DC	Default configuration
DF	Display field replaceable unit (FRU) information
DI	Disconnect remote or LAN console
DNS	Set DNS configuration
FW	Upgrade MP firmware
HE	Display help for menu or command
ID	Display or modify system information
IT	Modify MP inactivity timers
LC	LAN configuration
LDAP	LDAP configuration
LM	License management
LOC	Display and configure locator LED
LS	LAN status
MR	Modem reset
MS	Modem status
PC	Remote power control
PG	Paging parameter setup
PR	Power restore
PS	Power management module status
RB	Reset BMC
RS	Reset system through RST signal
SA	Set access options
SO	Configure security options

Table 5-3 Command Menu Commands and Descriptions (Continued)

Command	Description
SS	Display system processor status
SYSREV	Display all firmware revisions
TC	Reset through transfer of control (TOC)
TE	Tell (send a message to other users)
UC	User configuration
VDP	Display virtual diagnostic panel LEDs
WHO	Display connected management processor users
XD	Diagnostics or reset of management processor

Command Menu Command Summary

BP: Reset BMC passwords

This command resets baseboard management control (BMC) passwords (both USER and ADMIN passwords).

CA: Configure local and remote serial port parameters

Set up the local serial port parameters as follows:

- BAUD RATES: Input and output data rates are the same — 4800, 9600, 19200, 38400, 115200 bit/sec.
- FLOW CONTROL: Hardware uses RTS/CTS; software uses Xon/Xoff.

Set up the remote serial port parameters as follows:

- MODEM PROTOCOL: Bell or CCITT. (CCITT is a European standard; RTS/CTS signaling is used, as well as the Ring signal. Bell is a U.S. or simple mode.)
- BAUD RATES: Input and output data rates are the same — 4800, 9600, 19200, 38400 bit/sec.
- FLOW CONTROL: Hardware uses RTS/CTS; software uses Xon/Xoff.
- TRANSMIT CONFIGURATION STRINGS: Disable this setting whenever the modem being used is not compatible with the supported modem (MT5634ZBA).
- MODEM PRESENCE: When the modem might not always be connected, set this parameter to “not always connected.”

  Example: A modem attached through a switch. In mode “not always connected,” no dial-out functions are allowed: DIAL-BACK is disabled, and PAGING is not possible.

The MP mirrors the system console to the MP local, remote/modem, and LAN ports. One console output stream is reflected to all of the connected console users. If several different terminal types are used simultaneously by the users, some users might see unexpected results.

DATE: Display the current date

This command displays the current date, as best known to the MP. The usual source for the date is from the BMC, but if the BMC date is not available, the MP real-time clock is used. The real-time clock is only used when the MP is first powered on or rebooted, until it can obtain the correct date from the BMC.

DC: Default configuration—reset all MP parameters to the default configuration

This command sets all MP parameters back to their default values. The following parameters are reset:

```
Remote Console Serial Port Modem configuration: CA -remote DEFAULT
MP IP configuration                           : LC -all DEFAULT
Remote Access Configuration                   : SA -all DEFAULT
Command Interface configuration               : IT -all DEFAULT
MP Security configuration                     : SO -opt DEFAULT
MP Session configuration                      : IT -all DEFAULT
MP User configuration                         : UC -all DEFAULT
MP LDAP directory configuration               : LDAP -all DEFAULT
MP Paging configuration                       : PG -text DEFAULT
```

Use any of the following methods to reset passwords in the MP:

- In the UC command, change individual users or reset all users to default values.
- In the DC command, choose “Reset Security Configuration”.
- Reset passwords by pressing the MP reset button on the back panel of your HP server. After the MP reboots, the local console terminal displays a message for 5 seconds. Responding to this message in time allows a local user to reset the passwords.

NOTE All user information (logins, passwords, and so on) is erased using any of the previous reset methods.

DF: Display FRUID information

This command displays FRUID information from the BMC for FRU devices. Information provided includes serial number, part number, model designation, name and version number, and manufacturer.

DI: Disconnect remote/modem or LAN/WEB console

This command disconnects (hangs up) remote/modem, telnet, Web SSL, or SSH users from MP. It does not disable the ports. The remote console is no longer mirrored.

DNS: Set DNS configuration

This command enables you to configure the DNS server settings, whether DHCP is enabled or disabled.

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

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

FW: Activates MP firmware upgrade mode

This command activates the upgrade mode. This command is only available from the LAN port and the local serial port.

The upgrade is performed through the MP LAN by FTP, which must be operational. Information required for the upgrade needs to be entered through the FW command interface.

CAUTION If the upgrade process is interrupted at any time, the core I/O needs to be repaired or replaced.

The MP is reset at the end of the upgrade process.

HE: Display help for menu or command

This command displays the MP hardware and firmware version identity, and the date and time of firmware generation. If executed from the MP Main Menu, this command displays general information about the MP, and those commands available in the MP Main Menu. If executed in command mode, this command displays a list of command interface commands available to the user. It also displays detailed help information in response to a topic or command at the help prompt.

ID: Display or modify system information

This command enables the user to display and modify the following:

- SNMP contact information
- SNMP server information
- SPU host name

NOTE The SPU host name information is not retained across MP reboots.

IT: Modify MP inactivity timers

The session inactivity timeout prevents sessions to the system from being inadvertently left open. You can start a session by using the SE command or by dialing into the modem port if it is configured for O/S SESSION. An open session can prevent users from logging in to the MP through the port and can also prevent system applications from initiating an outbound connection. The inactivity timeout also prevents a session from being locked indefinitely if the system session is hung or if the system OS is hung. You cannot deactivate the session inactivity timeout.

The MP command interface inactivity timeout prevents a user from inadvertently keeping the MP locked in MP command mode. Other users are prohibited from entering commands if the MP is locked in MP command mode. You cannot deactivate the MP command interface inactivity timeout. 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:

- Session inactivity timeout: 1 to 1440 minutes (default is 60 minutes).
- MP 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 0, then no timeout is applied. A mirroring flow control condition ceases when no flow control condition exists on any port.

LC: LAN configuration (IP address, and so on)

This command displays and allows modification of the LAN configuration. Configurable parameters include:

- MP IP address
- DHCP status
- MP host name

- Subnet mask
- Gateway IP address
- Web console port number
- Link state
- SSH access port number

The MP host name set in this command is displayed at the MP command mode prompt. Its primary purpose is to identify the MP LAN interface in a DNS database.

If the IP address, gateway IP address, or subnet mask was obtained through DHCP, then you cannot change it without first disabling DHCP. If you change the host name, and the IP address was obtained through DHCP and DDNS is registered, then a delete old name request for the old host name and an add name request for the new hostname are sent to the DDNS server.

If you change the DHCP status to either Enabled or Disabled, then the IP address, subnet mask, and gateway address are set to their default values (127.0.0.1:0xffffff00). Also 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 Enabled to Enabled, the DNS parameters for DHCP are set to Enabled, and the Register with DDNS parameter is set to Yes.

LDAP: LDAP configuration This command displays and allows modification of the following LDAP directory settings:

- LDAP Directory Authentication (Enable or Disable): Designates whether a directory server is used to authenticate a user login.
- Local MP User database (Enable or Disable): Specifies whether the local MP User database is used in case of authentication failure through the LDAP Directory. Has to be enabled if LDAP is disabled.
- Directory server IP address: Designates the IP address of the directory server. This setting is required if you use directory services for user authentication.
- Directory server LDAP port: Designates the port used for LDAP communications.
- Object Distinguished Name (DN): Specifies the full distinguished name of the MP device object in the directory service. For example, CN=RILOE2OBJECT, CN=Users, DC=HP, DC=com. Distinguished names are limited to 256 characters.
- Directory User Search Context 1, 2, 3: Specify search contexts when authenticating a user. These settings point to areas in the directory service where users are located so the user does 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 128 characters each.

LM: License management

This command displays the current license status. Use it to enter a license key to enable the following features:

- Directory-based authentication and authorization
- SSH (secure shell)
- Group actions through Systems Insight Manager

LOC: Locator LED status

This command displays the current status of the locator LED.

LS: LAN status

This command displays all parameters and the current status of the MP LAN connections. The LAN parameters are not modified by the execution of this command.

MR: Modem reset

This command makes the MP send an `AT Z` command to the modem, which resets it. Any modem connections are lost. You can view the initialization results by using the `MS` command.

MS: Modem status—display modem status

This command displays the state of the modem lines connected to the remote/modem serial port. Update the display by pressing **Enter**. The `MS` command displays the current state of the status signals DCD, CTS, DSR, RI and the last state of the control signals DTR, and RTS set by the firmware.

PC: Power control—turn system power on and off

This command enables you to switch the system power on or off. A power cycle option is available that provides a 30-second delay between system power on and power off.

For proper system shutdown, shut down the OS before issuing this command, or use the `PC` command's graceful shutdown option.

NOTE This is roughly equivalent to turning the system power off at the front panel switch. There is no signal sent to the OS to bring the software down before power is turned off. To turn the system off properly, you must ensure that the OS is in the proper shutdown state before issuing this command. Use the proper OS commands or use the graceful shutdown option of the `PC` command.

PG: Paging parameter setup

This command enables you to configure the pagers and set triggering events.

A string description of the triggering event is sent with the page.

PR: Power restore policy configuration

Use this command to configure the power restore policy. The power restore policy determines how the system or chassis behaves when AC power returns after an AC power loss.

If PR is set to On, the system powers on after AC is applied. If PR is set to Off, the system stays powered off after AC is applied. You must first push the system power switch or execute a PC command to power on the system.

If PR is set to Previous, the power is restored to the state that was in effect when AC was removed or lost.

PS: Power status

This command displays on the console the status of the power management module.

RB: Reset BMC

This command resets the BMC by toggling a GPIO pin.

RS: Reset system through RST signal

IMPORTANT Under normal operation, shut down the OS before issuing the RS command.

This command causes the system (except the MP) to be reset through the RST signal.

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

SA: Set access options

This command configures access for LAN telnet, SSH, IPMI over LAN, remote/modem ports, and Web SSL.

If remote/modem, LAN or Web users are connected at the time a disable from this command is executed, then they are disconnected. Any future incoming connection request to the corresponding port is rejected.

SO: Configure security options and access control

This command monitors and changes systemwide security parameters.

The following are SO 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 (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.
- Number of Password Faults allowed: 1 to 10. This parameter defines the number of times a console can attempt to login before being rejected and having its connection closed.
- Web based to use SSL: Enabled/Disabled.
- Firmware upgrade: enables firmware upgrade from the EFI console of the server.
- MP reset: enables an MP reset through IPMI (from BMC, system, or IPMI over LAN).
- MP password reset: enables MP password reset through IPMI (from BMC, system, or IPMI over LAN).

SS: Displays the status of the system processors

This command displays the status of the system processors and which processor is the monarch.

SYSREV: Display all firmware revisions

This command displays current revisions of firmware in the system.

The following is an example of the SYSREV command output:

```
MP:CM> SYSREV

Current firmware revisions

MP  FW    : E.02.06

BMC FW    : 01.20

EFI FW    : 01.22

System FW : 01.40
```

TC: System reset through INIT or TOC (Transfer of Control) signal

Under normal operation, shut down the OS before issuing this command.

This command causes the system to be reset through the INIT (or TOC) signal. Execution of this command irrecoverably halts all system processing and I/O activity and restarts the computer system. It is different from the RS command in that the processors are signaled to dump state on the way down.

TE: Tell—send a message to other terminals

You can type a message of up to 255 characters. The message is broadcast to the other mirrored clients. Users in a session or CSP are not shown the message.

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

UC: User Configuration—controls user access

This command is used to enable an administrator to add, modify, re-enable, or delete any of the following user parameters:

- Login ID
- Password
- User Name
- User Workgroup
- User Access Rights
- User Operating Mode
- User Enabled
- Modem Dial-back
- Modem Dial-back Phone

All users have the right to log in to MP and to execute “Status” or “Read-only” commands (view event logs, check system status, power status, and so on) but not to execute any commands that would alter the state of MP or the system.

The commands available to all users are: CL, CSP, DATE, DF, HE, LS, MS, PS, SL, SS, SYSREV, TE, VFP, VDP, WHO, XD (status options)

An MP user can also have any (or all) of the following rights:

- Console Access: Right to access the system console (the host OS). This does not bypass host authentication requirements, if any.

  Commands: CO, SE

- 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 MP settings (as well as some system settings, such as the power restore policy).

  Commands: BP, CA, CG, CL (clear option), DC, DI, FW, ID, IT, LC, LDAP, LOC, MR, PG, RB, SA, SL (clear option), SO, XD (MP reset option)

VDP: Display virtual diagnostics panel LEDs

This command monitors the LEDs on the diagnostics panel.

NOTE This command is restricted to rx4640 and rp4440 systems.

WHO: Display a list of MP connected users

This 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.

For LAN and WEB console clients, the command displays the remote IP address. When DNS is integrated, the host name is displayed as well.

The local port now requires a login. A user must be logged in to the system, or no local port displays.

XD: Diagnostics or reset of MP

This command enables you to perform some simple checks to confirm the MP's health and its connectivity status. The following tests are available:

- MP Parameter Checksum
- Verify I2C connection (get BMC Device ID)
- LAN connectivity test using ping
- Modem self-tests

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.

NOTE You can also reset the MP through the Web interface, using the SO command plus its P command option, or by pressing the MP reset button.

---

6 MP Directory Services Installation and Configuration

You can install and configure MP directory services to leverage the benefits of a single point of administration for MP user accounts.

The following sections describe the features and functions, installation, and configuration of MP directory services:

- “Directory Services”
- “Directory Services for Active Directory”
- “Directory Services for eDirectory”
- “User Login Using Directory Services”
- “Certificate Services”
- “Directory-Enabled Management”
- “Directory Services Schema”

Directory Services

The following are benefits of directory integration:

- Scalability: The directory can be leveraged to support thousands of users on thousands of management processors.
- 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. A change at a single role then applies to all users and MP devices associated with that role.
- Single point of administration: You can use native administrative tools, like MMC and ConsoleOne, to administrate MP users.
- Immediacy: A single change in the directory rolls out immediately to associated MPs. This eliminates the need to script this process.
- Reuse of username and password: You can use existing user accounts and passwords in the directory without having to record or remember a new set of credentials for MP.
- Flexibility: You can create a single role for a single user on a single MP, you can create a single role for multiple users on multiple MPs, or you can use a combination of roles — whatever is suitable for your enterprise.
- Compatibility: MP directory integration applies to MP products. The integration supports the popular directories Active Directory and eDirectory.
- Standards: MP directory support builds on the LDAP 2.0 standard for secure directory access.

Features Supported by Directory Integration

MP Directory Services functionality enables you to:

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

Installing Directory Services for MP requires extending the directory schema. A Schema Administrator must complete extending the schema.

The local user database is retained. You can decide not to use directories, use a combination of directories and local accounts, or use directories exclusively for authentication.

Installation Prerequisites

Before installing directory services, you must do the following:

- Obtain an Integrated Lights-Out Advanced Pack license
- Configure LDAP. See “Configuring LDAP” on page 29 for more details.

Installing Directory Services

To successfully enable directory-enabled management on any MP, complete the following steps:

Step 1. Plan

Review the following sections:

- "Directory Services" on page 64
- "Directory Services Schema" on page 102
- "Directory-Enabled Management" on page 96

Step 2. Install

a. Download the HP Lights-Out Directory Package containing the schema installer, the management snap-in installer, and the migrations utilities from the HP Web site (http://www.hp.com/servers/lights-out).

b. Run the schema installer ("Schema Installer" on page 67) once to extend the schema.

c. Run the management snap-in installer ("Management Snap-In Installer" on page 69) and install the appropriate snap-in for your directory service on one or more management workstations.

Step 3. Update

a. Flash the ROM (Upgrade MP Firmware) on the MP with the directory-enabled firmware.

b. Set directory server settings and the distinguished name of the MP objects on the Directory Settings in the MP user interface.

Step 4. Manage

a. Create a management device object and a role object ("Directory Services Objects" on page 76) using the snap-in.

b. Assign rights to the role object, as necessary, and associate the role with the management device object.

c. Add users to the role object.

For more information on managing the directory service, see "Directory-Enabled Management" on page 96. Examples are available in "Directory Services for Active Directory" on page 70 and "Directory Services for eDirectory" on page 82.

Schema Documentation

To assist with the planning and approval process, HP provides documentation on the changes made to the schema during the schema setup process. To review the changes made to your existing schema, see "Directory Services Schema" on page 102.

Directory Services Support

MP supports the following directory services:

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

- Novell eDirectory 8.6.2
- Novell eDirectory 8.7

MP 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. This solution makes no distinction between eDirectory running on NetWare, Linux, or Windows®. To spawn an eDirectory schema extension requires Java™ 1.4.2 or later for SSL authentication.

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

- Windows® 2000 family
- Windows® Server 2003 family

MP supports eDirectory 8.6.2 and 8.7 running on one of the following operating systems:

- Windows® 2000 family
- Windows® Server 2003 family
- NetWare 5.X
- NetWare 6.X
- Red Hat Enterprise Linux AS 2.1
- Red Hat Linux 7.3
- Red Hat Linux 8.0

eDirectory Installation Prerequisites

Directory Services for MP uses LDAP over SSL to communicate with the directory servers. MP software is designed to install in an eDirectory Version 8.6.1 (and later) tree. HP does not recommend installing this product if you have eDirectory servers with a version earlier than eDirectory 8.6.1. Before installing snap-ins and schema extensions for eDirectory, read and have available the following technical information documents, available at Novell Support (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*

Installing Directory Services for MP requires extending the eDirectory schema. An administrator must complete extending the schema.

Schema Required Software

MP requires specific software, which extends the schema and provides snap-ins to manage the MP network. An HP Smart Component is available for download that contains the schema installer and the management snap-in installer. You can download the HP Smart Component from the HP Web site (http://www.hp.com/servers/lights-out).

Schema Installer

Bundled with the schema installer are one or more `.xml` files. These files contain the schema that 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.

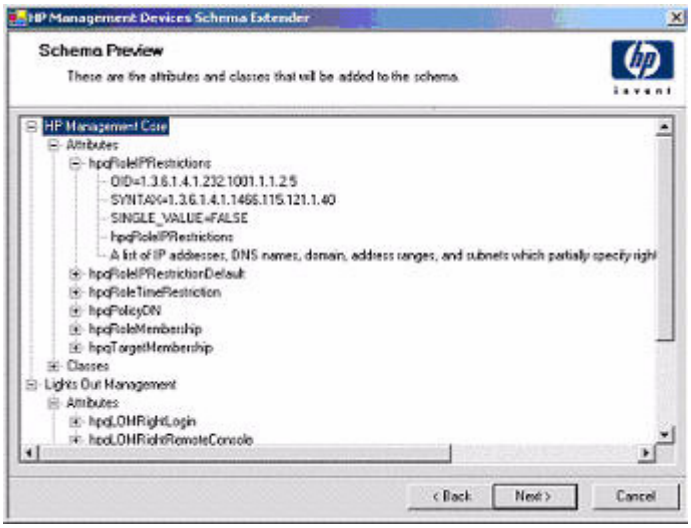
The installer includes three important screens:

- Schema Preview
- Setup
- Results

Schema Preview

The Schema Preview screen (Figure 6-1) enables you to view the proposed extensions to the schema. This screen reads the selected schema files, parses the XML, and displays it as a tree view. It lists all of the details of the attributes and classes that are installed.

Figure 6-1 Schema Preview Screen



Setup

Use the Setup screen (Figure 6-2) to enter the appropriate information before extending the schema.

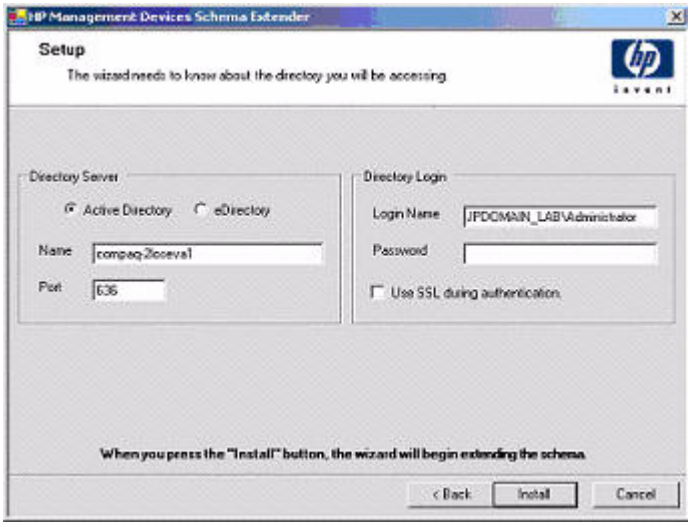
The Directory Server section of the Setup screen enables you to choose whether to use Active Directory or eDirectory, and to set the computer name and the port to be used for LDAP communications.

IMPORTANT Extending the schema on Active Directory requires that you are an authenticated Schema Administrator, that the schema is not write protected, and that the directory is 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 get write access to the schema on Windows® 2000 requires a change to the registry safety interlock. If you choose the Active Directory option, the schema extender attempts to make the registry change. It will only succeed if you have rights to do this. Write access to the schema is automatically enabled on Windows® Server 2003.

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

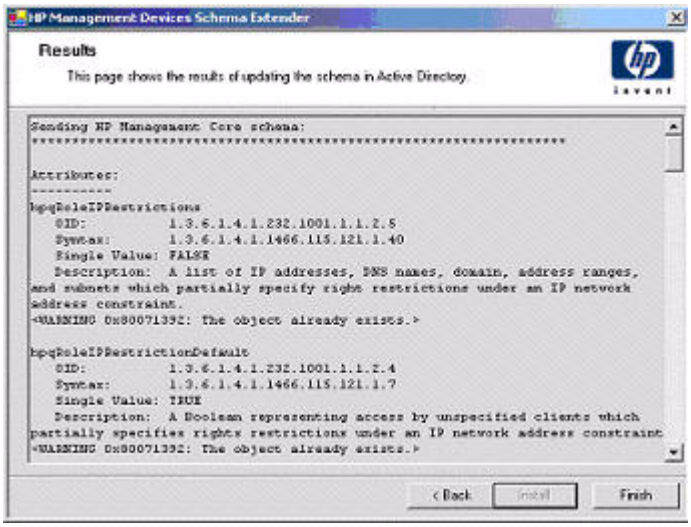
Figure 6-2 Schema Setup Screen



Results

The Results screen (Figure 6-3) displays the results of the installation, including whether the schema could be extended and what attributes were changed.

Figure 6-3 Schema Results Screen



Management Snap-In Installer

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

Use MP snap-ins to perform the following tasks in creating an MP directory:

- Create and manage the MP and role objects (policy objects will be supported at a later date)
- Make the associations between MP objects and role (or policy) objects

Directory Services for Active Directory

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

HP provides a utility to automate much of the directory setup process. You can download the HP Directories Support for Management Processors on the HP website (http://h18004.www1.hp.com/support/files/lights-out/us/index.html).

Active Directory Installation Prerequisites

Following are prerequisites for installing Active Directory:

- The Active Directory must have a digital certificate installed to enable MP to connect securely over the network.
- The Active Directory must have the schema extended to describe MP object classes and properties.
- The MP firmware must be Version E.03.01 or later.
- MP Advanced features must be licensed.

Directory Services for MP 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 Installing Directory Services for MP requires extending the Active Directory schema. You must be an Active Directory Schema Administrator to complete extending the schema.

- Extending the Schema in the Microsoft® Windows ® 2000 Server Resource Kit, available at http://msdn.microsoft.com
- Installing Active Directory in the Microsoft® Windows ® 2000 Server Resource Kit, available at http://www.microsoft.com/resources/documentation/Windows/2000/server/reskit/
- 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*

MP requires a secure connection to communicate with the directory service. This requires the installation of the Microsoft® CA. Refer to the following Microsoft® technical references:

- Appendix D—Configuring Digital Certificates on Domain Controllers for Secure LDAP and SMTP Replication (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/a0701.asp)
- Microsoft® Knowledge Base Article 321051: How to Enable LDAP over SSL with a Third-Party Certification Authority

Directory Services Preparation for Active Directory

To set up directory services for use with management processors, perform the following steps:

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

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

Step 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 if you have sufficient rights. You can also do this by setting **`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters\Schema Update Allowed`** in the registry to a non-zero value (refer to the "Order of Processing When Extending the Schema" section of Installation of Schema Extensions in the Windows® 2000 Server Resource Kit) or by doing the following (This step is not necessary if you are using Windows® Server 2003.):

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

---

a. Start MMC.

b. Install the Active Directory Schema snap-in in MMC.

c. Right-click **Active Directory Schema** and choose **Operations Master**.

d. Choose **The Schema may be modified on this Domain Controller**.

e. Click **OK**.

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

Step 4. Create a certificate or install Certificate Services. This step is necessary to create a certificate or install Certificate Services because MP communicates with Active Directory using SSL. You must install Active Directory before installing Certificate Services.

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

a. Launch Microsoft ® Management Console on the server and add the default domain policy snap-in (Group Policy, then browse to Default domain policy object).

b. Click **Computer Configuration>Windows Settings>Security Settings>Public Key Policies**.

c. Right-click **Automatic Certificate Requests Settings**, and choose **new>automatic certificate request**.

d. Using the wizard, choose the domain controller template and the certificate authority you want to use.

Step 6. Download the Smart Component, which contains the installers for the schema extender and the snap-ins. You can download the Smart Component from the HP Web site (http://www.hp.com/servers/lights-out).

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

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

Snap-In Installation and Initialization for Active Directory

Follow these steps to install the snap-ins and configure the directory service:

Step 1. Run the snap-in installation application to install the snap-ins.

Step 2. Configure the directory service to have the appropriate objects and relationships for MP management:

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

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

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

For more information on MP objects, see “Directory Services Objects” on page 76.

At a minimum, you must create:

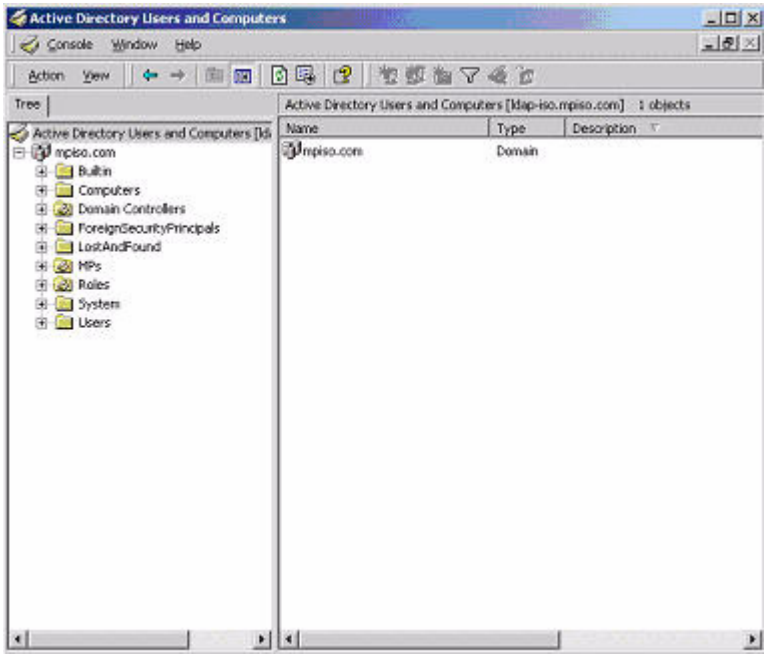
- One Role object that contains one or more users and one or more MP objects.
- One MP object corresponding to each MP that will be using the directory.

Example: Creating and Configuring Directory Objects for Use with MP 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.

Assume that a company has an enterprise directory including the domain mpiso.com, arranged as shown in Figure 6-4.

Figure 6-4 Directory Example



Step 1. Create an organizational unit to contain the MP devices managed by the domain. In this example, two organizational units are created, called Roles and MPs.

Step 2. Use the HP provided Active Directory Users and Computers snap-ins to create MP objects in the MPs organizational unit for several MP devices.

a. Right-click the **MPs** organizational unit found in the mpiso.com domain, and choose **NewHPObject**.

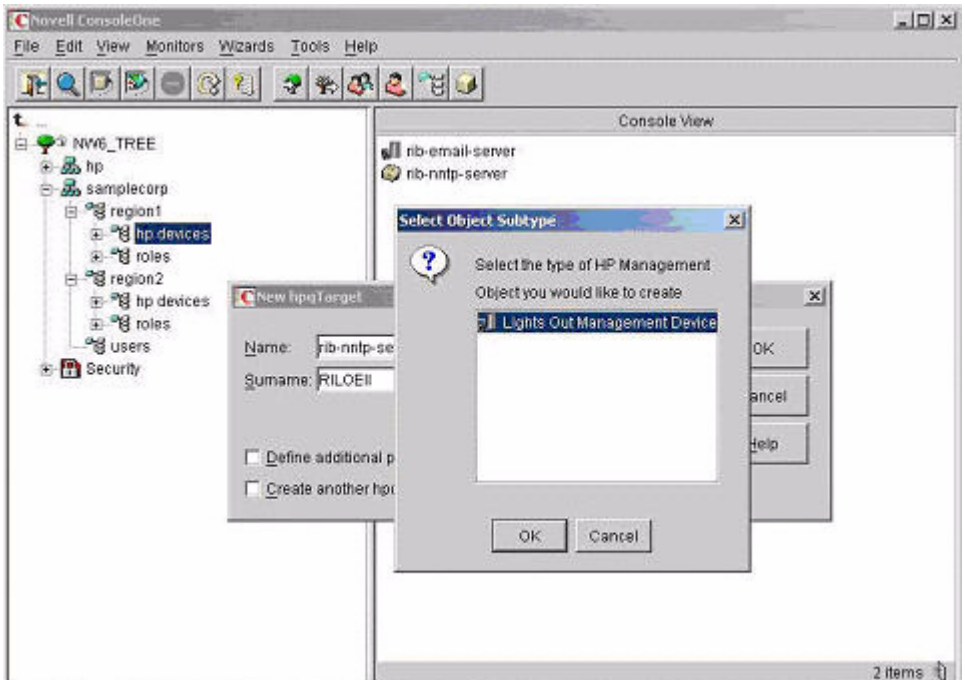
b. Choose **Device** for the type in the Create New HP Management Object dialog box (Figure 6-5).

c. Enter an appropriate name in the Name field of the dialog box. In this example, the DNS host name of the MP device, lpmp, is used as the name of the MP object, and the surname is MP.

d. Enter and confirm a password in the Device LDAP Password and Confirm fields (this is optional).

e. Click **OK**.

Figure 6-5 Create New HP Management Object Dialog Box



Step 3. Use the HP provided Active Directory Users and Computers snap-ins to create HP Role objects in the Roles organizational unit.

Step 4. Right-click the **Roles** organizational unit, choose **New**, then **Object**.

a. Choose **Role** for the type field in the Create New HP Management Object dialog box.

b. Enter an appropriate name in the Name field of the dialog box. In this example, the role contains users trusted for remote server administration and will be called remoteAdmins. Click **OK**.

c. Repeat the process, creating a role for remote server monitors called remoteMonitors.

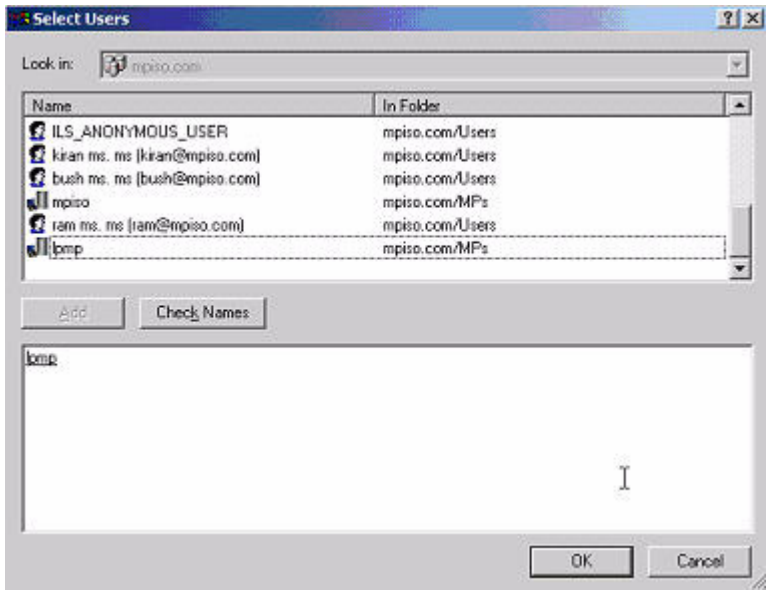
Step 5. Use the HP provided Active Directory Users and Computers snap-ins to assign the roles rights, and associate the roles with users and devices.

a. Right-click the **remoteAdmins** role in the Roles organizational unit in the mpiso.com domain, and choose **Properties**.

b. Choose the **HP Devices** tab, then click **Add**.

c. Using the Select Users dialog box (Figure 6-6), choose the MP object created in step 2: **lpmp** in folder mpiso.com/MPs. Click **OK** to close the dialog, and then click **Apply** to save the list.

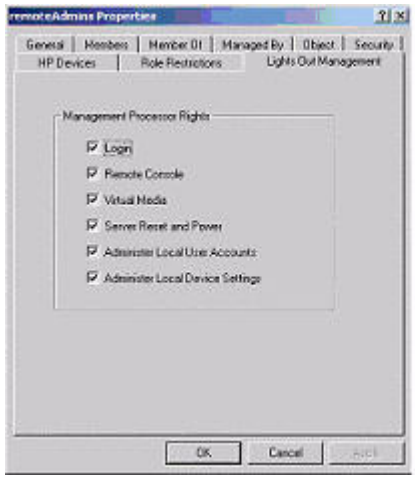
Figure 6-6 Select Users Dialog Box



Add users to the role. Click the Members tab, and add users using the Add button and the Select Users dialog box. The devices and users are now associated.

Step 6. Use the Lights Out Management tab (Figure 6-7) to set the rights for the role. All users and groups within a role have the rights assigned to the role on all of the MP devices managed by the role. In this example, the users in the remoteAdmins role are given full access to the MP functionality. Click the checkboxes next to each right, and then click **Apply**. Click **OK** to close the property sheet.

Figure 6-7 Lights-Out Management Tab



Step 7. Using the same procedure as 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 add users to the remoteMonitors role using the Members tab. Then, on the Lights Out Management tab, click the **Login** checkbox. Click **Apply** and **OK**. Members of the remoteMonitors role will be able to authenticate and view the server status.

User rights to any MP are calculated as the sum of all the rights assigned by all the roles in which the user is a member, and the MP is a managed device. Following the preceding examples, if a user is in both the remoteAdmins and remoteMonitors roles, he or she has all the rights, because the remoteAdmins role has those rights.

To configure MP and associate it with an MP object used in this example, use settings similar to the following on the MP Directory Settings TUI:

```
RIB Object DN = cn=lpmp,ou=MPs,dc=mpiso,dc=com
Directory User Context 1 = cn=Users,dc=mpiso,dc=com
```

For example, to gain access, user Mel Moore (with the unique ID MooreM, located in the Users organizational unit within the mpiso.com domain, who is also a member of one of the remoteAdmins or remoteMonitors roles) would be allowed to log in to the MP. He would enter **`mpiso\moorem`**, or **`moorem@mpiso.com`**, or **`Mel Moore`**, in the Login Name field of the MP 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 the managed device and user or groups already contained within the directory service. User management of MP requires three basic objects in the directory service:

- MP object
- Role object
- User objects

Each object represents a device, user, or relationship that is required for directory-based management.

NOTE After you install the snap-ins, you must restart ConsoleOne and MMC to show the new entries.

After the snap-in is installed, you can create MP objects and MP roles in the directory. Using the Users and Computers tool, you can:

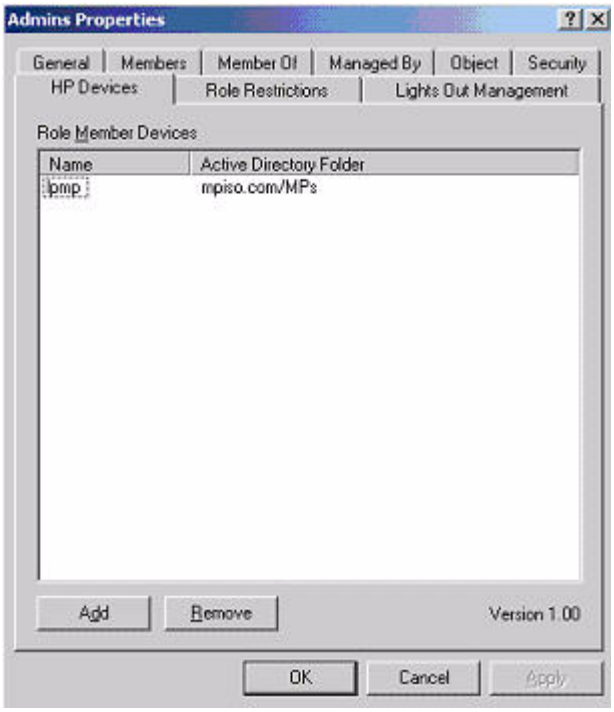
- Create MP and role objects.
- Add users to the role objects.
- Set the rights and restrictions of the role objects.

Active Directory Snap-Ins

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

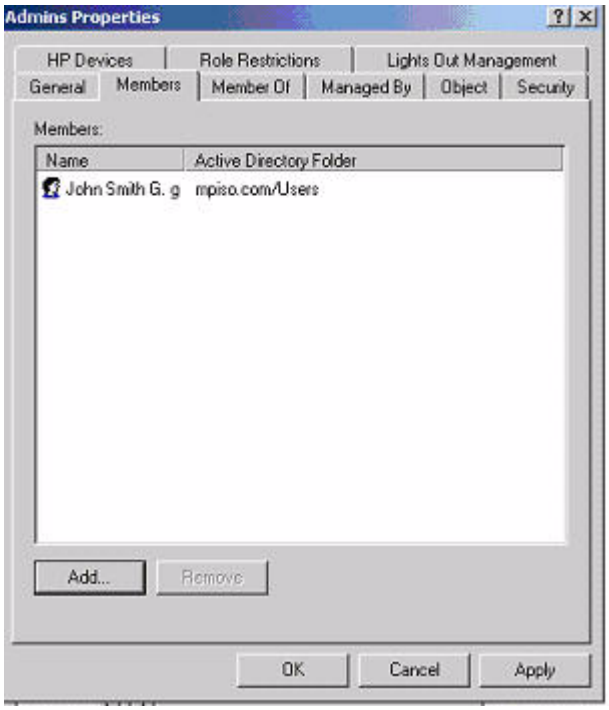
Managing HP Devices Within a Role Use the HP Devices tab (Figure 6-8) to add the HP devices to be managed within a role. Clicking Add enables you to browse to a specific HP device and add it to the list of member devices. Clicking Remove enables you to browse to a specific HP device and remove it from the list of member devices.

Figure 6-8 HP Devices Tab



Managing Users Within a Role After user objects are created, use the Members tab (Figure 6-9) to manage the users within the role. Clicking Add enables you to browse to the specific user you want to add. Highlighting an existing user and clicking Remove removes the user from the list of valid members.

Figure 6-9 Members Tab



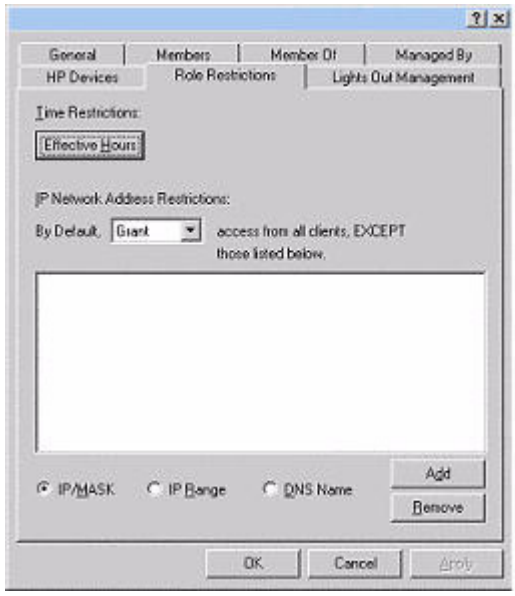
Setting Login Restrictions

The Role Restrictions subtab (Figure 6-10) enables you to set login restrictions for the role. These restrictions include:

- Time Restrictions
- IP Network Address Restrictions
  - IP/Mask
  - IP Range

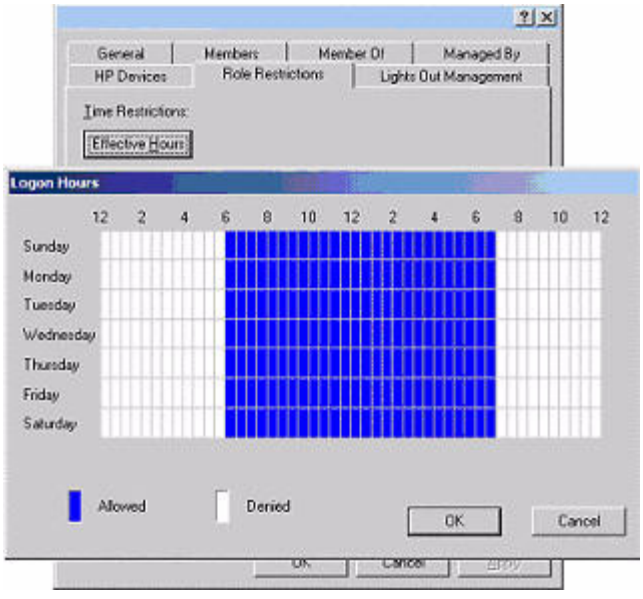
— DNS Name

Figure 6-10 Role Restrictions Subtab



Setting Time Restrictions You can manage the hours available for login by members of the role by clicking the Effective Hours button in the Role Restrictions tab. In the Logon Hours pop-up window (Figure 6-11), you can choose 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 you can change a section of squares by clicking and holding the mouse button, dragging the cursor across the squares to be changed, and releasing the mouse button. The default setting is to allow access at all times.

Figure 6-11 Logon Hours Pop-Up Window



Defining Client IP Address or DNS Name Access You can grant or deny access to an IP address, IP address range, or DNS names.

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

Step 1. To restrict an IP address, choose **IP/MASK** in the Role Restrictions tab and click **Add**.

Step 2. The new restriction pop-up window displays. In the New IP/Mask Restriction pop-up window (Figure 6-12), enter the information and click **OK**.

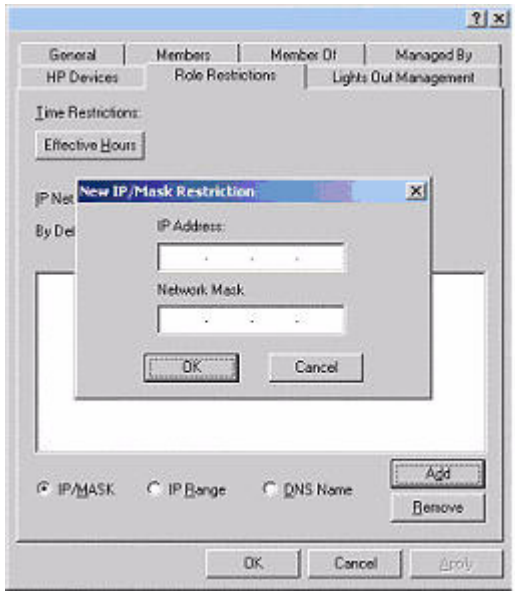
Step 3. The DNS Name option enables you to restrict access based on a single DNS name or a subdomain, entered in the form of host.company.com or *.domain.company.com. Choose **DNS Name** in the Role Restrictions tab and click **Add**.

Step 4. The New DNS Name Restriction pop-up window displays. Enter the information and click **OK.**

Step 5. Click **OK** to save the changes.

To remove any of the entries, highlight the entry in the display list and click Remove.

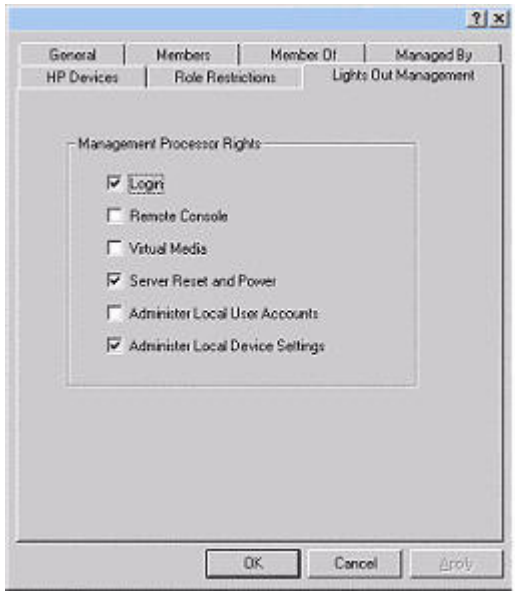
Figure 6-12 New IP/Mask Pop-Up Window



Setting User or Group Role Rights

After you create a role, you can choose rights for the role. You can make users and group objects members of the role, giving the users or group of users the rights granted by the role. Use the Lights Out Management tab (Figure 6-13) to manage rights.

Figure 6-13 Lights Out Management Tab



The available rights are:

- Login—This option controls whether users can log in to the associated devices and execute Status or Read-only commands (view event logs and console logs, check system status, power status, and so on) but not execute any commands that would alter the state of MP or the system.
- Remote Console—This option enables you to access the system console (the host OS).
- Virtual Media—This option is currently not supported.
- Server Reset and Power—This option enables you to execute MP power operations to remotely power on, power off, or reset the host platform, as well as configure the system's power restore policy.
- Administer Local User Accounts—This option enables you to administer local MP user accounts.
- Administer Local Device Settings— This option enables you to configure all MP settings, as well as reboot MP and update MP firmware.

Directory Services for eDirectory

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

Snap-In Installation and Initialization for eDirectory

See “Snap-In Installation and Initialization for Active Directory” on page 72 for step-by-step instructions on using the snap-in installation application.

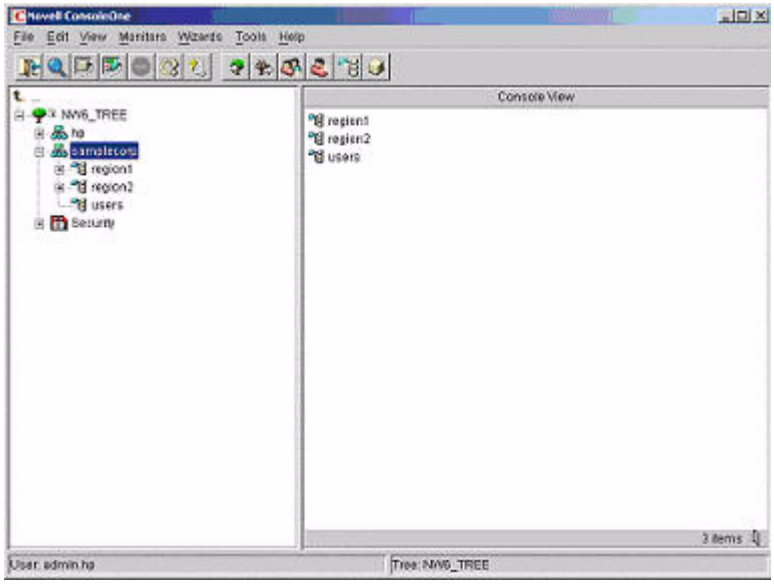
NOTE After you install snap-ins, you must restart ConsoleOne and MMC to show the new entries.

Example: Creating and Configuring Directory Objects for Use with MP Devices in eDirectory

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

Assume samplecorp has an enterprise directory arranged according to the Figure 6-14.

Figure 6-14 Roles and Devices Example



Begin by creating organizational units in each region to contain the MP devices and roles specific to that region. In this example, two organizational units are created, called roles and hp devices, in each organizational unit (region1 and region2).

Creating Objects

Follow these steps to create MP objects:

Step 1. Use the HP provided ConsoleOne snap-ins to create MP objects in the hp devices organizational unit for several MP devices.

Step 2. Right-click the **hp devices** organizational unit, found in the region1 organizational unit, and choose **New**, then **Object**.

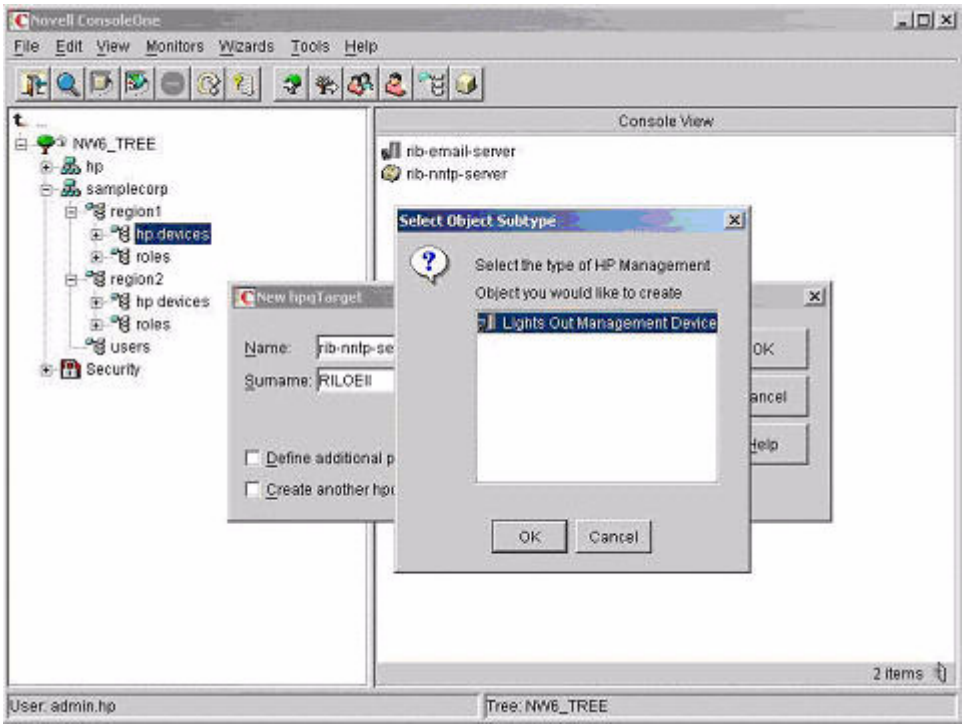
a. Choose **hpqTarget** from the list of classes, and click **OK**.

b. Enter an appropriate name and surname in the New hpqTarget dialog box. In this example, the DNS host name of the MP device, rib-email-server is used as the name of the MP object, and the surname is RILOEII (MP). Click **OK**.

c. The Select Object Subtype dialog box (Figure 6-15) appears. Choose **Lights Out Management Device** from the list, and click **OK**.

d. Repeat the process for several more MP devices with DNS names rib-nntp-server and rib-file-server-users1 in hp devices under region1, and rib-file-server-users2 and rib-app-server in hp devices under region2.

Figure 6-15 Select Object Subtype Dialog Box



Creating Roles

Follow these steps to create roles:

Step 1. Use the HP provided ConsoleOne snap-ins to create HP Role objects in the roles organizational units.

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

b. Choose **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. Click **OK**.

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

Step 2. Repeat the process, creating a role for remote server monitors, named remoteMonitors, in roles in region1, and a remoteAdmins and a remoteMonitors role in roles in region2.

Step 3. Use the HP provided ConsoleOne snap-ins 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 choose **Properties**.

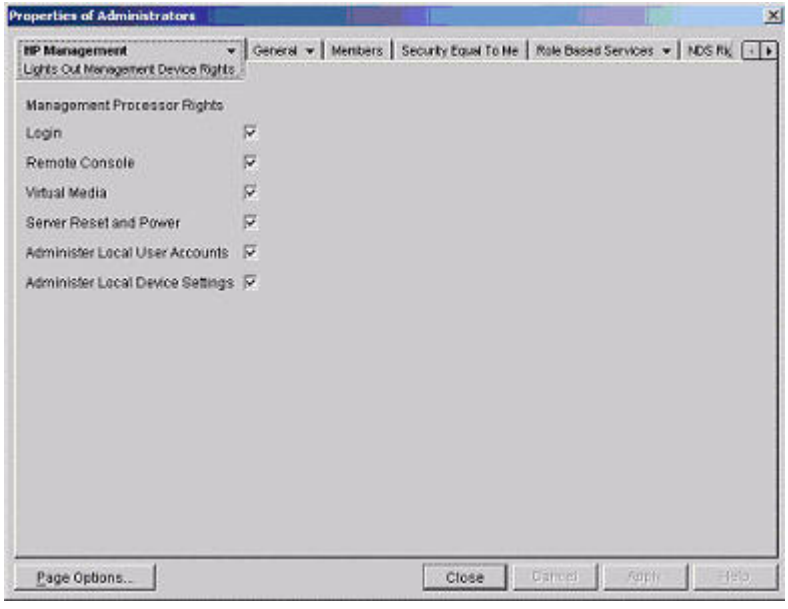
b. Choose the Role Managed Devices subtab of the HP Management tab, and click **Add**.

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

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

e. The devices and users are now associated. Use the Lights Out Management Device Rights subtab of the HP Management tab (Figure 6-16) to set the rights for the role. All users within a role will have the rights assigned to the role on all of the MP devices managed by the role. In this example, the users in the remoteAdmins role are given full access to the MP functionality. Choose the boxes next to each right, and click **Apply**. Click **Close** to close the property sheet.

Figure 6-16 Setting Role Rights



Step 4. Using the same procedure as in step 3, edit the properties of the remoteMonitors role:

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

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

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

User rights to any MP 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 MP device is a managed device. Following the preceding examples, if a user is in both the remoteAdmins and remoteMonitors roles, he or she will have all the rights, because the remoteAdmins role has those rights.

To configure a MP device and associate it with an MP object used in this example, use settings similar to the following on the MP Directory Settings TUI.

NOTE Use commas, not periods, in LDAP Distinguished Names to separate each component.

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

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

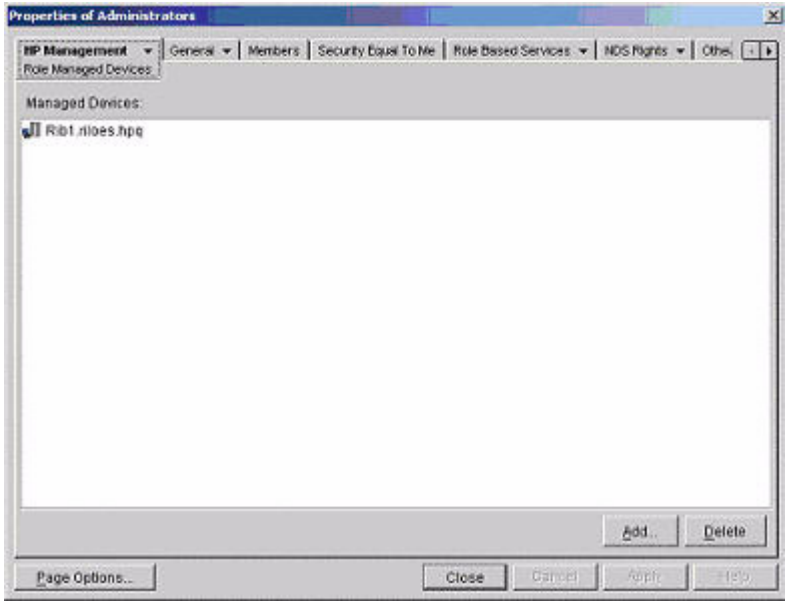
Directory Services Objects for eDirectory

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

Adding Role Managed Devices

Use the Role Managed Devices subtab under the HP Management tab (Figure 6-17) to add the HP devices to be managed within a role. Clicking Add enables you to browse to the specific HP device and add it as a managed device.

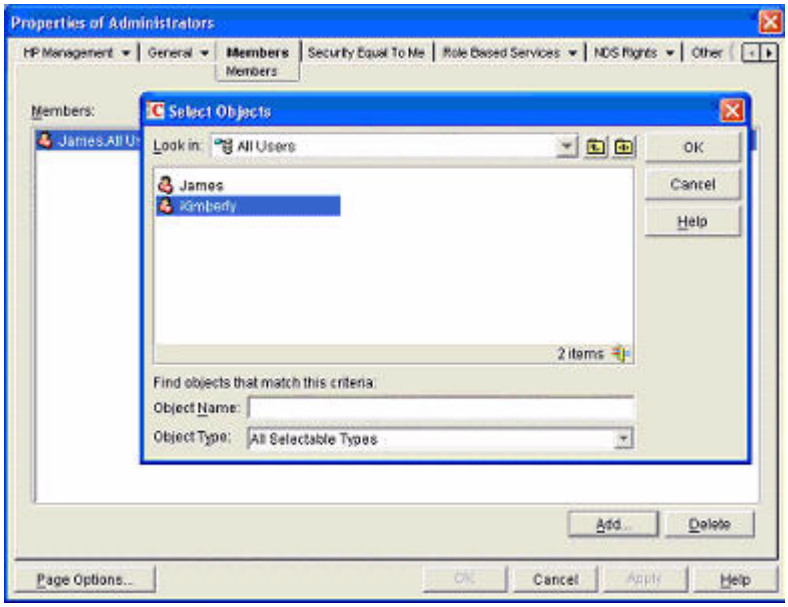
Figure 6-17 Role Managed Devices Subtab



Adding Members

After you create user objects, use the Members tab to manage the users within the role. Clicking Add enables you to browse to the specific user you want to add. Highlighting an existing user and clicking Delete removes the user from the list of valid members.

Figure 6-18 Members Tab (eDirectory)



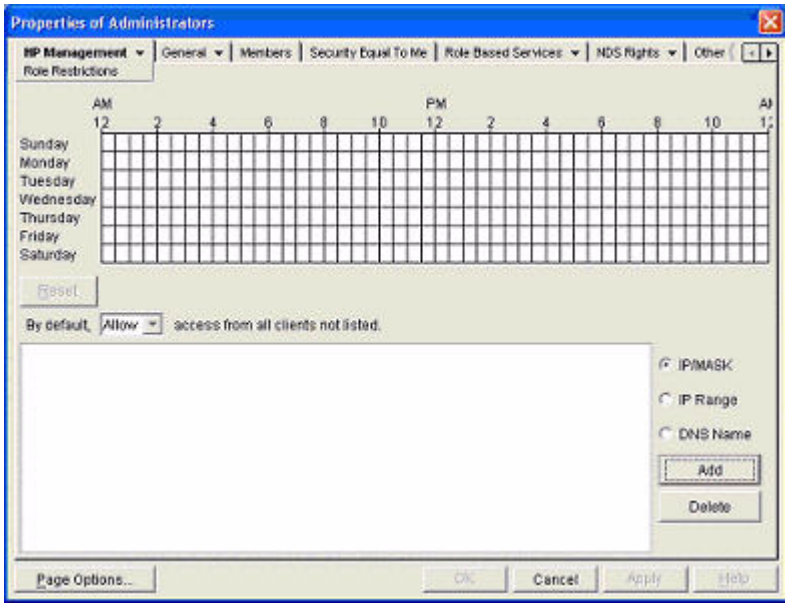
Setting Role Restrictions

The Role Restrictions subtab (Figure 6-18) enables you to set login restrictions for the role. These restrictions include:

- Time Restrictions
- IP Network Address Restrictions
  - IP/Mask
  - IP Range

- DNS Name

Figure 6-19 Role Restrictions Subtab (eDirectory)



Setting Time Restrictions

You can manage the hours available for login by members of the role by using the time grid displayed in the Role Restrictions subtab (Figure 6-19). 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 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.

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

Step 1. To restrict an IP address, choose **IP/MASK** in the Role Restrictions subtab and click **Add**.

Step 2. The Add New Restriction pop-up for the IP/Mask option is shown. In the Add New Restriction pop-up window (Figure 6-20), enter the information, and click **OK**.

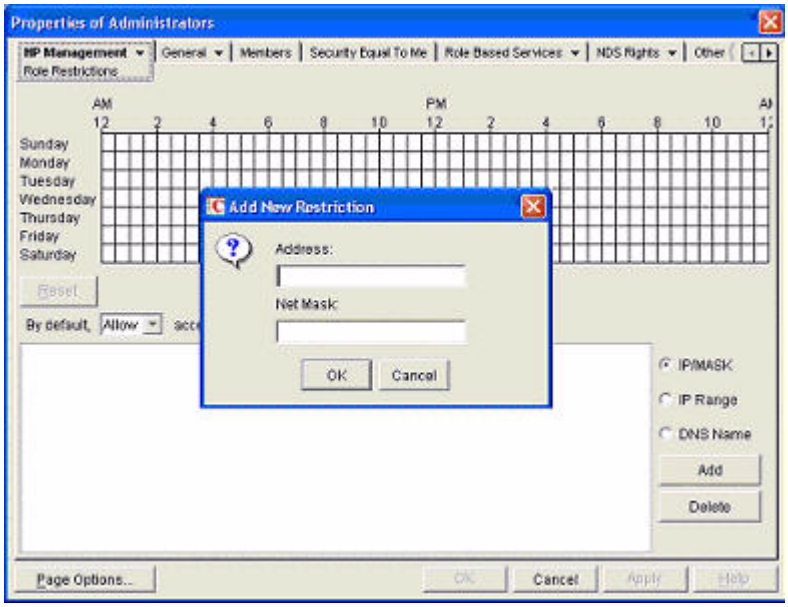
Step 3. The DNS Name option enables you to restrict access based on a single DNS name or a subdomain, entered in the form of host.company.com or *.domain.company.com. Choose **DNS Name** in the Role Restrictions subtab and click **Add**.

Step 4. The New DNS Name Restriction pop-up window displays. Enter the information and click **OK.**

Step 5. Click **Apply** to save the changes.

To remove any of the entries, highlight the entry in the display field and click Delete.

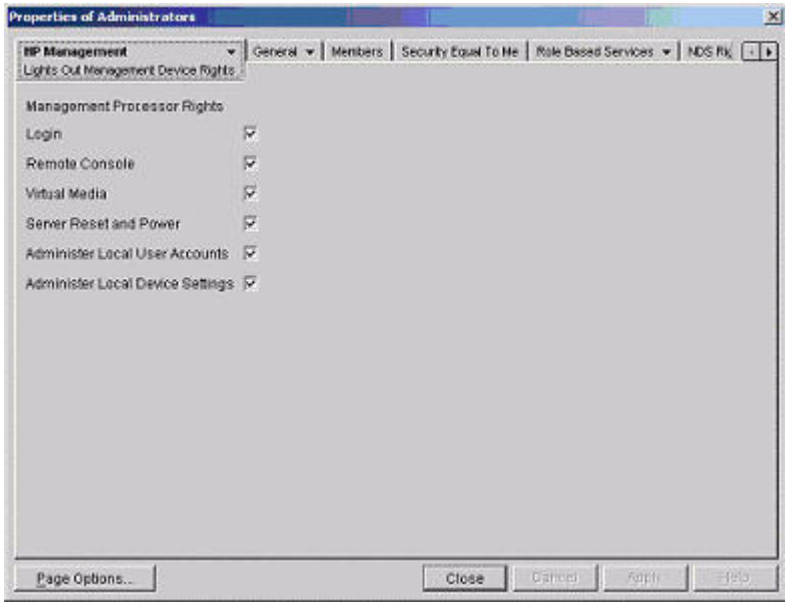
Figure 6-20 Add New Restriction Pop-Up Window



Setting Lights-Out Management Device Rights

After you create a role, you can choose rights for the role. You can make users and group objects members of the role, giving the users or group of users the rights granted by the role. Use the Lights Out Management Device Rights subtab of the HP Management tab (Figure 6-21) to manage rights.

Figure 6-21 Lights-Out Management Device Rights Tab



The available rights are:

- Login—This option controls whether users can log in to the associated devices and execute Status or Read-only commands (view event logs and console logs, check system status, power status, and so on) but not execute any commands that would alter the state of MP or the system.
- Remote Console—This option enables you to access the system console (the host OS).
- Virtual Media—This option is currently not supported.
- Server Reset and Power—This option enables you to execute MP power operations to remotely power on, power off, or reset the host platform, as well as configure system's power restore policy.
- Administer Local User Accounts—This option enables you to administer local MP user accounts.
- Administer Local Device Settings— This option enables you to configure all MP settings, as well as reboot MP and update MP firmware.

Snap-Ins Installation and Schema Extension for eDirectory on a Linux Platform

This section describes a method that does not require a Windows client to install snap-ins and schema extension for eDirectory on a Linux platform.

Schema extension is the addition of new classes to the existing classes. You can use these classes to create objects to support a specific utility. New classes, such as hpqTarget, hpqPolicy and hpq Role, are added. HP has created objects using these classes to support MP devices (created using the 'hpqTarget' class), and MP Admins and Monitors (created using the 'hpqRole' class). These objects support the Login Authentication utility to the MP device and enable MP users to execute commands based on their assigned roles.

Installing the Java Runtime Environment

As a prerequisite for extending the schema, you need to have Java Runtime Environment (JRE) 1.4.2 installed. To ensure that you have correct version of JRE installed on your system, perform the following steps:

Step 1. To determine the Java version, execute the following command:

```
# java -version
```

The Java version installed on your system is displayed.

Step 2. If Java is not installed on your system, execute the following command:

```
# rpm -iv j2re-1_4_2_04-linux-i586.rpm
```

NOTE You can download this `rpm` file from the java.sun.com Web site.

Step 3. Execute the following command if:

- Java is installed and the version is older than 1.4.2.
- You want to upgrade the Java version and uninstall the older version.

```
# rpm -Uv j2re-1_4_2_04-linux-i586.rpm
```

Step 4. Add the entry **`/usr/java/j2re1.4.2_04/bin`** into the `.bash_profile` file.

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. You need to create this directory because it is not present. Creation of the directory and copying of the two `.jar` files to the hp directory are done automatically when the `hpdsse.sh` file is executed.

NOTE The `hpdsse.sh` file is obtained when the `Schema.tar` tarball is extracted. This process is explained in the Schema Extension section. You can download schema extensions from the link http://h18013.www1.hp.com/products/servers/management/directorysupp/index.html. Choose Software and Drivers, and the Operating System for the schema extension you want to install.

Schema Extension:

To obtain the `hpdsse.sh` file, do the following:

Step 1. Download the tar file to the Linux system on which eDirectory is installed.

Step 2. Extract the tar file to obtain the `hpdsse.sh` file by executing the following command:

```
# tar -xvf Schema. tar
```

Step 3. Run this file by executing the following command:

```
# ./hpdsse.sh
```

This command displays the instructions. As per the instructions, provide the server name, admin DN, and admin password as command line arguments to extend the schema.

Step 4. To see the results, check the `schema.log` file, which is created after the schema extension is complete.

The log file must show the classes and attributes created. In addition it should show the result as Succeeded. If the objects already exist, the message Already Exists should appear in the log file.

The Already Exists message appears only when you try to run the same `.sh` file after schema extension is complete. The SSL port (636) is used during the schema extension. You verify this by running the **`netstat -nt | grep :636`** command while the `hpdsse.sh` file is being executed.

Verification of Snap-Ins and Schema Extension

To verify the snap-ins and schema extension, do the following:

Step 1. Launch ConsoleOne and log on to the tree.

Step 2. Check for the new classes by opening the Schema Manager from the Tools drop-down menu.

All the classes related to the HP Directory Services must be present in the classes list. The classes are ‘hpqRole,’ hpqTarget,’ ‘hpqPolicy,’ and ‘hpqLOMv100’.

Configuring Directory Settings in MP (LDAP Command)

Use the `LDAP` Command Menu command to configure MP LDAP directory settings. The following is an example of the `LDAP` command output:

```
[mp1] MP:CM> LDAPCurrent LDAP Directory Configuration:L - LDAP Directory Authentication: DisabledM - Local
MP User database      : EnabledI - Directory Server IP Address  : 127.0.0.1P - Directory Server LDAP Port
: 636D - Distinguished Name (DN)     : cn=mp,o=demo1 - User Search Context 1       : o=mp2 - User Search
```

```
Context 2       : o=demo3 - User Search Context 3       : o=testEnter parameter(s) to change, A to modify
All, or [Q] to Quit: aFor each parameter, enter:New value, or<CR> to retain the current value, orDEFAULT
to set the default value, orQ to QuitLDAP Directory Authentication:            E – Enabled  Current > D –
Disabled (default)Enter new value, or Q to Quit: e> LDAP Directory Authentication will be updatedLocal MP
User Accounts:             D - Disabled  (default)   Current > E - EnabledEnter new value, or Q to Quit:
<CR> -> Current Local MP User Accounts has been retainedDirectory Server IP Address:  Current -> 127.0.0.1
(default)Enter new value, or Q to Quit: 15.255.1.1-> Directory Server IP Address will be updatedDirectory
Server LDAP Port:  Current -> 636 (default)Enter new value, or Q to Quit: <CR>-> Current Directory Server
LDAP Port has been retainedDistinguished Name (DN):   Current -> cn=mp,o=demoEnter new value, or Q to
Quit: <CR> -> Current Distinguished Name has been retainedUser Search Context 1:         Current ->
o=mpEnter new value, or Q to Quit: <CR>-> Current User Search Context 1 has been retainedUser Search
Context 2:        Current -> o=demoEnter new value, or Q to Quit: <CR>-> Current User Search Context 2 has
been retainedUser Search Context 3:        Current -> o=testEnter new value, or Q to Quit: <CR>-> Current
User Search Context 3 has been retainedNew Directory Configuration (* modified values):*L – LDAP Directory
Authentication: Enabled M – Local MP User database      : Enabled*I - Directory Server IP Address
:15.255.1.1 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=testEnter 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

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

- DOMAIN\user name form (Active Directory Only)

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

  Example: jsmith@hp.com

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

- User name form

  Example: John Smith

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

- Local users—Login-ID

NOTE On the MP 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, do the following:

Step 1. Choose **Start>Settings>Control Panel**.

Step 2. Double-click **Add/Remove Programs**.

Step 3. Click **Add/Remove Windows Components** to start the Windows Components wizard.

Step 4. Choose the **Certificate Services** checkbox. Click **Next**.

Step 5. Click **OK** at the warning that the server cannot be renamed. The Enterprise root CA option is selected because there is no CA registered in the active directory.

Step 6. Enter the information appropriate for your site and organization. Accept the default time period of 2 years for the Valid for field. Click **Next**.

Step 7. Accept the default locations of the certificate database and the database log. Click **Next**.

Step 8. Browse to the `c:\I386` folder when prompted for the Windows® 2000 Advanced Server CD.

Step 9. Click **Finish** to close the wizard.

Verifying Directory Services

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

To verify that certificate services is installed, choose **Start>Programs>Administrative Tools>Certification Authority**. If Certificate Services is not installed, an error message appears.

Configuring Automatic Certificate Request

To specify that a certificate be issued to the server:

Step 1. Choose **Start>Run**, and enter **`mmc`**.

Step 2. Click **Add**.

Step 3. Choose **Group Policy**, and click **Add** to add the snap-in to the MMC.

Step 4. Click **Browse**, and choose the **Default Domain Policy** object. Click **OK**.

Step 5. Choose **Finish>Close>OK**.

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

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

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

Step 9. Choose the **Domain Controller** template, and click **Next**.

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

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

Directory-Enabled Management

This section is for administrators who are familiar with directory services and with the management processor (MP) product. You must be familiar with “Directory Services” on page 64 and comfortable with setting up and understanding the examples.

Directory-enabled remote management enables you to:

- Create MP objects

  You must create one MP device object to represent each device that will use the directory service to authenticate and authorize users. See “Directory Services” on page 64 for additional information on creating MP device objects for Active Directory (“Directory Services for Active Directory” on page 70) and eDirectory (“Directory Services for eDirectory” on page 82). In general, you can use the HP provided snap-ins to create objects. It is useful to give the MP device objects meaningful names, such as the device's network address, DNS name, host server name, or serial number.

- Configure MP Devices

  Every MP device that uses the directory service to authenticate and authorize users must be configured with the appropriate directory settings. See “Configuring Directory Settings in MP (LDAP Command)” on page 91 for details on the specific directory settings. In general, you configure each device with the appropriate directory server address, MP 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 their users and administrators into groups. In many cases, it is convenient to use the existing groups and associate the groups with one or more MP role objects. When the devices are associated with the role objects, you can control access to the MP 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. 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 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 the role.

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

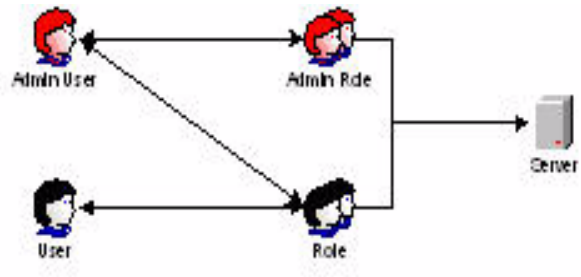
Using Multiple Roles

Most deployments do not require the same user to be in multiple roles managing the same device. However, these configurations are useful for building complex rights relationships. When building multiple-role relationships, users receive all the rights assigned by every applicable role. Roles can only grant rights, never revoke them. If one role grants a user a right, then the user has the right, even if the user is in another role that does not grant that right.

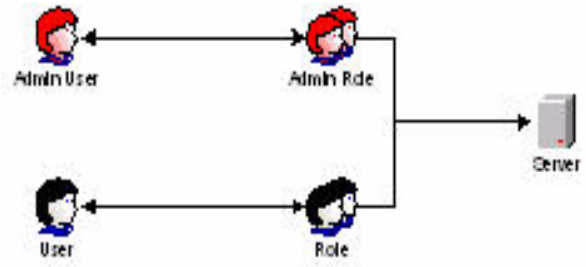
Typically, a directory administrator creates a base role with the minimum number of rights assigned and then creates additional roles to add additional rights. These additional rights are added under specific circumstances or to a specific subset of the base role users.

For example, an organization can have two types of users: administrators of the MP device or host server and users of the MP 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 MP administrators in that role, as well as to the administrative role.

The following figure 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 initial login, more advanced rights are assigned to the Admin User through the Admin Role—Server Reset and Remote Console.



In the following figure, the Admin User gains the Admin Role right in a different way. The Admin User initially logs in through the Admin Role and is assigned admin rights—Server Reset, Remote Console, and Login.



Creating Roles to Follow Organizational Structure

Often, the administrators within an organization are placed into a hierarchy in which subordinate administrators must assign rights independently of ranking administrators. In this case, it is useful to have one role that represents the rights assigned by higher-level administrators and to allow the subordinate administrators to create and manage their own roles.

Restricting Roles

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

For step-by-step instructions on how to create network and time restrictions on a role, see “Setting Role Restrictions” on page 87 or “Setting Time Restrictions” on page 88.

Role Time Restrictions

You can place time restrictions on MP roles. Users are granted the rights specified for the MP devices listed in the role, only if they are members of the role and meet the time restrictions for that role.

MP devices use local host time to enforce time restrictions. If the MP device clock is not set, the role time restriction fails unless no time restrictions are specified on the role.

Role-based time restrictions can only be satisfied if the time is set on the MP device. The time is normally set when the host is booted, and it is maintained by running the agents in the host operating system, which enables the MP device to compensate for leap year and minimize clock drift with respect to the host. Events, such as unexpected power loss or flashing MP firmware, can cause the MP device clock to not be set. Also, the host time must be correct for the MP 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 might be more native to your networking environment. An IP address and subnet mask range is typically specified using a subnet address and address bit mask that identifies addresses that are on the same logical network.

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

DNS-Based Restrictions

DNS-based restrictions use the network naming service to examine the logical name of the client machine by looking up machine names assigned to the client IP addresses. DNS restrictions require a functional name server. If the name service goes down or cannot be reached, DNS restrictions cannot be matched and will fail.

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

DNS restrictions can cause some ambiguity because a host can be multi-homed. DNS restrictions do not necessarily match one-to-one with a single system.

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

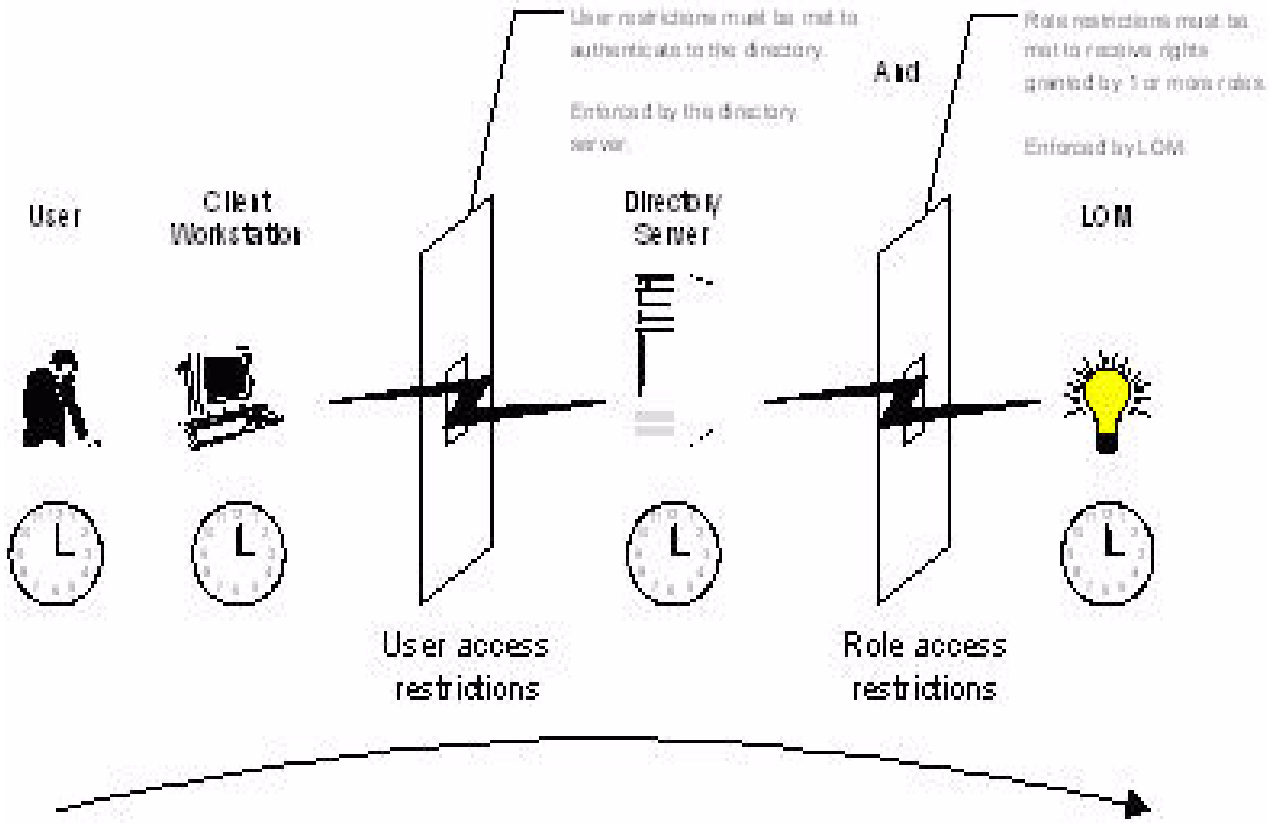
Role Address Restrictions

Role address restrictions are enforced by the MP firmware, based on the client's IP network address. When the address restrictions are met for a role, the rights granted by the role apply.

Address restrictions can be difficult to manage if access is attempted across firewalls or through network proxies. Either of these mechanisms can change the apparent network address of the client, causing the address restrictions to be enforced in an unexpected manner.

How Directory Login Restrictions Are Enforced

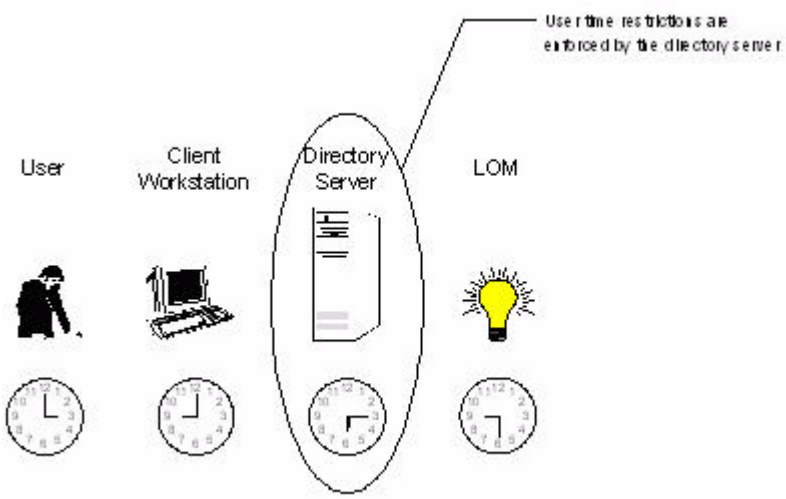
The following figure shows how two sets of restrictions potentially limit a directory user's access to MP devices. User access restrictions limit a user's access to authenticate to the directory. Role access restrictions limit an authenticated user's ability to receive MP privileges based on rights specified in one or more roles.



How User Time Restrictions Are Enforced

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 at the directory server, but if the directory server is located in a different time zone or a replica in a different time zone is accessed, then time zone information from the managed object can be used to adjust for relative time.

The directory server evaluates user time restrictions, but the determination can be complicated by time zone changes or by the authentication mechanism.



User Address Restrictions

You can place network address restrictions on a directory user account, and the directory server enforces these restrictions. Refer to the directory service documentation for details on the enforcement of address restrictions on LDAP clients, such as a user logging in to an MP device.

Network address restrictions placed on the user in the directory might not be enforced in the expected manner if the directory user logs in through a proxy server. When a user logs in to an MP device as a directory user, the MP device attempts authentication to the directory as that user, which means that address restrictions placed on the user account apply when accessing the MP device. However, because the user is proxied at the MP device, the network address of the authentication attempt is that of the MP device, not that of the client workstation.

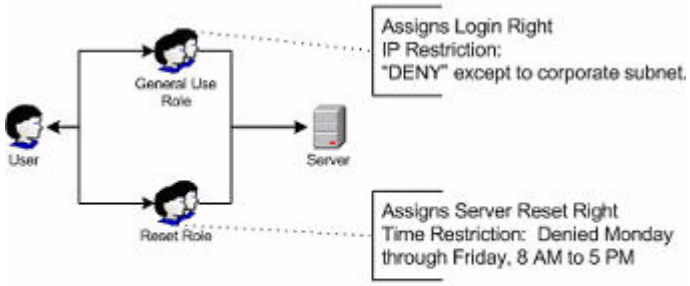
Creating Multiple Restrictions and Roles

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 MP administrators are allowed to use the MP device from within the corporate network but are only able to reset the server outside of regular business hours.

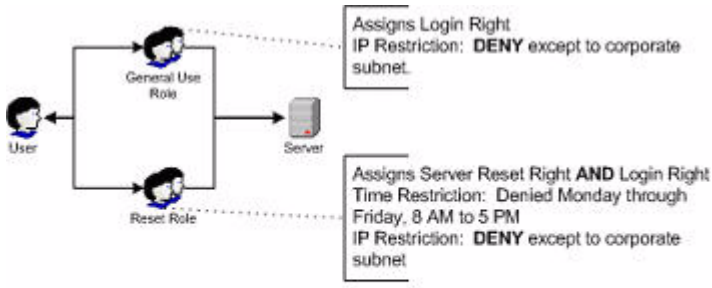
Directory administrators might be tempted to create two roles to address this situation, but extra caution is required. Creating a role that provides the required server reset rights and restricting it to an after-hours application might allow administrators outside the corporate network to reset the server, which is contrary to most security policies.

In this example, security policy dictates general use is restricted to clients within the corporate subnet, and server reset capability is additionally restricted to after hours.



Alternatively, the directory administrator could create a role that grants the login right and restrict it to the corporate network, then create another role that grants only the server reset right and restrict it to after-hours operation. This configuration is easier to manage but more dangerous because ongoing administration might create another role that grants users from addresses outside the corporate network the login right, which could unintentionally grant the MP administrators in the server Reset role the ability to reset the server from anywhere, provided they satisfy the time constraints of that role.

The previous configuration meets corporate security policy. However, adding another role that grants the login right can inadvertently grant server reset privileges from outside the corporate subnet after hours. A more manageable solution would be to restrict the Reset role, as well as the General Use role.



Directory Services Schema

A directory schema specifies the types of objects that a directory may have and the mandatory and optional attributes of each object type. The following sections describe both the HP management core, and the MP-specific LDAP object identifier classes and attributes.

HP Management Core LDAP Object Identifier Classes and Attributes

Object identifiers (OIDs) are unique numbers that are used in 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:

- Core classes
- Core attributes

Core Classes

Table 6-1 lists the core LDAP OID classes.

Table 6-1 Core Classes

Class Name	Assigned OID
hpqTarget	1.3.6.1.4.1.232.1001.1.1.1.1
hpqRole	1.3.6.1.4.1.232.1001.1.1.1.2
hpqPolicy	1.3.6.1.4.1.232.1001.1.1.1.3

Core Attributes

Table 6-2 lists the core LDAP OID attributes.

Table 6-2 Core Attributes

Attribute Name	Assigned OID
hpqPolicyDN	1.3.6.1.4.1.232.1001.1.1.2.1
hpqRoleMembership	1.3.6.1.4.1.232.1001.1.1.2.2
hpqTargetMembership	1.3.6.1.4.1.232.1001.1.1.2.3
hpqRoleIPRestrictionDefault	1.3.6.1.4.1.232.1001.1.1.2.4
hpqRoleIPRestrictions	1.3.6.1.4.1.232.1001.1.1.2.5
hpqRoleTimeRestriction	1.3.6.1.4.1.232.1001.1.1.2.6

Core Class Definitions

Table 6-3, Table 6-4, and Table 6-5 define the HP Management core classes.

hpqTarget

Table 6-3 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—1.3.6.1.4.1.232.1001.1.1.2.1hpqRole Membership—1.3.6.1.4.1.232.1001.1.1.2.2
Remarks	None

hpqRole

Table 6-4 hpqRole

OID	1.3.6.1.4.1.232.1001.1.1.1.2
Description	This class defines Role objects, providing the basis for HP products using directory-enabled management.
Class Type	Structural
SuperClasses	group
Attributes	hpqRoleIPRestrictions—1.3.6.1.4.1.232.1001.1.1.2.5hpqRoleIPRestrictionDefault—1.3.6.1.4.1.232.1001.1.1.2.4hpqRoleTimeRestriction—1.3.6.1.4.1.232.1001.1.1.2.6hpqTargetMembership—1.3.6.1.4.1.232.1001.1.1.2.3
Remarks	None

hpqPolicy

Table 6-5 hpqPolicy

OID	1.3.6.1.4.1.232.1001.1.1.1.3
Description	This class defines Policy objects, providing the basis for HP products using directory-enabled management.
Class Type	Structural
SuperClasses	top
Attributes	hpqPolicyDN—1.3.6.1.4.1.232.1001.1.1.2.1
Remarks	None

Core Attribute Definitions

Table 6-6 through Table 6-11 define the HP Management core class attributes.

hpqPolicyDN

Table 6-6 hpqPolicyDN

OID	1.3.6.1.4.1.232.1001.1.1.2.1
Description	This attribute provides the Distinguished Name of the policy that controls the general configuration of this target.
Syntax	Distinguished Name—1.3.6.1.4.1.1466.115.121.1.12
Options	Single Valued
Remarks	None

hpqRoleMembership

Table 6-7 hpqRoleMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.2
Description	This attribute provides a list of hpqTarget objects to which this object belongs.
Syntax	Distinguished Name—1.3.6.1.4.1.1466.115.121.1.12
Options	Multi Valued
Remarks	None

hpqTargetMembership

Table 6-8 hpqTargetMembership

OID	1.3.6.1.4.1.232.1001.1.1.2.3
Description	This attribute provides a list of hpqTarget objects that belong to this object.
Syntax	Distinguished Name—1.3.6.1.4.1.1466.115.121.1.12
Options	Multi Valued
Remarks	None

hpqRoleIPRestrictionDefault

Table 6-9 hpqRoleIPRestrictionDefault

OID	1.3.6.1.4.1.232.1001.1.1.2.4
Description	This attribute is a Boolean representing access by unspecified clients, which partially specifies rights restrictions under an IP network address constraint.
Syntax	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Options	Single Valued

Table 6-9 hpqRoleIPRestrictionDefault (Continued)

OID	1.3.6.1.4.1.232.1001.1.1.2.4
Remarks	If this attribute is TRUE, then IP restrictions will be satisfied for unexceptional network clients. If this attribute is FALSE, then IP restrictions will be unsatisfied for unexceptional network clients.

hpqRoleIPRestrictions

Table 6-10 hpqRoleIPRestrictions

OID	1.3.6.1.4.1.232.1001.1.1.2.5
Description	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.
Syntax	Octet String—1.3.6.1.4.1.1466.115.121.1.40
Options	Multi Valued
Remarks	This attribute is only used on Role objects. IP restrictions are satisfied when the address matches and general access is denied, and unsatisfied when the address matches and general access is allowed.Values are an identifier byte followed by a type-specific number of bytes specifying a network address. For IP subnets, the identifier is <0x01>, followed by the IP network address in network order, followed by the IP network subnet mask in network order. For example, the IP subnet 127.0.0.1/255.0.0.0 would be represented as <0x01 0x7F 0x00 0x00 0x01 0xFF 0x00 0x00 0x00>. For IP ranges, the identifier is <0x02>, followed by the lower bound IP address, followed by the upper bound IP address. Both are inclusive and in network order; for example, the IP range 10.0.0.1 to 10.0.10.255 would be represented as <0x02 0x0A 0x00 0x00 0x01 0x0A 0x00 0x0A 0xFF>For DNS names or domains, the identifier is <0x03>, followed by the ASCII encoded DNS name. DNS names can be prefixed with a * (ASCII 0x2A), to indicate they should match all names that end with the specified string; for example, the DNS domain *.acme.com is represented as <0x03 0x2A 0x2E 0x61 0x63 0x6D 0x65 0x2E 0x63 0x6F 0x6D>. General access is allowed.

hpqRoleTimeRestriction

Table 6-11 hpqRoleTimeRestriction

OID	1.3.6.1.4.1.232.1001.1.1.2.6
Description	This attribute represents a 7-day time grid, with 30-minute resolution, which specifies rights restrictions under a time constraint.
Syntax	Octet String {42}—1.3.6.1.4.1.1466.115.121.1.40
Options	Single Valued

Table 6-11 hpqRoleTimeRestriction (Continued)

OID	1.3.6.1.4.1.232.1001.1.1.2.6
Remarks	This attribute is only used on Role objects.Time restrictions are satisfied when the bit corresponding to the current local side real time of the device is 1 and unsatisfied when the bit is 0. The least significant bit of the first byte corresponds to Sunday, from 12 midnight to Sunday 12:30 AM. Each more significant bit and sequential byte corresponds to the next consecutive half-hour blocks within the week. The most significant (8th) bit of the 42nd byte corresponds to Saturday at 11:30 PM to Sunday at 12 midnight.

MP-Specific LDAP OID Classes and Attributes

The schema attributes and classes in Table 6-12 and Table 6-13 might depend on attributes or classes defined in the HP Management core classes and attributes.

MP Classes

Table 6-12 MP Classes

Class Name	Assigned OID
hpqLOMv100	1.3.6.1.4.1.232.1001.1.8.1.1

MP Attributes

Table 6-13 MP Attributes

Class Name	Assigned OID
hpqLOMRightLogin	1.3.6.1.4.1.232.1001.1.8.2.1
hpqLOMRightRemoteConsole	1.3.6.1.4.1.232.1001.1.8.2.2
hpqLOMRightVirtualMedia	1.3.6.1.4.1.232.1001.1.8.2.3
hpqLOMRightServerReset	1.3.6.1.4.1.232.1001.1.8.2.4
hpqLOMRightLocalUserAdmin	1.3.6.1.4.1.232.1001.1.8.2.5
hpqLOMRightConfigureSettings	1.3.6.1.4.1.232.1001.1.8.2.6

MP Class Definitions

Table 6-14 defines the MP core class.

hpqLOMv100

Table 6-14 hpqLOMv100

OID	1.3.6.1.4.1.232.1001.1.8.1.1
Description	This class defines the rights and settings used with HP Management Processor products.
Class Type	Auxiliary
SuperClasses	None
Attributes	hpqLOMRightConfigureSettings—1.3.6.1.4.1.232.1001.1.8.2.1hpqLOMRightLocalUserAdmin—1.3.6.1.4.1.232.1001.1.8.2.2hpqLOMRightLogin—1.3.6.1.4.1.232.1001.1.8.2.3hpqLOMRightRemoteConsole—1.3.6.1.4.1.232.1001.1.8.2.4hpqLOMRightServerReset—1.3.6.1.4.1.232.1001.1.8.2.5hpqLOMRightVirtualMedia—1.3.6.1.4.1.232.1001.1.8.2.6
Remarks	None

MP Attribute Definitions

Table 6-15 through Table 6-20 define the MP core class attributes.

hpqLOMRightLogin

Table 6-15 hpqLOMRightLogin

OID	1.3.6.1.4.1.232.1001.1.8.2.1
Description	Login Right for HP Management Processor products
Syntax	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Options	Single Valued
Remarks	The attribute is meaningful only on Role objects. If TRUE, members of the role are granted the right.

hpqLOMRightRemoteConsole

Table 6-16 hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.2
Description	Remote Console Right for Management Processor Products. Meaningful only on Role objects.
Syntax	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is only used on Role objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightRemoteConsole

Table 6-17 hpqLOMRightRemoteConsole

OID	1.3.6.1.4.1.232.1001.1.8.2.3
Description	Virtual Media Right for HP Management Processor products
Syntax	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is only used on Role objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightServerReset

Table 6-18 hpqLOMRightServerReset

OID	1.3.6.1.4.1.232.1001.1.8.2.4
Description	Remote Server Reset and Power Button Right for HP Management Processor products
Syntax	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is only used on Role objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightLocalUserAdmin

Table 6-19 hpqLOMRightLocalUserAdmin

OID	1.3.6.1.4.1.232.1001.1.8.2.5
Description	Local User Database Administration Right for HP Management Processor products
Syntax	Boolean—1.3.6.1.4.1.1466.115.121.1.7
Options	Single valued
Remarks	This attribute is only used on Role objects. If this attribute is TRUE, members of the role are granted the right.

hpqLOMRightConfigureSettings

Table 6-20 hpqLOMRightConfigureSettings

OID	1.3.6.1.4.1.232.1001.1.8.2.6
Description	Configure Devices Settings Right for HP Management Processor products
Syntax	Boolean—1.3.6.1.4.1.1466.115.121.1.7

Table 6-20 hpqLOMRightConfigureSettings (Continued)

OID	1.3.6.1.4.1.232.1001.1.8.2.6
Options	Single valued
Remarks	This attribute is only used on Role objects. If this attribute is TRUE, members of the role are granted the right.

7 Management Processor Ports and Indicators

All MP functions are available through the server LAN and the local and remote serial ports. The following sections describe the available MP port connectors, pinouts and LEDs:

- “Serial Ports”
- “Management Processor LAN Port”

Serial Ports

Figure 7-1 shows the serial port connector with numbered labels for each pin.

Figure 7-1 Serial Port Connector

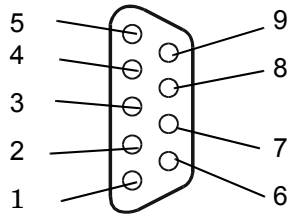


Table 7-1 maps the serial port connector pin number to its signal description.

Table 7-1 Serial Port Pinouts

Pin Number	Signal Description
1	Not applicable
2	Receive data
3	Transmit data
4	Not applicable
5	Ground
6	Not applicable
7	Request to send
8	Clear to send
9	Not applicable

Management Processor LAN Port

Figure 7-2 shows the MP LAN port connector pins and LEDs.

Figure 7-2 Management Processor LAN Port

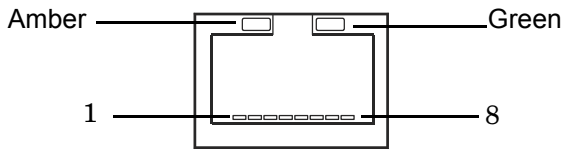


Table 7-2 maps the MP LAN port connector pin number to its signal description.

Table 7-2 Management Processor LAN Port Pinouts

Pin Number	Signal Description
1	TXP
2	TXN
3	RXP
4	Not used
5	Not used
6	RXN
7	Not used
8	Not used

Management Processor LAN LEDs (rx4640; rp4410/4440)

The internal management processor (MP) LAN uses an RJ-45 type connector. This connector has two LEDs (LAN link and LAN activity) that signal status and activity (Figure 7-3).

Figure 7-3 MP LAN LEDs (rx4640; rp4410/4440)

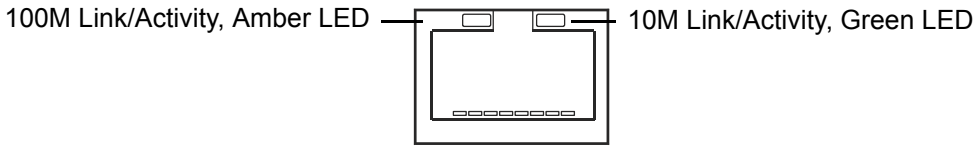


Table 7-3 describes the status of the system when a specific LED condition exists.

Table 7-3 MP LAN LED Status Descriptions (rx4640; rp4410/4440)

LED	Condition	Status
100M amber	On	Linked at 100 MB/s, no activity
100M amber	Blinking	Linked at 100 MB/s, activity present
10M green	On	Linked at 10MB/s, no activity
10M green	Blinking	Linked at 10MB/s, activity present

Management Processor LAN LEDs (rx1600; rx1620; rx2600; rx2620; rp3410/3440)

The management processor card uses an RJ-45 type connector. This connector has four LEDs that signal status and activity (Figure 7-4).

Figure 7-4 Management Processor LAN LEDs (rx1600; rx1620; rx2600; rx2620; rp3410/3440)

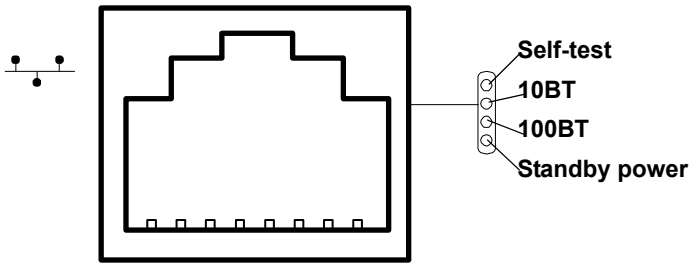


Table 7-4 describes the status of the system when a specific LED condition exists.

Table 7-4 Management Processor LAN LEDs (rx1600; rx1620; rx2600; rx2620; rp3410/3440)

LAN LED	Location	Color	State
Self-test	Top	Yellow	Management processor running selftest or error
		Off	Management processor has booted
10BT	2nd from top	Green	10BT link established
		Blinking green	10BT activity
		Off	No link or 100BT link
100BT	2nd from bottom	Green	100BT link established
		Blinking green	100BT activity
		Off	No link or 10BT link
Standby Power	Bottom	Green	Standby power on
		Off	Standby power off